



Includes Professor Messer's
Video Training + Practice Exams



CompTIA Security+ SY0-401

Official Study Guide

STUDENT EDITION



OFFICIAL

MULTI-LAYERED LEARNING
TOOLS INCLUDED



**CompTIA Security+ Certification
Support Skills (Exam SY0-401)**

G634eng ver094

Acknowledgements

Course Developer..... gtslearning



Editor James Pengelly

This courseware is owned, published, and distributed by **gtslearning**, the world's only specialist supplier of CompTIA learning solutions.

✉ sales@gtslearning.com

☎ +44 (0)20 7887 7999 ☎ +44 (0)20 7887 7988

✉ Unit 127, Hill House, 210 Upper Richmond Road,
London SW15 6NP, UK

COPYRIGHT

This courseware is copyrighted © 2014 *gtslearning*. Product images are the copyright of the vendor or manufacturer named in the caption and used by permission. No part of this courseware or any training material supplied by the publisher to accompany the courseware may be copied, photocopied, reproduced, or re-used in any form or by any means without permission in writing from the publisher. Violation of these laws will lead to prosecution.

All trademarks, service marks, products, or services are trademarks or registered trademarks of their respective holders and are acknowledged by the publisher.

LIMITATION OF LIABILITY

Every effort has been made to ensure complete and accurate information concerning the material presented in this course. Neither the publisher nor its agents can be held legally responsible for any mistakes in printing or for faulty instructions contained within this course. The publisher appreciates receiving notice of any errors or misprints.

Information in this course is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted.

Where the course and all materials supplied for training are designed to familiarize the user with the operation of software programs and computer devices, the publisher urges the user to review the manuals provided by the product vendor regarding specific questions as to operation.

There are no warranties, expressed or implied, including warranties of merchantability or fitness for a particular purpose, made with respect to the materials or any information provided herein. Neither the author nor publisher shall be liable for any direct, indirect, special, incidental, or consequential damages arising out of the use or the inability to use the contents of this course.

Warning All gtslearning products are supplied on the basis of a single copy of a course per student. Additional resources that may be made available from gtslearning may only be used in conjunction with courses sold by gtslearning. No material changes to these resources are permitted without express written permission from gtslearning. These resources may not be used in conjunction with content from any other supplier.

If you suspect that this course has been copied or distributed illegally,
please telephone or email gtslearning.

Table of Contents

Course Introduction	i
Table of Contents	iii
About This Course.....	ix
Module 1 / Security Threats and Controls	1
 Module 1 / Unit 1	
 Security Controls	3
Why is Security Important?	3
Security Policy.....	6
Security Controls	7
Identification	10
Authentication.....	12
Authorization	14
Basic Authorization Policies.....	17
Accounting	18
 Module 1 / Unit 2	
 Threats and Attacks	21
Vulnerability, Threat, and Risk.....	21
Social Engineering.....	24
Phishing	27
Malware.....	29
Trojans and Spyware.....	32
Preventing Malware.....	35
Anti-Virus Software.....	36
Removing Malware.....	39
 Module 1 / Unit 3	
 Network Attacks	41
Network Fundamentals.....	41
Sniffers and Protocol Analyzers.....	45
ARP Attacks	47
Replay and Man-in-the-Middle Attacks	49
Network Mappers and Port Scanners	52
Denial of Service Attacks.....	57
 Module 1 / Unit 4	
 Assessment Tools and Techniques	60
Vulnerability Assessments and Pentests	60
Security Assessment Techniques.....	61
Vulnerability Scanners.....	64
Honeypots and Honeynets	68
 Module 1 / Summary	
 Security Threats and Controls	70

Module 2 / Unit 1	
<i>Cryptography</i>	74
Uses of Cryptography.....	74
Cryptographic Terminology and Ciphers.....	75
Encryption Technologies	78
Cryptographic Hash Functions.....	79
Symmetric Encryption.....	81
Asymmetric Encryption.....	83
Diffie-Hellman.....	86
ECC and Quantum Cryptography	87
Transport Encryption	88
Cryptographic Attacks	89
Steganography	91
Module 2 / Unit 2	
<i>Public Key Infrastructure</i>	93
PKI and Certificates.....	93
Certificate Authorities	97
Implementing PKI	100
Creating Keys.....	101
Key Recovery Agents	103
Key Status and Revocation	104
PKI Trust Models	107
Cryptographic Standards	111
PGP / GPG.....	113
Module 2 / Unit 3	
<i>Password Authentication</i>	115
LAN Manager / NTLM.....	115
Kerberos.....	118
PAP and CHAP	121
Password Protection.....	122
Password Attacks	123
Module 2 / Unit 4	
<i>Strong Authentication</i>	128
Token-based Authentication	128
Biometric Authentication	131
Common Access Card.....	134
Extensible Authentication Protocol	135
RADIUS and TACACS+	137
Federation and Trusts	139
Module 2 / Unit 5	
<i>Authorization and Account Management</i>	143
Privilege Policies	143
Directory Services	145
Lightweight Directory Access Protocol.....	146
Windows Active Directory	149
Creating and Managing User Accounts	153
Managing Group Accounts	155

Account Policy Enforcement.....	158
User Rights, Permissions, and Access Reviews.....	162
Module 2 / Summary	
<i>Cryptography and Access Control</i>	<u>165</u>
Module 3 / Network Security	<u>167</u>
Module 3 / Unit 1	
<i>Secure Network Design</i>	<u>169</u>
Secure Network Topologies.....	169
Demilitarized Zones.....	171
Other Security Zones.....	173
Network Device Exploitation	175
Switches and VLANs.....	175
Switch Vulnerabilities and Exploits	178
Routers.....	180
Network Address Translation.....	184
Module 3 / Unit 2	
<i>Security Appliances and Applications</i>	<u>189</u>
Basic Firewalls	189
Stateful Firewalls	191
Proxies and Gateways.....	193
Implementing a Firewall or Gateway.....	194
Web and Email Security Gateways.....	197
Intrusion Detection Systems	201
IDS Analysis Engines	204
Monitoring System Logs	206
Module 3 / Unit 3	
<i>Wireless Network Security</i>	<u>211</u>
Wireless LANs.....	211
WEP and WPA	213
Wi-Fi Authentication	215
Additional Wi-Fi Security Settings.....	217
Wi-Fi Site Security	219
Module 3 / Unit 4	
<i>VPN and Remote Access Security</i>	<u>225</u>
Remote Access	225
Virtual Private Networks	228
IPSec	231
Remote Access Servers	234
Remote Administration Tools.....	235
Hardening Remote Access Infrastructure	238

Module 3 / Unit 5 <i>Network Application Security</i>	241
Application Layer Security	241
DHCP Security	243
DNS Security.....	245
SNMP Security	248
Storage Area Network Security.....	251
IPv4 versus IPv6.....	256
Telephony.....	257
Module 3 / Summary <i>Network Security</i>	262
Module 4 / Host, Data, and Application Security	264
Module 4 / Unit 1 <i>Host Security</i>	266
Computer Hardening	266
Host Security Management Plan	271
OS Hardening.....	272
Patch Management	275
Endpoint Security	281
Network Access Control	283
Module 4 / Unit 2 <i>Data Security</i>	287
Data Handling.....	287
Data Encryption.....	290
Data Loss Prevention	293
Backup Plans and Policies	296
Backup Execution and Frequency	301
Restoring Data and Verifying Backups	304
Data Wiping and Disposal	305
Module 4 / Unit 3 <i>Web Services Security</i>	309
HyperText Transport Protocol.....	309
SSL / TLS	310
Web Servers.....	315
Load Balancers	319
File Transfer	320
Module 4 / Unit 4 <i>Web Application Security</i>	324
Web Application Technologies.....	324
Web Application Databases.....	326
Web Application Exploits	328
Web Application Browser Exploits	331
Secure Web Application Design	334
Auditing Web Applications	335
Web Browser Security	336

Module 4 / Unit 5	
<i>Virtualization and Cloud Security</i>	345
Virtualization Technologies.....	345
Virtual Platform Applications.....	347
Virtualization Best Practices and Risks.....	350
Cloud Computing.....	355
Risks of Cloud Computing	358
Module 4 / Summary	
<i>Host, Data, and Application Security</i>	360
Module 5 / Operational Security	362
Module 5 / Unit 1	
<i>Site Security</i>	364
Site Layout and Access	364
Gateways and Locks	367
Alarm Systems	369
Surveillance.....	370
Hardware Security	373
Environmental Controls	375
Hot and Cold Aisles.....	378
RFI / EMI	379
Fire Prevention and Suppression.....	380
Module 5 / Unit 2	
<i>Mobile and Embedded Device Security</i>	385
Static Environments.....	385
Mitigating Risk in Static Environments.....	391
Mobile Device Security	393
Mobile Device Management	397
BYOD Concerns.....	398
Mobile Application Security.....	401
Bluetooth and NFC	403
Module 5 / Unit 3	
<i>Risk Management</i>	406
Business Continuity Concepts	406
Risk Calculation.....	409
Risk Mitigation	412
Integration with Third Parties	414
Service Level Agreements.....	418
Change and Configuration Management	420
Module 5 / Unit 4	
<i>Disaster Recovery</i>	423
Disaster Recovery Planning	423
IT Contingency Planning	425
Clusters and Sites	428

Module 5 / Unit 5	
<i>Incident Response and Forensics</i>	433
Incident Response Procedures.....	433
Preparation.....	434
Detection and Analysis	435
Containment.....	436
Eradication and Recovery.....	438
Forensic Procedures	439
Collection of Evidence	440
Handling and Analyzing Evidence	443
Module 5 / Unit 6	
<i>Security Policies and Training</i>	446
Corporate Security Policy	446
Operational Policies.....	449
Privacy and Employee Conduct Policies.....	451
Standards and Best Practice	453
Security Policy Training and User Habits.....	455
Module 5 / Summary	
<i>Operational Security</i>	459
Taking the Exams	461
Glossary	471
Index	495

About This Course

This course is intended for those wishing to qualify with CompTIA Security+ Certification. Security+ is foundation-level certification designed for IT administrators with 2 years' experience whose job role is focused on system security.

The CompTIA Security+ exam will certify that the successful candidate has the knowledge and skills required to identify risk, to participate in risk mitigation activities, and to provide infrastructure, application, information, and operational security. In addition, the successful candidate will apply security controls to maintain confidentiality, integrity, and availability, identify appropriate technologies and products, troubleshoot security events and incidents, and operate with an awareness of applicable policies, laws, and regulations.

[CompTIA Security+ syllabus](#)

Target Audience and Course Prerequisites

CompTIA Security+ is aimed at IT professionals with job roles such as security architect, security engineer, security consultant/specialist, information assurance technician, security administrator, systems administrator, and network administrator.

Ideally, you should have successfully completed the "CompTIA Network+ Support Skills" course and have around 24 months' experience of networking support or IT administration. It is not *necessary* that you pass the Network+ exam before completing Security+ certification, but it is *recommended*.

Regardless of whether you have passed Network+, it is recommended that you have the following skills and knowledge before starting this course:

- Know the function and basic features of the components of a PC.
- Use Windows Server to create and manage files and use basic administrative features (Explorer, Control Panel, Management Consoles).
- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers).
- Understand TCP/IP addressing, core protocols, and troubleshooting tools.

Optionally, you can take a prerequisites test to check that you have the knowledge required to study this course at the [gtslearning Freestyle](#) support site accompanying this study guide.

Course Outcomes

This course will teach you the fundamental principles of identifying risk and implementing security controls. It will prepare you to take the CompTIA Security+ exam by providing 100% coverage of the objectives and content examples listed on the syllabus. On course completion, you will be able to:

- Identify network attack strategies and defenses.
- Understand the principles of organizational security and the elements of effective security policies.
- Know the technologies and uses of cryptographic standards and products.
- Identify network- and host-based security technologies and practices.
- Describe how wireless and remote access security is enforced.
- Describe the standards and products used to enforce security on web and communications technologies.
- Identify strategies for ensuring business continuity, fault tolerance, and disaster recovery.

How Certification Helps Your Career

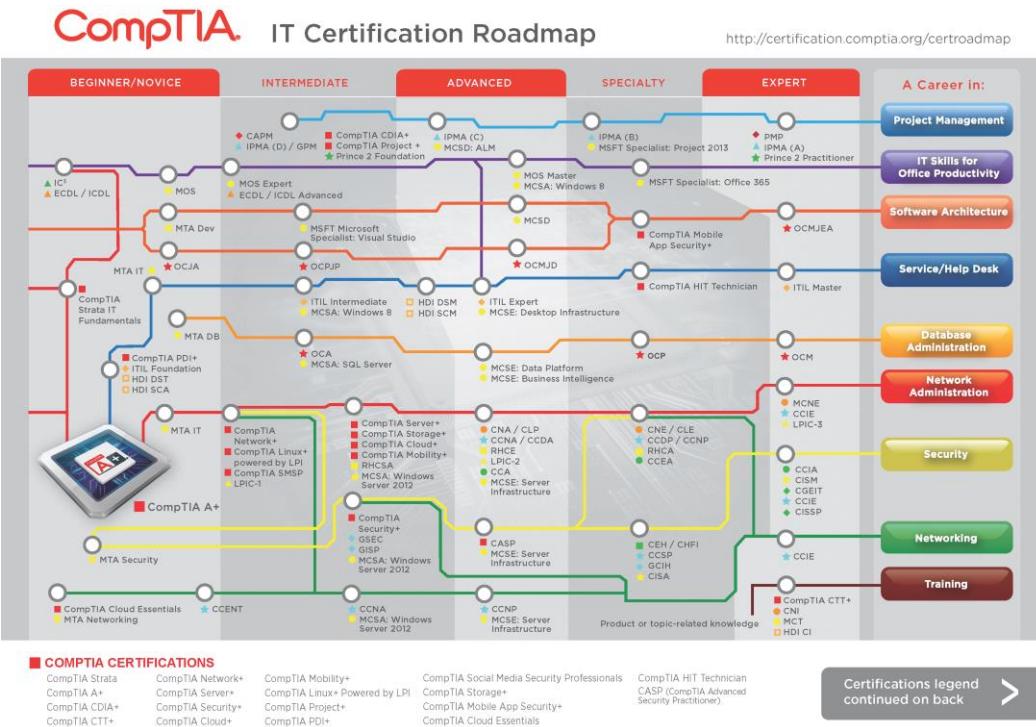
Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation, and promotion.



Benefits of certification

CompTIA Career Pathway

Completing this course will help you to pursue a career in providing system security support, in job roles such as security architect, security engineer, security consultant/specialist, information assurance technician, security administrator, systems administrator, and network administrator. CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.



View the CompTIA career pathway at gtsgo.to/iskbs

Study of the course can act as groundwork for more advanced training. Other security and network professional qualifications include the following:

- **CompTIA Advanced Security Practitioner (CASP)** - covers the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments.
- **CompTIA Mobile App Security+** - covers the knowledge and skills required to securely create a native iOS or Android mobile application, while also ensuring secure network communications and backend web services.
- **Certified Ethical Hacker (CEH)** - focuses on vulnerability and penetration analysis and testing. More information is available at www.eccouncil.org.
- **International Information Systems Security Certification Consortium (ISC)²** - offers the advanced CISSP (Certified Information System Security Professional) for security consultants, analysts, architects, and chief officers. More information is available at www.isc2.org.

- **Global Information Assurance Certification (GIAC / GSE)** - a series of rigorous qualifications operated by SANS (SysAdmin, Audit, Network, Security) Institute (www.sans.org). GIAC ranges from entry-level to advanced topic areas.
- **Certified Information Systems Auditor (CISA)** - the benchmark qualification for information systems auditing and control. Check www.isaca.org for more information.
- **Cisco Security Certifications** - validates the advanced knowledge required to secure a Cisco network, with certifications at CCNA, CCNP, and CCIE levels. Visit gtsgo.to/kpejq for more information.
- **Microsoft Certified Solutions Expert (MCSE)** - Windows-specific qualifications covering support and design of client and server infrastructure, as well as other Microsoft technologies. Visit gtsgo.to/k2col for more information.

About the Course Material

The CompTIA Security+ exam contains questions based on objectives and example content listed in the exam blueprint, published by CompTIA. The objectives are divided into six **domains**, as listed below:

CompTIA Security+ Certification Domain Areas	Weighting
1.0 Network Security	20%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	20%
4.0 Application, Data and Host Security	15%
5.0 Access Control and Identity Management	15%
6.0 Cryptography	12%

This course is divided into five **modules**, each covering a different subject area. Each module is organized into several **units**, containing related topics for study.

- Module 1 / Security Threats and Controls
- Module 2 / Cryptography and Access Control
- Module 3 / Network Security
- Module 4 / Host, Data, and Application Security
- Module 5 / Operational Security

As you can see, the modules in the course do not correspond directly to domains in the exam. Doing so would involve quite a lot of jumping around between different technologies. Instead, we try to cover topics in the most straightforward order for candidates at a foundation level to understand, starting with an overview of threats and attacks and proceeding to examine vulnerabilities and controls in different environments. Each module starts with a list of the CompTIA domain objectives and content examples that will be covered in each unit.

On the Freestyle course support website, you can find **Pre- and Post-assessment tests** for each unit. These are designed to identify how much you know about the topics covered in a unit before you study it and how much knowledge you have retained after completing a unit. You can use these tests in conjunction with your training provider to identify which units to focus on or to help you plan a self-study program.



There are notes on registering for the course support site and planning a self-study program later in this section.

Each unit in a module is focused on explaining the exam objectives and content examples. Each unit has a set of **review questions** designed to test your knowledge of the topics covered in the unit. Answers to the review questions are provided on the Freestyle course support website.

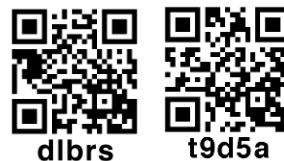
At the back of the book there is an **index** to help you look up key terms and concepts from the course and a **glossary** of terms and concepts used.

If you are studying with a training provider, you may also receive a "Labs" book containing the practical labs for you to complete in class.

The following symbols are used to indicate different features in the course book:

Icon	Meaning
	A tip or warning about a feature or topic.
	A reference to another unit, where more information on a topic can be found.
	A link to a Professor Messer video presentation. Click or use a QR scanner to open the link or enter gtsgo.to/ followed by the code printed under the QR graphic into your browser.
	Review questions to help test what you have learned.
	A hands-on exercise for you to practice skills learned during the lesson.

Integrated Learning with Professor Messer Video Tutorials



Professor Messer has long been a web hero for CompTIA certification students. With professionally-produced lessons covering the full exam objectives plus online forums, Professor Messer is a trusted online source for exam information. Professor Messer uses gtslearning's CompTIA certification courseware to develop and record his popular video training sessions. Now you can easily follow along with his video presentations using the links provided in this course book.

Each of the "TV static" icons above and in the rest of the book represents a Professor Messer video. The icons are called QR codes. They enable you to scan the link using a smartphone or tablet equipped with a camera. You can use the links in three ways:

- 1) If you have an ebook, just click the link to open the video in your browser.
- 2) If you have a QR code reader, open the app and point your camera at the icon to open the video in your phone or tablet's browser.
- 3) If you have a printed book but no reader, enter `gtsgo.to/` followed by the code printed under the QR graphic into your browser. For example, to access the code shown above, enter `gtsgo.to/dlbrs` into your browser.



We do endeavor to keep the video links up-to-date, but if you come across a broken link, please email the link code (for example "dlbrs") to support@gtslearning.com and we will update it.



If you have trouble scanning an icon, make sure the page is laid flat and try moving the camera closer to or farther from the image. Some topics feature more than one video link; you may have to cover the other link with your hand or a post-it to scan the one next to it.



As Professor Messer covers the objectives in domain order, some links are to segments of a longer video so do not be surprised if some video links do not play from the start.

Getting Started and Making a Study Plan

If you are completing this course as self-study, you need to plan your study habits. The best way to approach the course initially is to *read through* the whole thing quite quickly. On this first reading, do not worry if you cannot recall facts, get two similar technologies mixed up, or do not completely understand some of the topics. The idea is to get an overview of everything you are going to need to know. The first reading shouldn't take you too long - a few hours is plenty of time. You don't have to do it at one sitting, but try to complete the read through within about a week.

When you have completed your first read through, you should make a **study plan**. We've put a sample study plan on the course website, but you'll need to adjust it to account for:

- How much you know about IT security *already*.
- How much *time* you have to study each day or each week.
- *When* you want to (or have to) become Security+ Certified.

In your study plan, you'll identify how much time you want to spend on each unit and when you're going to sit down and do that study. We recommend that you study no more than one or two units per day. Studying a unit means reading it closely, making notes about things that come to mind as you read, using the glossary to look up terms you do not understand, then using the review questions on the course website to test and reinforce what you have learned.

Only you can decide how long you need to study for in total. Security+ Certification is supposed to represent the knowledge and skills of someone with 24 months of practical network security administrative experience. If you cannot get that experience, you will need to do a corresponding amount of study to make up. We have included practice tests for the course; these should give you a good idea of whether you are ready to attempt the exams.

You also need to think about *where* you are going to study. You need to find somewhere comfortable and where you are not subject to interruptions or distractions. You will also need a computer or tablet with an internet connection for the review and practical activities.



014i2

Using the Freestyle Support Site

Purchasing this book gives you free access to the course support website. The website contains **practice tests** to help you in your final preparations to take the CompTIA exam. You can find the **answers** to the end-of-unit review questions on the support site. There is also a **glossary** of terms that you can use while reading the book or as a revision aid.

To register for the website, visit the Freestyle site (gtsgo.to/oup4x) and complete the sign-up process.

The screenshot shows a web browser window with the URL <http://www.gtslearning.co...> in the address bar. The page title is "freestyle". On the left, there's a navigation menu with "HOME > LOGIN > NEW ACCOUNT". The main content area has a heading "Choose your username and password". It includes fields for "Username*" and "Password*", with a note below stating: "The password must have at least 8 characters, at least 1 digit(s), at least 1 lower case letter(s), at least 1 upper case letter(s)". Below this is a section titled "More details" containing fields for "Email address*", "Email (again)*", "First name*", "Surname*", "City/town*", and "Country*". A dropdown menu for "Select a country" is shown. At the bottom right of the form, there's a "100%" zoom indicator.

Creating an account

You will need to validate the account using your email address. When you have validated your account, open gtsgo.to/0l4i2 and log in if necessary. To register on the course, you will need to enter an enrollment key. The enrollment key is a word from this course book. For example, if challenged for the third word under the heading "Module 1" (on page one in the printed edition), you would enter **CompTIA**. Note that the challenge is case-sensitive.

Hands On Live Labs Free Trial and 10% Discount

If you want to gain practical experience using a live PC and network environment as you work through this course, why not head over to gtsgo.to/xv89t and take a look at our great value live lab package for CompTIA Security+. With **Hands On Live Labs**, you will get online browser-based access to real hardware and software without having to beg, borrow or steal time on expensive equipment. It's completely risk-free, as should you make a mistake, the hardware will reset.

Hands On Live Labs are the next best thing to real-world experience and a great way to prepare for CompTIA's new performance-based questions.

Take a FREE ONE HOUR TRIAL today at gtsgo.to/xv89t and you will see how it will ensure you are ready to take the certification exam.

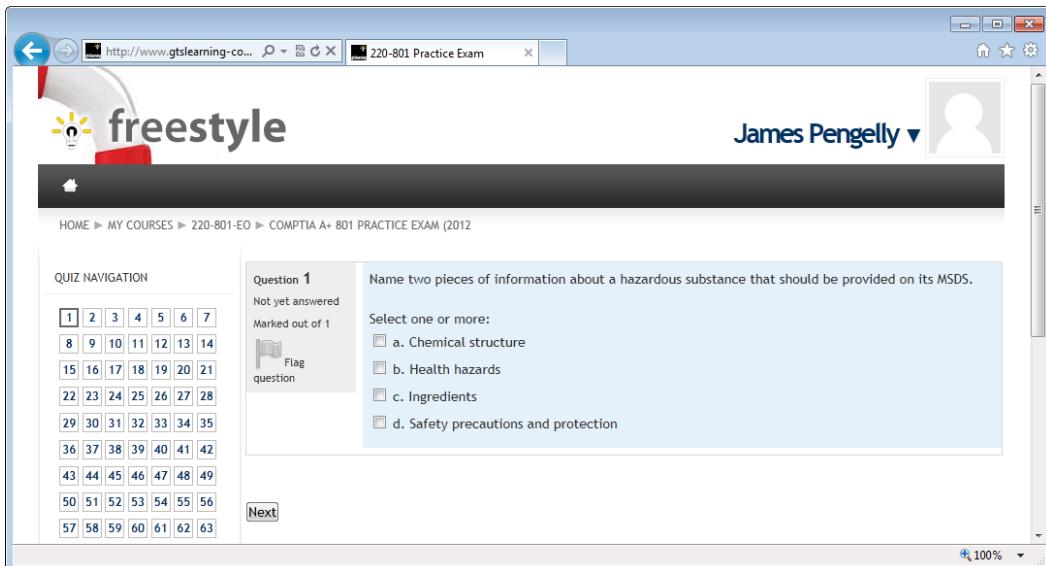
Plus, you can also save 10% on the cost of your **Hands On Live Labs** by using the voucher code: **secplus_pwn3**



In the course notes, look for the mouse icon to identify when to complete a lab.

Preparing for the Exams

When you've completed reading the units in detail, you can start to prepare for the exam. The "Taking the Exams" chapter and the support website contain tips on booking the test, the format of the exam, and what to expect.



The screenshot shows a web browser window for the '220-801 Practice Exam' on the gtslearning website. The user is logged in as 'James Pengelly'. The quiz navigation shows questions 1 through 63. Question 1 is selected and asks: 'Name two pieces of information about a hazardous substance that should be provided on its MSDS.' The options are: a. Chemical structure, b. Health hazards, c. Ingredients, and d. Safety precautions and protection. A 'Flag question' button is also present.

Get tests and practice exams to accompany the course at gtslearning's Freestyle site



When it comes to booking your test, you might be able to save money by using a voucher code from gtslearning. Check gtslearning's website (gtsgo.to/ljob) for any available offers.

Content Seal of Quality

This course has been approved under CompTIA's **Authorized Quality Curriculum Program (CAQC)**. The following text is provided by CompTIA in acknowledgement of this. This courseware bears the seal of **CompTIA Official Approved Quality Content**. This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.

The contents of this training material were created for the CompTIA **Security+ Certification SY0-401** exam covering the **2014 Edition** exam objectives and content examples. CompTIA has not reviewed or approved the accuracy of the contents of this training material and specifically disclaims any warranties of merchantability or fitness for a particular purpose. CompTIA makes no guarantee concerning the success of persons using any such "Authorized" or other training material in order to prepare for any CompTIA certification exam.



CAQC logo



It is CompTIA's policy to update the exam regularly with new test items to deter fraud and for compliance with ISO standards. The exam objectives may therefore describe the current "Edition" of the exam with a date different to that above. Please note that this training material remains valid for the stated exam code, regardless of the exam edition. For more information, please check the FAQs on CompTIA's website ([support.comptia.org](#)).

Four Steps to Getting Certified

This training material can help you prepare for and pass a related CompTIA certification exam or exams. In order to achieve CompTIA certification, you must register for and pass a CompTIA certification exam or exams. In order to become CompTIA certified, you must:

- 1) Review the certification objectives at [gtsgo.to/yd4ou](#) to make sure you know what is covered in the exam.
- 2) After you have studied for the certification, take a free assessment and sample test from CompTIA at [gtsgo.to/mmbfu](#) to get an idea what type of questions might be on the exam. You can also use gtslearning's free practice tests on Freestyle ([gtsgo.to/0l4i2](#)).
- 3) Purchase an exam voucher on the CompTIA Marketplace, which is located at [www.comptiastore.com](#). When it comes to booking your test, you might be able to save money by using a voucher code from gtslearning. Check gtslearning's website ([gtsgo.to/lbijob](#)) for any available offers.
- 4) Select a certification exam provider and schedule a time to take your exam. You can find exam providers at [gtsgo.to/4tij2](#).

Visit CompTIA online - [www.comptia.org](#) - to learn more about getting CompTIA certified. Contact CompTIA - call 866-835-8020 ext. 5 or email questions@comptia.org.

Module 1 / Security Threats and Controls

The following CompTIA Security+ domain objectives and examples are covered in this module:

CompTIA Security+ Certification Domain Areas	Weighting
1.0 Network Security	20%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	20%
4.0 Application, Data and Host Security	15%
5.0 Access Control and Identity Management	15%
6.0 Cryptography	12%

Domain Objectives/Examples	Refer To
2.1 Explain the importance of risk related concepts <i>Control types (Technical, Management, Operational) • Importance of policies in reducing risk (Least privilege)</i>	Unit 1.1 Security Controls
2.7 Compare and contrast physical security and environmental controls <i>Control types (Deterrent, Preventive, Detective, Compensating, Technical, Administrative)</i>	
5.2 Given a scenario, select the appropriate authentication, authorization or access control <i>Identification vs. authentication vs. authorization • Authorization (Least privilege, ACLs, Mandatory access, Discretionary access, Rule-based access control, Role-based access control) • Authentication (Multifactor authentication, Single sign-on, Access control, Implicit deny)</i>	
2.1 Explain the importance of risk related concepts <i>Vulnerabilities • Threat vectors</i>	Unit 1.2 Threats and Attacks
3.1 Explain types of malware <i>Adware • Virus • Spyware • Trojan • Rootkits • Backdoors • Logic bomb • Botnets • Ransomware • Polymorphic malware • Armored virus</i>	Unit 1.2 Threats and Attacks
3.2 Summarize various types of attacks <i>Spam • Phishing • Spim • Vishing • Spear phishing • Pharming • Malicious insider threat • Watering hole attack</i>	
3.3 Summarize social engineering attacks and the associated effectiveness with each attack <i>Shoulder surfing • Dumpster diving • Tailgating • Impersonation • Hoaxes • Whaling • Vishing • Principles / reasons for effectiveness (Authority, Intimidation, Consensus/Social proof, Scarcity, Urgency, Familiarity/liking, Trust)</i>	
4.3 Given a scenario, select the appropriate solution to establish host security <i>Anti-malware (Antivirus, Anti-spam, Anti-spyware, Pop-up blockers)</i>	

Domain Objectives/Examples	Refer To
<p>1.1 Implement security configuration parameters on network devices and other technologies <i>Protocol analyzers • Sniffers</i></p>	Unit 1.3 Network Attacks
<p>1.4 Given a scenario, implement common protocols and services <i>Protocols (TCP/IP, ICMP) • OSI relevance</i></p>	
<p>3.2 Summarize various types of attacks <i>Man-in-the-middle • DDoS • DoS • Replay • Smurf attack • Spoofing • Xmas attack • ARP poisoning</i></p>	
<p>3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities <i>Tools (Protocol analyzer, Port scanner, Banner grabbing)</i></p>	
<p>3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities <i>Interpret results of security assessment tools • Tools (Vulnerability scanner, Honeypots, Honeynets, Passive vs. active tools)</i></p>	Unit 1.4 Assessment Tools and Techniques
<p>3.8 Explain the proper use of penetration testing versus vulnerability scanning <i>Penetration testing (Verify a threat exists, Bypass security controls, Actively test security controls, Exploiting vulnerabilities) • Vulnerability scanning (Passively testing security controls, Identify vulnerability, Identify lack of security controls, Identify common misconfigurations, Intrusive vs. non-intrusive, Credentialled vs. non-credentialled, False positive) • Black box • White box • Gray box</i></p>	

Module 1 / Unit 1

Security Controls

Objectives

On completion of this unit, you will be able to:

- Understand why security policies and procedures are critical to protecting assets.
- Distinguish the types of security controls that can be deployed to protect assets.
- Describe the basis of access control systems: Identification, Authentication, Authorization, and Accounting.
- Know the use of different access control models.

Why is Security Important?

Most people, and by extension most organizations, are afraid of crime. A person may be worried that he will be mugged on the street or that his house may be burgled. In the last few years, the threat of **cybercrime** has become quite well publicized. Cybercrime means committing a crime using a computer system. For example, a **cracker** may gain access to a computer and steal data files from it or a **fraudster** may use a fake webstore to steal credit card details.

While people may be aware of cybercrime, they may not know precisely how to *deal* with it effectively. For example, a person may not know that if he sends credit card details in an email they become relatively easy to steal and misuse.

For an organization, its use of computer systems and internet technologies might have expanded considerably in the last few years. While the organization may be *concerned* about security, in many cases it will not have created an *effective* policy to deal with that concern. It may implement security procedures in one area but not another, like a homeowner with an impressive range of locks and alarms on the front door who leaves a bathroom window open at the back of the house when he goes to work.

Too many organizations think of security in terms of fitting locks on doors, configuring computer security accounts, or installing anti-virus and firewall software. While these are important, the people who use data and equipment are of greater significance. One essential problem for an organization to tackle is that its employees may not be sufficiently aware of the risks to security to take appropriate action as they complete their work. An organization needs to train each of its employees, so that they are alert and sensitive to security, without becoming so cautious that they cannot do their jobs.

Assets

Security is not an end in itself; businesses do not make money by being secure. Rather, security protects the **assets** of a company.

Assets are usually classified in the following ways:

- **Tangible** assets - these are physical items, such as buildings, furniture, computer equipment, software licenses, machinery, inventory (stock), and so on.
- **Intangible** assets - these are mostly information resources, including Intellectual Property (IP), accounting information, plans and designs, and so on. Intangible assets also include things like a company's reputation and image or brand.
- **Employees** - it is a commonplace to describe an organization's staff (sometimes described as "human capital") as its most important asset.

Most assets have a specific value associated with them (the **market value**), which is the price that could be obtained if the asset were to be offered for sale. In terms of security however, assets must be valued according to the **liabilities** that the loss or damage of the asset would create:

- Business continuity - this refers to an organization's ability to recover from incidents (any malicious or accidental breach of security is an incident).
- Legal - these are responsibilities in civil and criminal law. Security incidents could make an organization liable to prosecution (criminal law) or for damages (civil law). An organization may also be liable to professional standards and codes.

Why Is Data Important?

It is important to recognize what pieces of information are important. For example, the plans for an automobile manufacturer's new model are obviously vital and must be kept confidential, but other information may be important in less obvious ways. If an attacker obtains a company's organization chart, showing who works for whom, the attacker has found out a great deal about that organization and may be able to use that information to gain more.

Data can be essential to many different business functions:

- Product development, production, and maintenance.
- Customer contact information.
- Financial operations and controls (collection and payment of debts, payroll, tax, financial reporting).
- Legal obligations to maintain accurate records for a given period.
- Contractual obligations to third parties (Service Level Agreements).



The CIA Triad

Information is valuable to thieves and vulnerable to damage or loss. Data may be vulnerable because of the way it is stored, the way it is transferred, or both.

- Data used by an organization is *stored* in paper files, on computer disks and devices, and in the minds of its employees.
- Data may be *transferred* in the post, by fax, by telephone, or over a computer network (by file transfer, email, text messaging, or website). Data can also be transferred in conversation.



Data may be stored in paper records or on computer systems

Secure information has three properties, often referred to by the "**CIA Triad**":

- **Confidentiality** - this means that certain information should only be known to certain people.
- **Integrity** - this means that the data is stored and transferred as intended and that any modification is authorized.
- **Availability** - this means that information is accessible to those authorized to view or modify it.



The triad can also be referred to as "AIC", to avoid confusion with the Central Intelligence Agency.

It is important to recognize that information must be *available*. You could seal some records in a safe and bury the safe in concrete; the records would be secure, but completely inaccessible and for most purposes, completely useless.

Some security models and researchers identify other properties that secure systems should exhibit. The most important of these is **non-repudiation**. Non-repudiation means that a subject cannot deny doing something, such as creating, modifying, or sending a resource.

Security Policy

The implementation of a security policy might be very different for a school, a multinational accountancy firm, or a machine tool manufacturer. However each of these organizations, or any other organization (in any sector of the economy, whether profit-making or non-profit-making) should have the same interest in ensuring that its employees, equipment, and data are secure against attack or damage.

- 1) The first step in establishing a security policy is to obtain genuine **support** and **commitment** for such a policy *throughout* the organization.
- 2) The next step is to analyze **risks** to security within the organization. Risks are components, processes, situations, or events that could cause the loss, damage, destruction, or theft of data or materials.
- 3) Having identified risks, the next step is to implement **controls** that **detect** and **prevent** losses and procedures that enable the organization to **recover** from losses (or other disasters) with a minimum of interruption to business continuity.
- 4) The "final" step in the process is to review, test, and update procedures continually. An organization must ensure continued **compliance** with its security policy and the relevance of that policy to new and changing risks.

Roles and Responsibilities

As part of this process, employees must be aware of their **responsibilities** with regard to security. The structure of security responsibilities will depend on the size and hierarchy in place in an organization, but these roles are typical:

- Overall internal responsibility for security might be allocated to a Director of Security or Chief Information Security Officer (CISO), with the Chief Information Officer (CIO) / Chief Technology Officer (CTO) or Finance Director.
- Managers may have responsibility for a particular area; such as building control, ICT, or accounting.
- Technical staff may have responsibility for implementing, maintaining, and monitoring the policy. One notable job role is that of Information Systems Security Officer (ISSO).
- Non-technical staff have the responsibility of complying with policy and with any relevant legislation.
- External responsibility for security (due care or liability) lies mainly with directors or owners, though again it is important to note that all employees share some measure of responsibility.

Historically, responsibility for security might have been allocated to an existing business unit, such as ICT or accounts. However the goals of a network manager are not always well-aligned with the goals of security; network management being focused on availability over confidentiality.

Consequently, security is increasingly thought of as a dedicated function or business unit in its own right with its own management structure. This is one example of a concept called "separation of duties".

Security professionals working in such a role must be competent in a wide-range of disciplines, from network and application design, through to procurement and HR. The following activities might be typical of such a role:

- Participate in risk assessments and testing of security systems, and make recommendations.
- Specify, source, install, and configure secure devices and software.
- Set up and maintain document access control and user privilege profiles.
- Monitor audit logs and review user privileges and document access controls.
- Manage security-related incident reporting and response.
- Create and test business continuity and disaster recovery plans and procedures.

Security Controls

In the US, the **Computer Security Division** of the **National Institute of Standards and Technology (NIST)** is responsible for issuing the **Federal Information Processing Standards (FIPS)** plus advisory guides called **Special Publications**. Many of the standards and technologies covered in CompTIA Security+ are discussed in these documents.



The FIPS standards discussed in this course are available at gtsgo.to/cadtt. Special Publications are available at gtsgo.to/l7zdm.

A **security control** (or **countermeasure**) is something designed to make a particular asset or information system secure (that is, give it the properties of confidentiality, integrity, availability, and non-repudiation).



vvbg4

Control Types

The concept of security controls is best defined in **FIPS 200** and **NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems and Organizations)**. One of the objectives of these documents is to classify different types of security control. They do so by identifying security controls as belonging in one of 18 **families**, such as Access Control (AC), Audit and Accountability (AA), Incident Response (IR), or Risk Assessment (RA), which describe the basic functions of the controls.

Furthermore, each family is assigned to a **class**, based on the dominant characteristics of the controls included in that family. The classes identified by NIST are:

- **Technical** - the control is implemented as a system (hardware, software, or firmware). For example, firewalls, anti-virus software, and OS access control models are technical controls.
- **Operational / administrative** - the control is implemented primarily by people rather than systems. For example, security guards and training programs are operational controls rather than technical controls.
- **Management** - the control gives oversight of the information system. Examples could include risk identification or a tool allowing the evaluation and selection of other security controls.

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management



You do NOT need to memorize these identifiers for the exam. The table just illustrates how different families of security control could be classified.



Physical Security Control Types

The NIST schema isn't the only way of classifying security controls. **Physical** security controls (such as alarms, gateways, and locks) are often classed separately (under NIST they are a family of operational controls). As with the NIST classification, controls can be divided into two broad classes:

- **Administrative** - controls that determine the way people act, including policies, procedures, and guidance.
- **Technical** - controls implemented in operating systems, software, and hardware devices.

Whether administrative or technical, controls can also be classified according to the goal or function of the control in a simpler schema than the families identified by NIST.

- **Preventive** - the control physically or logically restricts unauthorized access. A directive can be thought of as an administrative version of a preventive control.
- **Deterrent** - the control may not physically or logically *prevent* access, but psychologically *discourages* an attacker from attempting an intrusion.
- **Detective** - the control may not prevent or deter access, but it will identify and record any attempted or successful intrusion.



As no single security control is likely to be invulnerable, it is helpful to think of them as delaying or hampering an attacker until the intrusion can be detected. The efficiency of a control is a measure of how long it can delay an attack.

- **Corrective** - the control responds to and fixes an incident and may also prevent its reoccurrence.
- **Compensating** - the control does not prevent the attack but restores the function of the system through some other means, such as using data backup or an alternative site.



1cyos

Access Control and ACLs

An **access control system** is the set of technical controls that govern how subjects may interact with objects. **Subjects** in this sense are users or software processes or anything else that can request and be granted access to a resource. **Objects** are the resources; these could be networks, servers, databases, files, and so on. In computer security, the basis of access control is usually an **Access Control List (ACL)**. This is a list of subjects and the rights or permissions they have been granted on the object. An access control system is usually described in terms of four main processes:

- **Identification** - creating an account or ID that identifies the user or process on the computer system.
- **Authentication** - proving that a subject is who or what it claims to be when it attempts to access the resource.
- **Authorization** - determining what rights subjects should have on each resource and enforcing those rights.
- **Accounting** - tracking authorized and unauthorized usage of a resource.

For example, if you are setting up an ecommerce site and want to enroll users, you need to select the appropriate controls to perform each function:

- Identification - you need to ensure that customers are legitimate. You might need to ensure that billing and delivery addresses match for instance and that they are not trying to use fraudulent payment methods.
- Authentication - you need to ensure that customers have unique accounts and that only they can manage their orders and billing information.
- Authorization - you need rules to ensure customers can only place orders when they have valid payment mechanisms in place. You might operate loyalty schemes or promotions that authorize certain customers to view unique offers or content.
- Accounting - the system must record the actions a customer takes.



6rmfm

Identification

Identification associates a particular user (or software process) with an action performed on a network system.

Authentication proves that a user or process is who it claims to be (that is, that someone or something is not masquerading as a genuine user).

Identification and authentication are vital first steps in the access control process:

- To prove that a user is who s/he says s/he is. This is important because access should only be granted to valid users (authorization).
- To prove that a particular user performed an action (accounting). This is important because a user should not be able to deny what they have done (non-repudiation).

A subject is identified on a computer system by an **account**. An account consists of an **identifier**, **credentials**, and a **profile**.

An identifier must be **unique**. For example, in Windows a subject may be identified by a username to system administrators and users but is actually defined on the system by a Security Identifier (SID) string. If the user account was deleted and another account with the same name subsequently created, the new account would have a new SID and therefore not inherit any of the permissions of the old account.

"Credentials" means the information used to authenticate a subject when it tries to access the user account. This information could be a username and password or smart card and PIN code.

The profile is information stored about the subject. This could include name and contact details and also group memberships.

Issuance / Enrollment

Issuance (or enrollment) are the processes by which a subject's credentials are recorded and issued and linked to the correct account and by which the account profile is created and maintained. Some of the issues involved are:

- Identity proofing - verifying that subjects are who they say they are *at the time the account is created*. Attackers may use **impersonation** to try to infiltrate a company without disclosing their real identity. Identity proofing means performing background and records checks at the time an account is created.



Websites that allow users to self-register typically employ a CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart). A CAPTCHA is usually a graphic or audio of some distorted letters and digits. This prevents a software process (bot) creating an account.

- Ensuring only valid accounts are created - for example preventing the creation of dummy accounts or accounts for employees that are never actually hired. The identity issuance process must be secured against the possibility of insider threats (rogue administrative users). For example, a request to create an account should be subject to approval and oversight.
- Secure transmission of credentials - creating and sending an initial password securely. Again, the process needs protection against snooping and rogue administrative staff. Newly created accounts with simple or default passwords are an easily exploitable "backdoor".
- Revoking the account if it is compromised or no longer in use.

Identity Management

Identity management refers to the issues and problems that must be overcome in implementing the identification and authentication system across different networks and applications.

A particular subject may have numerous "digital identities", both within and without the company. On a personal level, managing those identities is becoming increasingly difficult, forcing users into insecure practices, such as sharing passwords between different accounts.

These difficulties can be mitigated by two techniques:

- Password reset - automating the password reset process reduces the administration costs associated with users forgetting passwords, but making the reset process secure can be problematic.
- Single sign-on - this means that all network resources and applications accept the same set of credentials, so the subject only needs to authenticate once per session. This requires application compatibility and is difficult to make secure or practical across third-party networks.

Authentication



Assuming that an account has been created securely (the identity of the account holder has been verified), **authentication** verifies that only the account holder is able to use the account (and that the system may only be used by account holders). Authentication is performed when the account holder supplies the appropriate **credentials** to the system. These are compared to the credentials stored on the system. If they match, the account is authenticated.

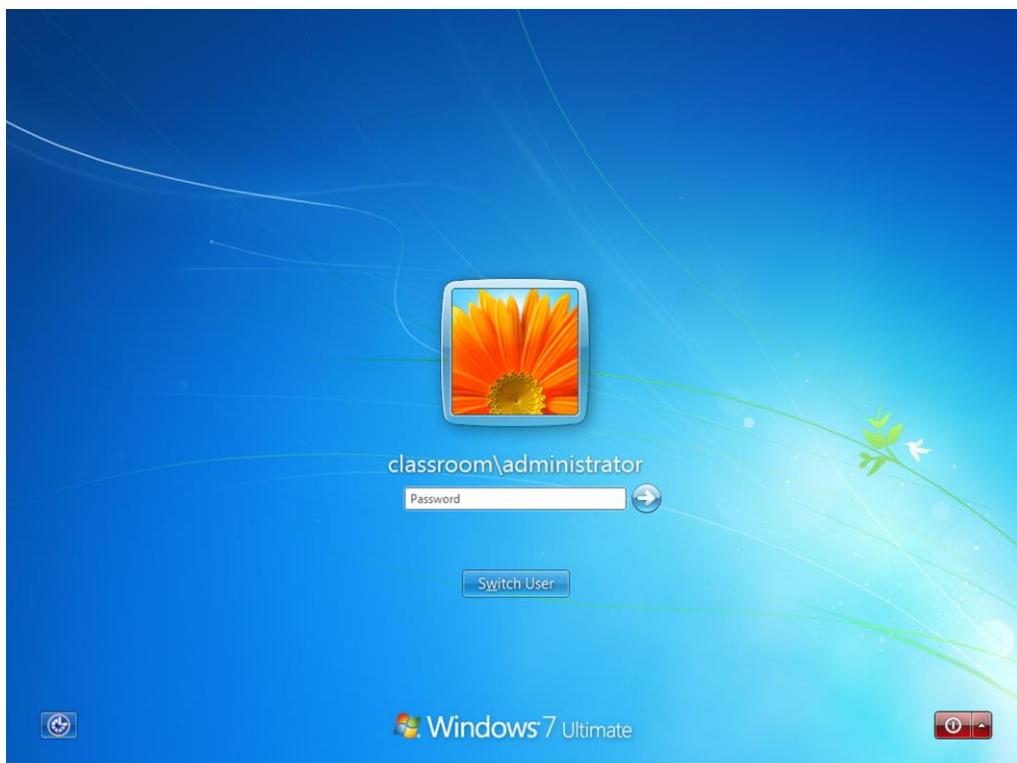
There are many different technologies for defining credentials. They can be categorized as the following factors:

- Something you **know** (such as a password).
- Something you **have** (such as a smart card).
- Something you **are** (such as a fingerprint).

Each has advantages and drawbacks.

Something You Know Authentication

The typical "something you know" technology is the log on: this comprises a **username** and a **password**. The username is typically not a secret (though it doesn't do to go round publishing it) but the password must be known only to the account holder. A **passphrase** is a longer password comprising a number of words. This has the advantages of being more secure and easier to remember. A **Personal Identification Number (PIN)** is another example of something you know.



Windows logon dialog

Another important concept in authentication based on facts that a person knows is **Personally Identifiable Information (PII)**. PII includes things such as full name, birth date, address, social security number, and so on. Some bits of information (such as a social security number) may be unique; others uniquely identify an individual in combination (for example, full name with birth date and street address).

PII is often used for password reset mechanisms and to confirm identity over the telephone. For example, PII may be defined as responses to challenge questions, such as "What is your favorite color / pet / movie?"

Disclosing PII inadvertently can lead to identity theft (where someone usurps a legally valid identity to conceal their illegal activities). PII can often be relatively easy to obtain so caution needs to be exercised when depending on this information for authentication.

Something You Have Authentication

There are various ways to authenticate a user based on something they have. Examples include a smart card, USB token, or key fob that contains a chip with authentication data, such as a **digital certificate**.



Digital certificates are an encryption technology. See [Unit 2.1](#) for more information about cryptography.

The card must be presented to a card reader before the user can be authenticated. A USB token can be plugged into a normal USB port.



GemPlus USB smart card reader (courtesy GemPlus image library)

When the card is read, the card software prompts the user for a **Personal Identification Number (PIN)** or password, which mitigates the risk of the card being lost or stolen.

Another option is a hardware token that generates a **one-time password**. The token displays a number that changes periodically; the number and frequency of changes is mathematically linked to an algorithm on the authenticating server, so inputting the correct code proves possession of the token.

The main concerns with "something you have" technologies are loss and theft and the chance that the device can be counterfeited. There are also hardware and maintenance costs.

Something You Are Authentication

"Something you are" means employing some sort of **biometric** recognition system. Many types of biometric information can be recorded, including fingerprint patterns, signature recognition, iris or retina recognition, or facial recognition. The chosen biometric information (the **template**) is scanned and recorded in a database. When the user wants to access a resource, s/he is re-scanned and the scan compared to the template. If they match to within a defined degree of tolerance, access is granted.



yk4sd

Multifactor Authentication

An authentication technology is considered "strong" if it combines the use of more than one type of technology (**multifactor**). Single factor authentication systems can quite easily be compromised: a password could be written down or shared, a smart card could be lost or stolen, and a biometric system could be subject to high error rates.

Two-factor authentication combines something like a smart card or biometric mechanism with "something you know", such as a password or PIN. Three-factor authentication combines all three technologies. An example of this would be a smart card with integrated thumb- or fingerprint reader. This means that to authenticate, the user must possess the card, the user's fingerprint must match the template stored on the card, and the user must input a PIN.



Multifactor authentication requires a combination of different technologies. For example, requiring a PIN along with Date of Birth may be stronger than entering a PIN alone, but it is not multifactor.



Multifactor authentication technologies are covered in more detail in [Unit 2.4](#).

Authorization



z0m75

Authorization is the process by which users (typically authenticated users) are granted rights to access and modify resources.

There are two important functions in authorization:

- The process of ensuring that only authorized rights are exercised (policy enforcement).
- The process of determining rights (policy definition)

Formal Access Control Models

An important consideration in designing a security system is to determine *how* users receive rights (or to put it another way, how Access Control Lists [ACL] are written). Access control or authorization models are generally classed as one of the following:

- Discretionary Access Control (DAC).
- Role-based Access Control (RBAC).
- Mandatory Access Control (MAC).

Discretionary Access Control (DAC)

Discretionary Access Control (DAC) stresses the importance of the **owner**. The owner is originally the creator of the resource, though ownership can be assigned to another user. The owner is granted **full control** over the resource, meaning that s/he can modify its ACL to grant rights to others.

This is the most flexible model and currently widely implemented in terms of computer and network security. In terms of file system security, it is the model used by UNIX/Linux distributions and Microsoft Windows.

As the most flexible model, it is also the weakest, because it makes centralized administration of security policies the most difficult to enforce. It is also the easiest to compromise, as it is extremely vulnerable to insider threats.

Role-based Access Control (RBAC)

Role-based Access Control (RBAC) adds an extra degree of administrative control to the DAC model. Under RBAC, a set of organizational roles are defined and users allocated to those roles.

Under this system, the right to modify roles is reserved to administrative accounts. Therefore the system is non-discretionary, as each user has no right to modify the ACL of a resource, even though they may be able to change the resource in other ways. Users are said to gain rights *implicitly* (through being assigned to a role) rather than *explicitly* (being assigned the right directly).



Ideally, the rights of a role are set at design time and not changed under normal operating conditions. This means that administrators can focus on membership of different role groups, rather than what the roles can do. It also makes it harder for an attacker to "escalate" permissions gained through a hacked user account.

RBAC can be *partially* implemented in Windows through the concept of group accounts. RBAC is the most commonly implemented system on computer networks, as it re-establishes centralized, administrative control over important resources. To fully implement RBAC, you also need to define what tasks users can perform in a given application. Object-based ACLs are not flexible enough to do this. You also need to "turn off" the discretionary aspect of the underlying OS - not something that is currently supported by Windows. You can read more about RBAC at NIST's site (gtsgo.to/gdgwm).

Mandatory Access Control (MAC)

Mandatory Access Control (MAC) is based on the idea of security clearance levels. Rather than defining access control lists on resources, each object and each subject is granted a clearance level (referred to as a **label**). If the model used is a hierarchical one (that is, high clearance users are trusted to access low clearance objects), subjects are only permitted to access objects at their own clearance level or below. Alternatively, each resource and user can be labeled as belonging to a domain (compartmentalized). A user may only access a resource if they belong to the same domain. This is referred to as "Need to Know".

The labeling of objects and subjects takes place using pre-established rules. The critical point is that these rules cannot be changed (except by the system owner) and therefore are also non-discretionary. Also, a subject is not permitted to change an object's label or to change their own label.

This type of access control is associated with military and secret service organizations, where the inconveniences forced on users are secondary to the need for confidentiality and integrity.

Rule-based Access Control

Rule-based access control is a term that can refer to any sort of access control model where access control policies are determined by system-enforced rules rather than system users. As such, RBAC and MAC are both examples of rule-based (or non-discretionary) access control.

As well as the formal models, rule-based access control principles are increasingly being implemented to protect computer and network systems founded on discretionary access from the sort of misconfiguration that can occur through DAC. One example is forcing applications such as web browsers to run in a "sandbox" mode, to prevent malicious scripts on a website from using the privileges of the logged on user to circumvent the security system. A key point is that privileges are restricted, *regardless* of the user's identity.

Basic Authorization Policies

The more privileges that you allocate to more users, the more you increase the risk that a privilege will be misused. Authorization policies help to reduce risk by limiting the allocation of privileges as far as possible.

Implicit Deny

Access controls are usually founded on the principle of **implicit deny**; that is, unless there is a rule specifying that access should be granted, any request for access is denied. This also means that a user must be authenticated to perform any action on the system.

This principle can be seen clearly in firewall policies. A firewall filters access requests using a set of rules. The rules are processed in order from top-to-bottom. If a request does not fit any of the rules, it is handled by the last (default) rule, which is to refuse the request.

Least Privilege

A complementary principle is that of **least privilege**. This means that a user should be granted rights necessary to perform their job and no more.



These principles apply equally to users (people) and software processes. Much software is written without regard to the principles of implicit deny and least privilege, making it less secure than it should be.



1usju

Single Sign-on (SSO)

Single Sign-On (SSO) means that a user only has to authenticate to a system once to gain access to all the resources to which the user has been granted rights. An example is the Kerberos authentication and authorization model. This means (for example) that a user that has authenticated with Windows is also authenticated with the Windows domain's SQL Server and Exchange Server services.



Kerberos authentication is discussed in [Unit 2.3](#).

The advantage of single sign-on is that each user does not have to manage multiple user accounts and passwords. The disadvantage is that compromising the account also compromises multiple services.

Single sign-on only tends to be implemented on enterprise networks. There have been various initiatives to try to extend the principle to web accounts (Microsoft's Live accounts, Facebook Login, and the PayPal e-commerce model for instance), but no scheme has achieved the sort of critical mass that would force mass acceptance. There would also be serious security concerns about using a common log in for different sites, especially where online banking sites are concerned.



It is critical that users do not re-use work passwords or authentication information on third-party sites. Of course, this is almost impossible to enforce, so security managers have to rely on effective user training.



Unit 2.4 discusses federated identity management, authentication, and authorization and the establishment of trusts between different domains.

Accounting

Accounting (or accountability or auditing) means recording when and by whom a resource was accessed.

Accounting is critical to security. The purpose of accounting is to track what has happened to a resource over time. As well as keeping a log of authorized access and edits, this can also reveal suspicious behavior and attempts to break through security.

Logs

Accounting is generally performed by **logging** actions automatically. All NOS and many applications and services can be configured to log events.

Logging generally needs to be enabled and configured by the administrator. The main decision is which events to record. Logs serve the following two general purposes:

- Accounting for all actions that have been performed by users. Change and version control systems depend on knowing when a file has been modified and by whom. Accounting also provides for non-repudiation (that is, a user cannot deny that they accessed or made a change to a file). The main problems are that auditing successful access attempts can quickly consume a lot of disk space and analyzing the logs can be very time-consuming.
- Detecting intrusions (or attempted intrusions). Here records of failure-type events are likely to be more useful, though success-type events can also be revealing if they show unusual access patterns.

Obviously, the more events that are logged, the more difficult it is to analyze and interpret the logs.

Also, logs can take up a large amount of disk space. When a log reaches its allocated size, it will start to overwrite earlier entries. This means that some system of backing up logs will be needed in order to preserve a full accounting record to points in time.

It is also critical that the log files be kept secure, so that they cannot be tampered with. Insider threats are particularly pertinent here as rogue administrators could try to doctor the event log to cover up their actions.

Surveillance

Surveillance is a means of accounting for physical access to a system (though electronic surveillance can also detect when a user accesses a computer system). Surveillance is also a type of access control, as it acts as a **deterrent** to those who would otherwise attempt to penetrate the system.

Incident Reporting

Incident reporting means informing the relevant person that there has been a security breach. Auditing software might do this automatically (for example, by emailing the administrator).

For situations not covered by software, there needs to be a clear policy for employees to follow:

- What is an incident? What should I report?
- To whom do I make the report?
- How quickly should I report an incident?



System auditing and scanning tools are covered in more detail in [Unit 1.3](#) and [Unit 1.4](#). Incident management is discussed in [Unit 5.5](#).



Review Questions / Module 1 / Unit 1 / Security Controls

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What is the difference between authorization and authentication?
- 2) What type of access control system is based on resource ownership?
- 3) True or false? A "Need to Know" policy can only be enforced using discretionary or role-based access control.
- 4) What steps should be taken to enroll a new user?
- 5) What is the basis of computer security accounting?
- 6) What term is used to describe a property of a secure network where a sender cannot deny having sent a message?
- 7) How does accounting provide non-repudiation?
- 8) You are implementing security controls to protect highly confidential information that must only be made available on a "Need to Know" basis. What class of security control should you investigate?
- 9) You have implemented a web gateway that blocks access to a social networking site. How would you categorize this type of security control?
- 10) The company you work for has suffered numerous intrusions due to poor password management by employees. Given a significant budget to mitigate the problem, what type of security control would you use?

Module 1 / Unit 2

Threats and Attacks

Objectives

On completion of this unit, you will be able to:

- Categorize vulnerabilities and threat agents and vectors.
- Understand social engineering and phishing attacks.
- Identify different types of malware and malware protection.

Vulnerability, Threat, and Risk



bxi0

In IT security, it is important to distinguish between the concepts of **threat**, **vulnerability**, and **risk**. These terms are not always used consistently. NIST uses the following definitions:

- **Vulnerability** - a weakness that could be triggered accidentally or exploited intentionally to cause a security breach.
- **Threat** - the potential for a **threat agent** or **threat actor** (something or someone that may trigger a vulnerability accidentally or exploit it intentionally) to "exercise" a vulnerability (that is, to breach security). The path or tool used by the threat actor can be referred to as the **threat vector**.
- **Risk** - the likelihood and impact (or consequence) of a threat actor exercising a vulnerability.
- **Control** - a system or procedure put in place to mitigate risk.



These definitions and more information on risk management are contained in SP800-30 (gtsgo.to/m8ye2). Vulnerability and risk assessments are covered in more detail in [Unit 1.4](#) and [Unit 5.3](#).

Types of Threat Agent

Threat agents can be placed in different categories. An "agent" need not be human for instance. Confidentiality, integrity, and availability could be threatened as much by an earthquake as they could by a hacker.

Hackers, Crackers, Black Hats, White Hats, and Script Kiddies

Experts in computer security are widely referred to as **hackers**. A **cracker** is someone who breaks into a computer system with the intent of causing damage or theft. Nowadays, the terms **Black Hat** (malicious) and **White Hat** (non-malicious) are more widely used.

A **script kiddie** is someone that uses hacker tools without necessarily understanding how they work or having the ability to craft new attacks. A **newbie** (or **n00b**) is one taking their first step into a larger world.

External Threats

Human threat sources described as external covers the whole range of malicious attackers that could pose a threat to the organization's assets, including crackers, script kiddies, thieves, organized crime, terrorists, war, and so on. Within these groups, further distinctions as to **motivation** can be made, such as whether an attacker is motivated by greed, curiosity, or has some sort of grievance.

It also helps to categorize threats as **structured** or **unstructured** (or **targeted** or **opportunistic**) depending on the degree to which your own organization is targeted specifically. For example, a criminal gang attempting to steal customers' financial data is a structured, targeted threat; a script kiddie launching some variant on the "I Love You" mail virus is an unstructured, opportunistic threat. The degree to which any given organization will be targeted by external threats depends largely on the value of its assets and the quality of its security systems.

A strong security system may be a deterrent to thieves; conversely it may be attractive to hackers seeking a challenge. It is important to understand the different motivations for attackers in order to design effective security systems.



Attacks become less effective when they are well-known so new threats appear all the time. To keep up-to-date, you should monitor websites and newsgroups. Apart from the regular IT magazines, some good examples include www.cert.org, www.sans.org, www.schneier.com, and www.grc.com. The annual SANS "Top 20" security attack targets is one of the most useful starting points (www.sans.org/top20/).



z62v1

Malicious Insider Threats

Malicious insider threat sources means attacks launched by the organization's own staff, partners, or contractors. One of the principal sources of research into computer security is the **Computer Emergency Response Team (CERT)** at Carnegie Mellon University. CERT's definition of a malicious insider is:

A current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

Again, the key point here is to identify likely motivations, such as employees who might harbor grievances or those likely to perpetrate fraud. An employee who plans and executes a campaign to modify invoices and divert funds is launching a structured attack; an employee who tries to guess the password on the salary database a couple of times, having noticed that the file is available on the network, is an opportunistic attack.

CERT identify the main motivators for insider threat as sabotage, financial gain, and business advantage.

Another key point is that technical controls are less likely to be able to deter structured insider threats, as insiders are more likely to be able to bypass them. Implementing operational and management controls (especially secure logging and auditing) is essential.



A guide to identifying and deterring insider threats is available at gtsgo.to/p6f9h.

Accidental

Another human threat source is the all-too-human propensity for carelessness. Misuse of a system by a naïve user may not intend harm but can nonetheless cause widespread disruption. Misconfiguration of a system can create vulnerabilities that might be exploited by other threat agents.

Natural Disaster

Natural disaster is fairly self-explanatory; these are threat sources such as river or sea floods, earthquakes, electrical storms, and so on. Natural disasters may be quite predictable (as is the case with areas prone to flooding or storm damage) or unexpected, and therefore difficult to plan for.



Natural disaster is one category of threat

Environmental

Environmental threat sources are those caused by some sort of failure in the built environment. These could include power or telecoms failure or pollution or accidental damage.

Legal and Commercial Threats

In addition to threats to assets and staff members, an organization can be made vulnerable because of misuse of equipment by its employees or attackers. Some examples include:

- Downloading or distributing obscene material.
- Defamatory comments published on social networking sites.
- Hijacked mail or web servers used for spam or phishing attacks.
- Third-party liability for theft or damage of personal data.
- Accounting and regulatory liability to preserve accurate records.

These cases are often complex, but even if there is no legal liability the damage done to the organization's reputation could be just as serious.

Social Engineering



Protecting against natural or environmental disasters is important but most of the focus in computer security is in deterring malicious external and insider threats. Attackers can use a diverse range of techniques to compromise a security system. A pre-requisite of many types of attack is to obtain information about the network and security system.

Social engineering refers to means of getting users to reveal confidential information.

Impersonation



Impersonation (pretending to be someone else) is one of the basic social engineering techniques.

The classic impersonation attack is for an attacker to phone into a department, claim they have to adjust something on the user's system remotely, and get the user to reveal their password. For this attack to succeed the approach must be convincing and persuasive.



Do you really know who's on the other end of the line?

To be persuasive, social engineering attacks rely on one or more of the following principles.

Familiarity / Liking

Some people have the sort of natural charisma that allows them to persuade others to do as they request. One of the basic tools of a social engineer is simply to be affable and likable and to present the requests they make as completely reasonable and unobjectionable. This approach is relatively low-risk as even if the request is refused, it is less likely to cause suspicion and the social engineer may be able to move on to a different target without being detected.

Consensus / Social Proof

The principle of "consensus" or "social proof" refers to the fact that without an explicit instruction to behave in a certain way, many people will act just as they think others would act.

A social engineering attack can use this instinct either to persuade the target that to refuse a request would be odd ("That's not something anyone else has ever said no to") or to exploit polite behavior (see "Tailgating" below).

Authority and Intimidation

Many people find it difficult to refuse a request by someone they perceive as superior in rank or expertise. Social engineers can try to exploit this behavior to intimidate their target by pretending to be someone senior. Another attack might be launched by impersonating someone who would often be deferred to, such as a police officer, judge, or doctor. Another technique is using spurious technical arguments and jargon. Social engineering can exploit the fact that few people are willing to admit ignorance. Compared to using a familiarity / liking sort of approach, this sort of adversarial tactic might be more risky to the attacker as there is a greater chance of arousing suspicion and the target reporting the attack attempt.

Scarcity and Urgency

Often also deployed by salespeople, creating a false sense of scarcity or urgency can disturb people's ordinary decision-making process. The social engineer can try to pressure their target by demanding a quick response. For example, the social engineer might try to get the target to sign up for a "time-limited" or "invitation-only" trial and request a username and password for the service (hoping that the target will offer a password they have used for other accounts).



Id3ua

Trust and Dumpster Diving

Being convincing (or establishing **trust**) usually depends on the attacker obtaining privileged information about the organization. For example, an impersonation attack is much more effective if the attacker knows the user's name. As most companies are set up towards customer service rather than security, this information is typically quite easy to come by. Information that might seem innocuous of itself, such as department employee lists, job titles, phone numbers, diary, invoices, or purchase orders, can help an attacker penetrate an organization through impersonation.

Dumpster Diving refers to combing through an organization's (or individual's) refuse to try to find useful documents (or even files stored on discarded removable media).



Remember that attacks may be staged over a long period of time. Initial attacks may only aim at compromising low-level information and user accounts but this low-level information can be used to attack more sensitive and confidential data and better protected management and administrative accounts.



20uyb

Shoulder Surfing

Shoulder surfing refers to stealing a password or PIN (or other secure information) by watching the user type it. Despite the name the attacker may not have to be in close proximity to the target - they could use high-power binoculars or CCTV to directly observe the target remotely.

Lunchtime Attack

Most authentication methods are dependent on the physical security of the workstation. If a user leaves a logged on workstation unattended, an attacker can gain access to the system using the logged on profile (often described as a **lunchtime attack**). Most operating systems are set to activate a password-protected screen saver after a defined period of no keyboard or mouse activity. Users should also be trained to lock or log off the workstation whenever they leave it unattended.



tw8aq

Tailgating

Tailgating (or **piggybacking**) is a means of entering a secure area without authorization by following close behind the person that has been allowed to open the door or checkpoint. This might be done without the target's knowledge or may be a means of an insider to allow access to someone without recording it in the building's entry log.

Another technique is to persuade someone to hold a door open, using an excuse such as "I've forgotten my badge / key".



5ifg4

Phishing

Phishing is a combination of social engineering and **spoofing** (disguising one computer resource as another). In the case of phishing, the attacker sets up a spoof website to imitate a target bank or ecommerce provider's secure website. The attacker then emails users of the genuine website informing them that their account must be updated, supplying a disguised link that actually leads to their spoofed site. When the user authenticates with the spoofed site, their log on details are captured. Another technique is to spawn a "pop-up" window when a user visits a genuine banking site to try to trick them into entering their credentials through the pop-up.



See [Unit 4.4](#) for more information on web security.



2xor2

Spear Phishing / Whaling

Spear phishing refers to a phishing scam where the attacker has some information that makes the target more likely to be fooled by the attack. The attacker might know the name of a document that the target is editing for instance and send a malicious copy or the phishing email might show that the attacker knows the recipient's full name, job title, telephone number or other details that help to convince the target that the communication is genuine.

A spear phishing attack directed specifically against upper levels of management in the organization (CEOs and other "big beasts") is sometimes called **whaling**. Upper management may also be more vulnerable to ordinary phishing attacks because of their reluctance to learn basic security procedures.

Vishing



While email is one of the most common vectors for phishing attacks, any type of electronic communication without a secure authentication method is vulnerable. Vishing describes a phishing attack conducted through a voice channel (telephone or VoIP for instance). For example, targets could be called by someone purporting to be their bank asking them to verify a recent credit card transaction and requesting their security details. It can be much more difficult for someone to refuse a request made in a phone call compared to one made in an email.

Similarly SMiShing refers to fraudulent SMS texts. Other vectors could include instant messaging or social networking sites.

Pharming

Pharming is another means of redirecting users from a legitimate website to a malicious one. Rather than using social engineering techniques to trick the user however, pharming relies on corrupting the way the victim's computer performs internet name resolution, so that they are redirected from the genuine site to the malicious one.

For example, if mybank.com should point to the IP address w.x.y.z, a pharming attack would corrupt the name resolution process to make it point to IP address a.b.c.d.



There are a number of ways of performing a pharming attack. See [Unit 3.5](#) for more information on name resolution and DNS security.



Watering Hole Attack

A **watering hole attack** is another type of directed social engineering attack. It relies on the probability that a particular group of targets may use an insecure third-party website. For example, staff running an international ecommerce site might use a local pizza delivery firm. If an attacker can compromise the pizza delivery firm's website, they may be able to install malware on the computers of the ecommerce company's employees and penetrate the ecommerce company systems.

Mitigating Social Engineering Attacks

Social engineering is best defeated by training users to recognize and respond to situations.

- Train employees only to release information or make privileged use of the system only according to standard procedures.

- Establish a reporting system for suspected attacks - though the obvious risk here is that a large number of false negatives will be reported.
- Train employees to identify phishing and pharming style attacks plus new styles of attack as they develop in the future.
- Train employees not to release any work-related information on third-party sites or social networks (and especially not to reuse passwords used for accounts at work).

Other measures include ensuring documents and information is destroyed before disposal, using multifactor access control, to put more than one or two barriers between an attacker and his or her target, and restricting use of administrative accounts as far as possible.



See [Unit 5.6](#) for more information on security policies. These can be used to inform and guide users.

Malware



temac

Malware is a catch-all term to describe malicious software threats and social engineering tools designed to vandalize or compromise computer systems.



fj6pp

Computer Viruses

Computer viruses are programs designed to replicate and spread amongst computers, usually by "infecting" executable applications or program code.

There are several different types of virus and they are generally classified by the different ways they can infect the computer (the **vector**). For example:

- **Boot sector viruses** - these attack the boot sector information, the partition table, and sometimes the file system.
- **Program viruses** - these are sequences of code that insert themselves into another executable program. When the application is executed, the virus code becomes active.
- **Script viruses** - scripts are powerful languages used to automate OS functions and add interactivity to web pages. Scripts are executed by an interpreter rather than self-executing. Most script viruses target vulnerabilities (exploits) in the interpreter.
- **Macro viruses** - these viruses affect Microsoft Office documents, and have become very prevalent because of the wide distribution of these documents, especially over the internet.

- **Multipartite viruses** - these use both boot sector and executable file infection methods of propagation.

What these types of viruses have in common is that they must infect a host file. That file can be distributed through any normal means - on a disk, on a network, or as an attachment through an email or instant messaging system.

Email attachment viruses (usually program or macro viruses in an attached file) often use the infected host's electronic address book to **spoof** the sender's address when replicating. For example, Alice's computer is infected with a virus and has Bob's email address in his address book. When Carlos gets an infected email apparently sent by Bob, it is the virus on Alice's computer that has sent the message.

Viruses are also categorized by their virulence. Some viruses are virulent because they exploit a previously unknown system vulnerability (a "zero-day" exploit); others employ particularly effective social engineering techniques to persuade users to open the infected file (an infected email attachment with the subject "I Love You" being one of the best examples of the breed).

While the distinguishing feature of a virus is its ability to replicate by infecting other computer files, a virus can also be configured with a **payload** that executes when the virus is activated. The payload can perform any action available to the host process. For example, a boot sector virus might be able to overwrite the existing boot sector, an application might be able to delete, corrupt, or install files, and a script might be able to change system settings or delete or install files.

Worms

Worms are memory-resident viruses that replicate over network resources. A worm is self-contained; that is, it does not need to attach itself to another executable file. They typically target some sort of vulnerability in a network application, such as a database server. The primary effect of a worm infestation is to rapidly consume network bandwidth as the worm replicates. A worm may also be able to crash an operating system or server application (performing a Denial of Service attack). Also, like viruses, worms can carry a payload that may perform some other malicious action (such as installing a backdoor).



zqts3

Logic Bombs

Some viruses do not trigger automatically. Having infected a system, they wait for a preconfigured time or date (**time bomb**) or system or user event (**logic bomb**). Logic bombs need not be viruses; a typical example is a system administrator bearing a grudge leaving a scripted trap that runs in the event of their account being deleted or disabled. Anti-virus software is unlikely to detect this kind of malicious script or program. This type of trap is also referred to as a **mine**.

Virus Alert Hoaxes



pxxpq

Hoax virus alerts are quite common. They are commonly sent as mass emails as a prank. Most advise you to forward the "alert" to everyone in your address book. Some hoax virus alerts describe a number of steps that you "must take" to remove the virus - following these steps may cause damage to your computer.

The screenshot shows the McAfee Security homepage. The top navigation bar includes links for 'Products & Services', 'Virus Information', 'Store', 'Support', 'Downloads', 'Log In', and 'My Account'. A central banner says 'Protect Your PC from Internet Threats' with a dropdown menu set to '1. Test and Protect my PC' and a 'Begin Test' button. On the left, a sidebar lists various resources like 'Product Recommender', 'Virus Removal Tools', 'Virus Calendar', 'Virus Hoaxes' (which is highlighted), 'Virus Glossary', 'Regional Virus Info', 'Alert Archive', 'Dispatch: Virus Newsletters', 'Security News Network', 'Anti-Virus Tips', and 'Online Guide for Parents'. Below this is a 'Subscriber Support' section with a search bar and a 'Search' button. A 'Related Links' section follows. The main content area is titled 'Virus Hoaxes' and discusses the nature of virus hoaxes, warning users not to open attachments from unknown sources. It also mentions AOL4FREE as an example of a hoax virus writer. A bulleted list provides tips: 'Always remain vigilant' and 'Never open a suspicious attachment'. A section titled 'McAfee.com Virus Hoax Listings' provides links to various hoax entries.

Virus Hoaxes

There are a lot of viruses out there. But some aren't really out there at all. Virus hoaxes are more than mere annoyances, as they may lead some users to routinely ignore all virus warning messages, leaving them vulnerable to a genuine, destructive virus.

Next time you receive an urgent virus warning message, be sure to check the list of known virus hoaxes below.

Remember: Never open an email attachment unless you know what it is--even if it's from someone you know and trust.

Remember that virus writers can use known hoaxes to their advantage. For example, AOL4FREE began as a hoax virus warning. Then somebody distributed a destructive trojan attached to the original hoax virus warning! The lessons are clear:

- Always remain vigilant
- Never open a suspicious attachment

McAfee.com Virus Hoax Listings

!!UNAVAILABLE!? Mobile Phone Hoax	Guts to Say Jesus hoax
10000 Hoax	Happy New Year Hoax
48 Hours Hoax	Intel Special Offer Hoax
A Moment Of Silence Hoax	Internet Flower hoax
A Virtual Card For You Hoax	Irina Hoax

Information about virus hoax alerts from www.mcafee.com

If you have an anti-virus application, your anti-virus vendor may provide a virus alerting service. You can also check the vendor's site for a list of virus dangers. You should use anti-virus software to remove a virus from an infected file. If anti-virus software does not work, you can look for further instructions from the vendor's website or contact your system administrator.



do3ay

Spam and Spim

Spam is unsolicited email messages, the content of which is usually advertising pornography, miracle cures for various personal conditions, or bogus stock market tips and investments. Spam is also used to launch phishing attacks and spread viruses and worms. Spam needs to be filtered before it reaches the user's inbox or it can have a severe impact on productivity. Most email applications now ship with junk mail filters or you can install a filter at the organization's mail gateway.

The main problem with spam filters is that they can block genuine messages too, leading to missed communications.

Spim and **spit** are the same sort of thing except that they are distributed through instant messaging or VoIP telephony respectively.

Trojans and Spyware

Other types of malware are not classed as viruses as they do not necessarily try to replicate (make copies of themselves). They can be just as much of a security threat as viruses however.



5bfbi

Trojans and Botnets

A **Trojan Horse** (often just simply called a **Trojan**) is a program (often harmful) that pretends to be something else. For example, you might download what you think is a new game, but when you run it, it deletes files on your hard drive; or the third time you start the game, the program emails your saved passwords to another person. There is also the case of **rogueware** or **scareware** fake anti-virus, where a web pop-up claims to have detected viruses on the computer and prompts the user to initiate a full scan, which installs the attacker's Trojan.

Many Trojans function as **backdoor** applications. Once the Trojan backdoor is installed, it allows the attacker to access the PC, upload files, and install software on it. This could allow the attacker to use the computer in a **botnet**, to launch Denial of Service (DoS) attacks or mass-mail spam.



See [Unit 1.3](#) for more information about botnets and Denial of Service.

The attacker also usually establishes some means of secretly communicating with the compromised machine (a **covert channel**). One means of doing this, called the Loki Project, is to embed data in ICMP status messages. Another technique is to use random high TCP or UDP ports and encryption to disguise the contents of packets. Another example is encoding information in parts of a TCP packet (such as a sequence number field or source IP field); this is called **TCP/IP steganography** (hiding a secret message within a public one).

Backdoors

A **backdoor** is typically an access method that is installed without the user's knowledge. This might arise because the user has unwittingly installed malware such as a Trojan but backdoors can be created in other ways too.

Programmers may create backdoors in software applications to use for testing and development that are subsequently not removed when the application is deployed. This is more likely to affect bespoke applications but there have been instances of known backdoors and exploits in commercial software.

Backdoors are also created by misconfiguration of software or hardware that allows access to unauthorized users. Examples include leaving a router configured with the default administrative password, having a Remote Desktop connection configured with an insecure password, or leaving a modem open to receive dial-up connections.



Spyware and Adware

Spyware is a program that monitors user activity and sends the information to someone else. It may be installed with or without the user's knowledge.

Aggressive spyware or Trojans known as "key loggers" actively attempt to steal confidential information, by capturing a credit card number by recording key strokes entered into a web form for example. Another spyware technique is to spawn browser pop-up windows to try to direct the user to other websites, often of dubious provenance.

Adware is any type of software or browser plug-in that displays adverts. Some adware may exhibit spyware-like behavior however, by tracking the websites a user visits and displaying targeted ads for instance.

The distinction between adware and spyware is sometimes blurred. Generally speaking, if the user is not able to give informed consent and/or the application cannot be uninstalled by normal means then it's spyware. If the user accepts the use of their data and the program generally behaves like any other commercial software installation, then it's adware. Of course, informed consent may involve reading a 30 page license agreement. There's also the case that a website may host user-data tracking software without making the user aware of it.

The screenshot shows the 'Actual Spy - Unregistered Version' application window. The title bar reads 'Actual Spy - Unregistered Version'. The menu bar includes 'Start monitoring', 'Stop monitoring', 'Hide', 'Clear all logs', 'Registration', 'Help', and 'Exit'. The main interface has a sidebar with icons for 'PC Activity', 'Internet Activity', 'Report', 'Settings', and 'About'. The 'PC Activity' tab is selected, showing a table with columns: Time, Window Caption, Application Path, and Username. One entry is listed: '7/10/2014 12:33:59 PM' under Time, with empty fields for Window Caption, Application Path, and Username. Below the table is a text area titled 'Keystrokes:' containing a log of typed text. The log includes: '\\server.classroom.local', '[Enter]', 'administrator[Tab][SHIFT]Pa[SHIFT]\$w0rd', '[Enter]', 'word', '[Enter]', '[SHIFT]My[Space]secret[Space]thoughts[Space]of[Space]evil[CTRL]s'. There is a checkbox 'Show characters only' below the log. At the bottom of the window are buttons for 'Refresh', 'Delete', 'Delete all', 'Search', and 'Match case'. Status information at the bottom includes 'Status: started', 'Total records: 10', 'Text logs size: 737.00 Bytes', and 'Screenshots size: 0.00 Bytes'.

ActualSpy

Rootkits



3022z

Many Trojans cannot conceal their presence entirely and will show up as a running service. Often the service name is configured to be similar to a genuine process to avoid detection. For example, a Trojan may use the filename "run32d11" to masquerade as "run32dll". One class of backdoor that is harder to detect is the **rootkit**.

Rootkits work by changing core system files and programming interfaces, so that local shell processes, such as Explorer, taskmgr, or tasklist on Windows or ps or top on Linux, plus port scanning tools such as netstat no longer reveal their presence (at least, if run from the infected machine). They also contain tools for cleaning system logs, further concealing the presence of the Trojan. The most powerful rootkits operate in kernel mode, infecting a machine through a corrupted device driver or kernel patch. A less effective type of rootkit operates in user mode, replacing key utilities or less privileged drivers.



Software processes can run in one of a number of "rings". Ring 0 is the most privileged (it provides direct access to hardware) and so should be reserved for kernel processes only. Ring 3 is where user mode processes run; drivers and I/O processes may run in Ring 1 or Ring 2. This architecture can also be complicated by the use of virtualization.

There are also proof-of-concept rootkits that can reside in firmware (either the computer BIOS or an adapter card or hard drive BIOS). These in theory would survive any attempt to remove the rootkit by formatting the drive and reinstalling the OS.



gsoal

Ransomware

Ransomware is a type of malware that tries to extort money from the victim. One class of ransomware will display threatening messages, such as requiring Windows to be reactivated or suggesting that the computer has been locked by the police because it was used to view child pornography or for terrorism. This may block access to the computer by installing a different shell program but this sort of attack is usually relatively trivial to fix. Another class of ransomware attempts to encrypt data files on any fixed, removable, and network drives. If the attack is successful, the user will be unable to access the files without obtaining the private encryption key, which is held by the attacker. If successful, this sort of attack is extremely difficult to mitigate, unless the user has up-to-date backups of the encrypted files.



See [Unit 2.1](#) for more information about encryption.

Ransomware uses payment methods such as wire transfer, bitcoin, or premium rate phone lines to allow the attacker can extort money without revealing his or her identity or being traced by local law enforcement.

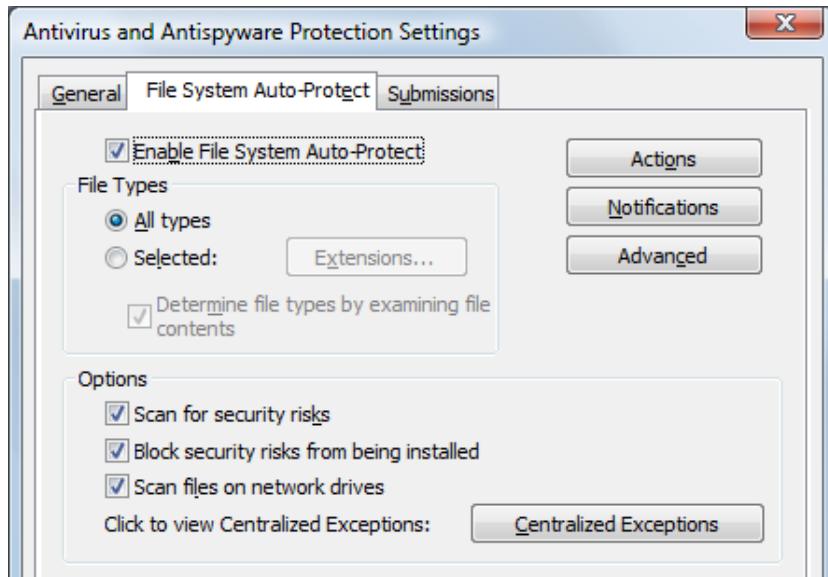
Preventing Malware

Viruses and worms could easily be described as a "mature" threat. There are thousands of examples, some of which have been extraordinarily virulent ("Melissa", "I Love You", "Code Red", "Slammer", or "Conficker" for instance). Anti-virus techniques are essential to mitigating the effect of these threats, as well as more targeted malware attacks, such as Trojans and spyware. While anti-virus software is important, informed and sensible user behavior and corporate security policies are the best defense against malware. A number of steps can be taken to reduce the risk of virus infection:

- Carry out regular backups that allow data to be recovered, in case of loss due to a virus infection.
- Apply operating system and application security patches.
- Install (and keep up-to-date) a virus checker on workstations and servers. Most network anti-virus software can be configured to push updates at clients automatically and force scanning of file and email systems.



When configuring anti-virus software, it is vital to configure the proper exceptions. Real-time scanning of some system files and folders can cause serious performance problems, especially on servers.



Configuring anti-virus scan options

- Configure filtering on the messaging server - this will prevent most unsolicited messages (spam) arriving at the server from getting to the users' mailboxes.
- Properly secure servers and workstations - remember that a virus can only infect other program files if it has write permissions on the files. Ensure that all system and program files are properly secured. Do not grant users more than sufficient permissions. Do not log on using administrative privileges except to perform administrative tasks.

- Educate users about not running untrusted installers and browser plug-ins - and supplement this with procedures that will prevent files, such as executables and Office macros, from being allowed to run. This could be accomplished (for instance) by only allowing digitally signed code to be executed.
- Educate users to help them identify phishing sites by inspecting the URL and looking for the telltale signs of a faked site, such as incorrect logos, spelling errors, or pop-up login forms.
- Audit system events (such as logons) and review logs for unusual activity.

Anti-Virus Software



29zx4

Anti-virus (A-V) software uses a database of known virus patterns (**definitions**) plus **heuristic** (meaning to learn from experience) malware identification techniques to try to identify infected files and prevent viruses from spreading. Typically the software is configured to run automatically when a user or system process accesses a file. The anti-virus software scans the file and blocks access if it detects anything suspicious. The user can then decide either to try to **disinfect** the file, **quarantine** it (block further access), or **delete** it.

The A-V scanner runs at boot-time to prevent boot sector viruses from infecting the computer. Most types of software can scan system memory (to detect worms), email file attachments, removable drives, and network drives.

The latest anti-virus software usually includes anti-Trojan software, as well as spam, adware, and spyware blockers.

The screenshot shows the Symantec Endpoint Protection Manager Console interface. The left sidebar has icons for Home, Monitors, Reports, Policies, Clients, and Admin. The main area has several sections:

- Security Status:** Shows a red 'X' icon and the message "Security Status - Attention Needed". Below is a table of Action Summary by Detection Count:

Action	Viruses	Security Risks
Cleaned	0	0
Suspicious	0	0
Blocked	0	0
Quarantined	0	0
Deleted	0	0
Newly Infected	0	0
Still Infected	0	0
- Risks Per Hour: Last 12 Hours:** A chart showing risks over time, currently at 0.
- Status Summary:** Shows the number of computers affected by various issues:

	Computers
Antivirus Engine Off	0
Auto-Protect Off	0
Tamper Protection Off	0
Restart Required	0
Host Integrity Failed	0
- Virus Definitions Distribution:** Shows the latest Symantec Version (2008-08-05 rev. 037) and Manager Version (2008-08-05 rev. 037). It also displays a table of definitions and computers:

Definitions	Computers
2008-08-05 rev. 037	6
- Security Response:** Shows the latest outbreak change (04/04/2007 01:06:00) and lists top threats and latest threats, both currently empty.
- Watched Applications Summary:** Shows occurrences of commercial application detection and forced TruScan Proactive Threat Detection, both at 0.
- Favorite Reports:** Includes links to Top Sources of Attack and Top Risk Detections Correlation.

Symantec Endpoint Protection Manager enables centralized monitoring and oversight of anti-virus, anti-spyware, firewall, and application/device control

Anti-virus (or anti-malware) software tends to come as either personal security suites, designed to protect a single host, or network security suites, designed to be centrally managed from a server console. Most anti-virus software is designed for Windows PCs and networks, as these are the systems that have been most affected by viruses and worms. Malware can be designed to attack any sort of OS however and it is increasingly likely that the major vendors develop versions of their scanners for Linux and Mac OS X.

Some of the major vendors are Symantec (including the Norton brand), McAfee, Computer Associates (CA), Trend Micro, Kaspersky, and BitDefender.



A-V Resistance

Some viruses have mechanisms to try to defeat anti-virus software. Some examples of these strategies are:

- **Stealth** - the virus intercepts commands from anti-virus software and passes the software a clean version of the file; alternatively the virus may "jump" from file-to-file ahead of the virus scanner.
- **Modification** - anti-virus software mostly works by identifying known virus patterns (signatures). A **polymorphic** virus attempts to defeat this approach by changing itself (for example, by encrypting the virus code). A **metamorphic** virus completely re-compiles itself to infect new files.
- **Armor** - the virus code is protected, making it difficult for anti-virus software to analyze it. One technique is to obfuscate the virus code by putting unnecessary or misleading routines in it to make it hard to analyze and identify the virus' true structure and purpose.
- **Retrovirus** - the virus seeks to disable the anti-virus software.
- **Slow and sparse** infectors - these attempt to stay "under the radar" by replicating slowly.

The best anti-virus software contains routines to defeat these techniques.

Anti-spyware Software

Security software to control spyware is built into anti-virus software suites. One of the difficulties is in distinguishing between adware (that the user may accept) and spyware. Running spyware scanners may identify legitimate software as spyware and disable it, if not used carefully.



In the early days of spyware and adware threats, a number of tools dedicated to identifying those specific threats were developed. These include HijackThis, Spybot S&D, and Microsoft's Windows Defender.

Anti-spam Software

Most email software comes with built-in spam (or junk mail) filters. These filters need to be kept up-to-date in order to protect against the latest spamming techniques. If the filter tags a message as spam, it posts it to a "Junk" email folder and no notification is displayed to the user. The user can inspect the junk folder manually to retrieve any legitimate messages that have been blocked by accident (false positives).

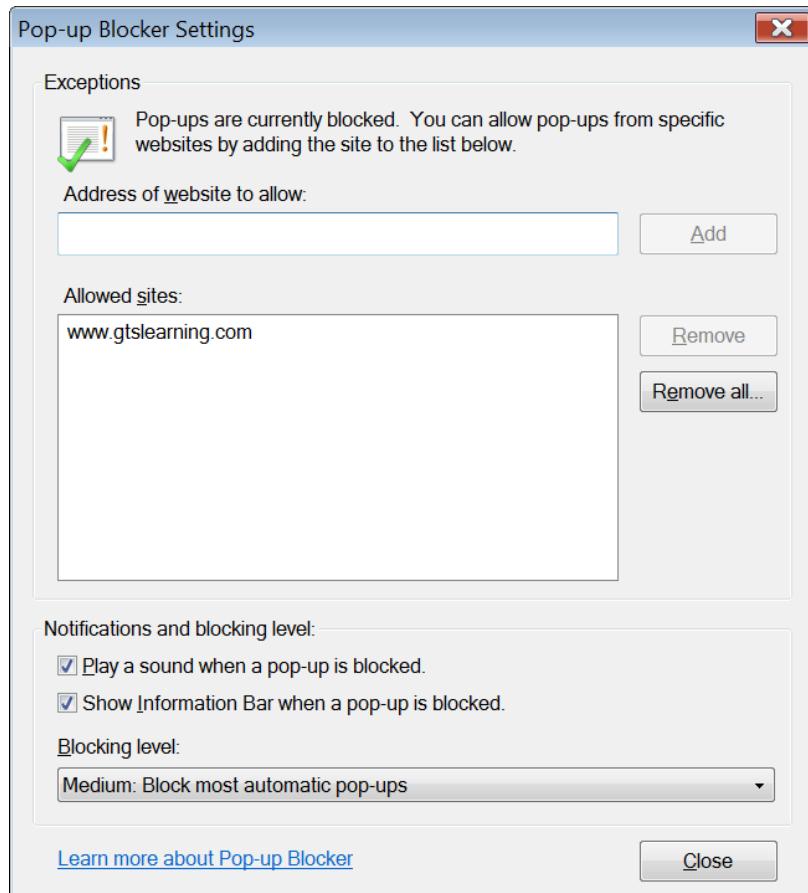
As well as detecting spam automatically, these tools allow the user to blacklist known spammer domains or to whitelist known safe senders.



Host-based spam filters are fine for home users but enterprise networks will usually deploy a mail gateway to filter spam before it reaches the company's internal mail servers. See [Unit 3.2](#) for more information about gateways and proxies.

Pop-up Blockers

A **pop-up** is a window that opens on top of the current browsing window. Pop-ups used for advertising often "spawn" automatically using JavaScript. Pop-ups can also be implemented using Flash. While there may be some legitimate uses of pop-ups (to display help with a login form for instance), they are more typically associated with unwanted and aggressive advertising. Most browsers now have functions to restrict the use of JavaScript pop-ups to approved sites; some can also restrict Flash pop-ups.



Removing Malware

If a computer is infected by a virus, follow the directions in your anti-virus program for cleaning (or **disinfecting**) it. If you cannot clean a file, and have a backup copy, use it to restore the file. Check the files you restore to make sure that your backups are not infected. For assistance, check the website and support services for your anti-virus software. In some cases, you may have to follow a further procedure to remove the virus or Trojan Horse (such as booting into Safe Mode or Recovery Console).

The screenshot shows the Symantec Security Response portal. At the top, there's a navigation bar with links for Norton, Business, Partners, Store, About Symantec, Overview, Solutions, Products, Services, Training, Support, Security Response (which is highlighted in yellow), Resources, and Store. Below the navigation is a breadcrumb trail: Symantec.com > Business > Security Response. A sub-header "Security Response" is followed by a brief description: "Security Response provides your Enterprise with world-class analysis and protection from viruses, blended threats, security risks and vulnerabilities".

On the left, there are two tables: "Latest Threats & Risks" and "Vulnerabilities".

Latest Threats & Risks:

Severity	Name	Detected	Protected*
	Trojan.Ushedixinf	06/28/2008	06/28/2008
	Trojan.Ushedix	06/28/2008	06/28/2008
	Joke.Blueod		06/27/2008
	Trojan.Blueod	06/27/2008	06/27/2008

Vulnerabilities:

Name	Detected
Microsoft DirectX SAMI File Parsing Stack Buffer Overfl...	June 10, 2008
Microsoft Internet Explorer HTML Objects' substringData...	June 10, 2008

To the right, there's a "ThreatCon" section with a "LEVEL 1: NORMAL" indicator. It says "Level 1 since 06/30/08 00:00 GMT" and lists several detected threats: Trojan.Ushedix, Trojan.Ushedix.inf, Trojan.Blueod, Packed.Generic.155, Packed.Generic.159, and Packed.Generic.160.

At the bottom of the portal interface, a note reads: "Symantec's Security Response portal showing current threat status, recent viruses and vulnerabilities, and search options for the malware database".

Anti-virus software will not necessarily be able to recover data from infected files. Also, if a virus does disrupt the computer system, you might not be able to run anti-virus software anyway and would have to perform a complete system restore.



A zero-day virus (or exploit) is one that is triggered on the same day that it is discovered (that is, anti-virus software or application patches cannot protect against it because it is unknown).

Removing Trojans and Rootkits

Anti-virus software may have routines for removing Trojans and rootkits, but the most secure way is to remove the computer from the network, re-partition and re-format the drives, then reinstall the OS, applications, and data from backup (provided you have a backup that was made before the installation of the rootkit).

It is also important to configure a firewall on the network to block outgoing communications. This makes it more difficult for the backdoor application to send data back to the attacker.



Review Questions / Module 1 / Unit 2 / Threats and Attacks

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What is a lunchtime attack?
- 2) When considering non-accidental threats, what important distinctions can be made to identify different threat sources?
- 3) Apart from natural disaster, what type of events threaten physical damage to assets?
- 4) What distinguishes a rootkit from other types of Trojan?
- 5) True or false? All backdoors are created by malware such as rootkits.
- 6) What techniques does anti-virus software use to identify threats?
- 7) What techniques do viruses use to avoid detection by anti-virus software?
- 8) How do social engineering attacks succeed?
- 9) Is the goal of social engineering to gain access to premises or a computer system?
- 10) What is shoulder surfing?



If you have access to the Hands On Live Labs, complete the "Threats / Trojans and Malware Protection" and "Application Data / Establish Host Security" labs now.

Module 1 / Unit 3

Network Attacks

Objectives

On completion of this unit, you will be able to:

- Understand the relevance of the OSI model to network technologies and protocols.
- Describe the function of network sniffers and protocol analyzers.
- Describe procedures and products used to survey and test security systems.
- Describe network attacks, such as scanning, spoofing, Man-in-the-Middle, replay, and Denial of Service.

Network Fundamentals



rjoha

Many of the network, transport, and application protocols in use on private networks and the internet were designed without any regard for security. Protocols such as HTTP, FTP, and SMTP are vulnerable to packet sniffing because they were designed to transmit information in plain text, making it simple to identify passwords and other confidential data. Devices communicating using these protocols do not typically authenticate with one another, making them vulnerable to spoofing.

In most cases, particular problems have been patched, either by a new version of the protocol or by inventing a workaround. The alternative is to deploy completely re-engineered protocols, such as IPv6. However, gaining acceptance for such transitions on a public network such as the internet is extremely difficult.

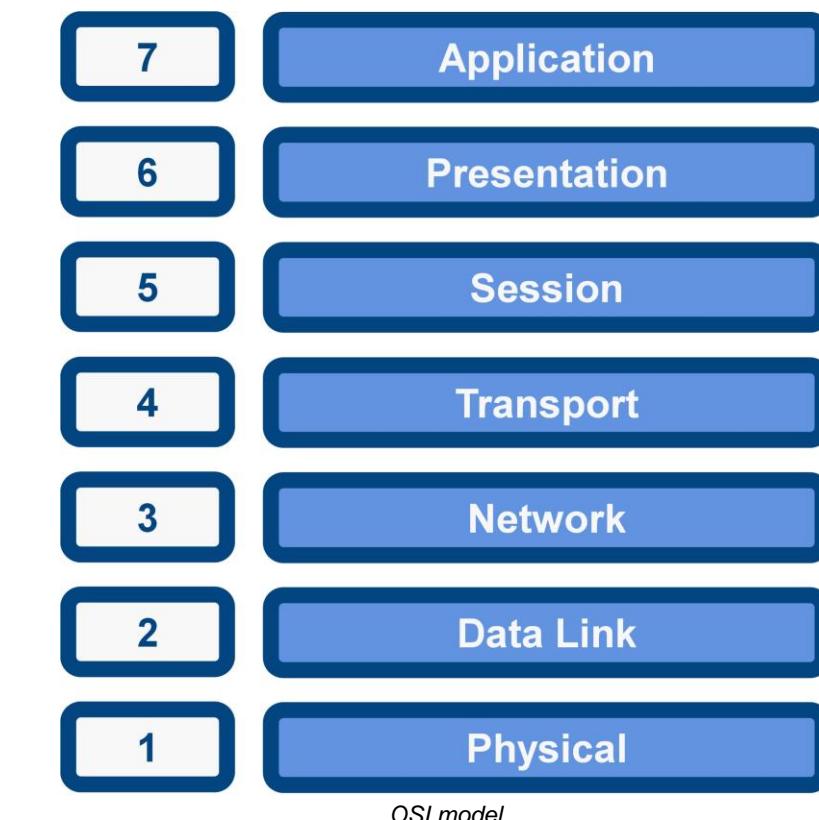
The OSI Model

In order to understand how attacks can be launched against networks, you must have a good understanding of network topology, protocols, and devices. This section provides a brief summary of the key information.



You should be familiar with this information already. If you are uncertain, please refer to the CompTIA Network+ Support Skills training course.

The **International Organization for Standardization (ISO)** developed the **Open Systems Interconnection (OSI)** reference model in 1977. It was designed to aid understanding of how a network system functions in terms of both the hardware and software components.



Although a theoretical rather than a practical tool, the OSI model has proved invaluable in designing, constructing, and understanding networks. It has increased network interoperability by providing a general model for protocol and specification design.

As the complexity of computer hardware and software increases, the problem of successfully communicating between these systems becomes more difficult. Dividing these difficult problems into "sub-tasks" allows them to be readily understood and solved more easily. Using this layered approach means that a vendor can work on the design and debugging for a particular layer without affecting any of the others.

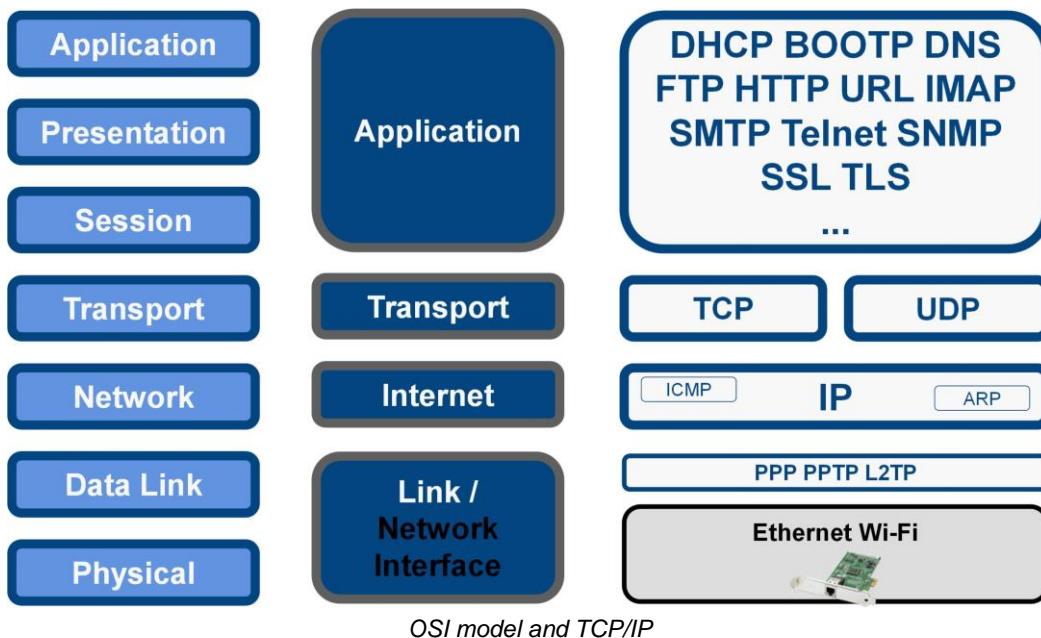
Each layer performs a different group of tasks required for network communication. Although not all network systems implement layers using this *structure*, they all implement each *task* in some way. The OSI model serves as a functional guideline for network communication and it does not specify any standard. The model is also useful in terms of analyzing the security properties of network protocols and devices.

TCP/IP Protocol Suite

Of even more interest than the OSI model in terms of practical networking, the TCP/IP protocol maps to a four-layer conceptual model: Application, Transport, Internet, and Link (or Network Interface). This model is referred to as the **Internet Protocol Suite** or the **ARPA model** or **DoD model** (after the US Department of Defense, which sponsored development of TCP/IP). As shown below, each layer in the Internet Protocol Suite corresponds to one or more layers of the OSI model.

Link Layer / Network Interface

The **link** (or **network interface**) layer is the equivalent of the OSI physical and data link layers as it defines the host's connection to the network. This layer comprises the hardware and software involved in the interchange of frames between computers. The technologies used can be LAN-based (Ethernet), WAN-based (T-carrier, ISDN, or DSL for instance), or wireless (Wi-Fi).



Internet Layer

The **internet** (or more precisely **internetwork**) layer provides addressing and routing functions. It uses a number of protocols (notably the **Internet Protocol [IP]** and **Address Resolution Protocol [ARP]**) to ensure the delivery of packets.

Transport Layer

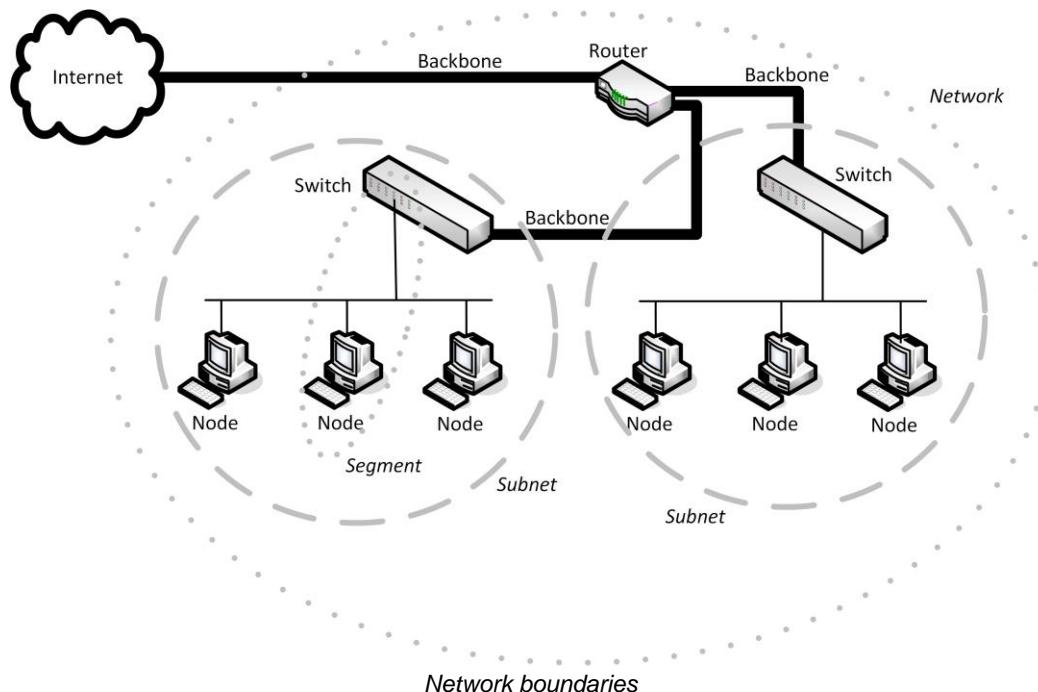
The **transport** layer provides communication between the source and destination computers and breaks application layer information into segments. TCP/IP provides two methods of data delivery:

- Connection-oriented delivery using the Transport Control Protocol (TCP).
- Connectionless delivery using the User Datagram Protocol (UDP).

Application Layer

This is the layer at which most TCP/IP services (high level protocols such as FTP, HTTP and SMTP) are implemented. UNIX-like applications interface with the TCP/IP application protocols using an Application Programming Interface (API) called **Berkeley Socket Interface**. A similar (but not identical) version of this was created for Windows and is generally referred to as **Winsock**. These interfaces allow programmers to call functions of TCP/IP application protocols in software applications such as a web browser or FTP client.

Network Boundaries



The graphic above illustrates typical network boundaries and the network devices used to implement them. The whole network is connected to the wider internet via a **router**. The router is also used to divide the network into two **subnets** (addressing at layer 3 of the OSI model or the IP layer of the DoD model). Devices within a subnet are all in the same **broadcast domain**.

Within each subnet, a **switch** is used to allow **nodes** to communicate with one another and (through the router) the other subnet and the internet. The link between each node and the switch is a **segment** (collision domain). High bandwidth **backbone segments** are used between the router and the internet and the router and the two switches.

While attacks at the Physical (PHY) layer are possible (eavesdropping on cable or wireless transmissions or cutting a cable to perform a DoS attack for instance), protocols and attacks against them start operating at the Data Link layer. Any attack at layer 2 usually requires physical access to the network. In the graphic above for instance the attacker would need to use a computer connected to the switch.



See [Unit 5.1](#) for more information about site and physical security procedures.



Sniffers and Protocol Analyzers

In order to craft successful attacks on a network, an attacker must learn as much as possible about it. One of the most important tools in network security (for attack and defense) is a **protocol analyzer**. This is the tool that facilitates **eavesdropping**.

Sniffer

A **sniffer** is a tool that captures frames moving over the network medium. This might be a cabled or wireless network.



Often the terms sniffer and protocol analyzer are used interchangeably.

A simple software-based sniffer will simply interrogate the frames received by the network adapter by installing a special driver. Examples include **libpcap** (for UNIX and Linux) and its Windows version **winpcap**. These software libraries allow the frames to be read from the network stack and saved to a file on disk. Most also support capture filters to reduce the amount of data captured. A hardware sniffer might be capable of tapping the actual network media in some way or be connected to a switch port. Also, a hardware sniffer might be required to capture at wirespeed on 1+ Gbps links. A workstation with basic sniffer software may drop large numbers of frames under heavy loads.

Promiscuous Mode and Sniffing Switched Ethernet

By default, a network card only receives frames that are directed to that card (unicast or multicast traffic) or broadcast messages. Most sniffers can make a network adapter work in **promiscuous mode**, so that it receives all traffic within the Ethernet broadcast domain, whether it is intended for the host machine or not.

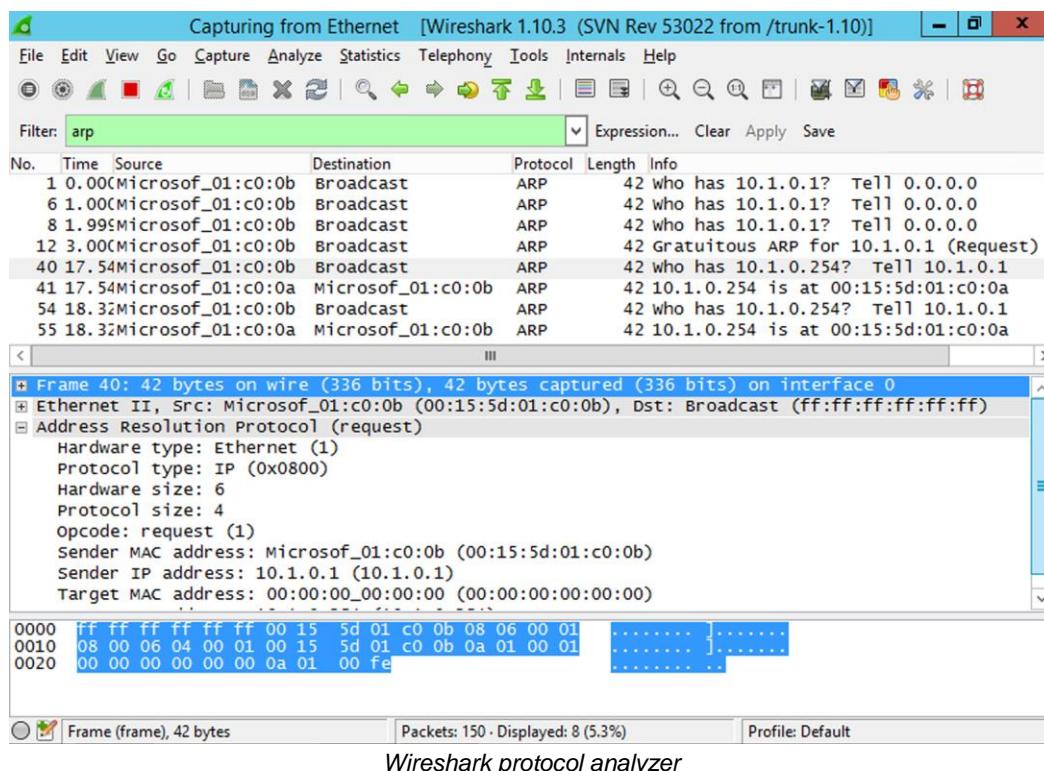
While this approach works for hosts connected via a hub, hubs are almost completely obsolete. On a switched network, the switch makes decisions about which port to forward traffic to, based on the destination address and what it knows about the hosts connected to each port. To sniff all traffic on a switched network, the switch must be overcome using an arp poisoning attack (see below) or similar. Most switches also support **port mirroring**. This allows traffic on one or more standard ports to be duplicated to a designated port. This allows legitimate traffic sniffing applications to monitor network traffic.

Protocol Analyzer

A **protocol analyzer** (or **network analyzer**) works in conjunction with a sniffer to perform traffic analysis. Protocol analyzers can decode a captured frame to reveal its contents in a readable format. You can choose to view a summary of the frame or choose a more detailed view that provides information on the OSI layer, protocol, function, and data.

Examples of packet capture software include:

- Wireshark - network analysis for all the major OS platforms.
- Microsoft Network Monitor - packet capture and analysis on wired and wireless LANs.
- Kismet - Linux-based packet sniffer for WLANs.
- tcpdump - command-line packet capture for UNIX / Linux platforms.
- Dsniff - suite of UNIX / Linux tools for packet capture and penetration testing.
- Ettercap - suite of tools for packet capture and spoofing available for all the major OS platforms.



Another function of some protocol analyzers is network monitoring. This involves reporting performance-related information, such as throughput and the most active hosts and protocols.

Packet Injection

Some attacks depend on sending forged or spoofed network traffic. Often network sniffing software libraries also allow frames to be inserted (or injected) into the network stream. There are also tools that allow for different kinds of packets to be crafted and manipulated. Well-known tools used for packet injection include Dsniff ([gtsgo.to/wizjk](#)), Ettercap ([gtsgo.to/a5gmm](#)), hping ([gtsgo.to/eqc28](#)), Nemesis ([gtsgo.to/l4lxr](#)) and Scapy ([gtsgo.to/by3in](#)).

Preventing Eavesdropping

Eavesdropping requires physical access to the network and the ability to run the protocol analyzer software. This means that in order to prevent eavesdropping you need to control the use of this kind of software by making sure that it is only installed and used by authorized users. You also need to prevent the unauthorized attachment of devices. This is typically achieved by configuring some sort of switch port security.

You can also mitigate eavesdropping by ensuring that the network traffic (or at least confidential information passing over the network) is encrypted.



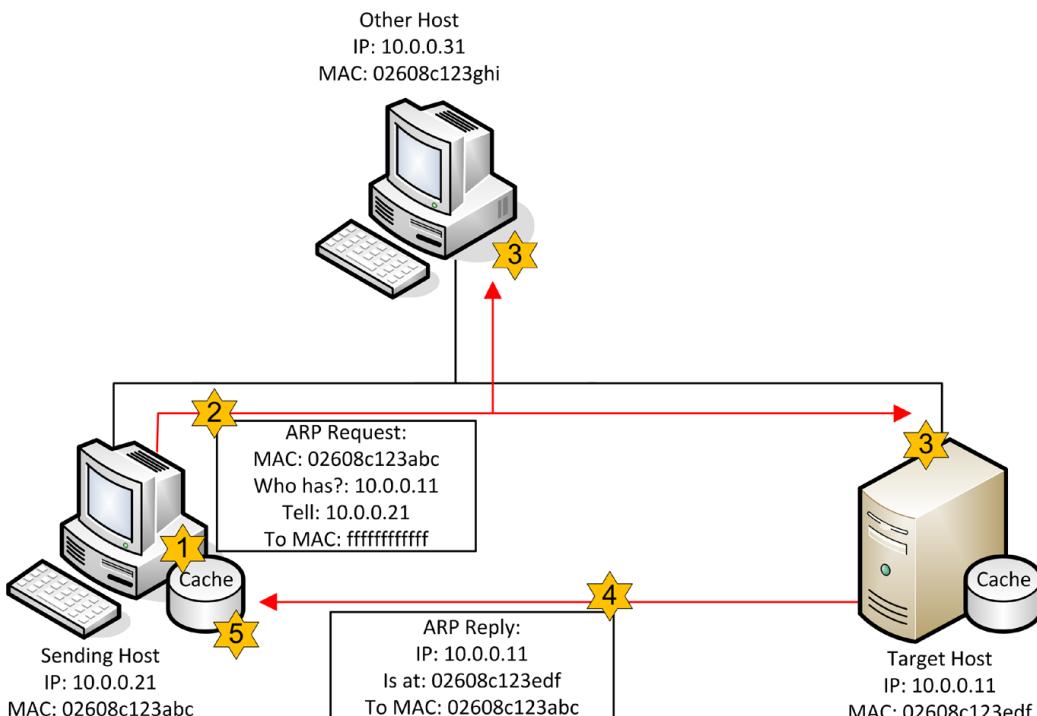
Sniffers are also available to eavesdrop on wireless networks. You cannot realistically prevent these from being used so the only option is to encrypt. See [Unit 4.3](#) for more information on transport encryption.



ARP Attacks

In terms of TCP/IPv4, the most significant protocol operating at the Data Link layer is the **Address Resolution Protocol (ARP)**.

ARP maps a network interface's hardware (MAC) address to an IP address. Normally, a device that needs to send a packet to an IP address but does not know the receiving device's MAC address broadcasts an **ARP Request** packet and the receiving device responds with an **ARP Reply**.



ARP in action - an ARP broadcast is used when there is no MAC:IP mapping in the cache and is received by all hosts on the same network but only the host with the requested IP should reply

ARP Poisoning

An **ARP spoofing** (or **poisoning**) attack works by broadcasting *unsolicited* ARP reply packets. Because ARP is an "antiquated protocol" with no security, the receiving devices trust this communication and update their MAC:IP address cache table with the spoofed address.

A trivial ARP poisoning attack could also be launched by adding static entries to the target's ARP cache. A more sophisticated attack can be launched by running software such as Dsniff, Cain and Abel, or Ettercap from a computer attached to the same switch as the target.



Obviously the attacker has to compromise the computer to do this. These tools would be recognized as malware by anti-virus software.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	ThomsonT_08:46:9a	Broadcast	ARP	who has 192.168.1.66?
2	0.000870	ThomsonT_08:46:9a	Broadcast	ARP	who has 192.168.1.64?
3	0.001845	ThomsonT_08:46:9a	Broadcast	ARP	who has 192.168.1.65?
4	0.001865	Intel_02:78:50	ThomsonT_08:46:9a	ARP	192.168.1.65 is at 00

Frame 4 (42 bytes on wire, 42 bytes captured)
 Ethernet II, Src: Intel_02:78:50 (00:19:d2:02:78:50), Dst: ThomsonT_08:46:9a (00:26:44:08:46:9a)
 Address Resolution Protocol (reply)
 Hardware type: Ethernet (0x0001)
 Protocol type: IP (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: reply (0x0002)
 [Is gratuitous: False]
 Sender MAC address: Intel_02:78:50 (00:19:d2:02:78:50)
 Sender IP address: 192.168.1.65 (192.168.1.65)
 Target MAC address: ThomsonT_08:46:9a (00:26:44:08:46:9a)
 Target IP address: 192.168.1.254 (192.168.1.254)

0000 00 26 44 08 46 9a 00 19 d2 02 78 50 08 06 00 01 .&D.F... .xp... 0010 08 00 06 04 00 02 00 19 d2 02 78 50 c0 a8 01 41xp...A 0020 00 26 44 08 46 9a c0 a8 01 fe .&D.F... ..
--

Ready to load or capture | Packets: 47 Displayed: 47 Marked: 0 Dropped: 0 | il : Default

Contents of an ARP reply frame showing fields in the frame header - this is a genuine ARP transaction but hacking software tools can rewrite information in these headers to spoof MAC addresses

The usual target will be the subnet's default gateway (the router that accesses other networks). If the attack is successful, all traffic destined for the remote network will be sent to the attacker. The attacker can perform a Man-in-the-Middle attack, either by monitoring the communications (forwarding them to the router to avoid detection) or modifying the packets before forwarding them. The attacker could also perform a Denial of Service attack (not forwarding the packets).

There are utilities that can detect ARP spoofing attacks. Another option is to use switches that can perform "port authentication", preventing connected devices from changing their MAC address.



[Unit 3.2](#) and [Unit 4.1](#) have more information on these network security techniques and countermeasures.

MAC Flooding

A variation of the attack (**MAC flooding**) can be directed against a switch. If a switch's cache table is overloaded by flooding it with frames containing different (usually random) source MAC addresses, it will typically start to operate as a hub (failopen mode). The alternative would be to deny network connections to any of the attached nodes. As hubs broadcast communications to all ports, this makes sniffing network traffic much easier.



The cache table is referred to as Content Addressable Memory (CAM) so the attack is also called CAM table overflow.

Replay and Man-in-the-Middle Attacks

A **spoofing** (or **masquerade**) attack involves the attacker imitating some sort of resource that the victim thinks is genuine.

Replay Attack



A **replay** attack involves the attacker capturing data packets that contain authentication data, such as usernames and passwords or cryptographic session keys. The attacker subsequently resends these packets to try to re-enable the session.

Replay attacks can be mitigated by time-stamping or sequencing data packets or authentication information.

Man-in-the-Middle Attack

A **Man-in-the-Middle (MitM)** attack is where the attacker sits between two communicating hosts, and transparently captures monitors, and relays all communication between the hosts. A MitM attack could also be used to covertly modify the traffic too.

One way to launch a MitM attack is to use Trojan software to replace some genuine software on the system. Man-in-the-Middle attacks can also be launched against antiquated protocols, such as ARP on a local network or DNS on the web. Another type of MitM attack attempts to subvert the digital certificates that are supposed to ensure confidentiality, integrity, and authentication on public networks (PKI).



Cryptography and PKI are covered in [Unit 2.1](#) and [Unit 2.2](#).

MitM attacks can be defeated using mutual authentication, where both server and client exchange secure credentials.



IP Spoofing

At layer 3, networks are connected by **routers**, so if you can communicate with a router you can (in theory) launch attacks against it and against the network (or subnet) it services. This could mean that the attacker is "inside" the network (on a computer connected to a local subnet) or "outside" it (attacking from the internet for instance).

The identifying headers in TCP/IP packets can quite easily be modified using software. In an IP spoofing attack, the attacker changes the source and/or destination address recorded in the IP packet. IP spoofing is done to disguise the real identity of the attacker's host machine. The technique is also used in most Denial of Service attacks to mask the origin of the attack and make it harder for the target system to block packets from the attacking system.

Contents of an IP datagram showing the headers - note the source and destination addresses are easily discovered (and just as easily changed with the right software tool)

Some examples of IP spoofing tools include Mendax, spoofit.h, ipspoof, Juggernaut, and hunt.

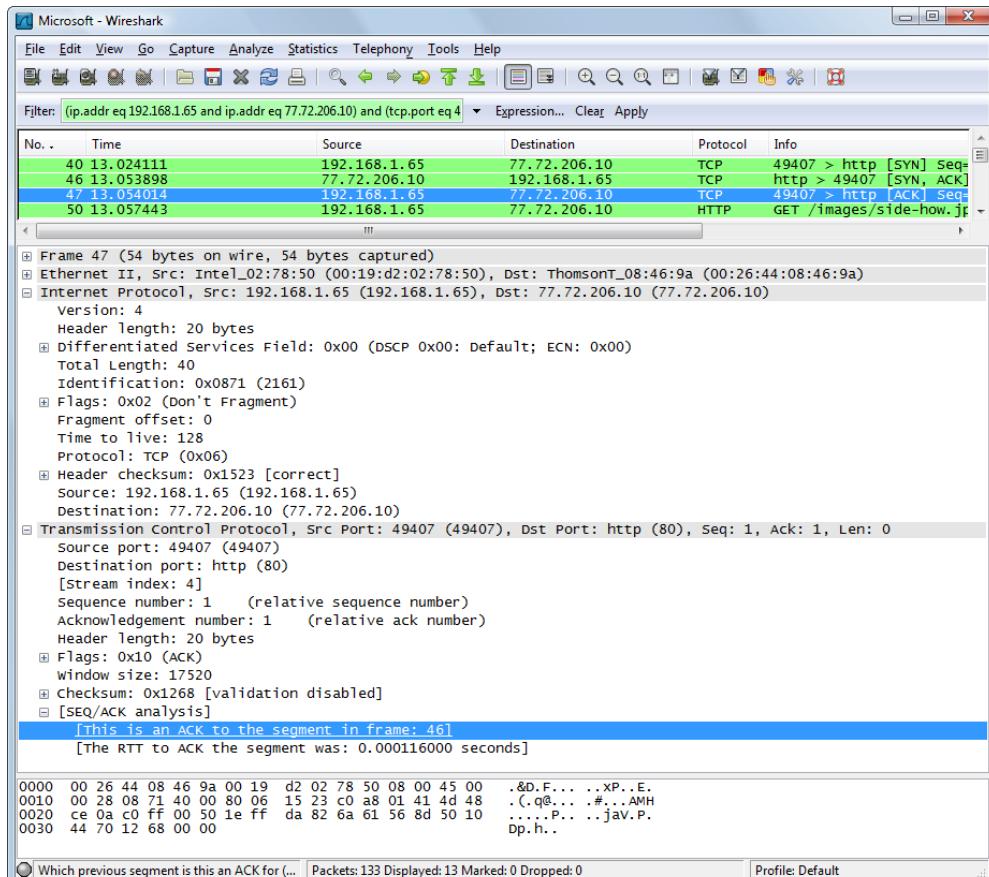
TCP/IP Hijacking

A more complex use of IP spoofing is to launch a type of Man-in-the-Middle attack, where the attacker intercepts and modifies the communications between two hosts.

The layer 3 protocol IP is connectionless, but at layer 4 (the transport layer) applications often work using multiple communications between client and server that must be processed in a particular order.

The **Transmission Control Protocol (TCP)** provides reliable, connection-oriented communications. It is the session protocol used by most TCP/IP applications. A session is established using a three-way handshake:

- 1) The client sends a SYN packet to the server.
- 2) The server responds with a SYN/ACK packet.
- 3) The client responds with an ACK packet.
- 4) The server opens a session with the client.



This frame capture shows the TCP handshake segments used to establish a request for web resources (HTTP session) - frame 40 is the client SYN, frame 46 is the server's SYN-ACK, and frame 47 (the contents of which are shown [note the sequence and acknowledgement numbers]) is the client ACK

When an application is using TCP (as most applications do), as well as spoofing the IP address, the attacker must take account of the sequence and acknowledgement numbers recorded in the TCP packets.

There are two means of doing this:

- Non-blind (or informed) spoofing - if the attacker is on the same subnet, s/he can sniff the sequence and acknowledgement numbers from a valid session and then construct packets that disrupt the existing session and subsequently re-establish it (hijacking). The victim host is fooled into believing it is still communicating with the original client.

Another non-blind spoofing technique is to make the attacker's computer a "Man-in-the-Middle" router. This could be accomplished by an ARP poisoning attack or some kind of attack on the routing protocol in use.

- Blind spoofing - the attacker must have some way of predicting the sequence and acknowledgement numbers used. To do this, they must have knowledge of the way the victim system crafts its TCP packets.



TCP/IP hijacking can be defeated by using communications encryption. See [Unit 3.4](#) and [Unit 4.3](#) for more information.

Hijacking UDP sessions is simpler. One example is attacking DNS queries (DNS often uses UDP). The attacker intercepts a DNS query from a client, performs some sort of DoS attack on the legitimate DNS server, and responds to the client with fake name resolution information.



ICMP Redirect

The **Internet Control Message Protocol (ICMP)** generates status and error messages for an IP link and can be invoked using IP diagnostic utilities, such as **ping** and **tracert**.

One of the functions built into ICMP is a **redirect message** (also called a Type 5 message). If the default router for a subnet wants a host to use an alternative router, it can send it a redirect message with the IP of an alternative router. The host then adds that route to its routing table and uses it for the duration that the route is cached.

As ICMP has no authentication mechanism, an attacker could spoof the default gateway's IP address and send ICMP redirects to a host to trick it into routing communications through the attacker's machine (Man in the Middle) or to an invalid IP (blackhole or Denial of Service).

You can disable processing of redirect messages by hosts (in Windows you edit a registry key to do this). You can also block ICMP traffic from external networks using a firewall. If you need other ICMP functions to work across subnets you could block Type 5 messages specifically.



A number of other ICMP-based DoS attacks are discussed later in this unit. Firewalls are discussed in [Unit 3.2](#).

Network Mappers and Port Scanners



As mentioned earlier, a successful attack often depends on gathering information about the target system first. An attacker might do this using social engineering methods - to gather staff names and possibly even passwords for instance - but there are also a number of scanning tools that can probe networks and computer systems to give the attacker a great deal of information about how they are configured.

In this context, the term **footprinting** is often used to describe an attack that tries to learn the configuration of a network (its topology, protocols, numbers of hosts, and its security systems for instance) while **fingerprinting** targets a specific host (a computer or router for instance).

Footprinting

Footprinting or **network mapping** means gathering information about the way the network is built and configured and the current status of hosts. The following information is all of use:

- Protocols, services, and applications running on the network.
- Host workstation and server OS types and patch status.
- Network addresses and host names.
- Network interconnect device types and status.
- Network security appliances and software.
- User accounts and groups (especially administrative / root accounts) and passwords.

This sort of information may legitimately be gathered by network management software, such as Microsoft's System Center products or HP's OpenView. Such suites can be provided with credentials to perform authorized scans and obtain detailed host information via management protocols such as the Simple Network Management Protocol (SNMP).

Host discovery can be performed by pinging a range of IP addresses (a **ping sweep**) or using ARP broadcasts. There are also tools such as Nmap that can perform the same sort of function stealthily or try to overcome barriers to host discovery, such as blocking ICMP requests at firewalls, by using non-standard ping commands. Such "dual use" tools can be used both to prove system security and attack it.

A network administrator needs to ensure that unauthorized ports are not open on the network. These could be a sign of some sort of Trojan or backdoor server. Such tools often try to hide themselves from diagnostic port scans however.



Fingerprinting

Fingerprinting or **port scanning** specifically aims to enumerate the TCP or UDP application ports that are "open" on a host. Any application or process that uses IP for its transport is assigned a unique identification number called a **port**. Valid port numbers range from 0 to 65,535. Port numbers for some server applications are pre-assigned by the **Internet Assigned Numbers Authority (IANA)** from the registered port range 0 - 49151. Numbers 0 through 1023 are described as "well-known" ports and are assigned to standard TCP/IP application protocols, such as DNS, HTTP, or SMTP.



An application server does not have to use the standard / default port. A custom port could be configured to try to obscure use of a particular protocol.

Ports outside the registered range are described as ephemeral or dynamic and are intended for use on server applications on private networks only or by clients. Clients dynamically assign a port for each new connection (the source port). For example, a client may contact an HTTP server on port 80 and receive replies from the server on source port 49152. For its next connection, it may specify source port 49153, and so on.

The following ports are commonly monitored by attackers:

#	TCP / UDP	Process	Description
20	TCP	ftp-data	File Transfer Protocol - Data
21	TCP	ftp	File Transfer Protocol - Control
22	TCP / UDP	ssh	Secure Shell (including Secure Copy [scp] and Secure FTP [sftp])
23	TCP / UDP	telnet	Telnet
25	TCP / UDP	smtp	Simple Mail Transfer Protocol
42	TCP / UDP	nameserver	Windows Internet Name Service
53	TCP / UDP	domain	Domain Name System
67	UDP	bootps	BOOTP / DHCP Server
68	UDP	bootpc	BOOTP / DHCP Client
69	UDP	tftp	Trivial FTP
80	TCP	http	HTTP
88	TCP	kerberos	Kerberos authentication protocol
110	TCP	pop3	Post Office Protocol version 3
115	TCP	sftp	Simple File Transfer Protocol
119	TCP	nntp	Network News Transfer Protocol
123	UDP	ntp	Network Time Protocol
135	TCP / UDP	epmap	Microsoft Remote Procedure Call (RPC)
137	UDP	netbios-ns	NetBIOS Name Service
138	UDP	netbios-dgm	NetBIOS Datagram Service
139	TCP	netbios-ssn	NetBIOS Session Service
143	TCP / UDP	imap4	Internet Mail Access Protocol
161	TCP / UDP	snmp	Simple Network Management Protocol
162	TCP / UDP	snmptrap	SNMP trap
179	TCP	bgp	Border Gateway Protocol
389	TCP / UDP	ldap	Lightweight Directory Access Protocol
443	TCP	https	HTTP Secure
445	TCP / UDP	smb	Microsoft File and Printer Sharing
515	TCP	printer	Line Printer Daemon
631	TCP / UDP	ipp	Internet Printing Protocol
989	TCP	ftps-data	FTP over SSL - Data
990	TCP	ftps	FTP over SSL - Control

Port Scanners and the Xmas Attack



The **netstat** tool can be used on Windows and Linux to investigate open connections on a local computer. Commonly-used remote port scanning tools include Nmap, Nessus, SuperScan, and Atelier Web Security Port Scanner. These identify which ports are "listening" and therefore which applications are running on the network's external interface.

```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\Nmap>nmap -A -T4 192.168.1.131
Starting Nmap 4.20 < http://insecure.org > at 2007-01-08 15:49 GMT Standard Time
Interesting ports on 192.168.1.131:
Not shown: 1677 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
25/tcp    open  smtp         Microsoft ESMTP 6.0.3790.0
53/tcp    open  domain       Microsoft DNS
80/tcp    open  http         Microsoft IIS webserver 6.0
88/tcp    open  kerberos-sec Microsoft Windows kerberos-sec
119/tcp   open  nntp         Microsoft NNTP Service 6.0.3790.0 <posting ok>
135/tcp   open  msrpc?      Microsoft RPC
139/tcp   open  netbios-ssn  Microsoft LDAP server
389/tcp   open  ldap         Microsoft Windows 2003 microsoft-ds
445/tcp   open  microsoft-ds Microsoft Windows 2003 microsoft-ds
464/tcp   open  kpasswd5?
563/tcp   open  snews?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1025/tcp  open  NFS-or-IIS?
1026/tcp  open  msrpc        Microsoft Windows RPC
1043/tcp  open  msrpc        Microsoft Windows RPC
```

Nmap port scanner output

These work by using different scanning techniques. Mostly, the software sends a packet with certain flags set to each port to find out whether the target system responds. The main ones are SYN, UDP, TCP Null, FIN, and ACK. The **Xmas Tree attack** (or just "Xmas attack") probes a router by setting the FIN, PUSH, and URG flags in a TCP packet all at once. As this packet is atypical, it is possible to identify the operating system running on the router from its response.



Firewalls and IDS are deployed to protect networks from eavesdropping, spoofing, and DoS attacks. See [Unit 3.2](#) for more information.

Another option is to try to establish a session (TCP Connect), but this is less stealthy. There is also the "Dumb Scan", where the scan is launched from a bot or zombie.



[insecure.org](#) (developer of nmap) is a good resource for further information.

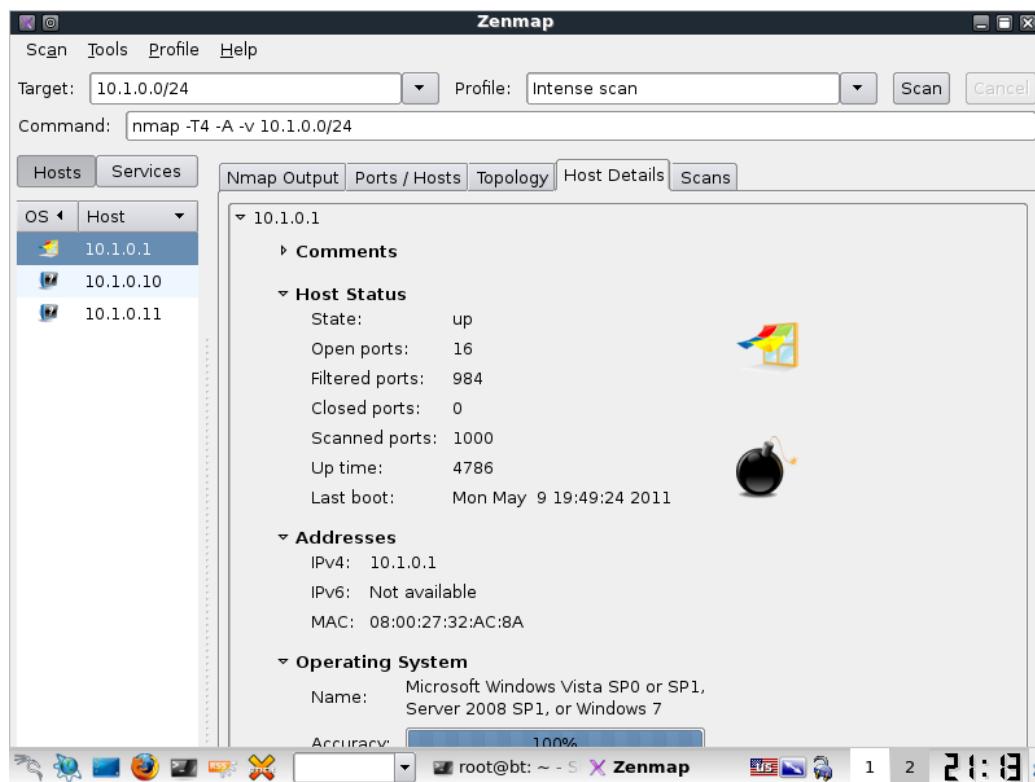
Related techniques, called "War Dialing" and "War Driving", look for unsecured modems or wireless access points. War dialer software, such as ToneLoc, can scan blocks of numbers looking for modem dial tones.

Banner Grabbing



As mentioned above, when a host running a particular operating system responds to a port scan, the syntax of the response might identify the specific operating system. This fact is also true of application servers, such as web servers, FTP servers, and mail servers. The responses these servers make often include several headers or banners that can reveal a great deal of information about the server.

Banner grabbing refers to probing a server to try to elicit any sort of response that will identify the server application and version number, or any other interesting detail about the way the server is configured. This information allows an attacker to identify whether the server is fully patched and to look up any known software vulnerabilities that might be exposed.



A tool such as Nmap can discover hosts connected to the network and report on their configuration



Vulnerability scanning tools are discussed in [Unit 1.4](#).



Client applications broadcast information in the same way. For example, a web browser will reveal its type and version number when connecting to a server.



5dhr8

Denial of Service Attacks

A **Denial of Service (DoS)** attack causes a service at a given host to fail or to become unavailable to legitimate users. Typically, DoS attacks focus on overloading a service. It is also possible for DoS attacks to exploit design failures or other vulnerabilities in application software. An example of a physical DoS attack would be cutting telephone lines or network cabling or switching off the power to a server. DoS attacks may simply be motivated by the malicious desire to cause trouble. They may also be part of a wider attack, such as precursor to a DNS spoofing attack.



Remember that it is crucial to understand the different motives attackers may have.

Most DoS attacks attempt to deny bandwidth to web servers connected to the internet. They focus on exploiting historical vulnerabilities in the TCP/IP protocol suite. TCP/IP was never designed for security; it assumes that all hosts and networks are trusted.

Other application attacks do not need to be based on consuming bandwidth or resources. Attacks can target known vulnerabilities in software to cause them to crash; worms and viruses can render systems unusable or choke network bandwidth.



5xu0c

Distributed DoS Attacks / Botnets

Most bandwidth-directed DoS attacks are **distributed**. This means that the attacks are launched from multiple, compromised computers (referred to as a **botnet**).

Typically an attacker will compromise one or two machines to use as "handlers" or "masters" or "herders". The handlers are used to compromise hundreds or thousands or millions of **zombie** (agent) PCs with DoS tools (**bots**) forming a **botnet**. To compromise a computer, the attacker must install a backdoor application that gives them access to the PC. They can then use the backdoor application to install DoS software and trigger the zombies to launch the attack at the same time.

Large botnets are necessary to overcome the high bandwidth of targets, which tend to be organizations with a large internet presence, such as government departments, Microsoft, banks, e-commerce sites, and so on. The increasing use of "always-on" broadband connections means that attackers can target a large base of naïve home users with the aim of compromising their PCs.

TCP-based DoS Attacks

A **SYN flood** attack subverts the TCP handshake process by withholding the client's ACK packet. Typically, the client's IP address is spoofed, meaning that a random IP is entered so the server's SYN/ACK packet is misdirected. A server can maintain a queue of pending connections. When it does not receive an ACK packet from the client, it resends the SYN/ACK packet a number of times before eventually giving up on the connection after a set timeout.

The problem is that a server may only be able to manage a limited number of pending connections, which the DoS attack quickly fills up. This means that the server is unable to respond to genuine traffic.

A more powerful TCP SYN flood attack is a type of **Distributed Reflection DoS (DRDoS)** or **amplification** attack. In this attack, the client spoofs the *victim's* IP address and attempts to open connections with multiple servers. Those servers direct their SYN/ACK responses to the *victim* server. This rapidly consumes the victim's available bandwidth.

UDP-based DoS Attacks

UDP provides unreliable, connectionless communications. An example of a DRDoS attack using UDP packets is the **Fraggle** attack, a different version of Smurf. In this attack, the attacker spoofs the victim's IP address and uses it to broadcast UDP packets aimed at obsolete diagnostic ports (echo, chargen, or discard).

Smurf Attack

ICMP provides status and error messaging for an IP link. ICMP messages can be spoofed for the purpose of redirecting traffic or preventing it from exiting a subnet. A number of other ICMP-based DoS attacks can be used to overwhelm servers.

In a **Smurf** attack, the client spoofs the *victim's* IP address and pings the broadcast address of a third-party network (one with many hosts; referred to as the "amplifying network"). Each host directs its echo responses to the *victim* server. This rapidly consumes the victim's available bandwidth.

A ping flood is a less sophisticated attack where an attacker tries to overwhelm the victim network's bandwidth by bombarding it with ICMP traffic.



Most network DoS threats are prevented by ensuring software is patched and by using firewalls and Intrusion Detection Software. These topics are covered in [Unit 3.2](#) and [Unit 4.1](#).



Review Questions / Module 1 / Unit 3 / Network Attacks

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) Is it possible to eavesdrop on the traffic passing over a company's internal network from the internet?
- 2) Why might an ARP poisoning tool be of use to an eavesdropper?
- 3) What type of tool(s) would be used in a footprinting attack?
- 4) Is it possible to discover what ports are open on a web server from another computer on the internet?
- 5) How does a replay attack work?
- 6) Why are most network DoS attacks distributed?
- 7) What can you use to mitigate ARP poisoning attacks?
- 8) What is a Fraggle attack?



If you have access to the Hands On Live Labs, complete the "Network Security / Protocol Analyzers" and "Threats / Network Vulnerabilities" labs now.

Module 1 / Unit 4

Assessment Tools and Techniques

Objectives

On completion of this unit, you will be able to:

- Describe and distinguish vulnerability assessments and penetration testing.
- Identify types and proper uses of vulnerability scanners and penetration testing tools.
- Describe the purpose of a honeypot or honeynet.

Vulnerability Assessments and Pentests

We saw earlier that a necessary part of attacking a network is to gather information about it. This technique can also be used by security professionals to probe and test their own security systems.

When information gathering is conducted by a "white hat", assessments are usually classed as either **vulnerability scanning** or **penetration testing**.



Vulnerability Scanning

Vulnerability scanning is the process of auditing a network (or application) for known vulnerabilities. Recall that a vulnerability is a weakness that could be triggered accidentally or exploited maliciously by a threat agent to cause a security breach. An unpatched software application, a host with no anti-virus software, and an administrator account with a weak password are examples of vulnerabilities.

Vulnerability scanning is likely to be a precursor to a more comprehensive **risk assessment**. A risk assessment considers the likelihood and impact of threat sources that could exploit vulnerabilities.



Risk assessments are covered in [Unit 5.3](#).

Vulnerability scanning generally uses **passive** techniques. A vulnerability scanner would probe the network or application to try to discover issues but would not attempt to exploit any vulnerabilities found.



3z6g6

Penetration Testing

A **penetration test (pentest)** or **ethical hacking** essentially involves thinking like an attacker and trying to *penetrate* the security systems that have been set up. A pentest might involve the following steps:

- **Verify a threat exists** - use surveillance, social engineering, network scanners, and vulnerability assessment tools to identify vulnerabilities that could be exploited.
- **Bypass security controls** - look for easy ways to attack the system. For example, if the network is strongly protected by a firewall, is it possible to gain access to a computer in the building and run malware from a USB stick?
- **Actively test security controls** - probe controls for configuration weaknesses and errors, such as weak passwords or software vulnerabilities.
- **Exploiting vulnerabilities** - prove that a vulnerability is high risk by exploiting it to gain access to data or install malware.

The key difference to passive vulnerability scanning is that an attempt is made to *actively test* security controls and *exploit* any vulnerabilities discovered. For example, a *vulnerability scan* may reveal that an SQL Server has not been patched to safeguard against a known exploit. A *penetration test* would attempt to use the exploit to perform code injection and compromise the server. This provides active testing of security controls; even though the exploit exists, the permissions on the server might prevent an attacker from using it.

Security Assessment Techniques

There are many models and frameworks for conducting vulnerability scans and penetration tests. A good starting point is NIST's **Technical Guide to Information Security Testing and Assessment (SP 800-115)**, available at gtsgo.to/f8sd8. SP 800-115 identifies three principal activities within an assessment:

- Testing the object under assessment to discover vulnerabilities or to prove the effectiveness of security controls.
- Examining assessment objects to understand the security system and identify any logical weaknesses. This might highlight a lack of security controls or a common misconfiguration.
- Interviewing personnel to gather information and probe attitudes towards and understanding of security.

The first step in planning an audit will be to determine the scope of the assessment and a methodology then put in place the resources to carry them out (qualified staff, tools, budget, and so on).

Scope

Vulnerability scans and penetration testing will generally be divided into three classes: those aimed at determining external threats, those aimed at identifying insider threats, and those aimed at application software development.

Assessing security controls against external threats will focus on perimeter security and protocols and applications (routing and remote access, DNS, firewalls, email, web services, and so on). Detecting vulnerabilities to insider threats may look more at access controls, administrative privileges, password security, host-based intrusion detection, operational procedures, auditing, and so on.

An application software vulnerability assessment will look at the way the application has been developed and implemented.



Vulnerabilities in software applications (notably web applications) are covered in [Unit 4.4](#).

Establishing a Methodology

It is often helpful to use third-parties to perform vulnerability scans and / or pentests, or at least, for assessments to be performed by people other than those who set up the security system. This is the best means of identifying vulnerabilities that may have been overlooked by the security team.

The drawback of using a third-party is the level of trust that must be invested in them; the drawback of using internal staff is that they might not possess the knowledge and skills typical of criminal hackers. The EC-Council Certified Ethical Hacker certification (gtsgo.to/vhz3p) has been designed to demonstrate ability and experience in this subject area.

Regardless of the consultant's background, when commissioning third-party security surveys, it is vital to establish the ground rules. These should be made explicit in a contractual agreement and backed by senior management.



These guidelines also apply to assessments performed by employees.

Some things to consider are:

- Use "No holds barred" testing - the consultant will try to use any means to penetrate as far into the network and information systems as possible.
- Use perimeter testing - having demonstrated that a vulnerability exists, the consultant will stop and not attempt to exploit the breach or view confidential data.

- Attack profile - attacks come from different sources and motivations. You may wish to test both resistance to external (targeted and untargeted) and insider threats. You need to determine how much information about the network to provide to the consultant:
 - Black Box (or blind) - the consultant is given no privileged information about the network and its security systems.
 - White Box (or full disclosure) - the consultant is given complete access to information about the network.
 - Gray Box - the consultant is given some information; typically, this would resemble the knowledge of junior or non-IT staff to model particular types of insider threat.



This terminology is also used to discuss vulnerability testing of specific applications. In this context, white box means testing with knowledge of and access to precompiled source code while black box means testing against the compiled executable and gray box is a combination of methods.

- Test system or production environment - ideally, tests would be performed in a test environment that accurately simulates the production environment. However, this is expensive to set up. Using the production environment risks service outages and data loss, especially with the "no holds barred" approach.

Both vulnerability assessments and penetration testing can be disruptive to a network. Most types of scanning software generate a large amount of network traffic and perform "port enumeration" against devices such as servers and routers. This can overload the network and cause devices to crash. Penetration testing can self-evidently crash a network and may even damage data, if performed carelessly.

- Out of hours - whether the consultant should only perform testing out of hours to avoid causing problems on a production network. The problem here is that network policies and intrusion detection systems are generally configured to view out of hours access as suspicious, so the penetration testing is not taking place in the network's "real world" state.
- Informing staff - should the survey be performed with or without the knowledge of staff? If the former, there is no opportunity to assess their response; if the latter, there is considerable scope for generating alarm and bad feeling.



A test where the attacker has no knowledge of the system but where staff are informed that a test will take place is referred to as a blind (or single blind) test. A test where staff are not made aware that a pentest will take place is referred to as a double blind test.

- Informing outside agencies - suppliers (such as ISP or telecoms), partners, and agencies (such as the police) may need to be informed. This is particularly important if the test will involve connectivity devices such as routers that are owned by a third-party (an ISP-managed router for instance).
- Full disclosure of test results to the company in a timely manner.
- Confidentiality and non-disclosure (to third-parties) by the consultant.

Vulnerability Scanners



Numerous tools are available to facilitate vulnerability scanning and penetration testing. Footprinting and fingerprinting tools (and to some extent tools that facilitate attacks such as spoofing and password cracking) are of the "dual-use" kind that make them useful to both attackers and defenders.



sectools.org is a useful resource for researching the different types and uses of security assessment tools.

A **vulnerability scanner** is a type of network mapper that aims to detect whether the network is exposed to any threats. To that end, as well as mapping the network for hosts and detecting running services, they use techniques such as banner grabbing to scan for things such as patch level, security configuration and policies, network shares, unused accounts, weak passwords, rogue access points and servers, anti-virus configuration, and so on. This provides **passive testing of security controls**; ideally such scans should be blocked.

OpenVAS-Client

Report for scope: SERVERx (Task: classroom)

Comments Options Report

Name

- Global Settings
- classroom
 - REPORT 20110509-22
- SERVERx

Host/Port/Severity

Reported by NVT "Using NetBIOS to retrieve information from the host"

The following 5 NetBIOS names have been gathered :

- SERVER1 = This is the computer name registered for this host
- CLASSROOM1 = Workgroup / Domain name
- CLASSROOM1 = Workgroup / Domain name (Domain Controller)
- SERVER1 = Computer name
- CLASSROOM1

The remote host has the following MAC address on its adapter 08:00:27:32:ac:8a

If you do not want to allow everyone to find the NetBIOS name of your computer, you should filter incoming traffic to this port.

Risk factor : Medium
CVE : CAN-1999-0621

Scan took place from Mon May 9 22:34:34 2011 to Mon May 9 22:41:36 2011

Message log

New code since OpenVAS-Client: Copyright 2007, 2008, 2009 Greenbone Networks GmbH

root@bt: ~ - S X OpenVAS-Client 1 2 22:43

The tool then compiles a report and classifies each **identified vulnerability** with an impact warning. Each scanner is configured with a database of known vulnerabilities. Most tools also suggest current and ongoing remediation techniques.

A scanner can be implemented purely as software or as a security appliance, connected to the network. One of the best known software scanners is **Tenable Nessus**. As a previously open source program, Nessus also provides the source code for many other scanners. Some other products include SAINT, eEye Retina, and Rapid7 NeXpose.

Another class of scanner aims to identify **web application** vulnerabilities specifically. Tools such as Nikto look for known software exploits, such as SQL injection and XSS, and may also analyze source code and database security to detect insecure programming practices.



Web application security is covered in detail in [Unit 4.4](#).

As with anti-malware software, a vulnerability scanner needs to be kept up-to-date with information about known vulnerabilities.

Intrusive versus Non-intrusive Scanning

Many vulnerability scanners will support a range of different scanning techniques. You can choose which type of scans to perform for any given test. The main distinction between scan types is between **intrusive** and **non-intrusive** test routines.

A non-intrusive (or non-invasive) scanning technique, such as banner grabbing, will not normally cause performance problems in the server or host being scanned.



While non-intrusive scans do not aim to disrupt a host, the scans can still take up network bandwidth and resources on the network servers. Scans could also cause routers or servers to crash.

Intrusive or invasive scanning techniques usually involve an attempt to exploit detected vulnerabilities. This reduces **false positives** (reporting a vulnerability that does not actually exist) and makes it easier to verify a threat exists (that is, is the vulnerability truly exploitable by a threat agent?).

You should also be alert to the possibility of **false negatives**; that is potential vulnerabilities that are not identified in the scan. This risk can be mitigated somewhat by running repeat scans periodically and by using more than one vendor's scanner.

Also, because intrusive techniques depend on pre-compiled scripts, they do not reproduce the success that a skilled and determined hacker might be capable of and can therefore create a false sense of security. Using disruptive tests is also hugely problematic on a production network.

Credentialed versus Non-credentialed Scanning

A **non-credentialed scan** is one that proceeds without being able to log on to a host. Consequently, the only view obtained is the one that the host exposes to the network. These are often also referred to as remote scans. The test routines may be able to include things such as using default passwords for service accounts and device management interfaces but they are not given any sort of privileged access.

A **credentialed scan** is given a user account with log on rights to various hosts plus whatever other permissions are appropriate for the testing routines. This sort of test allows much more in-depth analysis, especially in detecting when applications or security settings may be misconfigured. It also demonstrates what an insider attack or one where the attacker has compromised a user account may be able to achieve.



Bear in mind that the ability to run a vulnerability test with administrative credentials is itself a security risk.

Identifying Lack of Controls and Misconfigurations

As well as matching known software exploits to the versions of software found running on a network, a vulnerability scan or pentest would also look at the configuration of security controls and application settings and permissions. It might try to identify whether there is a lack of controls that might be considered necessary or whether there is any misconfiguration of the system that would make the controls less effective or ineffective, such as anti-virus software not being updated or management passwords left configured to the default for instance.

Generally speaking this sort of testing requires a credentialed scan. It also requires specific information about best practices in configuring the particular application or security control.

As an illustration, there are also a couple of tools included with Windows or available for download to help to secure the system:

- The **Security Configuration and Analysis** snap-in allows the administrator to compare the configuration of a Windows client or server computer against a predefined template (baseline). Microsoft includes a number of predefined templates in the Security Templates snap-in. The **secedit** tool provides the same sort of functionality at the command line.
- The **Microsoft Baseline Security Analyzer** tool (gtsgo.to/rt2t1) assists administrators in analyzing the security configuration of Windows networks.
- **Microsoft Security Assessment Tool (MSAT)** is a best practice tool designed to assist the risk assessment process (gtsgo.to/7xfmg).

The screenshot shows the Microsoft Baseline Security Analyzer 2 interface. On the left, there's a navigation pane with links like 'Welcome', 'Pick a computer to scan', 'Pick multiple computers to scan', 'Pick a security report to view', and 'View a security report' (which is selected). Below that is a 'See Also' section with links to 'Microsoft Baseline Security Analyzer Help', 'About Microsoft Baseline Security Analyzer', and 'Microsoft Security Web site'. Under 'Actions', there's a 'Print' button. The main area is titled 'View security report' and shows 'Sort Order: Score (worst first)'. It displays 'Security Update Scan Results' with two items:

Score	Issue	Result
X	Windows Security Updates	78 security updates are missing. 3 service packs or update rollups are missing. What was scanned Result details How to correct this
X	Scanning Requirements	1 scanning requirements are missing. A complete scan could not be performed. What was scanned Result details How to correct this

Below this is a 'Windows Scan Results' section. At the bottom, there are buttons for 'Previous security report' and 'Next security report'. A message box at the bottom right says: 'A new version of MBSA is available! Click [here](#) to go to the download page'.

Microsoft Baseline Security Analyzer

- The **Microsoft Security Compliance Manager** details best practice for hardening client server operating systems and ensuring policy compliance on enterprise networks (gtsgo.to/k74yu).

Interpreting Scan Results

It would be a mistake to rely too heavily on the generic risk assessment made by any one tool. For example, a tool may discover a number of separate low risk vulnerabilities; it may not be appropriate to assume that the system as a whole is therefore low risk however as the combination of vulnerabilities may present a medium or high risk attack opportunity. Consequently it is important to make a thorough interpretation of the results by skilled security professionals rather than assuming use of the scanner alone will deliver a secure system.

Another developing area is the correlation of information produced by different security tools, such as vulnerability scanners and intrusion detection products with network access control. Standards for identifying and reporting vulnerabilities, malware, security configurations, and event logging are being developed by **MITRE** (measurablesecurity.mitre.org). MITRE developed the system of **Common Vulnerabilities and Exposures (CVE)** identifiers. These are used in NIST's vulnerability database (nvd.nist.gov). The **Security Content Automation Protocol (SCAP)** allows compatible scanners to determine whether a computer meets a particular configuration baseline from NIST's database (scap.nist.gov).

The **Open Vulnerability and Assessment Language (OVAL)** is an XML schema for describing system security state and querying vulnerability reports and information. The SANS Top 20 (www.sans.org/top20) and Bugtraq (gtsgo.to/ouc4g) are other examples of vulnerability databases.

Honeypots and Honeynets



A **honeypot** is a computer system set up to attract attackers, with the intention of analyzing attack strategies and tools, to provide early warning of attack attempts, or possibly as a decoy to divert attention from actual computer systems. Another use is to detect *internal* fraud, snooping, and malpractice. A **honeynet** is an entire decoy network. This may be set up as an actual network or simulated using an emulator.

Deploying a honeypot or honeynet can help an organization to improve its security systems, but there is the risk that the attacker can still learn a great deal about how the network is configured and protected from analyzing the honeypot system. Many honeypots are set up by security researchers investigating malware threats, software exploits, and spammers' abuse of open relay mail systems. These systems are generally fully exposed to the internet. On a real network, a honeypot is more likely to be located in a protected but untrusted area between the internet and the private network (a "DMZ") or on the private network itself (though fully isolated from it). This provides early warning and evidence of whether an attacker has been able to penetrate to a given security zone.

A honeypot is typically implemented as software running on a decoy workstation. This is referred to as a **low interaction** honeypot. Examples include BackOfficer Friendly, HoneyD, and Specter. The software simulates an OS (UNIX or Windows) and typical services (SMTP, Telnet, FTP, and HTTP for instance) and responds to requests to unused IP addresses on your network. The problem here is that attackers may be able to detect that they are dealing with honeypot software quite easily.

A more complex option is a **high interaction** honeypot, which is an actual decoy system installed with real applications and loaded with tempting, but useless, data. The system also runs a honeypot agent, designed to capture all hacker activities and transmit them to a reporting server. High interaction honeypot software products include Symantec's Decoy Server and open source software from honeynet.org.

As well as the cost and complexity of configuring the system, there is the risk that the decoy system will quickly be compromised and used to launch further attacks or abuse, either against your internal network or against other internet hosts. Another consideration is that employing this type of trap may make your organization more of a target in the future.

The critical point of a honeypot is that all the attacker's actions are logged (and optionally that alerts are generated to notify the administrator when incidents take place). The logs are normally transmitted to a separate server so that they cannot be compromised by the attacker. As well as gathering information, it could be possible to use evidence collected via a honeypot to prosecute an attacker, though this is a largely untested area of criminal law.



See [Unit 5.5](#) for more information about computer forensic procedures and prosecuting computer crime.



Review Questions / Module 1 / Unit 4 / Assessment Tools and Techniques

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What general precautions should you take before contracting someone to perform system scanning?
- 2) What is meant by a black box pentest?
- 3) What are the disadvantages of performing penetration testing against a simulated test environment?
- 4) Why should an ISP be informed before pentesting takes place?
- 5) True or false? A honeypot is designed to prevent network attacks by intercepting them and trapping them within a secure, decoy environment.



If you have access to the Hands On Live Labs, complete the "Threats / Vulnerability Scanning" lab now.

Module 1 / Summary

Security Threats and Controls

In this module, you learned some basic information security principles and about the types of attacks that can be directed against data and networks.

Module 1 / Unit 1 / Security Controls

- Security policies are essential in reducing risk to an organization's assets.
- Security controls can be classed in different ways, such as technical, operational, and management.
- Access control systems require Identification, Authentication, Authorization, and Accounting (Auditing).
- Different methods can be used for identification and authentication, including username/password, certificate, token (one-time password), or biometric.
- Multifactor and mutual authentication provide stronger authentication.
- Authorization controls can be designed using different access control models (Discretionary, Role-based, or Mandatory).
- Single sign-on technologies simplify identity, authentication, and authorization management but can introduce single points of failure.
- Accounting systems provide an audit trail of access attempts and use of system privileges.

Module 1 / Unit 2 / Threats and Attacks

- A threat is the potential for a threat source to exercise a vulnerability (weakness in the security system) either accidentally or maliciously.
- It is important to identify different threat agents and vectors. These can be classed as natural disaster, external, insider, environmental, and accidental.
- Social engineering and phishing are information gathering and penetration techniques, aimed at exploiting lack of user awareness and confidence in dealing with security and technical issues.
- Malware threats such as viruses, Trojans, rootkits, spyware, and botnets can be designed either to vandalize systems or to steal information.
- Security software can be implemented on the desktop and many products now combine the functions of anti-malware, firewall, and intrusion prevention. Careful configuration and user education are essential however if this software is to perform effectively and it can be vulnerable to direct attack by malware.

Module 1 / Unit 3 / Network Attacks

- Security administrators should be aware of network attack strategies and appropriate defenses. Attacks generally focus on weaknesses in protocols or software.
- TCP/IP protocols were not originally designed with security mechanisms. Most are vulnerable to eavesdropping; by attaching a sniffer to a network, an attacker can record, view, and possibly modify information passing through the network using a protocol analyzer.
- At layer 2 (data link) attackers can use ARP poisoning to launch spoofing, Man in the Middle, replay, or Denial of Service (DoS) attacks.
- At layer 3 (network / internet) and above attackers can use IP spoofing and hijacking tools and vulnerabilities in protocols such as ICMP to intercept sessions or launch DoS attacks.
- Footprinting and fingerprinting aim to gather information about the network while spoofing allows an attacker to masquerade as a trusted host or site. Port and network scanning tools can reveal information about networks and servers, such as host names, server applications, usernames, and so on.
- Denial of Service (DoS) disrupts legitimate access to a resource. Distributed attacks utilize multiple compromised computers (botnets) to flood the victim.

Module 1 / Unit 4 / Assessment Tools and Techniques

- Vulnerability assessments and penetration testing / ethical hacking can be used to test an organization's defenses, but the scanning can also be disruptive to the network.
- Vulnerability scanners can identify known weaknesses in OS and applications software from a database of vulnerabilities. Pentest tools are also able to launch exploits.
- A honeypot is a decoy computer system designed to analyze attack strategies without compromising the production network.

Module 2 / Cryptography and Access Control

The following CompTIA Security+ domain objectives and examples are covered in this module:

CompTIA Security+ Certification Domain Areas	Weighting
1.0 Network Security	20%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	20%
4.0 Application, Data and Host Security	15%
5.0 Access Control and Identity Management	15%
6.0 Cryptography	12%

Domain Objectives/Examples	Refer To
2.9 Given a scenario, select the appropriate control to meet the goals of security <i>Confidentiality (Encryption, Access controls, Steganography) • Integrity (Hashing, Digital signatures, Non-repudiation)</i>	Unit 2.1 Cryptography
6.1 Given a scenario, utilize general cryptography concepts <i>Symmetric vs. asymmetric • Session keys • In-band vs. out-of-band key exchange • Fundamental differences and encryption methods (Block vs. stream) • Transport encryption • Non-repudiation • Hashing • Steganography • Digital signatures • Elliptic curve and quantum cryptography • Ephemeral key • Perfect forward secrecy</i>	
6.2 Given a scenario, use appropriate cryptographic methods <i>MD5 • SHA • RIPEMD • AES • DES • 3DES • HMAC • RSA • Diffie-Hellman • RC4 • One-time pads • Blowfish • TwoFish • DHE • ECDHE • Comparative strengths and performance of algorithms • Cipher suites (Strong vs. weak ciphers)</i>	
2.9 Given a scenario, select the appropriate control to meet the goals of security <i>Integrity (Certificates)</i>	Unit 2.2 Public Key Infrastructure
4.4 Implement the appropriate controls to ensure data security <i>Hardware based encryption devices (HSM)</i>	
6.1 Given a scenario, utilize general cryptography concepts <i>Key escrow • Use of proven technologies</i>	
6.2 Given a scenario, use appropriate cryptographic methods <i>PGP/GPG</i>	
6.3 Given a scenario, use appropriate PKI, certificate management and associated components <i>Certificate authorities and digital certificates (CA, CRLs, OCSP, CSR) • PKI • Recovery agent • Public key • Private key • Registration • Key escrow • Trust models</i>	

Domain Objectives/Examples	Refer To
3.2 Summarize various types of attacks <i>Password attacks (Brute force, Dictionary attacks, Hybrid, Birthday attacks, Rainbow tables)</i>	Unit 2.3 Password Authentication
5.1 Compare and contrast the function and purpose of authentication services <i>Kerberos</i>	
5.2 Given a scenario, select the appropriate authentication, authorization or access control <i>Authentication (CHAP, PAP) • Authentication factors (Something you know) • Identification (Username)</i>	
6.2 Given a scenario, use appropriate cryptographic methods <i>NTLM • NTLMv2 • CHAP • PAP • Key stretching (PBKDF2, Bcrypt)</i>	
1.5 Given a scenario, troubleshoot security issues related to wireless networking <i>EAP • PEAP • LEAP</i>	Unit 2.4 Strong Authentication
5.1 Compare and contrast the function and purpose of authentication services <i>RADIUS • TACACS • TACACS+ • XTACACS • SAML</i>	
5.2 Given a scenario, select the appropriate authentication, authorization or access control <i>Authentication (Tokens, Common access card, Smart card, TOTP, HOTP) • Authentication factors (Something you are, Something you have, Something you do) • Identification (Biometrics, Personal identification verification card) • Federation • Transitive trust/authentication</i>	
2.3 Given a scenario, implement appropriate risk mitigation strategies <i>User rights and permissions reviews</i>	Unit 2.5 Authorization and Account Management
3.5 Explain types of application attacks <i>LDAP injection</i>	
3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques <i>Hardening (Password protection • Disabling unnecessary accounts)</i>	
5.1 Compare and contrast the function and purpose of authentication services <i>LDAP • Secure LDAP</i>	
5.2 Given a scenario, select the appropriate authentication, authorization or access control <i>Authorization (Time of day restrictions)</i>	
5.3 Install and configure security controls when performing account management, based on best practices <i>Mitigate issues associated with users with multiple account/roles and/or shared accounts • Account policy enforcement (Credential management, Group policy, Password complexity, Expiration, Recovery, Disablement, Lockout, Password history, Password reuse, Password length, Generic account prohibition) • Group based privileges • User assigned privileges • User access reviews • Continuous monitoring</i>	

Module 2 / Unit 1

Cryptography

Objectives

On completion of this unit, you will be able to:

- Understand the use of cryptography to ensure confidentiality, integrity, authentication, and non-repudiation.
- Identify and differentiate hashing, symmetric, and asymmetric encryption technologies and uses.
- Select an appropriate cryptographic method for a given scenario.
- Identify different types of cryptographic attacks.
- Understand uses for steganography.

Uses of Cryptography



Cryptography (literally meaning "secret writing") has been around for thousands of years. It is the art of making information secure.

A typical message can be understood and often modified by anyone able to get access to it. A cryptographic (or encrypted) message can only be understood by someone with the right decrypting cipher. Without the cipher, the message looks like gobbledegook. The crucial point is that cryptography removes the need to store or transfer messages securely. It does not matter if a message is stolen or intercepted, because the thief will not be able to understand or change what has been stolen.



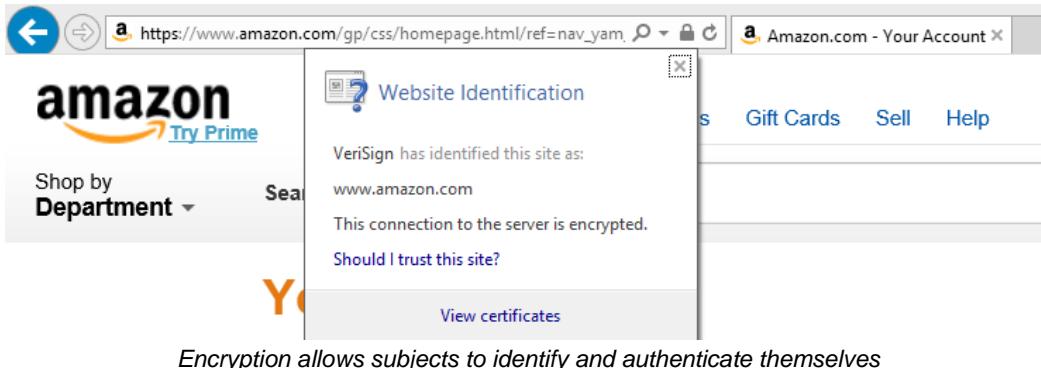
Of course, for this to be true the cipher must be kept secure.

The first use of cryptography was **confidentiality**, and this remains a very important application. With **transport encryption** for instance, confidentiality means that a message cannot be deciphered without having the appropriate cipher and key (or alternatively the means to crack the cipher). Cryptography has other uses for information security, as described below.

Authentication and Access Control

If you are able to encrypt a message in a particular way, it follows that the recipient of the message knows with whom he is communicating (that is, the sender is authenticated). Of course, the recipient must trust that only the sender has the means of encrypting the message...

This means that encryption can form the basis of identification, authentication, and access control systems.



Non-repudiation

Non-repudiation is linked to identification and authentication. It is the concept that the sender cannot deny sending the message. If the message has been encrypted in a way known only to the the sender, it follows that the sender must have composed it.

Integrity

As well as being unintelligible, a message that has been encrypted cannot be changed, so encryption guarantees the message is tamper-proof.



If you think about it, you should realize that most of the applications listed above depend on the recipient not being able to encrypt the message (or the recipient would be able to impersonate the sender). This is an important point, addressed by modern encryption systems.



Encryption has malicious uses too. For example, the Zippo Trojan encrypts a user's files then attempts to extort the user for money. This is called ransomware. Malware can also use encryption to evade detection.

Cryptographic Terminology and Ciphers

The following terminology is used to discuss cryptography:

- Plaintext (or cleartext) - this is an unencrypted message.
- Ciphertext - an encrypted message.
- Cipher - this is the process (or algorithm) used to encrypt and decrypt a message.

- Cryptanalysis - this is the art of breaking or "cracking" cryptographic systems.



The term message is used to mean data normally transmitted between a sender and receiver. Data need not be transmitted to be encrypted though. For example, encryption is widely used to protect data archived onto tape systems or hard disks.

In discussing cryptography and attacks against encryption systems, it is customary to use a cast of characters to describe different actors involved in the process of an attack. The main characters are:

- Alice - the sender of a (genuine) message.
- Bob - the intended recipient of the message.
- Eve - someone passively snooping on messages.
- Mallory - a malicious attacker attempting to subvert the message in some way.

Historically, cryptography operated using simple substitution or transposition ciphers.

Substitution Cipher

A substitution cipher involves replacing units (a letter or blocks of letters) in the plaintext with different ciphertext. Typical substitution ciphers rotate or scramble letters of the alphabet.

For example, rot13 (an example of a Caesarian cipher) rotates each letter 13 places (so A becomes N for instance). The ciphertext "Uryyb Jbeyq" means "Hello World".

Transposition Cipher

In contrast to substitution ciphers, the units in a transposition cipher stay the same in plaintext and ciphertext but their order is changed, according to some mechanism.

See if you can figure out the cipher used on the following example:
"HLOOLELWRD".

Mechanical Ciphers

Substitution and transposition ciphers were often implemented using machines, such as the German military's Enigma machine, used during the Second World War.

Frequency Analysis

Substitution and transposition ciphers are vulnerable to cracking by frequency analysis. Frequency analysis depends on the fact that some letters and groups of letters appear more frequently in natural language than others. These patterns can be identified in the ciphertext, revealing the cipher used for encryption.

Frequency analysis is still used in modern cryptanalysis.

Mathematical Ciphers

Interest in information theory and the use of computers from the mid twentieth century led to the development of increasingly sophisticated ciphers based on mathematical algorithms to perform extremely complex transpositions and substitutions. These are the ciphers in widespread use today.

The basis of mathematical ciphers is to use an operation that is simple to perform one way (when all the values are known) but difficult to reverse. These are referred to as **trapdoor functions**. The aim is to reduce the attacker to blind guessing the correct value. Given a large enough range of values, this type of attack can be rendered computationally impossible.



If you're having trouble with the transposition cipher, try arranging groups of letters into columns. It's called a rail fence cipher.

Keys

Most ciphers use a **key** to increase the security of the encryption process. For example, if you consider the Caesar cipher rot13 described above, you should realize that the key is 13. You could use 17 to achieve a different ciphertext from the same method.

The key is important because it means that even if the cipher method is known, a message still cannot be decrypted without knowledge of the specific key. This is particularly important in modern cryptography. Attempting to hide details of the cipher amounts to "security by obscurity" and is likely to be easily broken. Modern ciphers are made stronger by being open to review (cryptanalysis) by third-party researchers.

The range of key values available to use with an algorithm is called the **keyspace**. The keyspace is roughly equivalent to 2^k where k is the size of the key. However, some keys within the keyspace may be considered easy to guess ("weak") and should not be used.

Keys are also used with random **Initialization Vectors (IV)**. If the key alone were used, plaintext values that were the same would output the same ciphertexts, creating patterns in the ciphertext that would make it more vulnerable to analysis.

One-Time Pad



The **One-Time Pad**, invented by Gilbert Vernam in 1917, is an unbreakable encryption mechanism. The one-time pad itself is the encryption key. It consists of *exactly the same number* of characters as the plaintext and must be generated by a *truly random* algorithm. To encode and decode the message, each character on the pad is combined with the corresponding character in the message using some numerical system. For example, a binary message might use XOR; an alphabetic message might use numbers for each letter and modular arithmetic. An XOR operation produces 0 if both values are the same and 1 if the values are different. Modular (or clock) arithmetic works with a discrete set of numbers (0 to 25 if you want to represent the alphabet) and works in a circle rather than a line to return the remainder. For example, when calculating time on a 12-hour clock, $7+6=1$ (the remainder when you divide 13 by 12).

Apart from the requirements to be the same length as the message and truly random, each pad must only ever be used once. Re-using a pad makes ciphertexts susceptible to frequency analysis. If used properly, one-time pads are unbreakable. Unlike a cipher employing transposition and/or substitution, there are no clues about the plaintext stored within the ciphertext, apart from its length. However, the size (for anything but short messages) and secure distribution of the pad make it an unsuitable method for modern cryptography. The method is still in use where no means of computer-assisted cryptography is available though. Also, the operation of stream ciphers and quantum cryptography is similar to that of a one-time pad.

Encryption Technologies

Three different types of encryption are used in ICT systems: **hash functions**, **symmetric** encryption, and **asymmetric** encryption. Often two or more of these three different types are used together in the same product or technology.

Different technologies have different applications in different products, but the basic criteria for comparing standards are:

- **Security** - the comparative strength of one cipher over another largely depends on the bit-strength of the key and the quality of the algorithm.



Cipher strength cannot depend on keeping the operation of the cipher a secret (security by obscurity). To do so breaks Schneier's Law: "Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break. It's not even hard. What is hard is creating an algorithm that no one else can break, even after years of analysis. And the only way to prove that is to subject the algorithm to years of analysis by the best cryptographers around." (Bruce Schneier gtsgo.to/hIjp0)

- **Performance** - some technologies require more processing and memory power, making them slower and unsuitable for mobile devices.
- **Cost** - many standards are open and royalty free; some are not.



There are US government standards approving use of different encryption technologies. These are covered in [Unit 2.2](#).

Cryptographic Hash Functions



xmci1



qai15

Hash functions are widely used in computer programming to create a short representation of data. These functions are used for things like **checksums**, to ensure the validity of data.

A *cryptographic* hash function produces a fixed length string, called a **message digest**, from a variable length string. The function is designed so that it is impossible to recover the original message from the digest (**one-way**) and so that different messages are unlikely to produce the same digest (a **collision**).

Hash functions are used for confidentiality (to store passwords securely), and authentication, non-repudiation, and integrity (as part of a digital signature). Two of the most commonly used cryptographic hash algorithms are SHA-1 and MD5.

Secure Hash Algorithm (SHA)

The **Secure Hash Algorithm (SHA)** is one of the **Federal Information Processing Standards (FIPS)** developed by the **National Institute of Standards and Technology (NIST)** for the US government. SHA was created to address possible weaknesses in MDA (see below). There are two versions of the standard in common use:

- SHA-1 - this was quickly released (in 1995) to address a flaw in the original SHA algorithm. It uses a 160-bit digest.
- SHA-2 - these are variants using longer digests (up to 512 bits).

There are some concerns about the long-term security of SHA, but it is widely implemented as part of security standards and protocols, such as SSL, IPsec, and the Digital Signature Standard (DSS).

```
C:\Users\James\Downloads>fciv -sha1 "c:\users\james\documents\photo.jpg"
// File Checksum Integrity Verifier version 2.05.
baa30028bd0cac06b9d200993dda7e613c0af4e6 c:\users\james\documents\photo.jpg
C:\Users\James\Downloads>_
```

Computing an SHA value from a file

Message Digest Algorithm (MDA / MD5)

The **Message Digest Algorithm** was designed in 1990 by Ronald Rivest, one of the "fathers" of modern cryptography. The most widely used version is MD5, released in 1991, which uses a 128-bit hash value. MD5 is no longer considered secure as ways have been found to exploit collisions in the cipher. It is still widely used in operating systems and software applications for password storage.

RIPEMD

The **Research and Development in Advanced Communications Technologies in Europe (RACE)** is a program set up by the European Union (EU). The **RACE Integrity Primitives Evaluation Message Digest (RIPEMD)** was designed as an alternative to MD5 and SHA. RIPEMD-160 offers similar performance and encryption strength to SHA-1.

HMAC

A **Message Authentication Code (MAC)** is a means of proving the integrity and authenticity of a message. To produce a MAC rather than a simple digest, the message is combined with a secret key (see below). As the secret key should be known only to sender and recipient and cannot be recovered from the MAC (the function is one-way), in theory only the sender and recipient should be able to obtain the same MAC and so prove the message's origin and that it has not been tampered with.

A **Hash-based Message Authentication Code (HMAC)**, described in [RFC 2104](#), is a particular means of generating a MAC, using the MD5 (HMAC-MD5), SHA-1 (HMAC-SHA1), or SHA-2 (HMAC-SHA2) algorithm. In an HMAC, the key and message are combined in a way designed to be resistant to "extension" attacks against other means of generating MACs.



Symmetric Encryption

In symmetric encryption, a single **secret key** is used both to encrypt and decrypt data. Alternatively, there may be two keys but one is easy to determine from possession of the other.



Symmetric encryption is also referred to as single-key or private-key or shared secret. Note that "private key" is also used to refer to part of the public key cryptography process (see below), so take care not to confuse the two uses.

The secret key is so-called because it must be kept secret. If the key is lost or stolen, the security is breached. The main problem with symmetric encryption is secure distribution and storage of the key. This problem becomes exponentially greater the more widespread the key's distribution needs to be. The main advantage is speed, as symmetric key encryption is far faster than asymmetric encryption.

Symmetric encryption is used for confidentiality only. Because the same key must be used to encrypt and decrypt information, it cannot be used to prove someone's identity (authentication and non-repudiation). If you tell someone the key to allow them to read a message that you have sent to them, they would gain the ability to impersonate you....



The problem of key distribution is usually solved by exchanging the keys using asymmetric encryption. Alternatively, an offline (or out-of-band) method can be used, such as using a courier service to deliver the key on a disk.

There are two types of symmetric encryption: block and stream ciphers.



Block and Stream Ciphers

7o3tg

In a **block cipher**, the plaintext is divided into equal-size blocks (usually 64- or 128-bit). If there is not enough data in the plaintext, it is **padded** to the correct size using some string defined in the algorithm. For example, a 1200-bit plaintext would be padded with an extra 80 bits to fit into 10 x 128-bit blocks. Each block is then subjected to complex transposition and substitution operations, based on the value of the key used.

As described by Claude Shannon in 1949, block ciphers must exhibit the properties of **confusion** and **diffusion**.

- Confusion means that the key should not be derivable from the ciphertext. This is achieved through substitution units called S-boxes. Each S-box operates differently and the S-box used in a particular operation is determined by the key.

- Diffusion means that if any one bit of the plaintext is changed, many bits in the ciphertext should change as a result (half of them in fact). Diffusion is obtained through transposition (swapping the order of bits around; again using operations determined by the value of the key).

Most ciphers increase security by encrypting the data more than once (**rounds**).

Unlike a block cipher, in a **stream cipher** each bit or byte of data in the plaintext is encrypted one at a time. Like a one-time pad, the plaintext is combined with a separate randomly-generated message. Unlike a one-time pad, this is not predetermined but calculated from the key (keystream generator) and an Initialization Vector (IV) that ensures the key produces a unique ciphertext from the same plaintext.



4rv2I

DES / Triple DES (3DES)

The **Data Encryption Standard** was developed between 1972 and 1977 by IBM for the NSA. It is another of the FIPS developed by NIST for the US government. The algorithm used in DES is based on IBM's Lucifer cipher. It is a block cipher using 64-bit blocks and a 56-bit key.

DES was shown to be flawed, prompting the development (in 1998) of Triple DES, where the plaintext is encrypted three times using different keys (typically one round with key1 then with key2 then with key1 again, though sometimes three different keys are employed). Triple DES is still in use though is largely being replaced by the faster and more secure AES.

AES / AES256

The **Advanced Encryption Standard (AES)** was adopted as a replacement for DES by NIST in 2001. It is faster and more secure than DES. AES is also a block cipher, with a block size of 128 bits and key sizes of 128, 192, or 256 bits. AES is the preferred choice for many new applications. As an open standard it is patent-free.



AES is also referred to as Rijndael, after the algorithm developed by its inventors, Vincent Rijmen and Joan Daemen. This algorithm was selected after a competition (most of the ciphers listed below were also entrants).

RC4

Rivest Ciphers (or **Ron's Code**) are a family of different encryption technologies designed by Ron Rivest (www.rsasecurity.com). The **RC4** cipher (often referred to as **Arcfour**) is a stream cipher using a variable length key (from 40 to 128 bits). RC4 is available for use in Secure Sockets Layer (SSL) and Wired Equivalent Privacy (WEP).

Blowfish / Twofish

Blowfish was developed in 1993 by Bruce Schneier (www.schneier.com). It uses 64-bit blocks and variable key sizes (32 - 448 bits). Blowfish is both secure and fast. A related cipher **Twofish** was developed by an extended team to enter the AES competition. Twofish uses a larger block size (128-bit) and keys up to 256 bits long. Both Blowfish and Twofish were made available copyright and patent-free by their inventors.



gs7sy

Asymmetric Encryption

In asymmetric encryption (or Public Key Cryptography as it is more commonly called), a **secret private key** is used to decrypt data. A mathematically related **public key** is used to encrypt data. This public key can be widely and safely distributed to anyone with whom the host wants to communicate, because the private key *cannot* be derived from the public key.

This can work the other way around; the private key can be used for encryption and the public key for decryption. This provides the mechanism for digital signatures. Only the sender (Alice) could have created the signature because only Alice knows the private key linked to the public key that can decrypt the signature.

The problem with asymmetric encryption is that it involves quite a lot of computing overhead. Where a large amount of data is being encrypted on disk or transported over a network, asymmetric encryption is inefficient. Consequently, asymmetric encryption is mostly used for privacy (public key encryption), authentication and non-repudiation (digital signatures), and key agreement or exchange.



936sq

RSA Security

Ron Rivest, Adi Shamir, and Leonard Adleman published the RSA cipher in 1977 (www.rsasecurity.com). RSA is widely deployed as a solution for creating digital signatures and key exchange. It is the basis of Secure Sockets Layer (SSL) and public key cryptography.



RSA depends on the difficulty of finding the prime factors of very large integers. Refer to the SANS white paper "Prime Numbers in Public Key Cryptography" (gtsgo.to/8aoku) for more information.

RSA block sizes and key lengths are variable according to the application, with larger keys offering more security. RSA can only be used to encrypt short messages. The maximum message size is the key size minus 11 in bytes. For example, a key size of 2048 bit allows a maximum message size of 245 bytes: $(2048 / 8) - 11$.

DSA / ElGamal

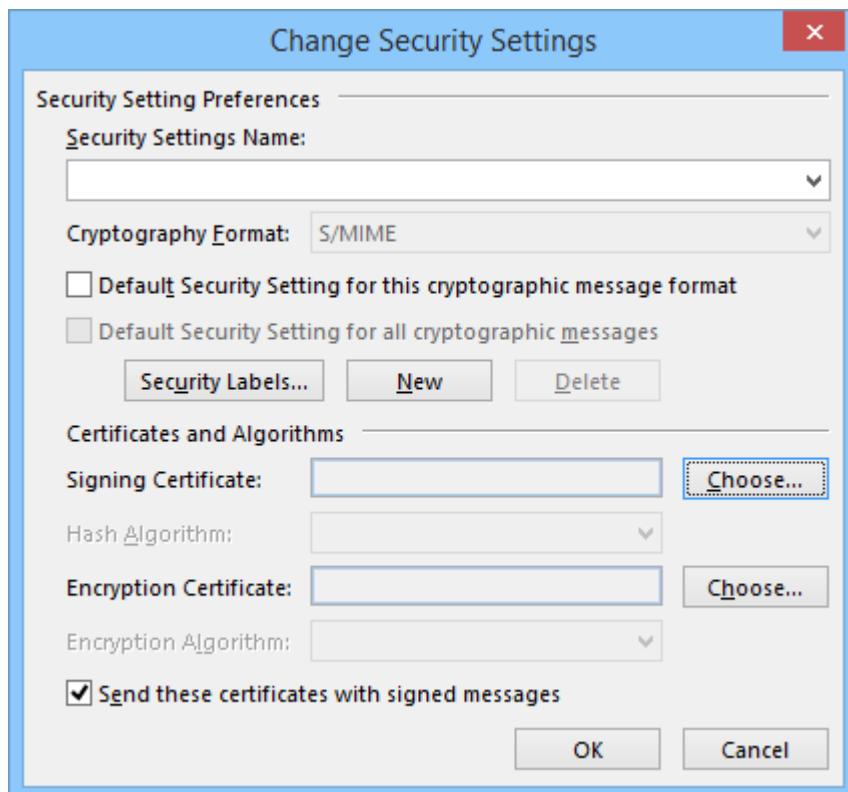
The ElGamal algorithm, published by Taher Elgamal, is another means of generating private and public key pairs. An adaptation of the algorithm was used by NIST in its **Digital Signature Algorithm (DSA)**.



Digital Signatures

A **digital signature** is used to prove the identity of the sender of a message and to show that a message has not been tampered with since the sender posted it. This provides authentication, integrity, and non-repudiation. It works as follows:

- 1) The sender (Alice) creates a digest of the message, using a pre-agreed secure hash algorithm (such as SHA or MD5), and then *encrypts* the digest using her **private key**.
- 2) The resultant **signature** is then attached to the original document and delivered.
- 3) The recipient (Bob) *decrypts* the signature using Alice's **public key**, resulting in the original hash.
- 4) Bob then calculates his *own* message digest of the document (using the same algorithm as Alice) and *compares* it with Alice's digest.
- 5) If the two digests are the *same*, then the data has not been tampered with during transmission, and Alice's identity is *guaranteed*. If either the data had changed or a malicious user (Mallory) had intercepted the message and used a different private key, the digests would not match.



Configuring Outlook email client application to use digital signatures

Digital Envelopes

Secret-key (symmetric) encryption is generally *faster* than public key cryptography and better suited to digital sealing of large amounts of data. Therefore, often, both are used. This type of key exchange system is known as a **digital envelope**. It works as follows:

- 1) Alice encrypts the message using a secret-key cipher such as AES or Blowfish.
- 2) The secret key itself is encrypted using public key cryptography (with Bob's public key) then attached to the encrypted message and sent to Bob. In this context, the secret key is often referred to as a **session** key.



It is important that a new session key be generated for each session and destroyed at the end of a session.

- 3) Bob uses his private key to decrypt the secret key.
- 4) Bob uses the secret key to decrypt the message.



In all these implementations, it is critical that the private key be kept secure and available only to the authorized user. The private key could be kept on a computer (and secured by the user login) or it could be stored on a PIN-protected smart card or USB fob.

Digital Certificates

When using public/private key pairs, a subject will make his or her public key freely available. The question then arises of how anyone can trust the identity of the person or server issuing the public key. The solution is to have a third party (a Certificate Authority) validate the use of the public key by issuing the subject with a **certificate**. The certificate is signed by the Certificate Authority. If the client trusts the Certificate Authority, they can also trust the public key wrapped in the subject's certificate.

The process of issuing and verifying certificates is called **Public Key Infrastructure (PKI)**.



See [Unit 2.2](#) for more information about certificates and Public Key Infrastructure (PKI).



wf5g5

Diffie-Hellman

Diffie-Hellman (D-H) is a key agreement protocol, published in 1976 by Whitfield Diffie and Martin Hellman. These authors also acknowledge the work of Ralph Merkle and suggest that the protocol be referred to as Diffie-Hellman-Merkle.

D-H itself is not used to encrypt messages or to authenticate senders. It is used to securely agree a key to use to encrypt messages using a symmetric encryption algorithm, such as RC4 or AES. The process works (in simple terms) as follows:

- 1) Alice and Bob agree on shared integers (p and g) to use for key generation. These values can be known to eavesdroppers without compromising the process.
- 2) Alice and Bob each choose different private integers (a and b). These values must not be disclosed to anyone else (Alice does not tell Bob a and Bob does not tell Alice b).
- 3) Alice and Bob calculate integers (A and B) based on the shared and private values and send those to one another (for example, $A = g^a \text{ mod } p$).
- 4) Alice and Bob now both know p , g , A , and B . Alice knows a and Bob knows b . Alice and Bob use a and B and b and A to generate a shared secret (s). s is used to generate the session key for another cipher, such as RC4 or AES.
- 5) An eavesdropper (Eve) might know p , g , A , and B but without knowledge of a or b cannot derive s .

The protocol must also be used with a secure authentication system, or it is vulnerable to Man-In-The-Middle attacks. When Alice and Bob try to agree on shared integers (p and g) to use for key generation, the Man-in-the-Middle (Mallory) intercepts the messages and sends "mp" and "mg" to Bob and Alice. Mallory can then sit between Alice and Bob, decrypting and possibly modifying each message from either, before sending it on. To prevent this Alice and Bob must digitally sign the packets containing the public value they are using ($g^a \text{ mod } p$).

D-H key sizes are described in groups. The commonly used groups are group 1 (768-bit), group 2 (1024-bit), group 5 (1536-bit), and group 2048 (2048-bit obviously). The most notable use of D-H is in IPsec (as part of the Internet Key Exchange protocol [IKE]). D-H can also be used in the Transport Layer Security (TLS) protocol to provide Perfect Forward Secrecy. This is referred to as **DHE (Diffie-Hellman Ephemeral mode)** but is called **EDH** in some cipher suites.



ECC and Quantum Cryptography

Diffie-Hellman key exchange and the RSA cipher are based on the simplicity of multiplying numbers against the difficulty of finding the factors of large numbers. There are some indications that these methods will become vulnerable to improved cryptanalysis techniques.

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is another means of producing the related values to use as the basis of a trapdoor function. ECC was published by Neal Koblitz and Victor Miller in 1985, though they arrived at the idea independently of one another.

The principal advantage of ECC over RSA's algorithm is that there are no known "shortcuts" to cracking the cipher or the math that underpins it, regardless of key length. Consequently, ECC used with a key size of 256 bits is very approximately comparable to RSA with a key size of 2048 bits.

ECC with D-H Ephemeral mode (ECDHE) provides a Perfect Forward Secrecy (PFS) mechanism for Transport Layer Security (TLS). This is likely to be increasingly widely adopted over the next few years.

Quantum Cryptography

"Quantum" cryptography is a developing field of cryptography and cryptanalysis, based on quantum physics rather than math. The (very) basic takeaway message from quantum physics is that a photon (a light particle) has spin and until it is measured, the photon spins in all directions at the same time (it is unpolarized). When a photon passes through a filter to measure its spin, its state (spin direction) is determined (the photon is polarized). This cannot be measured again by a third party as the act of measurement destroys the information obtained in the previous act of measurement.

These strange properties of photons can be used to encode binary information (qubits). They can also be the basis of a secret key generation system, referred to as **Quantum Key Distribution (QKD)**. Alice sends Bob a stream of polarized photons using different filters over a quantum channel. Bob uses a different sequence of different filters to determine the state of each photon. Bob then uses an authenticated public communications channel to tell Alice the sequence of filters he used and Alice confirms which of the filters was a match, discarding any results that did not match. The remaining results are converted into qubits representing a shared secret known only to Alice and Bob that could be used to encrypt longer messages.

As Eve can only monitor the discussion about which filters were used (intercepting the photons would change their state), there is no means of anyone other than Bob recovering the message itself. A weakness arises if the public communications channel (used to exchange information about the filters) can be subverted by Mallory, performing a Man-in-the-Middle attack.

The main challenge to a practical implementation of quantum cryptography is being able to transmit and measure photons reliably over long distances. Commercially-useful products are not likely to become available in the short term.

The other major impact of the properties discovered by quantum physics is in cryptanalysis. The future promises a generation of quantum computers, capable of operating much faster than the solid state devices we use now. This could make current math-based ciphers much more vulnerable to brute force attacks.

Transport Encryption



hcc1k

Transport encryption refers to encrypting data as it is sent over a network. Examples include IPsec (for any IP-based network) and other encrypted Virtual Private Network (VPN) protocols, Secure Sockets Layer / Transport Layer Security (SSL/TLS) for TCP/IP application protocols such as HTTPS, and WEP and WPA for wireless networks.



nam15

In-band Versus Out-of-Band Key Exchange

Key exchange is the process by which sender and receiver agree on which key to use for encryption. Symmetric encryption involves sender and receiver using the same key. In this instance, transmitting the key securely is a huge problem. You could use a secure **out-of-band** transmission method, such as sending the key by courier or transmitting it verbally but these methods increase the risk that the key will be compromised. It is also difficult to distribute such a key securely between more than two people.

In asymmetric encryption, because the sender and receiver use public and private keys that are linked but not derivable (no one can obtain the private key from possession of the public key) **in-band** key exchange (over an unencrypted channel) is straightforward.

- For confidentiality, Bob just tells Alice his public key. Alice uses this public key to encrypt a confidential message to Bob, confident that only Bob owns the private key that will allow the message to be decrypted.
- For authentication, Alice tells Bob her public key and sends him a signature, encrypted using her private key. Bob can decrypt Alice's signature using the public key, confident that only Alice's private key would have been able to encrypt that signature.

Session Keys

Transport encryption often makes use of a different key for each **session**. This type of key is often referred to as an **ephemeral key**. This improves security because even if an attacker can obtain the key for one session, the other sessions will remain confidential. This massively increases the amount of "cracking" that an attacker would have to perform to recover an entire "conversation".

Asymmetric encryption provides a solution to the problem of exchanging keys. It allows Alice and Bob to securely exchange or agree some sort of shared secret for use in generating symmetric encryption session keys. This exchange can be made in-band (over "normal" network channels) because eavesdropping on the exchange does not allow an attacker to determine what key has actually been agreed.

Where an ephemeral key is generated for each session, this system is referred to as **Perfect Forward Secrecy (PFS)**. PFS is principally used to improve the confidentiality of messages exchanged using SSL.



See [Unit 4.3](#) for more information about the use of PFS under SSL. PFS is also used with IPsec, covered in [Unit 3.4](#).



Cryptographic Attacks

Malicious attacks on modern encryption systems are generally made for two reasons:

- To decipher encrypted data without authorization.
- To impersonate a person or organization by appropriating their digital signature or certificate.

In addition, non-malicious cryptanalysis is undertaken on encryption systems with the purpose of trying to detect weaknesses in the technology.

Mathematical Attacks

No encryption system is perfect. Encryption technology considered unbreakable today could become vulnerable to the improved technology or mathematical techniques of 1, 10, 20, or 50 years' time.

Weaknesses discovered in a particular technology "in the lab" do not necessarily mean that the system is vulnerable in practice. There is always a trade-off between security, cost, and interoperability. Malicious mathematical attacks are difficult to launch and the chances of success against up-to-date, proven technologies and standards are remote.



Many attacks are directed against the implementation of a particular algorithm in software products rather than the algorithm itself. In 2014, a rather spectacular vulnerability in iOS and OS X emerged meaning that SSL certificate validation was disabled by a mistaken code update. Another even more spectacular vulnerability emerged in OpenSSL in the same year (Heartbleed) that potentially allows attackers to recover a private key from a server.

Mathematical attacks often depend on the attacker having a known plaintext with its corresponding ciphertext. Another method is to input plaintexts with very small differences and to analyze the ciphertext output.

Cryptographic Man-in-the-Middle and Replay Attacks

These attacks depend on capturing the communications between two parties. They do not break the cryptographic system but exploit vulnerabilities in the way it is *used*.

A **Man-in-the-Middle** attack is typically focused on public key cryptography.

- 1) Mallory eavesdrops the channel between Alice and Bob and waits for Alice to request Bob's public key.
- 2) Mallory intercepts the communication, retaining Bob's public key, and sends his own public key to Alice.
- 3) Alice uses the key to encrypt a message and sends it to Bob.
- 4) Mallory intercepts the message and decrypts it using his private key.
- 5) Mallory then encrypts a message (possibly changing it) with Bob's public key and sends it to Bob, leaving Alice and B oblivious to the fact that their communications have been compromised.

This attack is prevented by using secure authentication of public keys, such as associating the keys with certificates.

A **replay** attack consists of intercepting a key or password hash then reusing it to gain access to a resource. This type of attack is prevented by using once-only session tokens or timestamping sessions.

Side Channel Attacks

While extremely difficult to launch in practice, side channel attacks represent a completely different approach to cryptanalysis. The theory is that by studying physical properties of the cryptographic system, information may be deduced about how it works.

Side channel attacks means monitoring things like timing, power consumption, and electromagnetic emanation. Obviously it is necessary to obtain a physical copy of the cryptographic system or to have some extremely sophisticated monitoring equipment installed.



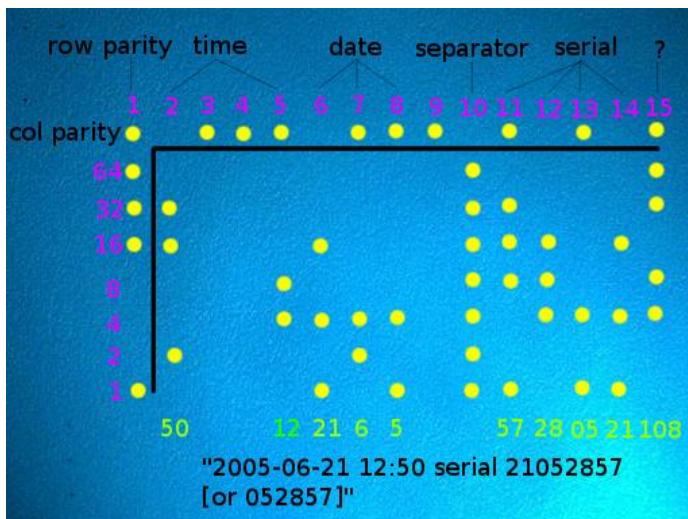
Steganography

Steganography (literally meaning "hidden writing") is a technique for obscuring the presence of a message. Typically, information is embedded where you would not expect to find it (a message hidden in a picture for instance). The container document or file is called the **covert text**.

One example of steganography is to encode messages within TCP packet data fields to create a covert message channel. Another approach is to change the least significant bit of pixels in an image file (the cover file); this can code a useful amount of information without distorting the original image noticeably.

Another example is to use the design and color of bank notes to embed a watermark. This method is employed by the **Counterfeit Deterrence System (CDS)**. CDS is now incorporated on banknotes for many currencies. When a copy device or image editing software compatible with CDS detects the watermark embedded in the currency design, it prevents reproduction of the image, displaying an error message to the user. Anti-counterfeiting measures for currency are overseen by **Central Bank Counterfeit Deterrence Group (CBCDG [www.rulesforuse.org])**.

Another example of steganography is the automatic incorporation of watermarks on all printed output by some models of printer. These watermarks are printed as tiny yellow dots, invisible to the naked eye (the picture below was taken with a microscope and the dots have been overlaid with markers). The pattern identifies the printer model, serial number, and date and time of printing. This prevents output from commercial printers being used for forging secure documents, such as banknotes or passports.



Analysis of automatic device and date identification watermark
(Image courtesy Electronic Frontier Foundation [www.eff.org])

When used to conceal information steganography amounts to "security by obscurity", which is usually deprecated. However, a message can be encrypted by some mechanism before embedding it, providing confidentiality. The technology can also provide integrity or non-repudiation; for example it could show that something was printed on a particular device at a particular time, which could demonstrate that it was genuine or a fake, depending on context.



Review Questions / Module 2 / Unit 1 / Cryptography

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What is the principal use of symmetric encryption?
- 2) What features of a one-time pad make the system cryptographically secure?
- 3) Which offers better security - MD5 or SHA?
- 4) Which symmetric cipher is being selected for use in many new products?
- 5) What is the process of digitally signing a document?
- 6) How are cryptographic authentication systems protected against replay attacks?
- 7) What technique might be used to detect the presence of a hidden message within a file?
- 8) You want to ensure that data stored on backup media cannot be read by third-parties. What type of security control should you choose?
- 9) You are distributing a software application to clients and want to provide them with assurance that the executable file has not been modified. What type of security control is appropriate for this task?
- 10) Your company issues vouchers by email for various products and events. What security control could you use to prove the authenticity of the vouchers?

Module 2 / Unit 2

Public Key Infrastructure

Objectives

On completion of this unit, you will be able to:

- Describe the components and usage of Public Key Infrastructure.
- Know the function and format of X.509 digital certificates.
- Describe the function of Certificate Authorities and Certificate Policy in PKI.
- Describe the process of key management under PKI.
- Identify the use of different PKI trust models.
- Identify cryptographic standards and proven technologies associated with PKI and PGP/GPG.

PKI and Certificates



5jxt

Public key cryptography solves the problem of securely distributing encryption keys when you want to communicate securely with others or authenticate a message that you send to others.

- When you want others to send you confidential messages, you give them your public key to use to encrypt the message. The message can then only be decrypted by your private key, which you keep known only to yourself.
- When you want to authenticate yourself to others, you create a signature and sign it by encrypting the signature with your private key. You give others your public key to use to decrypt the signature. As only you know the private key, everyone can be assured that only you could have created the signature.

The basic problem with public key cryptography is that you may not really know with whom you are communicating. The system is vulnerable to Man-in-the-Middle attacks.

This problem is particularly evident with e-commerce. How can you be sure that a shopping site or banking service is really maintained by who it claims? The fact that the site is distributing public keys to secure communications is no guarantee of actual identity. How do you know that you are corresponding directly with the site, using its certificate? How can you be sure there isn't a Man-in-the-Middle intercepting and modifying what you think the legitimate server is sending you?

Public Key Infrastructure (PKI) aims to prove that the owners of public keys are who they say are. Under PKI, anyone issuing public keys should obtain a **Digital Certificate**. The validity of the certificate is guaranteed by a **Certificate Authority (CA)**. The validity of the CA can be established using various models, described later. The other advantage of PKI is that it provides a system for managing and distributing keys.

Digital Certificates

A **digital certificate** is essentially a wrapper for a subject's (or end entity's) public key. As well as the public key, it contains information about the subject and the certificate's issuer or guarantor. The subject could be a human user (for certificates allowing the signing of messages for instance) or a computer server (for a web server hosting confidential transactions for instance). Digital certificates are based on the X.509 standard approved by the International Telecommunications Union (ITU). This standard is incorporated into the Internet Engineering Taskforce's [RFC 5280](#). X.509 defines the fields (information) that must be present in the certificate. The standard provides interoperability between different vendors.



You will also see reference to **PKIX**, which is a working group set up by IETF to develop X.509 related standards, and **PKCS**, which are standards developed by RSA Security to promote the use of digital certificates (many of which have been incorporated into the IETF standards).

Field	Value
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	VeriSign Class 3 Secure Server...
Valid from	27 February 2014 01:00:00
Valid to	01 March 2015 00:59:59
Subject	www.amazon.com, Amazon.c...
Public key	RSA (2048 Bits)
Subject Alternative Name	DNS Name=updated.amazon.r...

```

30 82 01 0a 02 82 01 01 00 97 5f 89 e3 8f
ad fe 00 ad fd 48 95 e7 7f 8a 2f 7b e3 4e
d9 9e 3a 5a 07 9c 71 9b 8f 50 e0 fc f7 fb
9c 66 0f 42 d8 ad ee c2 8e 7d 40 ed 6d d9
94 79 22 e7 31 55 66 95 bd 25 bf f7 3d f4
84 0d 8e 6c 97 28 e4 2c 3d a3 76 5d a0 55
e7 d2 b6 14 99 b5 8c 5b e5 e6 2f ef db 48
10 dd 14 f4 06 7c fd 56 86 c1 4a 24 97 c9
f5 32 2b 5c 10 2c 4d 2c c7 b8 2e aa 15 99

```

[Edit Properties...](#) [Copy to File...](#)

Digital certificate details

There are various formats for encoding a certificate as a digital file. All certificates use an encoding scheme called **Distinguished Encoding Rules (DER)** to create a binary representation of the information in the certificate. A DER-encoded binary file can be represented as ASCII characters using Base64 **Privacy-enhanced Electronic Mail (PEM)** encoding. The file extensions .CER and .CRT are also often used, but these can contain either binary DER or ASCII PEM data.

Additionally, the .PFX or .P12 format allows the export of a certificate *along with its private key*. This would be used to archive or transport a private key. This type of file format is password-protected.

Certificate Fields

The information shown in the certificate includes the following:

Field	Usage
Version	The X.509 version supported (V1, V2, or V3).
Serial Number	A number uniquely identifying the certificate within the domain of its CA.
Signature Algorithm	The algorithm used by the CA to sign the certificate.
Issuer	The name of the CA, expressed as a Distinguished Name (DN).
Valid From / To	Date and time during which the certificate is valid.
Subject	The name of the certificate holder, expressed as a Distinguished Name (DN).
Public Key	Public key and algorithm used by the certificate holder.
Extensions	V3 certificates can be defined with extended attributes, such as friendly subject or issuer names, contact email addresses, and intended key usage.



A Distinguished Name is an identifier of an object in an X.500 directory. See [Unit 2.5](#) for more information on this topic.

When creating a web server certificate, it is important that the subject matches the Fully Qualified Domain Name by which the server is accessed or browsers will reject the certificate.

Where a company operates many subdomains, it is possible to use a single **wildcard certificate** to cover the whole domain. For example, a certificate issued to ***.widget.com** could be used to secure access to "store.widget.com" and "www.widget.com". Another option is to configure a **Subject Alternative Name** using a certificate extension field (see below).

Both these methods can cause problems with legacy browser software and some mobile devices. There is also greater exposure for the servers operating each subdomain should the certificate be compromised. Using separate certificates for each subdomain offers better security.

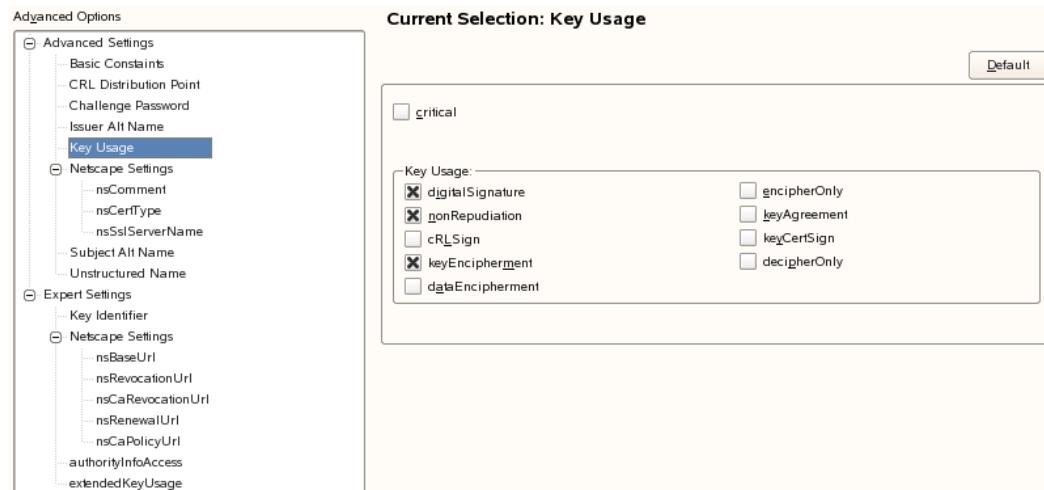
Certificate Extensions

Certificate extensions, defined for version 3 of the X.509 format, allow extra information to be included about the certificate. An extension consists of:

- Extension ID (extnID) - an object identifier.
- Critical - a Boolean (True or False) value indicating whether the extension is critical (see below).
- Value (extnValue) - the string value of the extension.

Certificates issued for private use can use **private**, **proprietary**, or **custom** extensions. Public certificates can use **standard** extensions; that is, **Object Identifiers (OID)** defined in the X.509 documentation. One of the most important standard extensions is **Key Usage**. This extension defines the purpose for which a certificate was issued:

- digitalSignature (0) - used to digitally sign documents.
- nonRepudiation (1) - used by a non-repudiation service. A non-repudiation service is an additional guarantor that the signer of a document really did sign it. This is the function of a notary in witnessing the physical signing of a document.
- keyEncipherment (2) - used for key exchange.
- dataEncipherment (3) - used to make data confidential.
- keyAgreement (4) - used for Diffie-Hellman key agreement.
- keyCertSign (5) - used by a CA for certificate signing.
- cRLSign (6) - used to sign a Certificate Revocation List (see below).
- encipherOnly (7) - used with Diffie-Hellman key agreement.
- decipherOnly (8) - used with Diffie-Hellman key agreement.



Defining key usage and other certificate settings in SUSE Enterprise Linux CA

An extension can be tagged as **critical**. This means that the application processing the certificate *must* be able to interpret the extension correctly; otherwise the certificate should be rejected.

In the case of a key usage extension marked as critical for instance, an application should reject the certificate if it cannot resolve the key usage value. This prevents a certificate issued (for example) for signing a CRL to be used for signing an email message. If key usage is *not* marked as critical, it effectively serves as a comment rather than controlling the certificate in any way.

Certificate Authorities



mgjqw

The **Certificate Authority (CA)** is the person or body responsible for issuing and guaranteeing certificates. Private CAs can be set up within an organization for internal communications. Most network operating systems, including Windows Server, have certificate services. For public or business-to-business communications however, the CA must be trusted by each party. Some organizations are large enough that users trust them to fulfill the CA administrative duties properly. In practice, most organizations use third-party CA services, such as Thawte/VeriSign, Microsoft, Computer Associates eTrust, and OpenCA (an open source PKI project).

The functions of a CA are as follows:

- Provide a range of certificate services useful to the community of users serviced by the CA.
- Ensure the validity of certificates and the identity of those applying for them (**registration**).
- Establish trust in the CA by users and government and regulatory authorities and enterprises such as financial institutions.
- Manage the servers (**repositories**) storing and administering the certificates.
- Perform key and certificate lifecycle management.

Req...	Requester Name	Binary Certificate	Certificate Template	Serial Number
2	BOOTKAMP1\Administr...	-----BEGIN CERTI...	User (User)	61b6abf6000...
4	BOOTKAMP1\Administr...	-----BEGIN CERTI...	User Signature Only...	61b87fd2000...

Microsoft Windows Server CA

Registration and CSRs



b3fca

Registration is the process by which end users create an account with the CA and become authorized to request certificates. The exact processes by which users are authorized and their identity proven are determined by the CA implementation. For example, in a Windows Active Directory network users and devices can often auto-enroll with the CA just by authenticating to Active Directory. Commercial CAs might perform a range of tests to ensure that a subject is who he or she claims to be. It is in the CA's interest to ensure that it only issues certificates to valid users or its reputation will suffer.

The registration function may be delegated by the CA to one or more **Registration Authorities (RA)**. These entities complete identity checking and submit CSRs (see below) on behalf of end users but do not actually sign or issue certificates.

When a subject wants to obtain a certificate, it completes a **Certificate Signing Request (CSR)** and submits it to the CA. The CSR is a Base64 ASCII file containing the information that the subject wants to use in the certificate, including its public key. The format of a CSR is based on the PKCS#10 standard. The CA reviews the certificate and checks that the information is valid. For a web server, this may simply mean verifying that the subject name and FQDN are identical and verifying that the CSR was initiated by the person administratively responsible for the domain, as identified in the domain's WHOIS records.



For a basic certificate, the CA might just email the administrative contact. There is the risk that this process could be compromised. Many CAs also offer an Extended Validation (EV) process that requires more rigorous identity checks.

If the request is accepted, the CA signs the certificate and sends it to the subject.

Certificate Policies

A CA will issue many different types of certificate, designed for use in different circumstances. Some typical uses are:

- SSL Web Server - guarantee e-commerce or information gathering websites. Differently graded certificates might be used to provide levels of security (for example, an online bank requires higher security than a site that collects marketing data).
- Code signing - guarantee the validity of a software application or browser plug-in.
- Registered Domain - prove the ownership of a particular domain.
- Personal email - secure personal email and file transfer communications.

Certificate policies define these different uses, typically following the framework set out in [RFC 2527](#). As an example of a policy, you could refer to the US Federal government's common policy framework for PKI (gtsgo.to/m53so).



Certificate templates for Windows Server CA

Different policies will define different levels of secure registration and authentication procedures required to obtain the certificate. A general purpose or low-grade certificate might be available with proof of identity, job role, and signature. A commercial grade certificate might require in-person attendance by the authorized person.

The screenshot shows the 'Advanced Certificate Request' page from Microsoft Active Directory Certificate Services. The URL is <https://server.classroom.local/certsrv/certreqma.asp>. The page has several sections:

- Certificate Template:** A dropdown menu set to 'User'.
- Key Options:**
 - Create new key set Use existing key set
 - CSP: Microsoft Enhanced Cryptographic Provider v1.0
 - Key Usage: Exchange Other
 - Key Size: 2048 (Min: 384, Max: 16384) (common key sizes: 512 1024 2048 4096 8192 16384)
 - Automatic key container name User specified key container name
 - Mark keys as exportable Enable strong private key protection
- Additional Options:**
 - Request Format: CMC PKCS10
 - Hash Algorithm: sha1 (Only used to sign request.)
 - Save request
 - Attributes: A list box containing '< >'.
 - Friendly Name: bob@classroom.com
- A 'Submit >' button at the bottom.

Obtaining a certificate from a Windows Server CA



An example of this is "High Assurance" SSL certificates. These are being introduced to provide extra assurance to consumers that an organization has been thoroughly investigated before being provided with a certificate. See [Unit 4.3](#) for details.

Implementing PKI



There are three main elements to PKI:

- Organization - the policies, standards, and administrators required to define and run the CA.
- Servers - computers to store, distribute, and authenticate certificates (**Certificate Repositories**).
- Clients - applications that allow users to read and trust or reject certificates.

As well as implementing the registration and certificate authority functions described above, another critical function in PKI (and in managing other cryptographic systems) is key management.

Key Management

Key management refers to the operations at various stages in a key's **lifecycle**. A key's lifecycle may involve the following stages:

- **Key Generation** - creating a secure key pair of the required strength, using the chosen cipher.
- **Certificate Generation** - to allocate a key pair to a user it is typically embedded in a digital certificate. At this point, it is critical to verify the identity of the user, so that the certificate can be trusted.
- **Distribution** - making the key pair (or certificate) available to the user. It is vital that the private key not be intercepted in transit.
- **Storage** - the user must take steps to store the private key securely, ensuring that unauthorized access and use is prevented. It is also important to ensure that the private key is not lost or damaged.
- **Revocation** - if a private key is compromised, it can be revoked before it expires.
- **Expiration** - a private key that has not been revoked expires after a certain period. Giving the key or certificate a "shelf-life" increases security.

Remember that in asymmetric encryption, keys are issued in pairs (a **key-pair**). If the private key linked to a public key is lost, data encrypted with the public key cannot be decrypted.



Key management also concerns symmetric keys, with the problem of secure distribution being particularly acute.

Key management can either be **centralized** (where one administrator or authority controls the process) or **decentralized** (where each user is responsible for his or her keys). Centralized management is typical of stand-alone or hierarchical trust models; decentralized management is typical of the Web of Trust model.



zs3th

Creating Keys

A key is a pseudo randomly generated integer of the required size (1024-bit or 2048-bit for instance), expressed in binary DER or ASCII PEM encoding. Generating integers that are sufficiently random is not a trivial task and it is possible to make a mistake, leading to a weak key (one that is easier to crack). The process is also CPU-intensive, meaning that it often has to be undertaken on dedicated hardware.

Re-using keys is bad practice and should be avoided.

Key Pair Usage

Keys (or certificates) have different **usages**, as set out in the Certificate Policy Statement. A key pair used for signatures should not also be used for encrypting data.

Consequently, a user may require **multiple key pairs**. This is because a key used to *encrypt* a document (providing confidentiality [or digital sealing]) should **not** also be used to *sign* a document (providing authentication and non-repudiation). If the same key is used for both purposes, and the encryption key is compromised, then *both* uses of the key are threatened. There is also the case that when a key is recovered (see below), the recovery agent could gain the ability to sign documents fraudulently.



4qij6

Storing and Distributing Keys

Once generated, the private key must be stored somewhere safe (a **repository**). Key storage can be either software- or hardware-based.

In software-based storage, the key is stored on a server. Security is provided by the operating system and this can be adequate for most functions, but this type of software-based storage is not considered secure enough for mission-critical key storage. One extra measure that can be taken is to disconnect the host system from any sort of network access and locate it in a very securely controlled physical environment.

Software-based distribution of keys (or in-band distribution) should only take place over a secured network. Distribution over the internet typically employs SSL.

Hardware-based storage and distribution is typically implemented using removable media, a smart card, or at the higher end, a dedicated key storage **Hardware Security Module (HSM)**.

A smart card may be a credit card style device, a USB device, or a SIM card (used with mobile phones). A smart card may therefore support a variety of interfaces, including a card reader or USB port. The main consideration with media and smart card-based storage is to physically secure the device and to keep the access method (typically protected by a pass code) secure. Another option is to use a **Trusted Platform Module (TPM)** chip in a PC or laptop to generate and store the private key.

Third-party key management HSM products, such as RSA Certificate Manager, AEP Keyper, or Certicom Trust Infrastructure, offer enterprise key management options. There are a number of solutions, some combining hardware and software devices and systems. One of the advantages of this type of system is that the process is often automated, meaning that the keys cannot be compromised by human involvement.



AEP Networks Keyper Hardware Security Module

M-of-N Control

As with most other security systems, people are a weak point. Access to a key must be logged and audited and is typically subject to **M-of-N** control. M-of-N control means that of n number of administrators permitted to access the system, m must be present for access to be granted. M must be greater than 1 and N must be greater than M . For example, when $m=2$ and $n=4$, any two of four administrators must be present.



Another way to use M-of-N control is to split a key between several storage devices (say 3 USB sticks; any 2 of which could be used to recreate the full key).

Staff authorized to perform key management must be carefully vetted and due care should be taken if these employees leave the business.



Key Recovery Agents

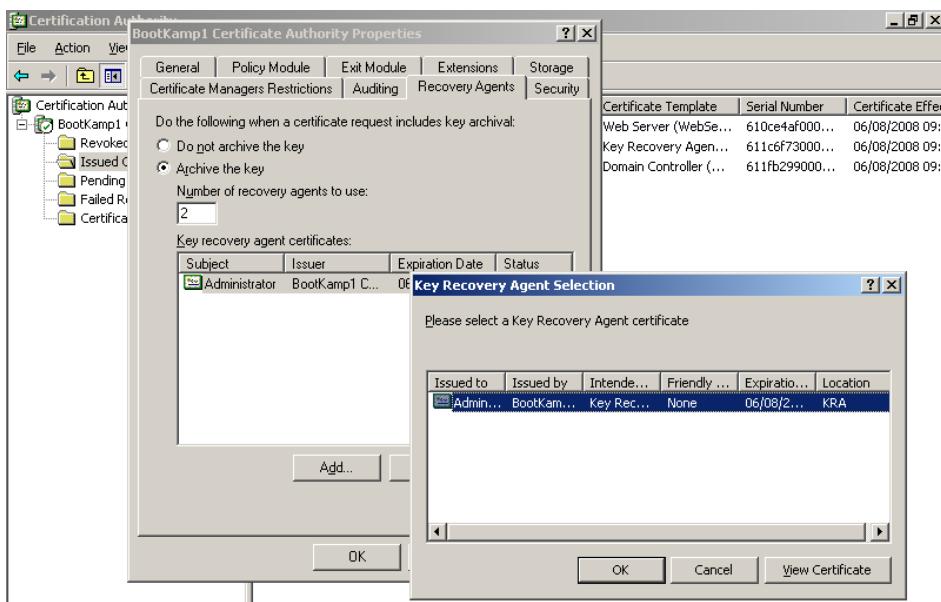
If the private key or secret used to encrypt data is lost or damaged, the encrypted data cannot be recovered unless a backup of the key has been made.

A significant problem with key storage is that if you make multiple backups of a private key, it is exponentially more difficult to ensure that the key is not compromised. On the other hand, if the key is not backed up, the storage system represents a single point of failure.

Key Recovery defines a secure process for backing up keys and/or recovering data encrypted with a lost key. This process might use "M of N" control to prevent unauthorized access to (and use of) the archived keys.

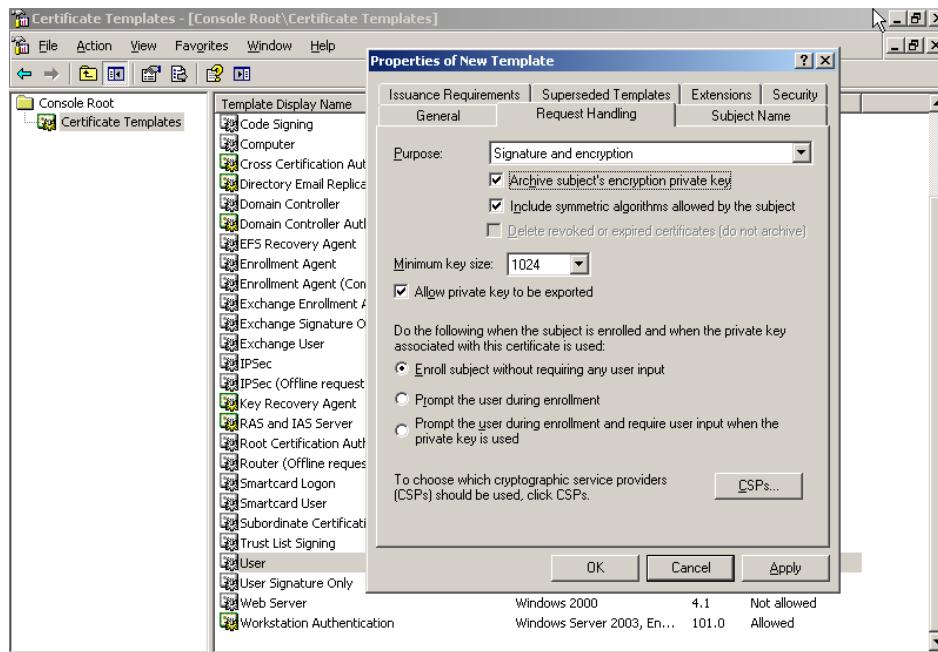
The general process to set up key recovery on a Windows Server CA is as follows:

- 1) Configure permissions to users or groups that can perform key recovery and publish the key recovery agent certificate.
- 2) Issue **Key Recovery Agents (KRA)** with Key Recovery Certificates.



Enabling key recovery in Windows Server Certificate Services

- 3) Enable key archival for the CA:
 - Specify the minimum number of KRAs required to perform recovery operations ("M of N" control)
 - Identify the KRAs with permission to recover the key
- 4) Create and publish certificate templates with archiving enabled.



Publishing a certificate template that allows key archival



Key Escrow

Escrow means that something is held independently. In terms of key management, this refers to archiving a key (or keys) with a third-party. This is a useful solution for organizations that don't have the capability to store keys securely themselves, but it invests a great deal of trust in the third-party.



Historically, governments have been sensitive about the use of encryption technology (clearly it is as useful to terrorists, criminals, and spies as it is to legitimate organizations). In the 1990s, the US government placed export controls on strong keys (128-bit and larger). It also tried to demand that all private keys were held in escrow, so as to be available to law enforcement and security agencies. This proposal was defeated by powerful counter arguments defending civil liberty and US commercial interests.



Key Status and Revocation

A key (or more typically a digital certificate) may be **revoked** or **suspended**.

- A revoked key is no longer valid and may not be "un-revoked".
- A suspended key may be re-enabled.

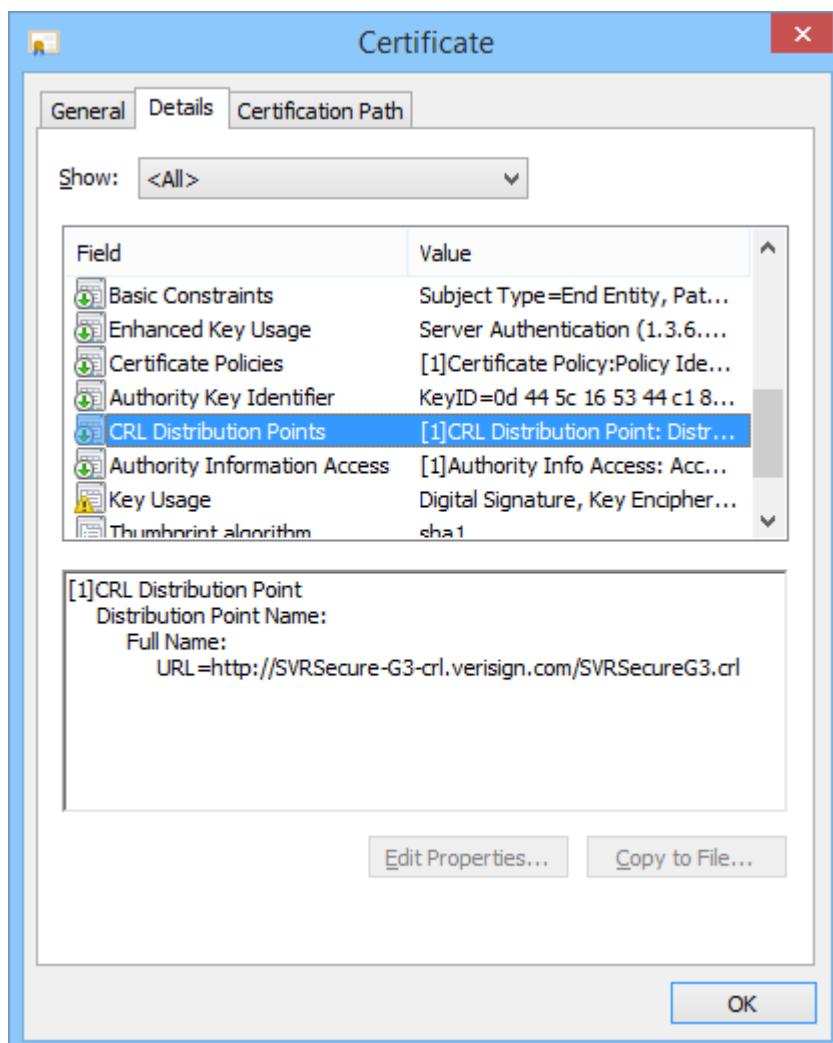
A certificate may be revoked or suspended by the owner or by the CA for many reasons. For example, the certificate or its private key may have been compromised, the business could have closed, a user could have left the company, a domain name could have been changed, the certificate could have been misused in some way, and so on.

These reasons are codified under the following choices:

- Unspecified (0)
- Key Compromise (1)
- CA Compromise (2)
- Affiliation Changed (3)
- Superseded (4)
- Cessation of Operation (5)
- Certificate Hold (6) [a suspended key]

CRLs and OCSP

It follows that there must be some mechanism for informing users whether a certificate is valid, revoked, or suspended. CAs must maintain a **Certificate Revocation List (CRL)** of all revoked and suspended certificates, which can be distributed throughout the hierarchy. A CRL has the following attributes:

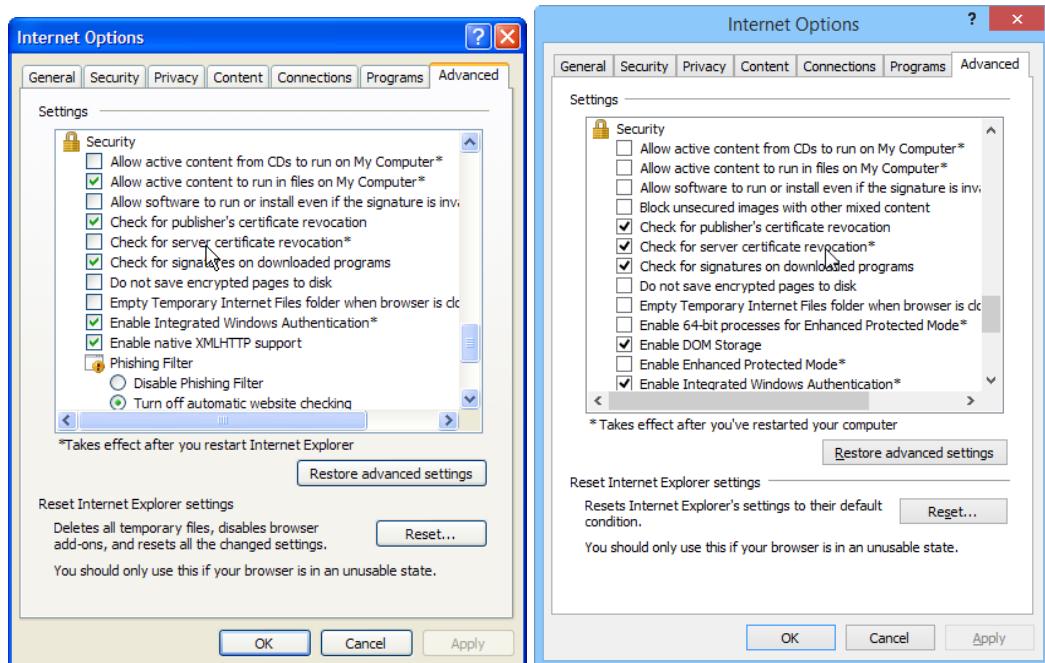


CRL Distribution Points should be defined in the certificate's fields

- Publish period - the date and time on which the CRL is published. Most CAs are set up to publish the CRL automatically.
- Distribution point(s) - the location(s) to which the CRL is published.
- Validity period - the period during which the CRL is considered authoritative. This is usually a bit longer than the publish period (for example, if the publish period was every 24 hours, the validity period might be 25 hours).
- Signature - the CRL is signed by the CA to verify its authenticity.

The publish period introduces the problem that a certificate might be revoked but still accepted by clients because an up-to-date CRL has not been published. Another problem is that the **CRL Distribution Point (CDP)** may not be included as a field in the certificate.

A further problem is that the browser (or other application) may not be configured to perform CRL checking.



Older versions of Internet Explorer are not configured to perform server CRL checking

Another means of providing up-to-date information is to check the certificate's status on an **Online Certificate Status Protocol (OCSP)** server, referred to as an **OCSP Responder**. Details of the OCSP responder service should be published in the certificate. OCSP is not always supported by browsers (Internet Explorer only supports OCSP for version 7+ for example).

Key Renewal

Typically a certificate is renewed *before* the old one expires. Where a user is in possession of a valid certificate, less administration is required in terms of checking identity than happens with a request for a new certificate.

When renewing a certificate, it is possible to use the existing key (referred to specifically as "key renewal") but this does not represent best practice. More typically, a new key is generated (the certificate is "re-keyed").

Expiration

When a key has expired, it is no longer valid or trusted by users. An expired key can either be archived or destroyed. Destroying the key offers more security but has the drawback that any data encrypted using the key will be unreadable. Whether a key is archived or destroyed will largely depend on what use the key was put to.

In software terms, a key can be destroyed by over-writing the data (deleting the data is not secure). A key stored on hardware can be destroyed by a specified erase procedure or by destroying the device.

PKI Trust Models



Another critical concept in PKI is the idea of the **trust model**. A trust model shows how users and different CAs are able to trust one another.

Single CA

In this simple model, a single CA issues certificates to users; users trust certificates issued by that CA and no other. The problem with this model is that it is restricted to users within a single organization and cannot model different relationships between user groups within a large organization.

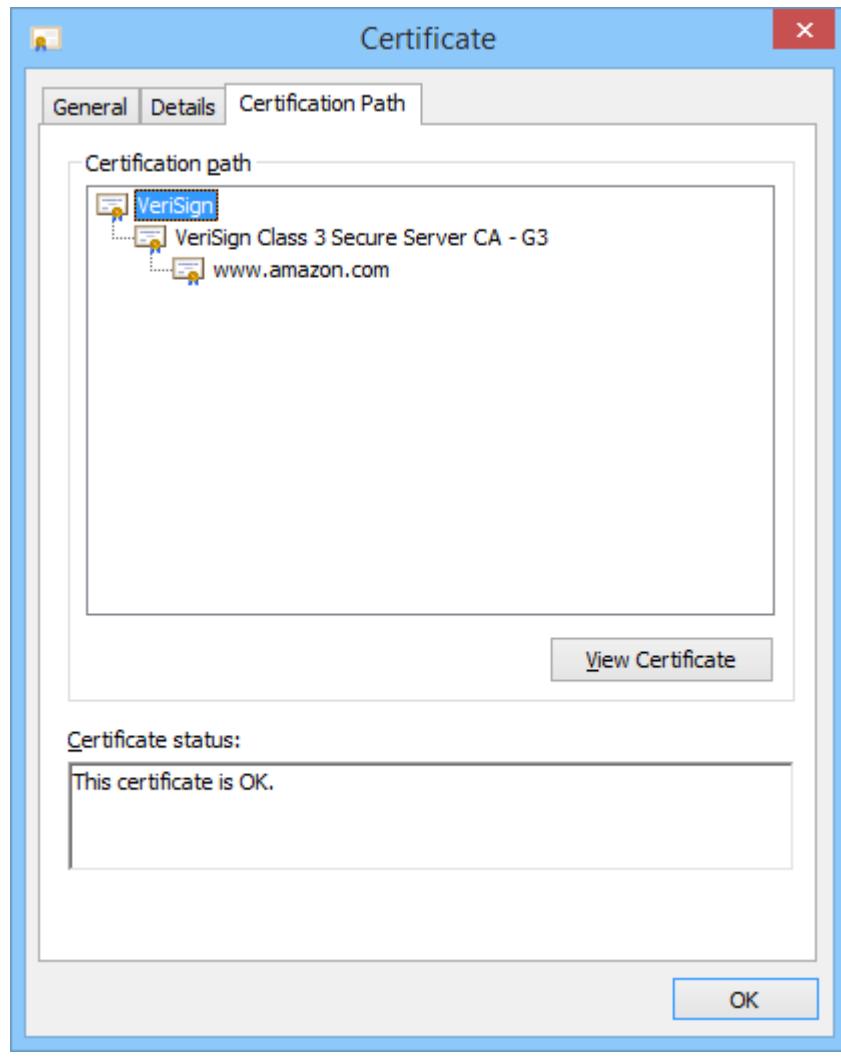
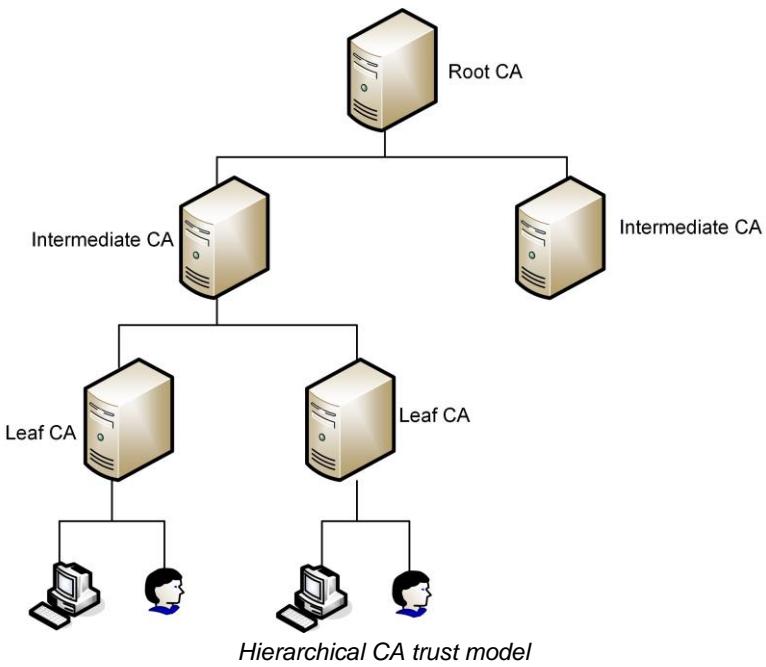
Hierarchical

In the hierarchical model, a single CA (called the **root**) issues certificates to a number of intermediate CAs. The intermediate CAs can issue certificates to leaf CAs, which can issue certificates to users. This model has the advantage that different CAs can be set up with different certificate policies, enabling users to perceive clearly what a particular certificate is designed for.

Each certificate can be traced back to the root CA along the **Certification Path**. The main problem with the hierarchical model is that the root is a single point of failure. If the root is damaged or compromised, the whole structure collapses.



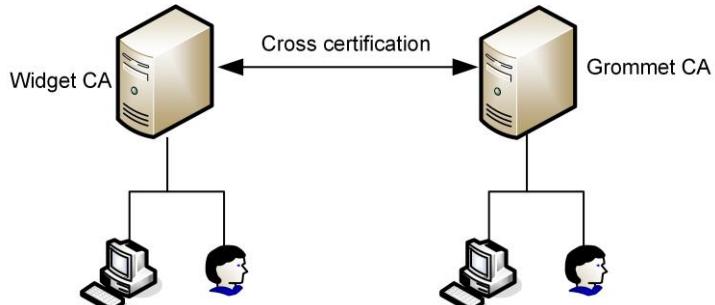
The root's certificate is self-signed. A secure configuration involves taking the root CA offline (that is, disconnecting it from any network). The drawback is that the CRL (see later) must be published manually. A useful way of creating an offline CA is to install the server as a Virtual Machine, archive the VM image to removable media, and store the media in a secure location (such as a safe).



Another problem is that there is limited opportunity for cross-certification, that is, to trust the CA of another organization. Two organizations could agree to share a root CA, but this would lead to operational difficulties that could only increase as more organizations join in.

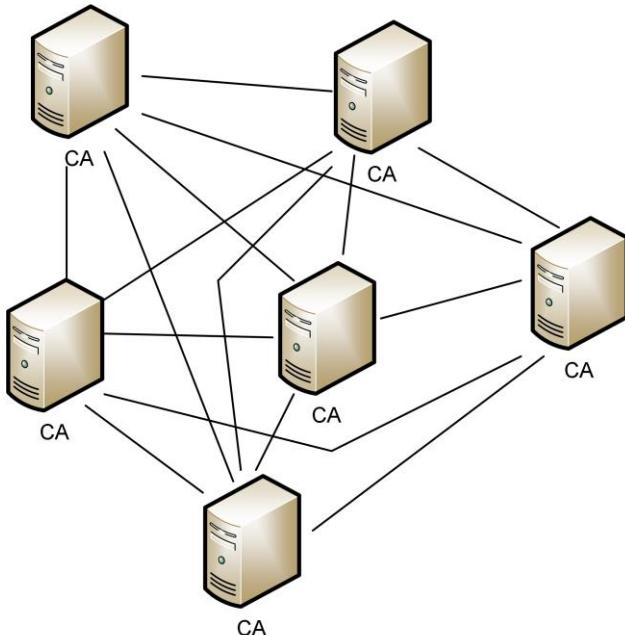
Mesh

This is one solution for cross-certifying CAs. Each root CA can issue certificates to other CAs in the mesh and trust certificates issued by these CAs. This can work well when only a few CAs are involved.



Cross certification - users in Widget and Grommet trust one another's certificates

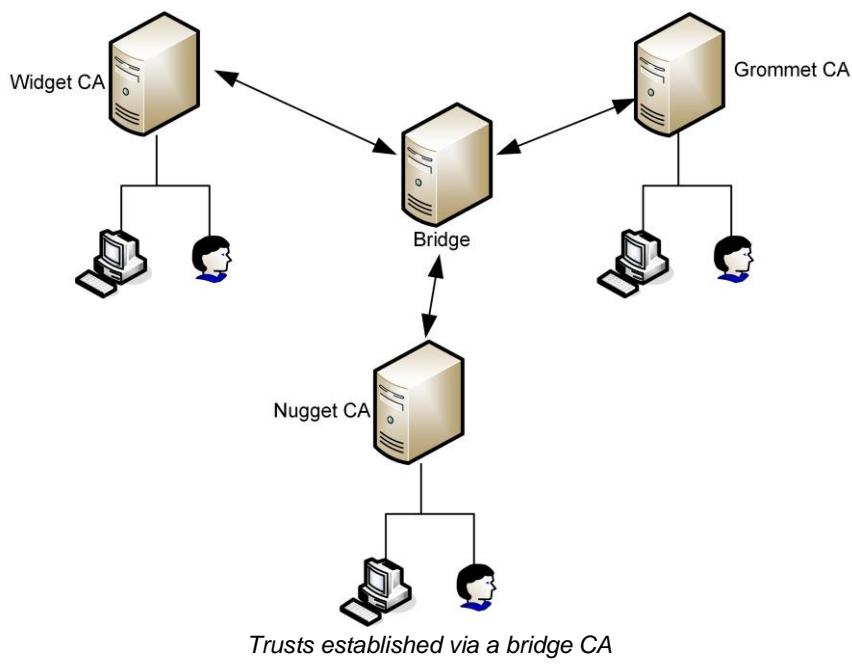
The problem with this solution is that it is not scalable to a large number of CAs. With each CA added, the number of cross-certifications that must be performed increases exponentially. It is more difficult to administer the mesh and ensure the security of all the CAs (one compromised CA would compromise the whole mesh).



Mesh relationships are not scalable

Bridge

The bridge model is an extension of the hierarchical model, developed by the Federal Bridge Certification Authority (FBCA). Here, root CAs can establish a trust relationship through an intermediate bridge CA.



Mutual Authentication

Certificates can be used for **one-way authentication**, where a server authenticates to a client. They can also be used in **mutual authentication**, where the server authenticates to the client and the client authenticates to the server. To set up mutual authentication, not only must the client trust the server's CA but the server must trust the client's CA. This would be accomplished using one of the trust models listed above.



The terms "server" and "client" are used in this description but note that such relationships would only generally be set up between two servers (for example, securing SMTP servers using SSL) or in peer-to-peer relationships. Maintaining secure certificates on workstations in a typical client-server network is usually too problematic to make mutual authentication worthwhile.

Web of Trust

Web of Trust is an alternative to PKI, rather than a PKI model itself. It is associated with the Pretty Good Privacy (PGP) system. In a web of trust, users sign one another's certificates. There is no central administration so the system has to be self-policing to weed out malicious users. Unlike the mesh PKI architecture, each user does not have to be certified by every other user (it is a **partial mesh**).



Another difficulty is for new users to build up a number of signatures. Key signing parties where users meet up to sign one another's keys in person are one way of getting round this.

The web of trust is useful for community and research groups but is not supported by commercial applications.

Cryptographic Standards

There are a number of standards for assessing the security of different encryption technologies and also for ensuring the interoperability and compatibility of such products when used on public networks such as the internet.



Protocols that use the different encryption technologies (such as IPsec, SSL/TLS, and SSH) are discussed [Unit 3.4](#) and [Unit 4.4](#).

Digital Certificates

As described above, digital certificates are based on the X.509 standard approved by the International Telecommunications Union. This standard is incorporated into the Internet Engineering Taskforce's [RFC 5280](#) and a number of related RFCs. The **Public Key Infrastructure (PKIX)** working group manages the development of these standards.

Public Key Cryptography Standards

RSA created a set of standards referred to as **PKCS (Public Key Cryptography Standards)** to promote the use of public key infrastructure. These standards help vendors to create security products that are interoperable. Most applications supporting certificate services do so via development toolkits created by PKI product vendors. Many of these depend in turn on the PKCS standards. The **PKIX Certificate Management Protocol (CMP)** provides a vendor-neutral implementation and also supports related PKCS standards. CMP is defined by [RFC 4210](#).

Some of the main standards are as follows:

- PKCS #1 - defines the properties of public/private key pairs and the algorithms for RSA encryption.
- PKCS #3 - defines Diffie-Hellman key agreement.
- PKCS #6 - the original (v1) standard for X.509 certificates. As noted above, the latest X.509 v3 standard is published as [RFC 5280](#).
- PKCS #7 - provides the basis for **S/MIME (Secure Multipart Internet Mail Extensions)**, allowing users to sign and encrypt email messages using digital certificates. S/MIME is published as the **Cryptographic Message Standard (CMS)** in [RFC 5652](#).
- PKCS #10 - format for requesting certificates from a CA.

FIPS

Federal Information Processing Standards (FIPS) are published by **NIST (National Institute of Standards and Technology)** for the US government. They define standards that must be adhered to for US federal government computer systems. These are often also adopted by commercial tenders and contracts.

FIPS 180 and FIPS 198

The **FIPS 198 Keyed-Hash Message Authentication Code (HMAC)** specifies the process of creating an HMAC to prove the integrity of a message. FIPS 180 defines the Secure Hash Algorithm (SHA) approved for creating HMACs.

FIPS 186

The **FIPS 186 Digital Signature Standard (DSS)** specifies requirements for digital signatures. The current version (FIPS 186-4) was released in 2013. The standard specifies the use of some variant of SHA to create a secure message digest and an asymmetric algorithm (DSA, RSA, or Elliptic Curve DSA [ECDSA]) to sign the message.

FIPS 140

The **FIPS 140** standard specifies requirements for cryptographic technologies, products, and protocols. The current version (FIPS 140-2) was released in May 2001. The standard designates validations for products at four security levels, with Level 4 being the highest. Vendors can have their products approved under the **Cryptographic Module Validation Program (CMVP)**. Testing and validation is performed by independent, accredited labs.

FIPS 201

FIPS 201 is a standard for identity verification of federal employees and contractors in order to gain access to federal facilities and information systems. This provides standards for biometric and smart card authentication.

Suite B

Suite B is a set of cryptographic algorithms mandated by the **National Security Agency (NSA)** for use by US government agencies. Suite A is an unpublished list of classified algorithms.

- Encryption (confidentiality) – AES-128 and AES-256.
- Digital Signature – ECDSA with 256- and 384-bit keys (Elliptic Curve algorithm).
- Key Exchange – Diffie Hellman with 256- and 384-bit keys.
- Cryptographic Hash – SHA-256 and SHA-384.

PGP / GPG

PGP stands for **Pretty Good Privacy**. It is a popular open standard for encrypting email communications and can also be used for file and disk encryption. It supports the use of a wide range of encryption algorithms.

PGP actually exists in two versions. The **PGP Corporation** develops a commercial product (now owned by Symantec). However PGP has also been ratified as an open internet standard with the name **OpenPGP** ([RFC 4880](#)). The principal implementation of OpenPGP is **Gnu Privacy Guard (GPG)**, which is available for Linux and Windows (gpg4win). The commercial and open versions of PGP are *broadly* compatible. In OpenPGP, for encrypting messages (symmetric encryption), you can use 3DES, CAST, Blowfish/Twofish, AES, or IDEA. For signing messages and asymmetric encryption, you can use RSA, DSA, or ElGamal. OpenPGP supports MD5, SHA, and RIPEMD cryptographic hash functions.

To use PGP, a user needs to install PGP software (usually available as a plugin for the popular mail clients). The user then creates his or her own certificate. In order to provide some verification that a certificate is owned by a particular user, PGP operates a **Web of Trust** model (essentially, users sign one another's certificates).

The contents of X.509 and PGP certificates are similar. The key difference is that PGP certificates can be signed by multiple users; X.509 certificates are signed by a single CA only. PGP certificates can also store more "friendly" information about the user (though this type of data could be added using attribute extensions to X.509 certificates). To generate a private key, the user must enter a passphrase. Obviously, the security of the certificate depends upon using a strong passphrase and keeping the phrase a secret. In order to generate a strong key, a passphrase should be longer than an ordinary password.

```
administrator@lamp:~$ gpg --gen-key
gpg (GnuPG) 1.4.10; Copyright (C) 2008 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
 (1) RSA and RSA (default)
 (2) DSA and Elgamal
 (3) DSA (sign only)
 (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 2048 bits
Please specify how long the key should be valid.
 0 = key does not expire
 <n> = key expires in n days
 <n>w = key expires in n weeks
 <n>m = key expires in n months
 <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N)
```



Review Questions / Module 2 / Unit 2 / Public Key Infrastructure

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What cryptographic information is stored in a digital certificate?
- 2) What does it mean if a certificate extension is marked as critical?
- 3) You are developing a secure web application. What sort of certificate should you request to show that you are the publisher of a program?
- 4) What are the weaknesses of a hierarchical trust model?
- 5) What trust model enables users to sign one another's certificates, rather than using CAs?
- 6) What options exist for creating a key repository?
- 7) What mechanism informs users about suspended or revoked keys?
- 8) What should be done before a certificate expires?
- 9) What does it mean if key recovery agent is subject to "M of N" control?
- 10) What does it mean if a cryptographic module is FIPS?



If you have access to the Hands On Live Labs, complete the "Cryptography / PKI Concepts" and "Cryptography / Certificate Management" labs now.

Module 2 / Unit 3

Password Authentication

Objectives

On completion of this unit, you will be able to:

- Describe the operation of and identify vulnerabilities in different authentication products and protocols:
 - LANMAN / NTLM
 - Kerberos
 - CHAP / PAP
- Describe effective password management policies.
- Summarize different types of attacks against passwords.

LAN Manager / NTLM



rxg3n

Most computer networks depend on "something you know" authentication using the familiar method of a user account protected by a password. A user account has three important properties:

- Username - a friendly name for the user to use when logging on to the system. This is often some combination of the user's first and last names or initials. The username does not have to be a secret, though it is unwise to reveal too much information to outsiders.



Generic or shared user accounts (administrator, root, or guest for instance) should usually be avoided as it makes auditing the actions of a particular person difficult.

- Password - this is a secret known only to the account holder used to authenticate against the account.
- Account ID - this is a unique identifier (usually numeric) by which the computer system manages the account. The important point is that if an account is deleted and then another account with the same username created, the new account will have a different ID and not have any of the permissions allocated to the old account.

There are many different ways of implementing account authentication on different computer systems and networks.

LAN Manager (LM) Authentication

LAN Manager (LM or LANMAN) was an NOS developed by Microsoft and 3Com. Microsoft used the authentication protocol from LM for Windows 9x networking. This protocol was later redeveloped as NTLM and NTLMv2. LM is a **challenge/response** authentication protocol. This means that the user's password is not sent to the server in plaintext.

- 1) When the server receives a logon request, it generates a random value called the challenge (or nonce) and sends it to the client.
- 2) Both client and server encrypt the challenge using the hash of the user's password as a key.
- 3) The client sends this response back to the server.
- 4) The server compares the response with its version and if they match, authenticates the client.



Note that the password hash itself is not transmitted over the network.

Passwords are stored using the 56-bit DES cryptographic function. This is not actually a true hash like that produced by MD5 or SHA but is intended to have the same sort of effect; the password is used as the secret key. In theory, this should make password storage secure, but the LM hash process is insecure for the following reasons:

- Alphabetic characters use the limited ASCII character set and are converted to upper case, reducing complexity.
- Maximum password length is 14 characters. Long passwords (over 7 characters) are split into two and encrypted separately; this means passwords that are 7 characters or less are easy to identify and makes each part of a longer password *more* vulnerable to brute force attacks.
- The password is not "salted" with a random value, making the ciphertext vulnerable to rainbow table attacks.



Refer back to [Unit 2..1](#) for information on cryptographic functions. Attacks against passwords are discussed later in this unit.

NTLM

The version of LM used for early versions of Windows NT fixed some of the problems in LM:

- The password is Unicode and mixed case and can be up to 127 characters long.
- The 128-bit MD4 hash function is used in place of DES.

NTLMv2

A substantially revised version of the protocol appeared in Windows NT4 SP4. While the basic process is the same, the responses are calculated differently to defeat known attacks against NTLM. An NTLMv2 response is an HMAC-MD5 hash (128-bit) of the username and authentication target (domain name or server name) plus the server challenge, a timestamp, and a *client* challenge. The MD4 password hash (as per NTLMv1) is used as the key for the HMAC-MD5 function.

NTLMv2 also defines other types of response that can be used in specific circumstances:

- LMv2 - provides "pass-through" authentication where the target server does not support NTLM but leverages the authentication service of a domain controller that does. LMv2 provides a mini-NTLMv2 response that is the same size as an LM response.
- NTLMv2 Session - provides stronger session key generation for digital signing and sealing applications (see the topic of "Kerberos" below for a discussion of the use of session keys).
- Anonymous - access for services that do not require user authentication (such as web servers).

LM / NTLM Vulnerabilities

The flaws in LM and NTLMv1 would normally be considered a historical curiosity as these mechanisms are obsolete, but one of the reasons that Windows password databases can be vulnerable to "cracking" is that they can store LM hash versions of a password for compatibility with legacy versions of Windows (pre Windows 2000). LM responses can also be accepted during logon (by default, the client sends both LM and NTLM responses) and therefore captured by a network sniffer.

If this compatibility is not required, it should be disabled, using the local or domain security policy (LMCompatibilityLevel or "LAN Manager Authentication Level"). Windows Vista/7 and Windows Server 2008 are the first products to ship with LM disabled by default.

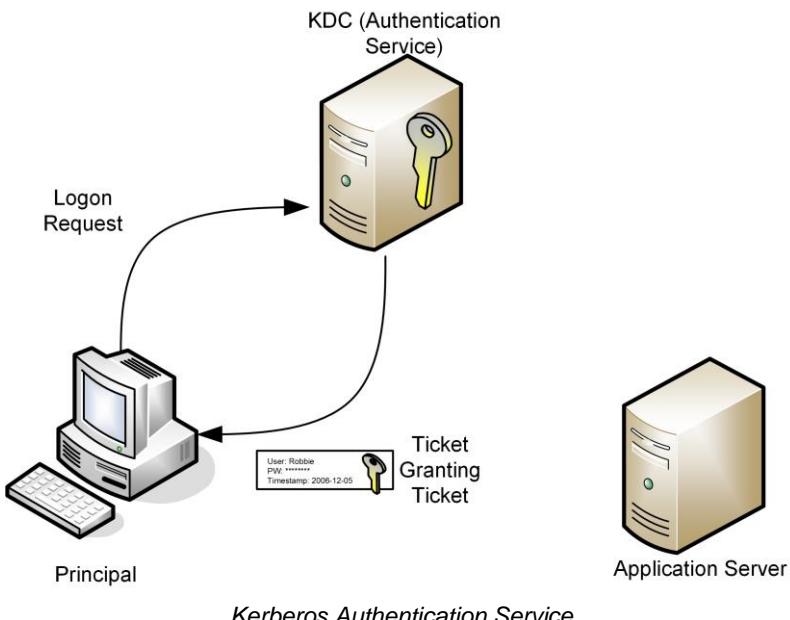
NTLM only provides for client authentication, making it vulnerable to Man-in-the-Middle attacks. Also, it does not support token or biometric authentication. For these reasons, Microsoft made Kerberos the preferred authentication protocol for Active Directory networks. NTLM is still the only choice for workgroups (non-domain networks). NTLMv2 should be used if possible. There are updates for Windows 9x clients (though not MS-DOS or Windows for Workgroups clients).

Kerberos



Kerberos is a network authentication protocol developed by the **Massachusetts Institute of Technology (MIT)** in the 1980s. The protocol has been ratified as a web standard by the IETF ([RFC 4120](#)). The idea behind Kerberos is that it provides a **single sign-on**. This means that once authenticated, a user is trusted by the system and does not need to re-authenticate to access different resources. The Kerberos authentication method was selected by Microsoft as the default provider for Windows 2000 (and later). Based on the Kerberos 5.0 open standard it provides authentication to Active Directory, as well as compatibility with other, non-Windows, operating systems.

Kerberos was named after the three-headed guard dog of Hades (Cerberus) because it consists of three parts. **Clients** request services from a **server**, which both rely on an intermediary - a **Key Distribution Center (KDC)** - to vouch for their identity. There are two services that make up a KDC: the **Authentication Service** and the **Ticket Granting Service**. The KDC runs on port 88 using TCP or UDP.



Kerberos Authentication Service

The **Authentication Service** is responsible for authenticating user logon requests. More generally, users *and* services can be authenticated; these are collectively referred to as principals. For example, when you sit at a Windows domain workstation and logon to the domain (Kerberos documentation refers to realms rather than domains, which is Microsoft's terminology), the first step of logon is to authenticate with a KDC server (implemented as a domain controller).

- 1) The client sends the AS a request for a **Ticket Granting Ticket (TGT)**. This is composed by encrypting the date and time on the local computer with the user's password hash as the key.



The password hash itself is not transmitted over the network.

- 2) If the user is found in the database and the request is valid (the user's password matches the one in the Active Directory database and the time matches to within 5 minutes of the server time), the AS responds with:
 - **Ticket Granting Ticket (TGT)** - this contains information about the client (name and IP address) plus a timestamp and validity period. This is encrypted using the *KDC's secret key*.
 - **TGS session key** for use in communications between the client and the *Ticket Granting Service (TGS)*. This is encrypted using a hash of the user's shared secret (password for instance).

The TGT is an example of a **logical token**. All the TGT does is identify who you are and confirm that you have been authenticated – it does not provide you with access to any domain resources.



The TGT (or user ticket) is time-stamped (under Windows they have a default maximum age of 10 hours). This means that workstations and servers on the network must be synchronized (to within 5 minutes) or a ticket will be rejected. This helps to prevent replay attacks.

Presuming the user entered the correct password, the client can decrypt the TGS session key but *not* the TGT. This establishes that the client and KDC know the same shared secret and that the client cannot interfere with the TGT.

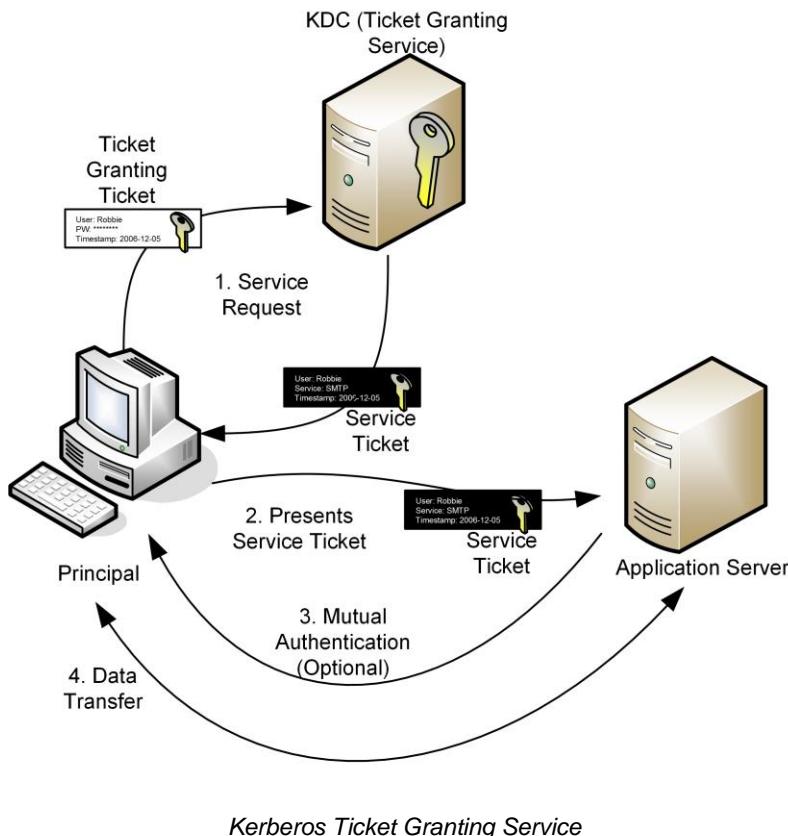
To access resources within the domain, the client requests a **Service Ticket** (a token that grants access to a target application server). This process of granting service tickets is handled by the **Ticket Granting Service (TGS)**.

- 3) The client sends the TGS a copy of its TGT and the name of the application server it wishes to access plus an authenticator, consisting of a time-stamped client ID encrypted using the TGS session key.

The TGS should be able to decrypt both messages using the KDC's secret key for the first and the TGS session key for the second. This confirms that the request is genuine (it also checks that the ticket has not expired and has not been used before [replay attack]).

- 4) The TGS service responds with:

- **Service session key** - for use between the client and the *application server*. This is encrypted with the TGS session key.
 - **Service ticket** - containing information about the user (such as a timestamp, system IP address, SID [Security Identifier] and the SIDs of groups they belong) and the service session key. This is encrypted using the *application server's secret key*.
- 5) The client forwards the service ticket, which it cannot decrypt, to the application server and adds another time-stamped authenticator, which is encrypted using the service session key.



Kerberos Ticket Granting Service

- 6) The application server decrypts the service ticket to obtain the service session key using its secret key, confirming that the client has sent it an untampered message. It then decrypts the authenticator using the service session key.
- 7) Optionally, the application server responds to the client with the timestamp used in the authenticator, encrypted using the service session key. The client decrypts the timestamp and finds that it matches the value already sent and can conclude that the application server is trustworthy.

This means that the server is authenticated to the client (referred to as **mutual authentication**). This prevents a **Man-In-the-Middle** style attack where a malicious user could intercept communications between the client and server.

- 8) The server now responds to client requests (assuming they conform to the server's access control list).



The data transfer itself is not encrypted (at least as part of Kerberos; some sort of transport encryption can be deployed).

One of the noted drawbacks of Kerberos is that the KDC represents a single point-of-failure for the network. In practice, backup KDC servers can be implemented (for example, Active Directory supports multiple domain controllers, each of which will be running the KDC service).

Kerberos can be implemented with a number of different algorithms: DES (56-bit), RC4 (128-bit), or AES (128-bit or better) for session encryption and the MD5 or SHA-1 hash functions. AES is supported under Kerberos v5 but in terms of Microsoft networking, only Windows Server 2008/2012 and Windows Vista/7/8 support it. A suitable algorithm is negotiated between the client and the KDC. The secret keys used to secure Kerberos authentication packets are generally derived from passwords rather than randomly generated; therefore care must be taken to choose strong passwords.

PAP and CHAP



A number of authentication protocols have been developed to work with remote access protocols.

Password Authentication Protocol

The **Password Authentication Protocol (PAP)** is unsophisticated authentication method developed as part of the TCP/IP **Point-to-Point Protocol (PPP)**, used to transfer TCP/IP data over serial or dial-up connections. It relies on clear text password exchange and is therefore obsolete for the purposes of any sort of secure connection. It is defined in [RFC 1334](#).

Challenge Handshake Authentication Protocol

The **Challenge Handshake Authentication Protocol (CHAP)** was also developed as part of PPP as a means of authenticating users over a remote link. It is defined in [RFC 1994](#). CHAP relies on an encrypted challenge in a system called a **three-way handshake**.

- 1) **Challenge** - the server challenges the client, sending a randomly generated challenge message.
- 2) **Response** - the client responds with a hash calculated from the server challenge message and client password.
- 3) **Verification** - the server performs its own hash using the password stored for the client. If it matches the response then access is granted; otherwise the connection is dropped.

The handshake is repeated with a *different* challenge message periodically during the connection (though transparently to the user). This guards against replay attacks (where a previous session could be captured and reused to gain access).

CHAP typically provides one-way authentication only. Cisco's implementation of CHAP (for example) allows for mutual authentication by having both calling and called routers challenge one another. This only works between two Cisco routers however. Microsoft's implementation of CHAP for Windows 2000 (and later) - MS CHAPv2 - also supports mutual authentication.



Password Protection

Password-based authentication methods are prone to user error. A **password management policy** instructs users on best practice in choosing and maintaining passwords. More generally, a password management policy should instruct users on how to keep their authentication method secure (whether this be a password, smart card, or biometric ID). The password management policy also needs to alert users to different types of social engineering attacks.

The "soft" approach to training users can also be backed up by "hard" policies defined on the network. For example, Windows security policies allow the administrator to define such things as password complexity, re-use of passwords, account lockouts, and so on.

Compliance can be enforced by "ethical" hacker methods. These use personnel and software to try to simulate different network attacks, such as scanning for insecure passwords.

Strong Passwords

The following rules enforce password complexity and make them difficult to guess or compromise:

- Length - the longer a password, the stronger it is:
 - A typical strong network password should be 8-14 characters
 - A longer password or passphrase might be used for mission critical systems or devices where logon is infrequent
- No single words - better to use word and number / punctuation combinations.
- No obvious phrases in a simple form - birthday, username, job title, and so on.
- Mix upper and lowercase (assuming the software uses case-sensitive passwords).
- Use an easily memorized phrase - underscored characters or hyphens can be used to represent spaces if the operating system does not support these in passwords.
- Do not write down a password or share it with other users.



If users must make a note of passwords, at the very least they must keep the note physically secure. They should also encode the password in some way. If the note is lost or stolen it is imperative that the password be changed immediately and the user account closely monitored for suspicious activity.

- Change the password periodically (password aging):
 - User passwords should be changed every 60-90 days
 - Administrative passwords should be changed every 30 days
 - Passwords for mission critical systems should be changed every 15 days



Another concern is personal password management. A typical user might be faced with having to remember tens of logons for different services and resort to using the same password for each. This is very insecure, as your security becomes dependent on the security of these other (unknown) organizations. Users must be trained to practice good password management (at the least not to re-use work passwords).



w4gmn

Password Attacks

When a user chooses a password, the password is converted to a hash using a cryptographic function, such as MD5 or SHA. This means that (in theory) no one except the user (not even the system administrator) knows the password as the plaintext should not be recoverable from the hash.

Most **password cracking** software works on the basis of exploiting known vulnerabilities in password transmission and storage algorithms (LM and NTLM hashes for instance). They can perform "brute force" attacks and use precompiled dictionaries and rainbow tables (see below) to break naively chosen passwords.

A password cracker can work on a database of hashed passwords. The following locations are used to store passwords:

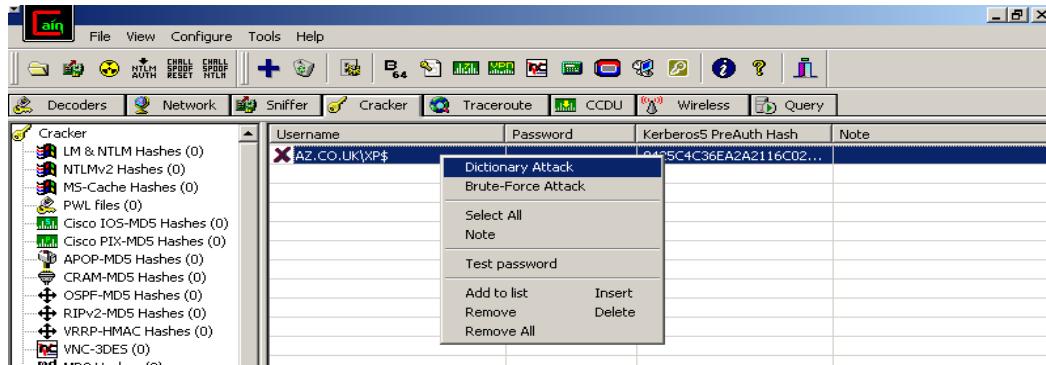
- %SystemRoot%\System32\config\SAM - local users and passwords (Security Account Manager) are stored as part of the Registry on Windows machines.
- %SystemRoot%\NTDS\NTDS.DIT - domain users and passwords are stored in the Active Directory database on domain controllers.
- On Linux, user account details and encrypted passwords are stored in /etc/passwd but this file is universally accessible. Consequently, passwords are sometimes moved to /etc/shadow, which is only readable by the root user.

Alternatively a packet sniffer might be used to obtain the client response to a server challenge in a protocol such as NTLM or CHAP/MS-CHAP. While these protocols avoid sending the hash of the password directly, the response is derived from the password hash in some way. Password crackers can exploit weaknesses in a protocol to calculate the hash and match it to a dictionary word or brute force it.

Password Crackers

Some well-known password cracking tools include:

- Cain and Abel - Windows password recovery with password sniffing utility.



Cain and Abel password cracker

- John the Ripper - multi-platform password hash cracker.
- THC Hydra - often used against remote authentication (protocols such as Telnet, FTP, HTTPS, SMB, and so on).
- Aircrack - sniffs and decrypts WEP and WPA wireless traffic.
- L0phtcrack - one of the best known Windows password recovery tools. There is also an open source version (ophcrack).

Brute Force Attack

A **brute force attack** attempts every possible combination in the key space in order to derive a plaintext (in this case the password) from a ciphertext (the hash). The key space is determined by the number of bits used (the length of the key). In theory, the longer the key, the more difficult it is to compute each value, let alone check whether the plaintext it produces is a valid password. Selecting a suitable key length with a strong password mitigates against brute force attacks. Other wise precautions include restricting the number of logon attempts and changing passwords periodically.



Note that restricting logons can be turned into a vulnerability as it exposes you to Denial of Service attacks. The attacker keeps trying to authenticate, locking out valid users.



Also be aware of horizontal brute force attacks. This means that the attacker chooses one or more common passwords ("password" or "123456" for instance) and tries them in conjunction with multiple usernames.

Dictionary and Rainbow Table Attacks

A **dictionary attack** can be used where there is a good chance of guessing the likely value of the plaintext (for instance, a non-complex password). Rather than attempting to compute every possible value, the software enumerates values in the dictionary. **Rainbow tables** refine the dictionary approach. The technique was developed by Phillip Oechslin and used in his Ophcrack Windows password cracker. The attacker uses a precomputed lookup table of all possible passwords and their matching hashes. Not all possible hash values are stored as this would require too much memory. Values are computed in "chains" and only the first and last values need to be stored. The hash value of a stored password can then be looked up in the table and the corresponding plaintext discovered.

Hash functions can be made more secure by adding salt! Salt is a random value added to the plaintext. This helps to slow down rainbow table attacks against a hashed password database, as the table cannot be created in advance and must be recreated for each combination of password and salt value. Rainbow tables are also impractical when trying to discover long passwords (over about 14 characters). UNIX and Linux password storage mechanisms use salt but Windows does not. Consequently in a Windows environment it is even more important to enforce password policies, such as selecting a strong password and changing it periodically.

Hybrid Attack

A **hybrid password attack** uses a combination of dictionary and brute force attacks. It is principally targeted against "naively strong" passwords, such as **james1**. The password cracking algorithm tests dictionary words and names in combination with a number of numeric prefixes and/or suffixes. Other types of algorithms can be applied, based on what hackers know about how users behave when forced to select complex passwords that they don't really want to make hard to remember. Other examples might include substituting "s" with "5" or "o" with "0".

Birthday Attack

A **birthday attack** is a type of brute force attack aimed at exploiting **collisions** in hash functions. A collision is where a function produces the *same* hash value for two *different* plaintexts. This type of attack can be used for the purpose of forging a digital signature. The attack works as follows: the attacker creates a malicious document and a benign document that produce the same hash value. The attacker submits the benign document for signing by the target. The attacker then removes the signature from the benign document and adds it to the malicious document, forging the target's signature. The trick here is being able to create a malicious document that outputs the same hash as the benign document. The birthday paradox means that the computational time required to do this is much less than might be expected.

The birthday paradox asks how large a group of people must be so that the chance of two of them sharing a birthday is 50%. The answer is 23, but people that are not aware of the paradox often answer around 180 ($365/2$).

The point is that the chances of someone sharing a *particular* birthday are small but the chances of any two people sharing *any* birthday get better and better as you add more people: $1 - (365 * (365-1) * (365 - 2) \dots * (365 - (N-1)) / 365^N)$

To exploit the paradox, the attacker creates multiple malicious and benign documents, both featuring minor changes (punctuation, extra spaces, and so on). Depending on the length of the hash, if the attacker can generate sufficient variations then the chance of matching hash outputs can be better than 50%. Also, far fewer variations on the message have to be discovered than in a pure brute force attack (launched by testing every *possible* combination). This means that to protect against the birthday attack, encryption algorithms must demonstrate collision avoidance (that is, to reduce the chance that different inputs will produce the same output). This method has been used successfully to exploit collisions in the MD5 function to create fake SSL certificates that appear to have been signed by a trusted root CA.

This type of attack cannot be used to crack password hashes directly. It is conceivable that an attacker could work out a hash that allows two different passwords to be used to access an account simultaneously.



Weak Key Attacks and Key Stretching

A key may be generated from a password. If the password is weak, an attacker may be able to guess or crack the password to derive the key. Also, the plain fact is that even a strong password is not a particularly good seed for a large key. A more secure method of creating a key is through the generation of a large, random (or pseudorandom) number. This is obviously not a solution for user passwords however. It is also not a trivial problem to design a random number generator that isn't vulnerable to cryptanalysis.

Another technique is to make the key generated from a user password stronger by - basically - mucking about with it lots of times. This is referred to as **key stretching**. The initial key may be put through thousands of rounds of hashing. This might not be difficult for the attacker to replicate so doesn't actually make the key stronger, but it slows the attack down as the attacker has to do all this extra processing for each possible key value. Key stretching can be performed by using a particular software library to hash and save passwords when they are created. Two such libraries are:

- **bcrypt** - an extension of the crypt UNIX library for generating hashes from passwords. It uses the Blowfish cipher to perform multiple rounds of hashing.
- **Password-Based Key Derivation Function 2 (PBKDF2)** - part of RSA security's public key cryptography standards (PKCS#5).

Another instance of a weak key is one that causes the cipher to malfunction. If a cipher produces weak keys, the technology using the cipher should prevent use of these keys. DES, RC4, IDEA, and Blowfish are examples of algorithms known to have weak keys. The way a cipher is implemented in software may also lead to weak keys being used. An example of this is a bug in the pseudorandom number generator for the OpenSSL server software for Debian Linux (discovered in 2008).



Review Questions / Module 2 / Unit 3 / Password Authentication

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) How are cryptographic systems protected against brute force attacks?
- 2) Why might a standalone installation of Windows XP be more vulnerable to password cracking than in Windows 7?
- 3) What key features are provided by Kerberos?
- 4) True or false? In order to create a service ticket, Kerberos passes the user's password to the target application server for authentication.
- 5) Why might forcing users to change their password every month be counterproductive?
- 6) A user maintains a list of commonly used passwords in a file located deep within the computer's directory structure. Is this secure password management?
- 7) Your company creates software that requires a database of stored encrypted passwords. What security control could you use to make the password database more resistant to brute force attacks?
- 8) In what scenario would PAP be an appropriate cryptographic method?



If you have access to the Hands On Live Labs, complete the "Application Data / Application Security" lab now.

Module 2 / Unit 4

Strong Authentication

Objectives

On completion of this unit, you will be able to:

- Describe the features of token-based and biometric authentication.
- Describe the operation of and identify vulnerabilities in different authentication products and protocols:
 - EAP / PEAP / LEAP
 - RADIUS
 - TACACS+
 - TOTP / HOTP
- Understand the use of federated identification and authentication services.

Token-based Authentication

The weaknesses inherent in relying on user-chosen passwords have prompted the development of other authentication factors. These are principally token-based and biometric methods.

There are various ways to authenticate a user based on something they have (a **token**). Typically this might be a smart card, USB token, or key fob that contains a chip with authentication data, such as a **digital certificate**.



Digital certificates are an encryption technology. See [Unit 2.1](#) for more information about cryptography.

Smart Cards

A **smart card** is a credit card-sized device with an integrated chip and data interface. Cards are either **contact-based**, meaning that it must be physically inserted into a reader, or **contactless**, meaning that data is transferred using a tiny antenna embedded in the card.

The ISO have published various ID card standards to promote interoperability, including ones for smart cards (ISO 7816 for contact and ISO 14443 for contactless types).

The card reader or scanner can either be built into a computer or connected as a USB peripheral device. A software interface is then required to read (and possibly write) data to the card. The software should comply with the PKCS#11 API standard. The latest generation of cards can generate their own keys, which is more secure than programming the card through software.



GemPlus USB smart card reader (courtesy GemPlus image library)

When the card is read, the card software prompts the user for a **Personal Identification Number (PIN)** or password, which mitigates the risk of the card being lost or stolen. This is called Two-Factor Authentication: something you have (the card) and something you know (the PIN).

Password Manager

A **password manager** (or sign-on manager or password filler) is a device combined with some sort of support software that provides single sign-on for applications that do not support other architectures, such as Kerberos. The device provides encrypted storage of user IDs and passwords. The software intercepts an application's request for a password and submits the user's credentials on their behalf.

One-time Password Tokens



RSA SecurID key fob token generator

A **One-time Password (OTP)** is one that is generated automatically (rather than being selected by a user) and used only once. Consequently it is not vulnerable to password guessing or sniffing attacks. An OTP is generated using some sort of hash function on a secret value plus a synchronization value (seed), such as a timestamp or counter. Other options are to base a new password on the value of an old password or use a random challenge value (nonce) generated by the server.

This sort of authentication device is typified by the SecurID token from RSA. The device generates a passcode based on the current time and a secret key coded into the device. An internal clock is used to keep time and must be kept precisely synchronized to the time on the authentication server. The code is entered along with a PIN or password known only to the user, to protect the system against loss of the device itself.

Open Authentication (OATH)



The **Initiative for Open Authentication (OATH)** is an industry body comprising mostly the big PKI providers, such as Verisign and Entrust, set up with the aim of developing an open strong authentication framework. "Open" means a system that any enterprise can link into to perform authentication of users and devices across different networks. "Strong" means that the system is based not just on passwords but on 2- or -3-factor authentication.

OATH has developed two algorithms for implementing **One Time Passwords (OTP)** on the web.

HMAC-based One-time Password Algorithm (HOTP)

HMAC-based One-time Password Algorithm (HOTP) is an algorithm for token-based authentication. HOTP is defined by [RFC 4226](#).

The authentication server and client token are configured with the same shared secret. This should be an 8-byte value generated by a cryptographically strong random number generator. The token could be a fob-type device or implemented as a smartphone app. The shared secret can be transmitted to the smartphone app as a QR code image acquirable by the phone's camera so that the user doesn't have to type anything. Obviously it is important that no other device is able to acquire the shared secret.

The shared secret is combined with a counter to create a one-time password when the user wants to authenticate. The device and server both compute the hash and derive an HOTP value that is 6-8 digits long. This is the value that the user must enter to authenticate with the server. The counter is incremented by one.



The server will be configured with a counter window to cope with the circumstance that the device and server counters move out of sync. This could happen if the user generates an OTP but does not use it for instance.

Time-based One-time Password Algorithm (TOTP)

The **Time-based One-time Password Algorithm (TOTP)** is a refinement of the HOTP. One issue with HOTP is that tokens can be allowed to persist unexpired, raising the risk that an attacker might be able to obtain one and decrypt data in the future.

In TOTP, the HMAC is built from the shared secret plus a value derived from the device's and server's local timestamps. TOTP automatically expires each token after a short window (60 seconds for instance). For this to work, the client device and server must be closely time-synchronized. TOTP is defined by [RFC 6238](#).

One well-known implementation of HOTP and TOTP is Google Authenticator.

Token-based Authentication Vulnerabilities

The main concerns with "something you have" technologies are loss and theft and the chance that the device can be counterfeited. Token-based security can be strengthened by linking device usage to some sort of biometric authentication (for example, incorporating a fingerprint reader on a smart card). In conjunction with a PIN, this provides three-factor authentication.

There are also equipment and maintenance costs. Token-based authentication is not always standards-based, so interoperability between products can be a problem.

Biometric Authentication

"Something you are" authentication means employing some sort of **biometric** recognition system. Many types of biometric information can be recorded, including fingerprint patterns, signature recognition, iris or retina recognition, or facial recognition. The first step in setting up biometric authentication is **enrollment**. The chosen biometric information is scanned by a **biometric reader** and converted to binary information. There are generally two steps in the scanning process:

- A **sensor module** acquires the biometric sample from the target.
- A **feature extraction module** records the significant information from the sample (features that uniquely identify the target).

There are various ways of deploying biometric readers. Most can be installed as a USB peripheral device. Some types (fingerprint readers) can be incorporated on a laptop or mouse chassis. Others are designed to work with entry systems.

The biometric **template** is recorded in a database stored on the authentication server. When the user wants to access a resource, s/he is re-scanned and the scan is compared to the template. If they match to within a defined degree of tolerance, access is granted.

Security of the template and storage mechanism is a key problem for biometric technologies.

- It should not be possible to use the template to reconstruct the sample.
- The template should be tamper-proof.
- Unauthorized templates should not be "injected".

Standard encryption products cannot be used as there needs to be a degree of "fuzzy" pattern matching between the template and the confirmation scan. Vendors have developed proprietary **biometric cryptosystems** to address security.

A corollary of the development of biometric cryptosystems is to use biometric information as the key when encrypting other data. This solves the template storage problem and the problem of secure key distribution (the person is the key) but not the one of pattern matching (that is, will the same biometric sample always produce the same key and if not, how would encrypted data be recovered?)

Another problem is that of dealing with templates that have been compromised; that is, how can the genuine user be re-enrolled with a new template (**revocability**)? One possible solution is to employ steganography to digitally watermark each enrollment scan. Another is to "salt" each scan with a random value or a password.

Biometric Technologies

As mentioned above, a number of different metrics exist for identifying people. These can be categorized as **physical** (fingerprint, eye, and facial recognition) or **behavioral** (voice, signature, and typing pattern matching).

The main problems with biometric technology generally are:

- Users can find it intrusive and threatening to privacy.
- The technology can be discriminatory or inaccessible to those with disabilities.
- Setup and maintenance costs.
- The chance that the technology can be counterfeited.
- Susceptibility to errors:
 - False negatives (where a legitimate user is not recognized); referred to as the False Rejection Rate (FRR) or Type I error.
 - False positives (where an interloper is accepted); referred to as the False Acceptance Rate (FAR) or Type II error.
 - False negatives cause inconvenience to users but false positives can lead to security breaches, and so is usually considered the most important metric.
 - The Crossover Error Rate (CER) is another metric by which biometric technologies are judged. The CER is the point at which FRR and FAR meet. The lower the CER, the more efficient and reliable the technology.
- Throughput (speed) - this refers to the time required to create a template for each user and the time required to authenticate. This is a major consideration for high traffic access points, such as airports or railway stations.

Fingerprint Recognition

Fingerprint recognition is the most widely implemented biometric technology. A fingerprint is a unique pattern and so lends itself to authentication. The technology required for scanning and recording fingerprints is relatively cheap and the process quite straightforward. Scanning devices are easy to implement, with scanners incorporated on laptop chassis, mice, keyboards, smartphones, and so on. The technology is also simple to use and non-intrusive, though it does carry some stigma from association with criminality. Reader and finger also need to be kept clean!



Microsoft IntelliMouse with fingerprint reader

Security can be defeated by fake fingers, though obviously this would require the most determined and well-resourced attacker. High-end scanners can detect whether the print comes from a real finger (that is, supplied with warm blood!)

A similar option is hand- or palmprint recognition, but this is considered less reliable and obviously requires bulkier devices.

Eye Recognition

There are two types of **eye recognition**:

- Retinal scan - an infrared light is shone into the eye to identify the pattern of blood vessels. Retinal patterns are very secure but the equipment required is expensive and the process is relatively intrusive and complex. False negatives can be produced by disease, such as cataracts.
- Iris scan - this matches patterns on the surface of the eye and so is less intrusive than retinal scanning (the subject can continue to wear glasses for instance) and a lot quicker. Iris scanning is the technology most likely to be rolled out for high-volume applications, such as airport security.

Facial Recognition

Where fingerprint and eye recognition focus on one particular feature, **facial recognition** records multiple key indicators about the size and shape of the face. The initial pattern needs to be recorded under optimum lighting conditions; depending on the technology this can be a lengthy process.

Again, this technology is very much associated with law enforcement, and is the most likely to make users uncomfortable about the personal privacy issues. Much of the technology development is in surveillance, rather than for authentication.

Behavioral Technologies

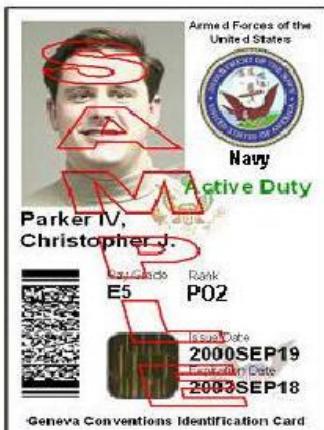
Behavioral technologies (sometimes classified as "Something you do") are often cheap to implement but tend to produce more errors than scans based on physical characteristics. They can also be discriminatory against those with disabilities:

- Voice - this is relatively cheap as the hardware and software required are built into many standard PCs and laptops. However, obtaining an accurate template can be difficult and time-consuming. Background noise and other environmental factors can also interfere with log on. Voice is also subject to impersonation.
- Signature - everyone knows that signatures are relatively easy to duplicate, but it is less easy to fake the actual signing process. Signature matching records the user making their signature (stroke, speed, and pressure of the stylus).
- Typing - this matches the speed and pattern of user input of a passphrase.

Common Access Card

Identification is the problem of issuing authentication credentials to the correct person and of ensuring that the authorized person is using the credentials. In a password-based system, you have to trust that the password is known only to the authorized person. In a token-based system, you have to ensure that the token can only be used by the authorized person.

In the US, the **Homeland Security Presidential Directive 12 (HSPD-12)** mandated that access to Federal property must be controlled by a secure identification and authentication mechanism (as defined in the FIPS-201 standard). As a result of this, two identity cards have been introduced:



Common Access Card

- **Common Access Card (CAC)** - issued to military personnel, civilian employees, and contractors to gain access to Department of Defense (DoD) facilities and systems.
- **Personal Identification Verification (PIV) Card** - for civilian Federal Government employees and contractors.

These cards allow the user to authenticate using a token (the card is a smart card) and passcode but the card also contains Personally Identifiable Information, including a photograph of the holder.

Other identity documents produced include the First Responder Access Credential (FRAC) - for emergency services personnel to gain access to Federal buildings during an emergency - and the ePassport (a passport with an embedded smart card).

Extensible Authentication Protocol



The **Extensible Authentication Protocol (EAP)** is designed to replace CHAP. It is defined in [RFC 3748](#). The protocol is designed to support different types of authentication; it defines a framework for negotiating authentication mechanisms rather than the details of the mechanisms themselves. Widely adopted now, vendors can write extensions to the protocol to support third-party security devices. EAP implementations can include smart cards, one-time passwords, biometric scanning, or simpler username and password combinations. EAP involves three components:

- **Supplicant** - this is the client requesting authentication.
- **Authenticator** - this is the device that receives the authentication request (such as a remote access server or wireless access point). The authenticator establishes a channel for the supplicant and authentication server to exchange credentials using the EAP over LAN (EAPoL) protocol. It blocks any other traffic.
- **Authentication Server** - the server that performs the authentication (typically an AAA server).



RADIUS and TACACS+ provide Authentication, Authorization, and Accounting (AAA) services. These protocols are covered later in this unit.

Some popular implementations of EAP are described below.

EAP-TLS

EAP-TLS ([RFC 5216](#)) is currently considered the strongest type of authentication and is very widely supported. An encrypted Transport Layer Security (TLS) tunnel is established between the supplicant and authentication server using public key certificates on the authentication server and supplicant.

As *both* supplicant and server are configured with certificates, this provides mutual authentication. The supplicant will typically provide a certificate using a smart card or a certificate could be installed on the client PC, possibly in a Trusted Platform Module (TPM).



Certificates are covered in [Unit 2.2](#). See [Unit 4.3](#) for more information about TLS.

Protected Extensible Authentication Protocol (PEAP)

In **Protected Extensible Authentication Protocol (PEAP)**, as with EAP-TLS, an encrypted tunnel is established between the supplicant and authentication server but PEAP only requires a server-side public key certificate. The supplicant does not require a certificate. With the server authenticated to the supplicant, user authentication can then take place through the secure tunnel with protection against sniffing, password-guessing/dictionary, and Man-in-the-Middle attacks. There are two versions of PEAP, each specifying a different user authentication method (also referred to as the "inner" method):

- PEAPv0 (EAP-MSCHAPv2) - uses MS-CHAPv2 for authentication. This is by far the most popular implementation.
- PEAPv1 (EAP-GTC) - Cisco's implementation.

PEAP is supported by Microsoft as an alternative to EAP-TLS. It is simpler and cheaper to deploy than EAP-TLS because you only need a certificate for the authentication server.

Lightweight EAP (LEAP)

Lightweight EAP (LEAP) was developed by Cisco in 2000 to try to resolve weaknesses in Wired Equivalent Privacy (WEP) and represents a very early implementation of EAP. When a client connects to an access point (the authenticator), it enables EAPoL and the client authenticates to the server and the server to the client. The server and client then calculate a transport encryption session key, which the server sends to the access point. This key is used to encrypt the rest of the session. LEAP relies on MS-CHAP to transmit authentication credentials. This means that LEAP is vulnerable to password cracking, as demonstrated by the ASLEAP cracking tool.



Wireless encryption and authentication is covered in [Unit 3.3](#).

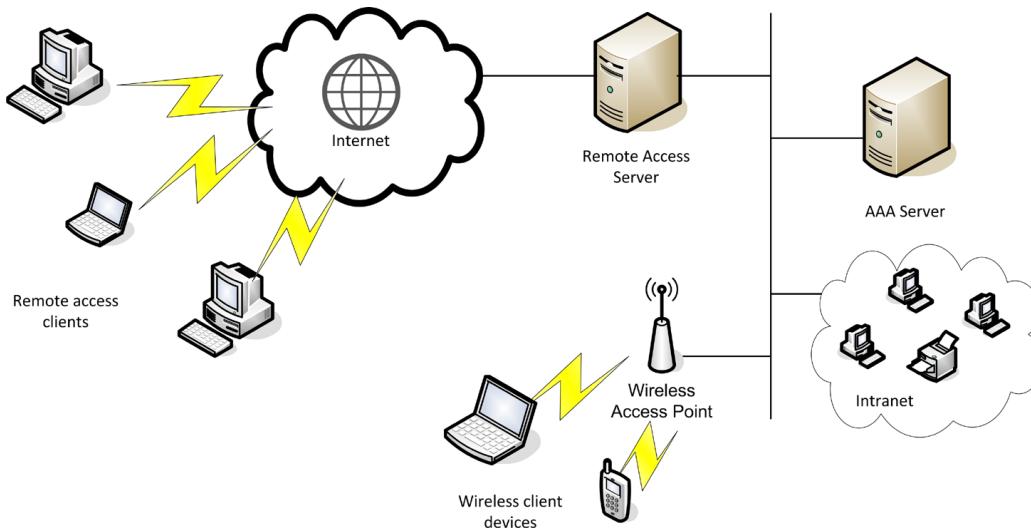
EAP-MD5

This is simply a secure hash of a user password. This method cannot provide mutual authentication (that is, the authenticator cannot authenticate itself to the supplicant). Therefore, this method is not suitable for use over insecure networks as it is vulnerable to Man-in-the-Middle, session hijacking, and password cracking attacks.



RADIUS and TACACS+

Enterprise networks and ISPs potentially need to support hundreds or thousands of users and numerous different remote and wireless access technologies and devices. The problem arises that each remote access device needs to be configured with authentication information and this information needs to be synchronized between them. A scalable authentication architecture can be developed using the RADIUS or TACACS protocols. Under both these protocols, authentication, authorization, and accounting are performed by a separate server (the AAA server). Remote access devices (such as routers, wireless access points, or network servers) function as client devices of the AAA server. Rather than storing authentication information, they pass this data between the AAA server and the remote user.



RADIUS

RADIUS stands for **Remote Authentication Dial-in User Service**. It is published as an internet standard in [RFC 2865](#). The RADIUS authentication process works as follows:

- 1) The remote user connects to a RADIUS client, such as an access point, switch, or remote access server.
- 2) The RADIUS client prompts the user for their authentication details, such as a username and password or digital certificate. Certificate-based authentication is available if the RADIUS product supports EAP. RADIUS support for EAP is not an official standard but is widely implemented. It is discussed in [RFC 3579](#).
- 3) The remote user enters the required information. The RADIUS client uses this information to create an Access-Request packet. The packet contains the following data:
 - Username and password (the password portion of the packet is encrypted using MD5). The Network Access Server and AAA server must be configured with the same shared secret. This is used to hash the user password.

- Connection type (port).
 - RADIUS client ID (IP address).
 - Message authenticator.
- 4) The Access-Request packet is encapsulated and sent to the AAA server using UDP on port 1812 (by default).
- 5) The AAA server decrypts the password (if the password cannot be decrypted the server does not respond). It then checks the authentication information against its security database. If the authentication is valid, it responds to the client with an Access-Accept packet; otherwise an Access-Reject packet is returned. Depending on the authentication method, there may be another step where the AAA server issues an Access-Challenge, which has to be relayed by the RADIUS client.
- 6) The client checks an authenticator in the response packet; if it is valid and an Access-Accept packet is returned, the client authenticates the user. The client then generates an Accounting-Request (Start) packet and transmits it to the server (on port 1813). It then opens a session with the user.
- 7) The server processes the Accounting-Request and replies with an Accounting-Response.
- 8) When the session is closed (or interrupted), the client and server exchange Accounting-Request (Stop) and Response packets.

There are a number of RADIUS server and client products. Microsoft has the Internet Authentication Server (IAS) / Network Policy Server (NPS) for Windows platforms and there are open-source implementations for UNIX and Linux (such as FreeRADIUS), as well as third-party commercial products (such as Cisco's Secure Access Control Server, Radiator, and Juniper Networks Steel-Belted RADIUS). Products are not always interoperable as they may not support the same authentication and accounting technologies.

TACACS+

Terminal Access Controller Access-Control System (TACACS+) is a similar protocol to RADIUS but designed to be more flexible and reliable. TACACS+ was developed by Cisco but is also supported on many of the other third-party and open source RADIUS server implementations.

Reliability is improved by using TCP (over port 49). TCP provides reliable delivery, making it easier to detect when a server is down. Another feature is that all the data in TACACS+ packets is encrypted (except for the header identifying the packet as TACACS+ data), rather than just the authentication data.



A TACACS protocol was developed in the 1980s and upgraded by Cisco as the proprietary protocol XTACACS in the 1990s. TACACS+ is incompatible with both of these.



Federation and Trusts

The proliferation of online accounts that users must manage and keep secure when interacting with work and consumer services, in the office and online, is a substantial threat to the security of all the networks that the user has accounts with. It also exposes people to risks such as identity theft. The goal of a sort of internet single-sign on, where a user has a single ID that they can use to authenticate against any network, is a very long way off. However many internet businesses are developing federated networks, allowing users to share a single set of credentials between multiple service providers.

Federation

Federation is the notion that a network needs to be accessible to more than just a well-defined group, such as employees. In business, a company might need to make parts of its network open to partners, suppliers, and customers and likewise have parts of their networks open to its staff. The company can manage its staff accounts easily enough. Managing accounts for each supplier or customer internally may be more difficult however. Federation means that the company trusts accounts created and managed by a different network. As another example, in the consumer world, a user might want to use both Google Apps and Twitter. If Google and Twitter establish a federated network for the purpose of authentication and authorization, then the user can log on to Twitter using his or her Google credentials or vice versa.

In these models, the networks perform **federated identity management**. The networks establish trust relationships so that the identity of a user (the **principal**) from network A (the **identity provider**) can be trusted as authentic by network B (the **service provider**). As well as trusts, the networks must establish the communications links and protocols that allow users to authenticate and be authorized with access permissions and rights.



As well as sign-on mechanisms, there also needs to be a way for the user to sign out securely (from each different site) and perform other elements of session management to prevent replay attacks.

Transitive Trust

Different kinds of trust relationships can be created to model different kinds of relationships. Each network can be thought of as a domain. Domains can establish parent-child or peer relationships.

- One-way trust - child trusts parent but parent does not trust child. For example, Domain B might be configured to trust Domain A. Users from Domain A can be authorized to access resources on Domain B. Users from Domain B however are *not* trusted by Domain A.
- Two-way - the domains are peers and both trust one another equally.

A trust relationship can also be non-transitive or transitive:

- Non-transitive trust - the trust relationship remains only between those domains.
- Transitive trust - the trust extends to other trusted domains. For example, if Domain A trusts Domain B, and Doman B trusts Domain C, then Domain A also trusts Domain C.

It is important to define the appropriate trust relationship at the outset of setting up the federated network. The trust relationship must reflect legal and regulatory commitments. For example, the identity manager needs to consider the impact of data protection legislation when sharing any identity data with a service provider.



Security Association Markup Language (SAML)

With a federated network there is also the question of how to handle user identity assertions and transmit authorizations between the principal, the service provider, and the identity provider. One solution to this problem is the **Security Association Markup Language (SAML)**. SAML was developed by the **Organization for the Advancement of Structured Information Standards (OASIS)**. The standard is currently on version 2.0.

- 1) The principal's User Agent (typically a browser) requests a resource from the Service Provider (SP), making a particular assertion of identity.
- 2) If the user agent does not already have a valid session, the SP redirects the user agent to the Identity Provider (IdP).
- 3) The user agent authenticates with the IdP. The IdP validates the supplied credentials and if correct provides an authorization token.
- 4) The user agent presents the SP with the authorization token.
- 5) The SP verifies the token and (if accepted) establishes a session and provides access to the resource.

SAML authorizations are written in **eXtensible Markup Language (XML)**. Communications are established using **HTTP/HTTPS** and the **Simple Object Access Protocol (SOAP)**. Tokens are signed using the XML signature specification. The use of a digital signature allows the SP to trust the IdP.



An XML signature wrapping attack allows a malicious user to strip the signature from a token and use it with a different token. The SAML implementation must perform adequate validation of requests to ensure that the signed token is the one being presented.

As an example of a SAML implementation, Amazon Web Services (AWS) can function as a SAML service provider. This allows companies using AWS to develop cloud applications to manage their customers' user identities and provide them with permissions on AWS without having to create accounts for them on AWS directly.

OpenID and OAuth

OpenID is the standard underpinning many of the "sign on with" features of modern websites. A solution such as SAML is typical of an enterprise-controlled federated identity management solution. OpenID is an example of a "user-centric" version of federated identity management. It allows users to select their preferred identity provider. This allows a consumer website (referred to as the **Relying Party [RP]**) to accept new users without having to go through an account creation step first, improving availability.

For example, [fantastic-holidays.com](#) wants to quickly accept authenticated users to participate in live chat with sales staff. It wants to authenticate users to reduce misuse of the chat application but does not want to force potential users to complete a sign-up form, which might act as a deterrent and reduce sales opportunities. Consequently, it becomes a relying party accepting [Google.com](#) or [Live.com](#) as identity providers. Later, if [fantastic-holidays.com](#) wins a sale and needs more information about the user, it can associate that identity with additional profile information, such as billing details. This profile information is owned and stored by [fantastic-holidays.com](#) and not shared with the identity provider.

With OpenID, the identity provider does not usually share any profile information or data with the relying party. This requires a different trust relationship to be established. To do so would require the user's consent.

OAuth is a protocol designed to facilitate this sort of transfer of information or resource between sites. With OAuth, the user grants an **OAuth consumer** site to access resources stored on an **OAuth provider** website.

OAuth stands for "Open Authorization" not "authentication". If authentication is required, the user authenticates with the OAuth provider (using a separate mechanisms), *not* with the OAuth consumer.



It is possible to configure exchange of profile information under OpenID but it is not the primary purpose of the standard. There are extensions to OpenID to allow it to use OAuth. Also, OpenID Connect is a new protocol providing an identity management layer over OAuth.



You should also be aware of Facebook Connect, which is a proprietary protocol with some of the features of both OpenID and OAuth. Facebook can work as an OpenID relying party and also supports OAuth.



With SAML, there is no direct contact between the SP and IdP, except that the SP must be configured to trust the IdP's digital signature. With OpenID and OAuth, the relying party and identity provider's servers communicate directly.



Review Questions / Module 2 / Unit 4 / Strong Authentication

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) True or false? An account requiring a password, PIN, and one-time password is an example of three-factor authentication.
- 2) What type of logon security is provided by OTP?
- 3) Apart from cost, what would you consider to be the major considerations for evaluating a biometric recognition technology?
- 4) Which type of eye recognition is easier to perform: retinal or iris scanning?
- 5) True or false? The holder of a Common Access Card can authenticate to a computer system using biometric information stored on the card.
- 6) Which remote authentication protocol supports smart cards?
- 7) What is a RADIUS client?
- 8) Which of TACACS, TACACS+, and XTACACS is most likely to be deployed on modern networks?
- 9) Your company has won a contract to work with the Department of Defense. What type of site access credentials will you need to provide?
- 10) You are working with a cloud services company to use their identity management services to allow users to authenticate to your network. The company will not establish a transitive trust between their network system and yours to allow you to access and update user profiles. Why would they refuse this and what impact will it have on your application?



If you have access to the Hands On Live Labs, complete the "Access Control / RADIUS" and "Application Data / Transitive Trust and Authentication" labs now.

Module 2 / Unit 5

Authorization and Account Management

Objectives

On completion of this unit, you will be able to:

- Understand privilege management policies and the assignment of rights to users, groups, and roles.
- Use directory services and system policies to configure rights and roles.
- Configure password protection and account restriction policies.
- Perform user access and rights and permissions reviews.



Privilege Policies

Privilege management focuses on access to network resources, but the same principles apply to physical access (for example, who may enter a server room or has keys to a safe).

Access Control Models

Recall that access control can be implemented using three models, in ascending order of restrictiveness:

- Discretionary Access Control (DAC) - the owner controls access to the resource by granting rights through the object's access control list.
- Role-based Access Control (RBAC) - resource access and usage is defined by administrators.
- Mandatory Access Control (MAC) - resource access is restricted by system policies.

Discretionary access control is typical of a **decentralized** workgroup or peer-to-peer network; role-based access control is typical of a **centrally-controlled** client-server network. In a decentralized network, each machine is configured with its own security database of users and access rights. In a centralized network, servers are configured with directories of objects (users and resources). Most enterprise networks are neither completely centralized nor completely decentralized. They tend to function on a hierarchical model with some delegation of control to organizations and organizational units.

Mandatory access control is a difficult model to implement and is typically used in very security-conscious organizations, such as the military or secret services. However, mandatory access control is also increasingly being built into operating system and application software as a means of protecting critical processes from abuse through a misconfigured or hacked DAC or RBAC account (such as may happen if the user installs a Trojan or triggers a virus).

An example of this is the Windows 7 OS, which uses a "sandbox" mode for administrative accounts called User Account Control. The OS restricts the privileges of certain processes and applications regardless of the privileges of the logged on user.

User, Group, and Role-based Management

One of the problems of privilege management is keeping track of what any one user *should* be allowed to do on the system compared to what they have *actually* been permitted to do.

User-assigned Privileges

The simplest (meaning the least sophisticated) type of privilege management is user-assigned privileges. In this model, each user is directly allocated rights. This model is only practical if the number of users is small. This is typically true of discretionary access control.

Group-based Privileges

Group-based privilege management simplifies and centralizes the administrative process of assigning rights by identifying sets of users that require the same rights. The administrator can then assign access rights to the group and membership of a group to a user. The user inherits access rights from the group(s) to which s/he belongs.

A user can be a member of multiple groups and can, therefore, receive rights and permissions from several sources.

Determining effective permissions when those set from different accounts conflict can be a complex task. Generally, a user will have the most effective allow permissions from all the accounts s/he belongs to but deny permissions (where the right to exercise a privilege is explicitly denied rather than just not granted) override allow permissions. Some of these complexities can be dealt with by implementing a role-based access control model.

Role-based Management

An ordinary group may have members that perform different roles. This is self-evidently true of the two default groups (Users and Administrators) in Windows for example. Most network administrators define groups that are targeted on job functions a bit more tightly, but the principle of group management is still that groups are *accretions* of users.

A **role** is a type of group where all the members perform the same function. Effectively, it means that there are more restrictive rules surrounding group membership. This is likely to require the creation of more groups than would be the case with ordinary group management, but allows fine-grained control over rights.

Another feature of a well-designed role-based access system is that a user is only granted the access rights of a given role for the time that they actually perform that role. Logically, a user can only have the rights for one role at a time. RBAC also includes the idea of restricting what tasks users can perform within an application. A limited example of this can be seen in Microsoft Word, which allows restrictions to be placed on word processing functions based on group membership. Microsoft also provides Authorization Manager for Windows Server enabling developers to create RBAC applications.



Shared Accounts

A **shared account** is one where the password (or other authentication credentials) are known to more than one person. Typically, simple SOHO networking devices do not allow for the creation of multiple accounts and a single "Admin" account is used to manage the device. Other examples include the default OS accounts, such as Administrator and Guest in Windows or root in Linux. Shared accounts may also be set up for temporary staff.

Obviously a shared account breaks the principle of non-repudiation and makes an accurate audit trail difficult to establish. It also makes it more likely that the password for the account will be compromised. When an account is shared, changing the password regularly becomes extremely troublesome.

Shared accounts should only be used where these risks are understood and accepted.



Directory Services

Directory services are the principal means of providing privilege management and authorization on an enterprise network.

Depending on the sort of access control model used, the **owner** or **systems administrator** can share resources (folders, printers and other resources) to make them available for network users. The resources can then be protected with a security system based around the **authentication credentials** provided by each user at logon to gain access to a system-defined **account**. Windows and UNIX / Linux systems all provide versions of this type of security.

When logging on to the network, the user *must* supply logon credentials. This username and password (or other authentication data) are compared with the server's **security database**, and if both match, the user is authenticated. The server security service generates an **access key** for the user. This contains the username and **group memberships** of the authenticated user.

All **resources** on server-based systems have an **Access Control List (ACL)** that is used to control access to the resource. The access list contains entries for all usernames and groups that have **permission** to use the resource. It also records the *level* of access available for each entry. For example, an access list may allow a user named **user1** to view the *name* of a file in a folder but not read the file *contents*.

Whenever the user *attempts* to access a resource, his or her access key is provided as identification. The server's security service matches username and group memberships from the access key with entries in the access list, and from this, it calculates the user's access privileges.

All this information is stored in a directory. Most directories are based on the LDAP standard. As well as enterprise networking directories, LDAP also provides a model for internet directory access, such as providing contact lists for IM (Instant Messaging) applications.

Lightweight Directory Access Protocol



glu29

All network resources are recorded as objects within a directory. A directory is like a database, where an **object** is like a record and things that you know about the object (**attributes**) are like fields. In order for products from different vendors to be interoperable, most directories are based on the same standard.

The main directory standard is the **X.500** series of standards, developed by the **International Telecommunications Union (ITU)** in the 1980s. As this standard is complex, most directory services are implementations of the **Lightweight Directory Access Protocol (LDAP)**. LDAP is not a directory standard but a protocol used to query and update an X.500 directory or any type of directory that can present itself as an X.500 directory.

LDAP is widely supported in current directory products (Windows Active Directory, Novell eDirectory, Apple OpenDirectory, or the open source OpenLDAP for instance).



The fact that different products are based on the same standard does not necessarily make them easily interoperable. A vendor's implementation of a standard may not be completely compliant.

LDAP uses TCP and UDP port 389 by default.

X.500 Distinguished Names

A **Distinguished Name** is a unique identifier for any given resource within the directory. A distinguished name is made up of *attribute=value* pairs, separated by commas. The most specific attribute is listed first and successive attributes become progressively broader. This most specific attribute is also referred to as the **Relative Distinguished Name**, as it uniquely identifies the object within the context of successive (parent) attribute values.

The types of attributes, what information they contain, and the way object types are defined through attributes (some of which may be required and some optional) is described by the directory **schema**. Some of the attributes commonly used are as follows:

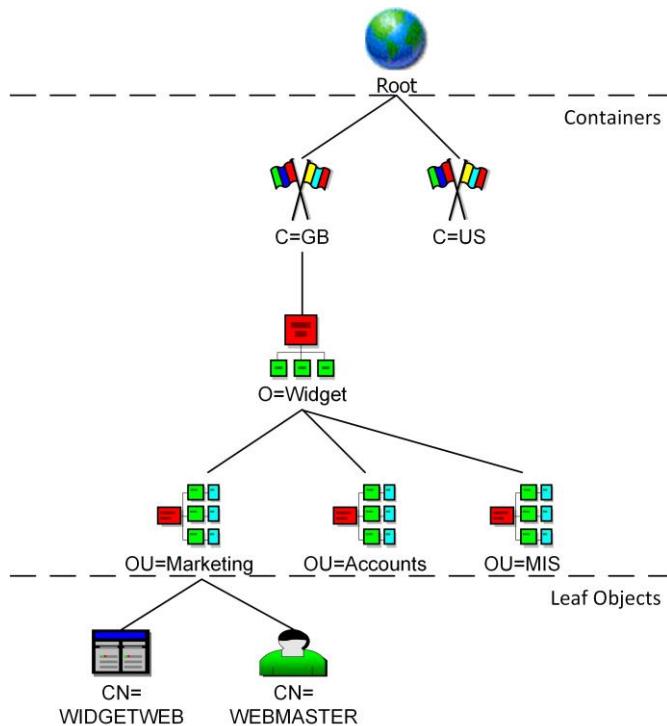
Attribute	Field	Usage
CN	Common Name	Identifies the person or object.
OU	Organizational Unit	A unit or department within the organization.
O	Organization	The name of the organization.
L	Locality	Usually a city or area.
ST	State	A state, province, or county within a country.
C	Country	The country's 2-character ISO code (such as c=US or c=UK).
DC	Domain Component	Components of the object's domain.

For example, the Distinguished Name of a web server operated by Widget in London might be:

```
CN=WIDGETWEB, OU=Marketing, O=Widget, L=London,
ST=London, C=UK, DC=widget, DC=com
```

Hierarchical Framework

X.500 directories are hierarchical (a **Directory Information Tree**). Each directory starts at the root and passes through a number of levels of **container** objects, such as country (optional), organization, and organizational units (also optional). Actual network resources, such as users, computers, printers, folders, or files, are referred to as **leaf** objects.



User Access and Security

LDAP itself provides no security and all transmissions are in plaintext, making it vulnerable to sniffing and Man-in-the-Middle (spoofing an LDAP server) attacks. Also, a server that does not require clients to authenticate is vulnerable to overloading by DoS attacks. However, secure LDAP can be implemented using another security protocol, such as IPsec or SSL / TLS.

Authentication (referred to as **binding** to the server) can be implemented in the following ways:

- No authentication - anonymous access is granted to the directory.
- Simple authentication - the client must supply its DN and password, but these are passed as plaintext. This method could be secured if using IPsec for transport across the network.
- Simple Authentication and Security Layer (SASL) - the client and server negotiate the use of a supported security mechanism. Typically, this will mean the use of either Kerberos or TLS (to provide strong certificate-based authentication).
- There is also an unofficial way of securing LDAP using SSL (the older version of TLS) called LDAPS. This is very similar to HTTPS and works over TCP port 636. SSL/TLS also provide a means for the server to authenticate to the client, providing mutual authentication.

If secure access is required, anonymous and simple authentication access methods should be disabled on the server.

Generally two levels of access will need to be granted on the directory: read-only access (query) and read/write access (update). This is implemented using an Access Control Policy, but the precise mechanism is vendor-specific and not specified by the LDAP standards documentation.

Unless hosting a public service, the LDAP directory server should also only be accessible from the private network. This means that LDAP ports (389 over TCP and UDP) should be blocked by a firewall from access over the public interface.

Where LDAP can be queried from some sort of web application, the application design needs to prevent the possibility of **LDAP injection** attacks. For example, if the web application presents a search form to allow the user to query a directory, a malicious user may enter a search string that includes extra search filters. If the input string is not properly validated, this could allow the user to bypass authentication or inject a different query, possibly allowing the attacker to return privileged information, such as a list of usernames or even passwords.

Windows Active Directory

In server-based Windows networks, the directory service is provided by **Active Directory**. The following notes discuss some of the organizational and administrative principles of planning an AD network. The same principles can apply to networks based around other directory products however.

Domain Controllers

The Active Directory is implemented as a database stored on one or more servers called **Domain Controllers (DC)**. Each server configured with AD maintains a copy of the domain database. The database is multi-master, which means that updates can be made to any copy and replicated to the other servers.



Domain Controllers provide a critical service. Without them, users are not able to log on to the network. The network design should ensure that these services are highly available.



It is also possible to implement Read-Only Domain Controllers (RODC). This allows users to authenticate but reduces the risk of a rogue administrator compromising trust management when the server is in a non-secure location (such as a branch office).

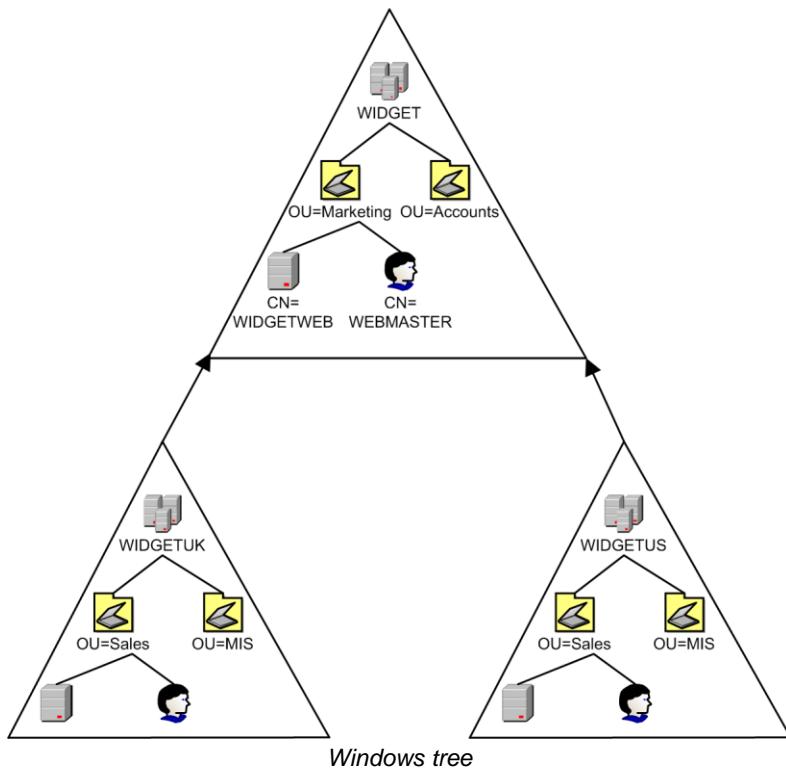
Domains

In legacy Windows networks, **domains** provided the primary grouping of users, groups, and computers. The simplest AD design is a single domain, representing the entire organization. Some organizations may require a more complex structure however.

Trees and Forests

In enterprise networks, multiple domains can be linked in a hierarchy, called a **tree**. For example, the widget.com parent domain (the root of the tree) could contain child domains (sales.widget.com, mis.widget.com, partners.widget.com, and so on). These domains have **two-way transitive trusts**, meaning that (for example) a user account in one domain in the tree could access resources (an application or file server for instance) in another domain.

Using fewer domains (one if possible) simplifies management. It is also cheaper; each domain must be supported by at least one domain controller server. Multiple domains might have been used in earlier Windows networks to provide different security boundaries and policies, delegate administrative control within very large organizations, or reduce replication traffic. In an Active Directory network these goals are generally better met by implementing Organizational Units (OU) or multiple forests (see below) to manage administrative and security boundaries and sites to manage replication traffic.



It is possible to configure multiple trees. For example, you might use two different public IDs within your organization. You might have a global ID (widget.com) and national subsidiaries (widget.co.uk and widget.de for instance). These different trees can be linked within the same **forest**. The domains within trees within the same forest also automatically have two-way transitive trusts so (for example) users configured within widget.co.uk could access resources configured within widget.com.

Finally, an enterprise might decide to use *multiple forests* across its network. Creating multiple forests incurs a substantial administrative overhead. The principal reason for doing so would be to create different security boundaries between parts of the organization. For example, a healthcare company might want to completely separate confidential patient data from sales and marketing functions. A user authenticated to the "sales" forest would not be able to access data stored in the "patient" forest. Administrative control is also separated.



The decision to use multiple forests is likely to focus on business needs. For example, there may be legal or regulatory reasons to have separate administrative control over some business functions.

Forests can also have different schemas. For example, installing the Microsoft Exchange communications server makes substantial changes to the AD schema. When testing the rollout of such a product, it may be preferable to install it to a different forest to avoid the complexity of rolling back changes to the production environment should the deployment be cancelled.

Organizational Units

Organizational Units (OU) provide a way of dividing a domain up into different administrative realms. For example, you might create OUs to delegate responsibility for administering different company departments or locations. For example, a "Sales" department manager could be delegated control with rights to add, delete, and modify user accounts but no rights to change account policies, such as requiring complex passwords, or manage users in the "Accounts" OU.

Generally speaking, defining OUs instead of multiple domains will simplify administration.

Sites

When you have networks based at separate geographic locations, you have to consider the effect of replication traffic on the network link. Replication between locations can be managed by configuring **sites**. Within a site (intrasite), replication occurs whenever there is a change or every 7 minutes. Between sites connected by a slow link (intersite) replication can be scheduled to particular times (when it will not impact other network operations) and the replication traffic can be compressed.



It is critical to carefully place domain controllers and DNS servers so that these services remain fully available at each site. If the services fail, users will not be able to access the network.

Active Directory Naming Strategy

A naming strategy allows better administrative control over network resources. The naming strategy should allow administrators to identify the type and function of any particular resource or location at any point in the directory information tree.

One of the first decisions is to determine how your AD namespace will integrate with your public DNS records. For example, you may make the AD namespace a delegated subdomain of your public DNS domain name (for example, ad-widget.widget.com). This solution isolates AD from the public internet and means that the DNS servers supporting the public domain name (widget.com) do not need to support Active Directory.



*You can simplify this for users by defining shorter explicit User Principal Names (UPN), usually as the user's email address. For example, instead of asking FredB to remember to log in as **ad-widget\fredb**, if FredB is configured with an explicit UPN he could use **fredb@widget.com**.*

Once you have chosen how the root of the namespace will integrate with public DNS you can devise how to structure AD in terms of Organization Units (OU).

The naming strategy for OUs does not need to be transparent to users as only domain administrators will encounter it. OUs represent administrative boundaries. They allow the enterprise administrator to delegate administrative responsibility for users and resources in different locations or departments. Consider the following guidelines:

- Do not create too many root level containers or nest containers too deeply (no more than five levels). Consider grouping root OUs by location or department:
 - Location - if different IT departments are responsible for services in different geographic locations.
 - Department - if different IT departments are responsible for supporting different business functions (sales and marketing, accounting, product development, fulfilment, and so on).
- Within each root-level "parent" OU, use separate child OUs for different types of object (server computers, client computers, users, groups). Use this schema consistently across all parent OUs.
- Separate administrative user and group accounts from standard ones.
- For each OU, document its purpose, its owner, its administrative users, the policies that apply to it (see below), and whether its visibility should be restricted.

When it comes to naming server, client computer, and printer objects, there are no "standard" best practices. Historically, using names from fantasy and science fiction or popular mythology was popular. One favored modern approach is to use the machine's service tag or asset ID. It is also often useful to denote the age of the machine and its type (PC, laptop, or tablet for instance). For servers, you may want to use a prefix that denotes the server function (`dc` for a domain controller, `exc` for Exchange, `sql` for SQL, and so on).

Some organizations try to encode information such as location, user, or department into the host name. The problem with this approach is that the user, location, or department that the device is associate with may change over time and keeping host names "synched" becomes increasingly problematic. Some organizations may use "random" names to try to conceal the function of a machine (to make it difficult for an attacker to identify critical servers for instance).



Use only allowed characters (as described in [RFC 1123](#)) in the namespace (A-Z, a-z, 0-9, and - [hyphen]). Names should not consist only of numbers. Also, restrict each label to 15 characters or less, to maintain compatibility with legacy Microsoft name resolution technologies (NetBIOS names).

Creating and Managing User Accounts

The purpose of a **user account** is to identify the individual as he or she logs on to the computer network. The user's identity is used to determine his or her access to network resources. It is also used for accounting, as actions performed by the user on system settings and resources can be logged and audited. It can also be linked to a **profile** that defines user settings for the workstation.



In Active Directory, users and groups are uniquely identified by a Security Identifier (SID) rather than the user or group name. This means that if the object is deleted and recreated with the same name, it will not inherit permissions granted to the deleted object.

Administrative Accounts

All server-based network operating systems provide an **administrative account**, which has access to all services and resources on a server. In Windows, this account is called **Administrator**; in Linux, it is called **root**.

It is best practice only to use these accounts to install the OS. Subsequently they are disabled. One or more accounts with administrative privileges are then created for named system admins (so that their actions can be audited). This makes it harder for attackers to identify and compromise an administrative account. This can be referred to as **generic account prohibition**.



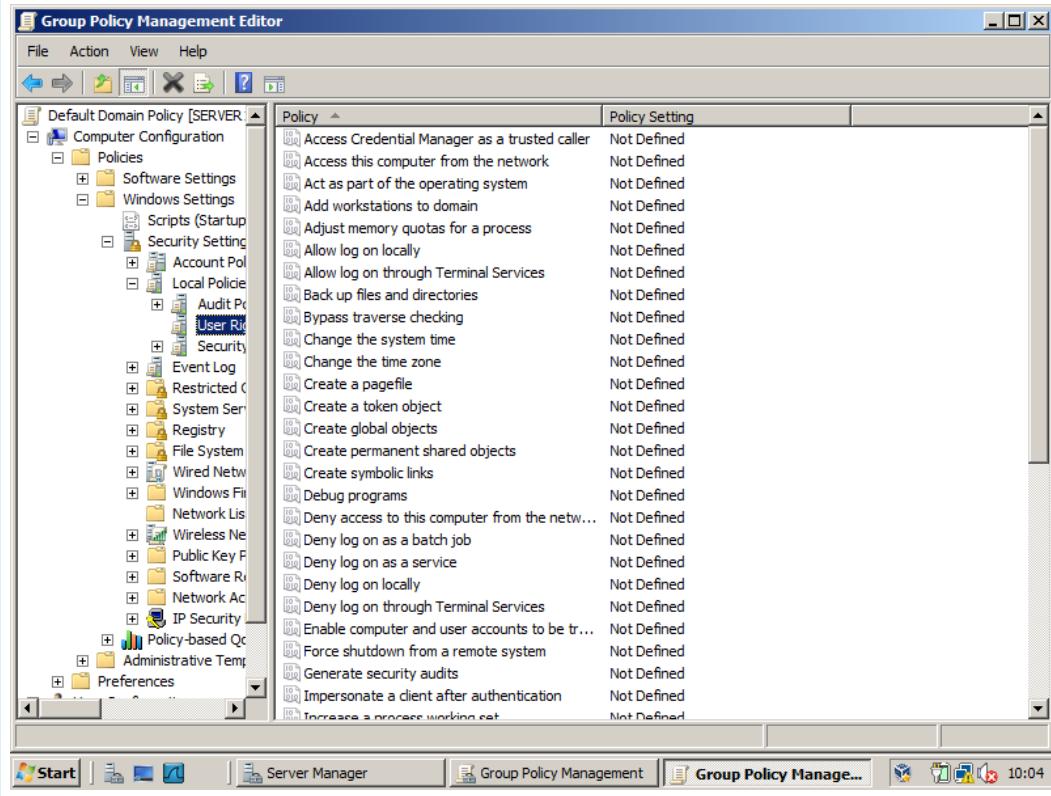
It is a good idea to restrict the number of administrative accounts as far as possible (the more accounts there are, the more likely it is that one of them will be compromised). On the other hand, you do not want administrators to share accounts as this compromises accountability.



As well as the administrator account, Windows also has a built-in Guest account. This account has limited privileges but can still logon to the desktop or shut down the machine. The Guest account is disabled by default on all recent versions of Windows.

An administrative account must be used when performing any security or configuration task on the server; for example, changing the system time, adding a user, or providing access to a resource.

The latest versions of Windows use User Account Control (UAC) to prevent administrative privileges from being invoked without specific authorization. In older versions administrators can use the Run As shortcut menu or command line option to access administrative privileges for a particular program. UNIX and Linux use the **su** or **sudo** commands. **su** could stand for "super user" or "set user". **su** allows the current user to act as root and is authenticated against the root password. **sudo** allows the user to perform commands configured in /etc/sudoers and is authenticated against the user's own password.



Actions that require administrative privileges are set as defaults in Windows but can also be configured differently if necessary

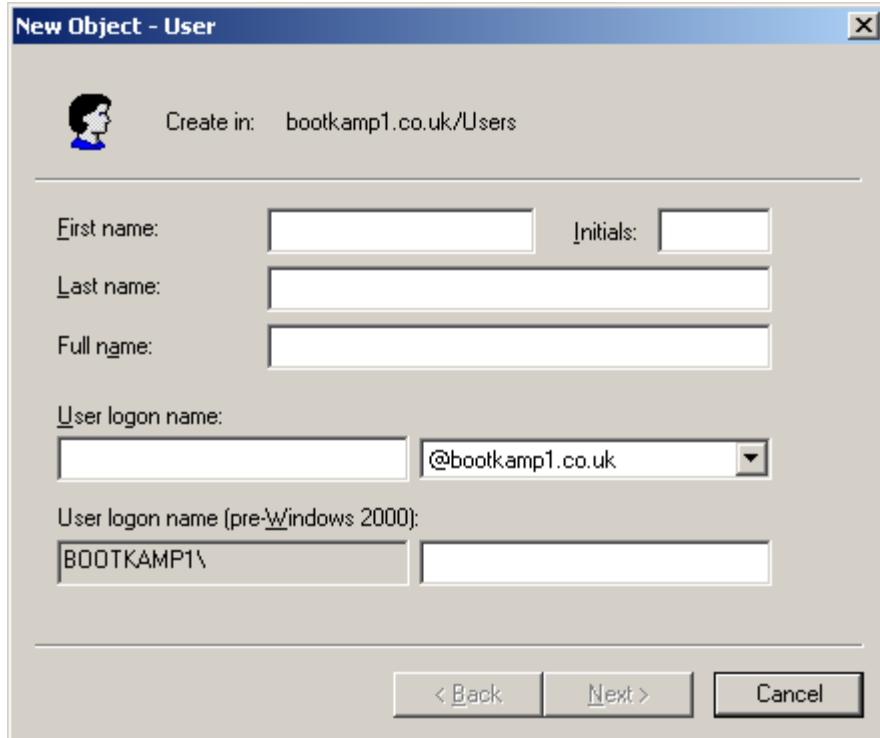
User Account Management in Windows

The screenshot shows the Active Directory Users and Computers console. The left pane shows the organizational structure. The right pane lists users and groups. A context menu is open over a user account, with 'User' highlighted.

Name	Type	Description
Administrator	User	Built-in account for administering the computer/domain
ASPNET	User	Account used for running the ASP.NET worker process (aspnet_wp.exe)
Cert Publishers	Security Group ...	Members of this group are permitted to publish certificates to the Active Di...
DnsAdmins	Security Group ...	DNS Administrators Group
UpdatePr...	Security Group ...	DNS clients who are permitted to perform dynamic updates on behalf of so...
Domain Admins	Security Group ...	Designated administrators of the domain
Domain Com...	Security Group ...	All workstations and servers joined to the domain
Guest	User	All domain controllers in the domain
Power Users	User	All domain guests
Administrators	Group	All domain users
Enterprise Admins	InetOrgPerson	Designated administrators of the enterprise
Guests	MSMQ Queue Alias	Members in this group can modify group policy for the domain
Help和支持中心	Printer	Built-in account for guest access to the computer/domain
IIS Worker Process Group	User	Group for the Help and Support Center
IIS_WebServer	Shared Folder	IIS Worker Process Group
IIS_WPG	User	Built-in account for anonymous access to Internet Information Services
Schema Admins	Security Group ...	Built-in account for Internet Information Services to start out of process a...
SQL Server 2008	Security Group ...	Servers in this group can access remote access properties of users
SQL Server 2008	Security Group ...	Designated administrators of the schema
SUPPORT_38...	User	Members in the group have the required access and privileges to be assign...
TelnetClients	Security Group ...	This is a vendor's account for the Help and Support Service
WSUS Adminis...	Security Group ...	Members of this group have access to Telnet Server on this system.
WSUS Repor...	Security Group ...	WSUS Administrators can administer the Windows Server Update Services ...
WSUS Repor...	Security Group ...	WSUS Administrators who can only run reports on the Windows Server Up...

Active Directory Management Tool

In a **Windows Active Directory Domain** environment, before you can manage accounts, you must log in as a user with membership of the **Domain Admins** or **Account Operators** groups. Changes to the domain security database can be *made* from any machine, but a domain controller must be available to accept the updates. A new user account is created by selecting the **New User** option from the context menu in **Active Directory Users and Computers**. If appropriate, a new user may be copied from an existing user or template account.



Adding a User Account

There are also local users and groups stored in the computer's Security Accounts Manager (SAM), which is part of the Registry. These accounts are managed using the **Local Users and Groups** tool or (if Simple File Sharing is enabled) the **User Accounts** applet in Control Panel. Local accounts can only access resources on the computer and have no permissions for Active Directory resources.

Managing Group Accounts

System administration can be simplified through the use of **group accounts**. Groups allow you to set **permissions** (or **rights**) for several users at the same time. Users are given membership of the group and then the group is given access to the resource or allowed to perform the action.



Avoid assigning permissions to user accounts directly. This makes permissions very difficult to audit (the process of checking that only valid users have access to given resources).

A user can be a member of multiple groups and can, therefore, receive rights and permissions from several sources.

Local, Global, and Universal Groups in Windows

Windows distinguishes between three scopes of group: **domain local**, **global**, and **universal**. The scope of a group refers both to who can be members of the group and where it can be used to determine access permissions.

- **Domain Local** groups can be used to assign rights to resources within the same domain only. Accounts or universal and global groups from any trusted domain can be a member of a domain local group.
- **Global** groups can contain only user and global or universal group accounts from the same domain but can be used to assign rights to resources in any trusted domain (essentially, the opposite of domain local scope).
- **Universal Groups** can contain accounts from any trusted domain and can also be used to grant permissions on any object in any trusted domain.

Microsoft's **AGDLP (Accounts go into Global groups, which go into Domain Local groups, which get Permissions)** system recommends putting user accounts into one or more global groups based on their role(s) within the company. The global groups are then assigned to domain local groups, which are assigned permissions over local resources, such as file shares and printers. This model provides scalability (in case additional domains are added later) and security (it is simpler to audit rights for users based on the role they have within the company).

Smaller organizations, especially those that know they will never have to support multiple domains, may find it simpler just to use global groups and assign both users and permissions to them. AGDLP is useful where the administrative function of assigning users to roles is separate from the administrative function of providing resources for each role.



Don't confuse "Domain Local" groups with "Local groups". "Local" groups can be configured on servers and workstations but only apply to that same computer.

Security and Distribution Groups

One use for groups is to assign permissions to access resources, as described above. This is referred to as a **security group**. You can also configure **distribution groups**, used to send messages to lists of recipients. Distribution groups cannot be configured with access permissions.

Built-in and Special Group Accounts

Windows and Active Directory include a number of default groups. These groups are already assigned sets of rights and permissions and can be used to simplify network management.

In addition to the built-in groups, Windows includes other groups that have special functions.

Everyone

The **Everyone** group includes all users from all domains. It cannot be deleted and it is used to provide the default permissions for resources; that is, **Full Permissions** for all users in the group. To secure the system, this default permission must be deleted and appropriate permissions assigned to other groups.

Guest (Anonymous) Users

Windows allows users to attach to the domain without providing a valid username and password. A valid username must be accompanied by the correct password, but a completely fictitious name can be used to secure guest access.



*The users with guest access to the domain **ARE** members of the **Everyone** group, so it is essential that permissions assigned to Everyone are carefully restricted.*

System Groups

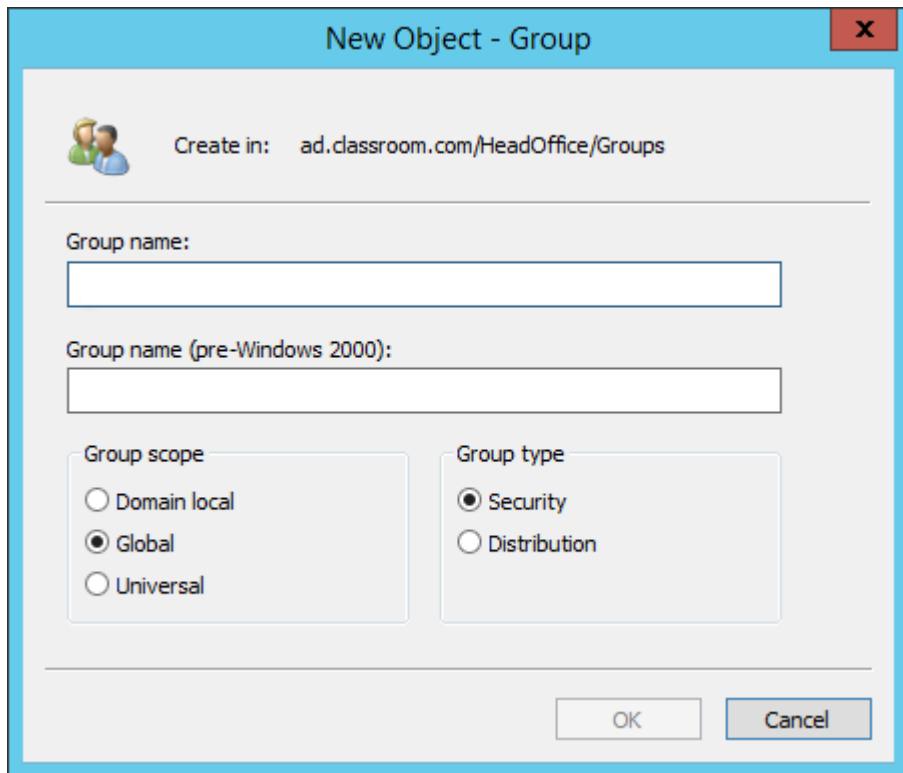
System groups are used internally by Windows and they cannot be assigned permissions. System groups include the following:

- **Interactive** – any local user of the computer.
- **Network** – any user connected over the network.
- **System** – the Windows operating system.
- **Creator/owner** – the user who created the directory or print job.

Creating Group Accounts

Groups can be created using either the **Active Directory Users and Computers** tool or **Local Users and Groups**. A user's group memberships can also be viewed and modified by selecting the **Member Of** tab on the **User Properties** dialog.

It is wise to develop a naming scheme to structure groups and keep them organized. Microsoft recommend distinguishing security and distribution groups and recording the scope of the group within the label. For example, **DIST-DLG-sales** would refer to a distribution list for sales used at the domain level; **SEC-GLO-accounts** would refer to a global security group for accounts staff.



Creating a group in Windows Server

For local and domain local groups, which should be used to assign permissions to resources, use the server name, file share, and permissions granted. For example, **SEC-DLG-CX0001-data-read** would represent a domain local group granted read permissions on a Data folder shared on a server named CX0001.

Account Policy Enforcement



Under Windows, the security configuration of the local machine and what a user is allowed to do are controlled via security policies.

Group Policy and Local Security Policy

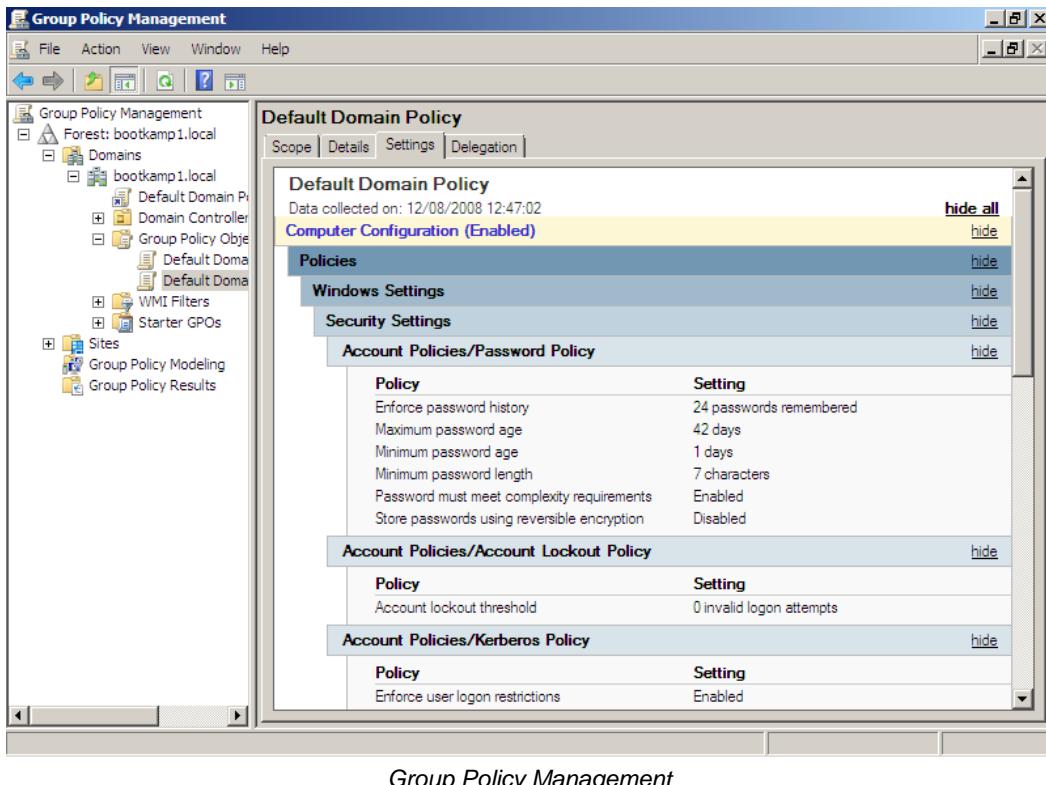
On a standalone workstation, these policies are configured via the **Local Security Policy** snap-in. Under Windows Server, they can be configured via **Group Policy Objects (GPO)**.

Group Policy Objects (GPO) are a means of applying security settings (as well as other administrative settings) across a range of computers and users. GPOs are linked to network administrative boundaries in Active Directory, such as sites, domains, and Organizational Units (OU).

GPOs can be used to configure software deployment, Windows settings, and (through the use of **Administrative Templates**) custom Registry settings. Settings can also be configured on a per-user or per-computer basis.

A system of inheritance determines the **Resultant Set of Policies (RSoP)** that apply to a particular computer or user. GPOs can be set to override or block policy inheritance where necessary.

Windows ships with a number of default **security templates** to provide the basis for GPOs (**configuration baselines**). These can be modified using the Group Policy Editor or Group Policy Management Console. GPOs can be linked to objects in Active Directory using the object's property sheet.



Password Protection Policies

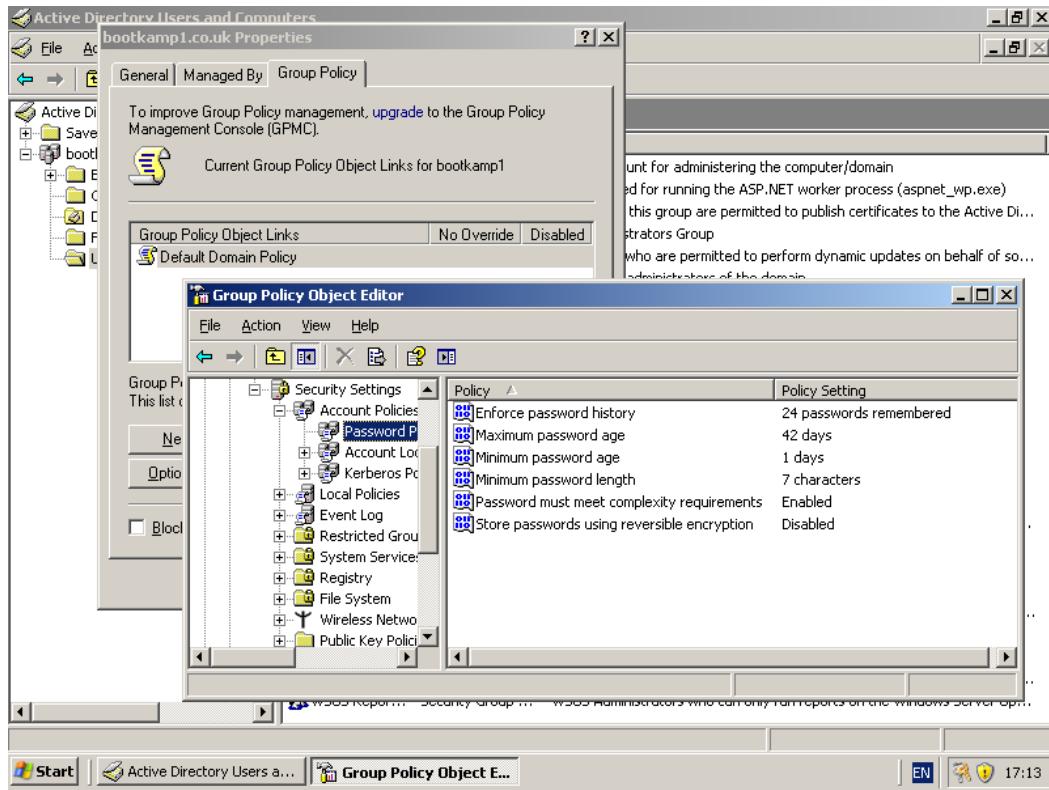
System-enforced policies can help to enforce credential management principles by stipulating particular requirements for users. Password protection policies mitigate against the risk of attackers being able to compromise an account and use it to launch other attacks on the network.



See [Unit 2.3](#) for more information on general password protection principles and password attack methods.

The table below provides some examples used by Windows.

Policy	Explanation
Minimum Password Length	A minimum acceptable password length is specified.
Password must meet complexity requirements	Enforce password complexity rules (that is, no use of username within password and combination of at least 6 upper/lower case alpha-numeric and non-alpha-numeric characters). Note that this only applies when passwords are created or changed (existing passwords are <i>not</i> tested against the policy).
Maximum password age	This configures a password expiration policy. When the time limit is reached, the user is forced to change the password.
Enforce password history / Minimum password age	This specifies that a unique password must be used when the user changes the password. The system remembers up to 24 previously used passwords so the minimum password age must be set to a value of 1 or greater to make the policy effective.
User cannot change password	This user account setting stops the user from changing his or her account password.
Password never expires	This user account setting can override a system password policy set to force a regular password change.



Configuring domain password policy using Group Policy



"Password reuse" can also mean using a work password elsewhere (on a website for instance). Obviously this sort of behavior can only be policed by "soft" policies.

Password Recovery

On a domain, if a user forgets a password, an administrator can reset it.

If the domain administrator password is forgotten, it can be reset by booting the server in Directory Service Restore Mode (this requires knowledge of the local administrator password).

Windows local accounts allow the user to make a password recovery disk. The user needs to remember to update this whenever the password is changed of course.

Account Restrictions

To make the task of compromising the user security system harder, account restrictions can also be used. These may be specific to a particular user or applied globally.

Policy	Explanation
Time Restrictions	For each account on the system, access to the server may be restricted to particular times. Periodically, the server checks whether the user has the right to continue using the network. If the user does not have the right, then an automatic logout procedure commences.
Station Restrictions	User access to the server can be restricted to a particular workstation or a group of workstations.
Concurrent Logons	By default, any user can log on to the domain from multiple workstations. If required, concurrent logons may be restricted to a specific number of connections.
Account Expiration Date	Setting an expiration date means that an account cannot be used beyond a certain date. This option is useful for accounts for temporary and contract staff.
Disable Account	Once an account is disabled, the user is denied access to the server until the network administrator re-enables the account.
Intruder Detection And Lock Out	The network administrator may specify a maximum number of incorrect logon attempts within a certain period. Once the maximum number of incorrect logons has been reached, the server disables the account. This prevents hackers trying to gain system access using lists of possible passwords.

User Rights, Permissions, and Access Reviews



rgdgd 9cuni

Where many users, groups, roles, and resources are involved, managing access privileges is complex and time-consuming. Setting privileges that are too restrictive creates a large volume of support calls; granting too many privileges to users weakens the security of the system.

The security manager also needs to take account of changes to resources and users. Resources may be updated, archived, or have their clearance level changed. Users may leave, arrive, or change jobs (roles). For example, if a user has moved to a new job, old privileges may need to be revoked and new ones granted. Managing these sort of changes efficiently and securely requires effective Standard Operating Procedures (SOPs) and clear and timely communication between departments (between IT and HR for instance).



The phrase "authorization creep" refers to an employee who gains more and more access privileges the longer they remain with the organization.

A user may also be granted elevated privileges temporarily (escalation). In this case, some system needs to be in-place to ensure that the privileges are revoked at the end of the agreed period.



Escalation also refers to malware and attacker techniques to compromise software vulnerabilities with the aim of obtaining elevated privileges on the system.

However, no system is perfect and therefore a system of auditing also needs to be put in place so that privileges are reviewed regularly. Auditing would include monitoring group membership and reviewing access control lists for each resource plus identifying and disabling unnecessary accounts.

In a mandatory access control environment, it means reviewing and testing the rules set up to control rights assignment and auditing the labels (security clearances) applied to users and resources.

The other aspect of auditing is configuring and reviewing event logs. Event logs serve two purposes:

- Maintain an audit trail of authorized access and changes to a resource.
- Detect unauthorized access (or access attempts) to a resource.



Configuring audit entries for a folder in Windows

Disabling Unnecessary Accounts

When an employee leaves a company, the employee's user account and privileges should be revoked. Depending on the security technologies in place, it may not be appropriate to delete the account (for example, from the point-of-view of recovering encrypted data) but it should be disabled. Thought must also be given to remote access. If the user was privy to highly confidential information, it may be necessary to change other accounts or security procedures. For example, the administrative passwords on network devices such as routers and firewalls might need to be changed. It is a critical point of security that account privileges should not be recycled. The next employee to perform the role should be allocated a new user account and privileges granted to that user account, rather than renaming an old one.

Continuous Monitoring

Continuous Monitoring refers to a process of continual risk re-assessment. This means performing routine audits of rights and privileges plus other key security metrics in "real time" (that is, every day rather than every week or every month for example).



Risk assessment is covered in more detail in [Unit 5.3](#).



Review Questions / Module 2 / Unit 5 / Authorization and Account Management

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) You are working on a privilege management policy and trying to work out a way to protect information that is restricted to executive-level employees from being snooped upon by IT administrative staff. Someone suggests locating the data on a PC that is not connected to the network. Why is this not an appropriate solution?
- 2) What are the advantages of a decentralized, discretionary access control policy over a mandatory access control policy?
- 3) What is the difference between group- and role-based management?
- 4) Under a rule-based access control model, how would a subject negotiate with the data owner for access privileges?
- 5) What container would you use if you want to apply a different security policy to a subset of objects within the same domain?
- 6) What authentication scheme is often used in conjunction with LDAP?
- 7) Why are the default OS user accounts a security risk?
- 8) A router appliance only supports a single administrative user. Given that at least two members of staff are required to be available to perform configuration updates on the router, what methods could you use to enforce accountability and non-repudiation?



If you have access to the Hands On Live Labs, complete the "Compliance / User Rights and Permissions" lab now.

Module 2 / Summary

Cryptography and Access Control

In this module, you learned about how cryptography is used to provide confidentiality, integrity, authentication, non-repudiation, and access control for computer storage and network systems. You also learned about access control technologies, including authenticating to local and remote servers and authorizing access to network resources.

Module 2 / Unit 1 / Cryptography

- A cryptographic system uses an algorithm in conjunction with keys to render information (plaintext) unreadable (ciphertext) to anyone not possessing the key.
- The three types of cryptographic algorithm are used for different purposes:
 - Hash functions (such as SHA, MD5, or RIPEMD) create an unrecoverable ciphertext
 - Symmetric functions (such as DES, AES, RC4, or Blowfish/Twofish) use the same key for encryption and decryption and are usually fast and lightweight to operate
 - Asymmetric functions (such as Diffie-Hellman (DHE/ECDHE) or RSA) use secure key exchange but can only be used on small amounts of data
- Confidentiality is usually provided by symmetric functions, but these face the problem of secure key exchange.
- Integrity, authentication, and non-repudiation are provided by digital signatures, which use a combination of hash and asymmetric functions.
- Cryptography systems can be vulnerable to attack, especially if the algorithm or key space has known vulnerabilities.
- Steganography means concealing a hidden message within a public one. Examples include covert communication channels and embedded printer ID data.

Module 2 / Unit 2 / Public Key Infrastructure

- Under PKI, certificates bind a particular public key to a user. The user is validated by a Certificate Authority (CA).
- A CA must put proper procedures in place to assure users that it is trustworthy. These include the validity of the registration process (by which users apply for certificates), certificate policies, and key management.
- CAs can enter into different trust relationships with one another, notably hierarchical, bridge, and mesh. Web of Trust is an alternative trust model to PKI, used by PGP certificates.

- Key management involves keeping private keys secure and notifying users when keys are expired, suspended, or revoked. There should also be procedures for data recovery, which is usually protected from abuse by M of N control. Key pairs should be issued for particular uses (for example, keys used to sign documents should not also be used for confidentiality).
- PKI standards are defined by the PKIX working group and published as RFCs. Many standards have been developed from RSA's PKCS. FIPS and Common Criteria EAL are used to certify cryptographic products.

Module 2 / Unit 3 / Password Authentication

- Configuring authentication requires the selection of effective protocols and procedures. Windows uses NTLMv2 for local authentication or Kerberos in a domain. Allowing compatibility with the older LM protocol makes password databases vulnerable.
- Remote authentication requires the secure transmission of credentials. Versions of CHAP are often used for basic password authentication.
- Password-based authentication depends entirely on the selection and maintenance of a strong password. Passwords are vulnerable to social engineering attacks and password crackers.

Module 2 / Unit 4 / Strong Authentication

- Strong authentication is implemented using token or biometric technologies along with a password or PIN.
- EAP is increasingly being deployed as a strong authentication solution.
- Many organizations use a RADIUS or TACACS+ server to integrate remote and wireless authentication with wired LAN authentication. AAA servers perform access control and authentication for client devices such as remote access servers and wireless access points.
- Federated identity management allows networks to share users, using protocols such as SAML to exchange authentication information. The trust relationships between networks must be carefully planned.

Module 2 / Unit 5 / Authorization and Account Management

- Privilege management means implementing an access control model so that use of resources only occurs with the proper authorization. This process also involves auditing and revoking privileges.
- Directory services supporting both user and group accounts plus configurable system policies allow fine-grained control over user rights.
- LDAP is a vendor-neutral means of querying a directory that conforms to the X.500 standard.
- An NOS such as Windows Server provides tools for managing users, groups, rights, and policies and for performing routine account maintenance and auditing.

Module 3 / Network Security

The following CompTIA Security+ domain objectives and examples are covered in this module:

CompTIA Security+ Certification Domain Areas	Weighting
1.0 Network Security	20%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	20%
4.0 Application, Data and Host Security	15%
5.0 Access Control and Identity Management	15%
6.0 Cryptography	12%

Domain Objectives/Examples	Refer To
1.1 Implement security configuration parameters on network devices and other technologies <i>Routers • Switches</i>	Unit 3.1 Secure Network Design
1.2 Given a scenario, use secure network administration principles <i>VLAN management • Secure router configuration • Loop protection • Network separation</i>	Unit 3.1 Secure Network Design
1.3 Explain network design elements and components <i>DMZ • Subnetting • VLAN • NAT • Layered security / Defense in depth</i>	Unit 3.1 Secure Network Design
1.1 Implement security configuration parameters on network devices and other technologies <i>Firewalls • Proxies • Web security gateways • NIDS and NIPS (Behavior based, Signature based, Anomaly based, Heuristic) • Spam filter • UTM security appliances (URL filter, Content inspection, Malware inspection) • Web application firewall vs. network firewall • Application aware devices (Firewalls, IPS, IDS, Proxies)</i>	Unit 3.2 Security Appliances and Applications
1.2 Given a scenario, use secure network administration principles <i>Rule-based management • Firewall rules • Access control lists • Flood guards • Implicit deny • Log analysis • Unified Threat Management</i>	Unit 3.2 Security Appliances and Applications
1.4 Given a scenario, implement common protocols and services <i>Ports (25, 110, 143)</i>	
2.1 Explain the importance of risk related concepts <i>False positives • False negatives</i>	
3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques <i>Monitoring system logs (Event logs, Audit logs, Security logs, Access logs) • Reporting (Alarms • Alerts • Trends) • Detection controls vs. prevention controls (IDS vs. IPS)</i>	
4.3 Given a scenario, select the appropriate solution to establish host security <i>Host-based firewalls • Host-based intrusion detection</i>	

Domain Objectives/Examples	Refer To
<p>1.5 Given a scenario, troubleshoot security issues related to wireless networking</p> <p>WPA • WPA2 • WEP • MAC filter • Disable SSID broadcast • TKIP • CCMP • Antenna Placement • Power level controls • Captive portals • Antenna types • Site surveys • VPN (over open wireless)</p>	Unit 3.3 Wireless Network Security
<p>3.4 Explain types of wireless attacks</p> <p>Rogue access points • Jamming/Interference • Evil twin • War driving • War chalking • IV attack • Packet sniffing • Replay attacks • WEP/WPA attacks • WPS attacks</p>	
<p>6.2 Given a scenario, use appropriate cryptographic methods</p> <p>WEP vs. WPA/WPA2 and pre-shared key</p>	
<p>1.1 Implement security configuration parameters on network devices and other technologies</p> <p>VPN concentrators</p>	Unit 3.4 VPN and Remote Access
<p>1.3 Explain network design elements and components</p> <p>Remote Access</p>	Security
<p>1.4 Given a scenario, implement common protocols and services</p> <p>Protocols (IPSec, SSH, SCP, TELNET) • Ports (22, 3389)</p>	
<p>6.2 Given a scenario, use appropriate cryptographic methods</p> <p>Use of algorithms/protocols with transport encryption (IPSec, SSH)</p>	
<p>1.3 Explain network design elements and components</p> <p>Telephony</p>	Unit 3.5 Network
<p>1.4 Given a scenario, implement common protocols and services</p> <p>Protocols (SNMP, DNS, IPv4 vs. IPv6, iSCSI, Fibre Channel, FCoE, NetBIOS) • Ports (53, 139)</p>	Application Security
<p>3.2 Summarize various types of attacks</p> <p>DNS poisoning • Typo squatting/URL hijacking</p>	
<p>4.4 Implement the appropriate controls to ensure data security</p> <p>SAN</p>	

Module 3 / Unit 1

Secure Network Design

Objectives

On completion of this unit, you will be able to:

- Describe the use of zones, DMZ, and layered security / defense in depth to plan network security.
- Know how subnets, VLANs, and NAT can be used to improve network security.
- Identify security considerations for network devices (switches and routers).

Secure Network Topologies

A **topology** is a description of how a computer network is physically or logically organized. It is essential to map the network topology when designing a computer network and to update the map when any changes or additions are made to it. The logical and physical network topology should be analyzed to identify points of vulnerability and to ensure that the goals of confidentiality, integrity, and availability are met by the design.



Subnetting

A subnet is a subdivision of a larger network, isolated from the rest of the network by means of routers (or layer 3 switches). Each subnet(work) is in its own broadcast domain.

Subnets can be used to represent geographical or logical divisions in the network. Geographical divisions might represent different floors of an office or networks connected by WAN links. Logical divisions might represent departmental functions or distinguish servers from clients.

Subnets are useful for security as traffic passing between each subnet can be subjected to filtering and access control at the router.

They also make it harder to "sniff" traffic (packet capture). Traffic is "compartmentalized" to each subnet, so if an attacker were able to place an eavesdropping device on the general network, they still would not be able to sniff traffic on an accounting subnet or network management services subnet. Using subnets can also restrict the impact of malware.



Packet sniffing can also be restricted to one segment by using switches rather than hubs (which is the case on most networks).

Zones

The main unit of a security topology is a **zone**. A zone is an area of the network (or of a connected network) where the security configuration is the same for all hosts within it. Network traffic between zones is strictly controlled, using a security device (typically a firewall).

A firewall is software or hardware that filters traffic passing into and out of the network. The firewall bases its decisions on a set of rules called an **Access Control List (ACL)**. For example, a basic firewall can allow or deny a host access based on its IP address or by the port it is requesting or a combination of both. Different types of firewall (and other filtering devices) can apply different - often more sophisticated - criteria in their ACLs.

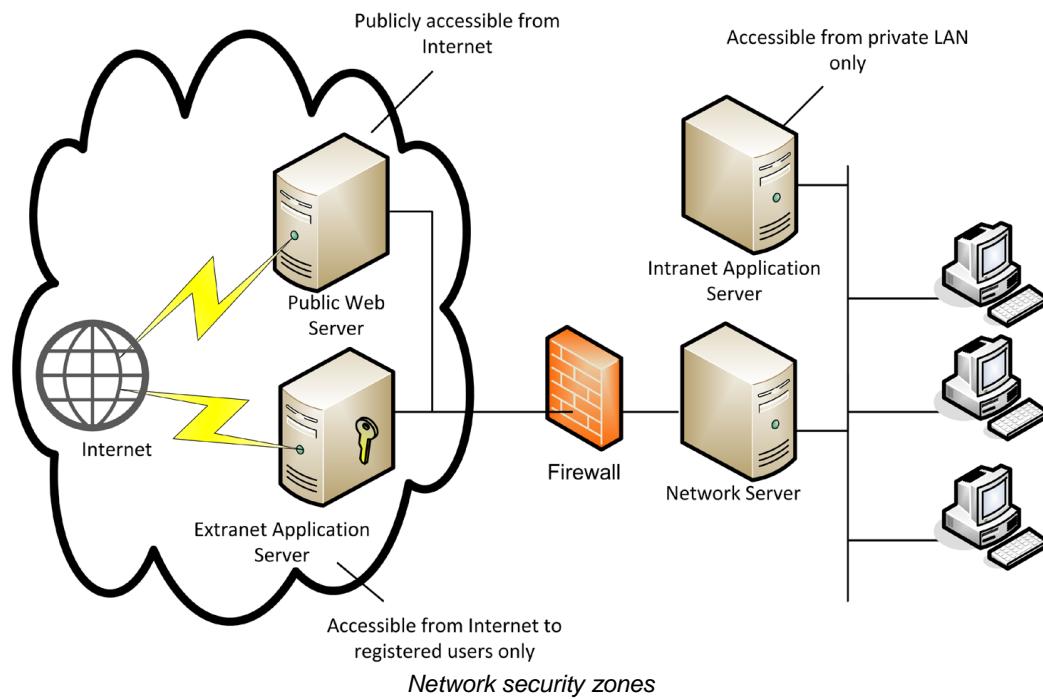
Dividing a network into zones implies that each zone has a different security configuration. The main zones are as follows:

- **Private network (intranet)** - this is a network of trusted hosts owned and controlled by the organization.



Hosts are trusted in the sense that they are under your administrative control and subject to the security mechanisms (such as anti-virus software, user rights, software updating, and so on) that you have set up to defend the network.

- **Extranet** - this is a network of semi-trusted hosts, typically representing business partners, suppliers, or customers. Hosts must **authenticate** to join the extranet.
- **Internet** - this is a zone permitting **anonymous** access (or perhaps a mix of anonymous and authenticated access) by untrusted hosts over the internet.





Demilitarized Zones

6mo46

The most important distinction between different security zones is whether a host is internet-facing. An internet-facing host accepts **inbound** connections from the internet. Internet-facing hosts are placed in **Demilitarized Zones (DMZ)**. A DMZ is also referred to as a perimeter network. The idea of a DMZ is that traffic cannot pass *through* it.

If communication is required between hosts on either side of a DMZ, a host within the DMZ acts as a **proxy**. It takes the request and checks it. If the request is valid, it re-transmits it to the destination. External hosts have no idea about what (if anything) is behind the DMZ.

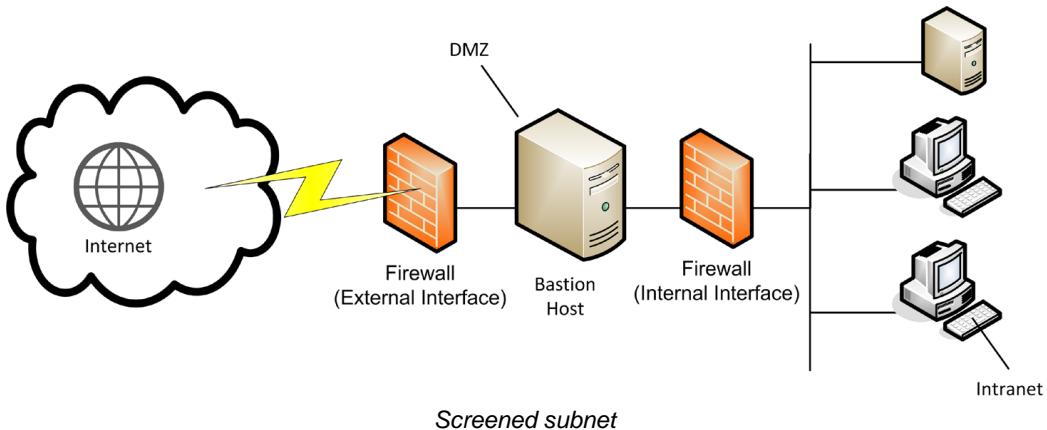
Both extranet and internet services are likely to be internet-facing, though an extranet could also be set up using leased line connections. Therefore the hosts that provide the extranet or public access services should be placed in a DMZ. These would typically include web servers, mail and other communications servers, proxy servers, and remote access servers.

The hosts in the DMZ are not fully trusted by the internal network because of the possibility that they could be compromised from the internet. They are referred to as **Bastion Hosts**. A bastion is a defensive structure in a castle. The bastion protrudes from the castle wall and enables the defenders to fire at attackers that have moved close to the wall. A bastion host would not be configured with any services that run on the local network, such as user authentication. Therefore, to configure a DMZ, two different security configurations must be enabled: one on the external interface and one on the internal interface. The DMZ and intranet are on different subnets so communications between them need to be routed.

There are two ways of implementing a DMZ: screened subnet and triple-homed firewall.

Screened Subnet

In this more secure configuration, two firewalls are placed at either end of the DMZ. One restricts traffic on the external interface; the other restricts traffic on the internal interface.

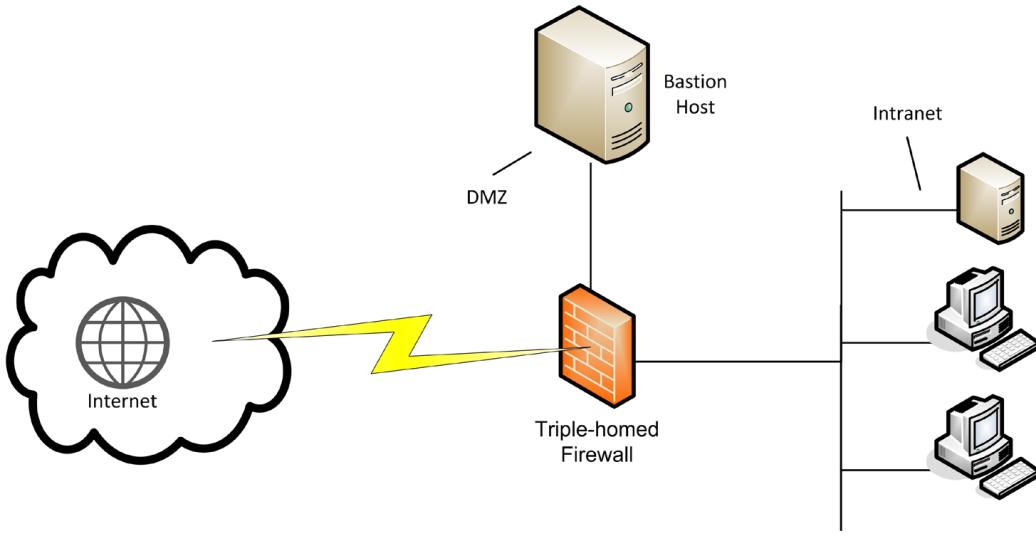


Screened subnet

Three-Legged Firewall

A three-legged (or triple-homed) firewall is one with three network ports:

- One port is the external interface.
- One port is the DMZ.
- One port is the internal interface.



Three-legged firewall

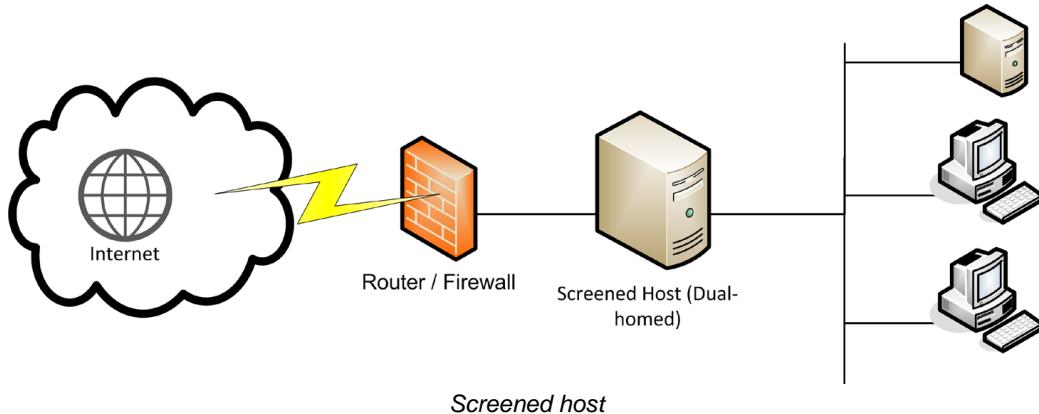
This is more complex to configure than a screened subnet. Also, the firewall represents a single point of failure and is easier to compromise. However, this configuration does save on costs.



Sometimes the term DMZ (or "DMZ host") is used by SOHO router vendors to mean an internet-facing host or zone not protected by the firewall. This might be simpler to configure and solve some access problems but makes the whole network very vulnerable to intrusion and DoS. A true DMZ is established by a separate network interface and subnet so that traffic between hosts in the DMZ and the LAN must be routed (and subject to firewall rules). Most SOHO routers do not have the necessary ports or routing functionality to create a true DMZ.

Screened Host

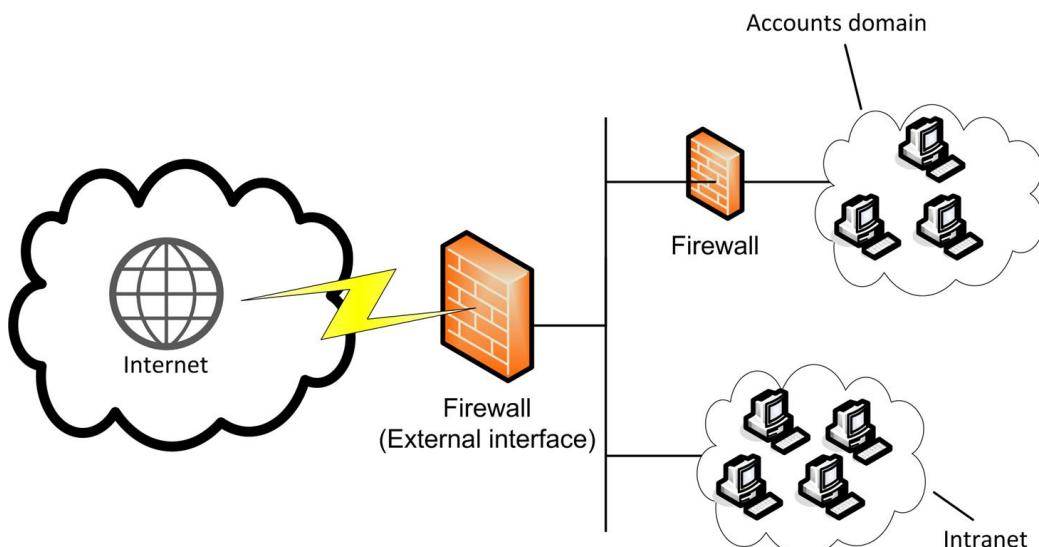
Smaller networks may not have the budget or technical expertise to implement a DMZ. In this case, internet access can still be implemented using a dual-homed proxy server acting as a **screened host**.



Other Security Zones

There is no single way of designing a network. Rather, a network will reflect the business needs of the organization. You may want to define your own security zones to suit business needs. Some examples are:

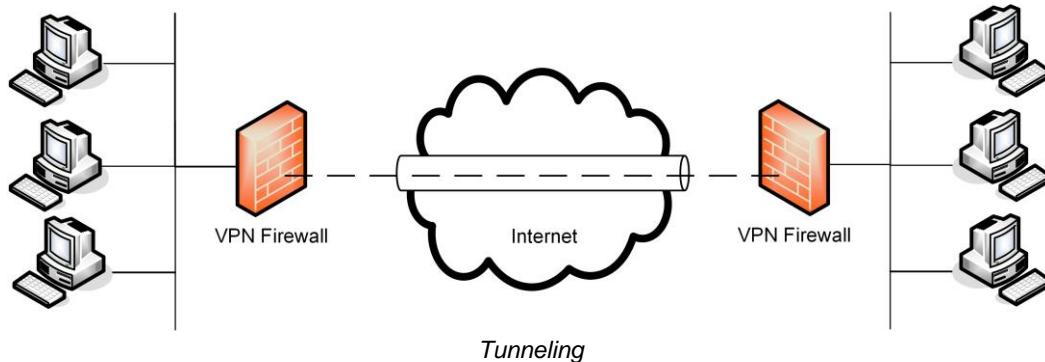
- A zone containing untrusted or semi-trusted hosts on the local network (for example, computers that are publicly accessible).
- Zones representing departmental functions.



Protecting hosts used by Accounting department with a firewall

Tunneling

Security can more or less be controlled on a local network, where all the machines and network infrastructure can be subject to inspection and intrusion detection. Unfortunately, modern networks must support access by hosts outside the local network. There are many ways of making these links, but one of the most popular is to use a remote device's ordinary internet connection and create a tunnel through the internet between the remote host and the private network. This is referred to as a **Virtual Private Network (VPN)**.



A remote host connecting through a VPN becomes part of the local network. While the connection can be made to a host in the DMZ, once the remote host is authenticated it has joined the LAN. This means that it is important that the remote host be subject to the same security policies (in terms of OS and software patch levels, configuration of anti-virus software, and so on) as any other local host.



Remote access and tunneling is covered in detail in [Unit 3.4](#).



Layered Security / Defense in Depth

Firewall-based security zones enforce what is commonly described as **perimeter security**. It is also necessary to configure security controls *within* the perimeter to cope with instances where either the perimeter security controls are breached or the attack is launched from within the perimeter. This is referred to as **layered security** or **defense in depth**.

Defense in depth means ensuring the security of **endpoints**, such as client and server devices, as well as the network perimeter. This can be provided by host-based firewalls and intrusion detection, anti-malware scanning, and Network Access Control (NAC). NAC means preventing devices from attaching to the network unless they meet a "health" policy that tests for update and A-V status and application control.



Firewalls and intrusion detection are covered in [Unit 3.2](#). Host security and Network Access Control are covered in detail in [Unit 4.1](#).

Network Device Exploitation

It can be tempting to think of network appliances such as switches and routers as "self-contained". In fact, these devices often run quite complex firmware and host services to enable remote management and configuration. This makes them vulnerable to a variety of attacks:

- Privilege escalation - driver software may be exploitable in the same way as applications software. For example, an attacker could craft a buffer overflow attack targeting a vulnerability in a network card driver.
- Weak passwords - devices such as wireless access points, switches, and routers ship with a default management password such as "password" or "admin" or the device vendor's name. These should be changed on installation. Also, the password used should be a strong one - most devices do not enforce complexity rules so the onus is on the user to choose something secure.
- Backdoor / default account - vendors sometimes deliberately install backdoors on devices such as routers and switches (often as a password reset mechanism). Another possibility is for someone with physical access to the device to reset it to the factory configuration.
- Denial of Service - an attacker able to compromise a network device is also likely to be able to launch a DoS attack against the network, either by disabling the device or reconfiguring it.

Most device exploits depend on the attacker having physical access to the appliance, though some vulnerabilities can be exploited over a network connection.



Site security is covered in more detail in [Unit 5.1](#).

Switches and VLANs



Early Ethernet networks used **hubs** as a means of connecting network segments. A hub is a multiport repeater; it takes the signal generated by a node and retransmits it to every port on the hub. All the ports are said to be in the same **collision domain**. A hub works at layer 1 of the OSI model (Physical Layer).

A **bridge** could be used to divide an overloaded network into separate segments. Each of the segments experiences far lower traffic loads since the bridge only passes signals from one segment to another if appropriate.

Intrasegment traffic (traffic between devices on the same segment) remains within this segment and cannot affect the other segments. A bridge works at layer 2 of the OSI model (Data Link Layer).

Most Ethernet installations have replaced hubs and bridges with switches to improve performance and security. Ethernet (or LAN) switches perform the same sort of function as a bridge but can provide many more ports (bridges only came with up to 4 ports). Each port is a separate **collision domain**. In effect, the switch establishes a point-to-point link between any two network nodes. This also means that (under normal circumstances) packet sniffers are restricted to capturing packets passing between two hosts, and cannot see unicast traffic from the rest of the network.



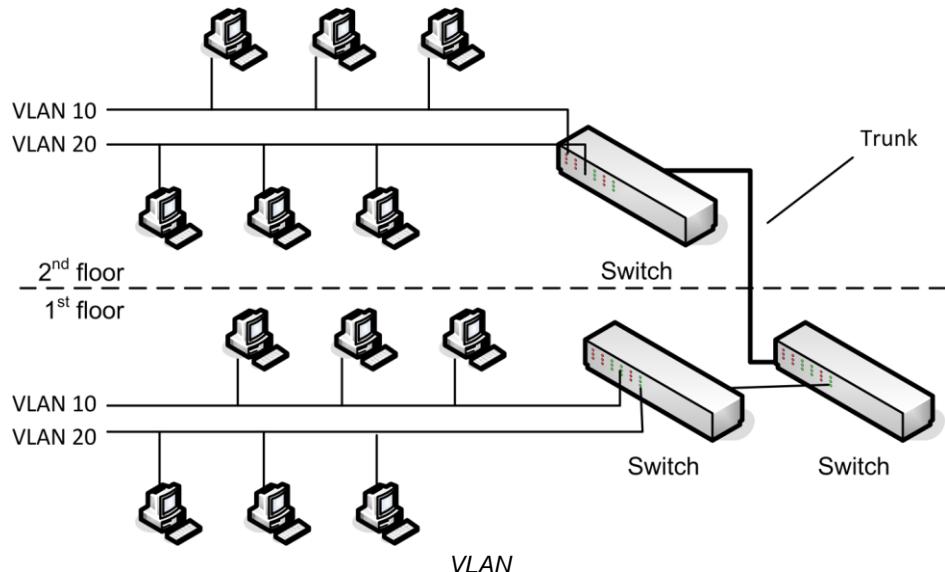
HP Procurve switch

Basic switches work at Layer 2 of the OSI model (Data Link Layer). There are also **Layer 3 switches** that work at the network layer however. This type of switch provides router-like functionality for large local networks. There are also content switches, which work at higher layers to provide functionality such as **load balancing**.



Virtual LAN (VLAN) Management

Through the use of switching technologies, computers connected by the same cabling and switch devices can appear to be in different broadcast domains. A single physical network is divided into multiple **Virtual LANs (VLAN)**. VLANs are defined by the **IEEE 802.1Q** standard. Cisco's proprietary **Inter-Switch Link (ISL)** is also widely used.



For example, ports 1 through 10 and 11 through 20 on a switch could be configured as two separate VLANs, typically each with their own subnet address. Communication between the groups of ports would only be possible via a router or layer 3 switch. Port-based switching is the simplest means of configuring a VLAN (static VLANs). Others (dynamic VLANs) include using the host's MAC address, protocol type, or even authentication credentials.

The screenshot shows the Dell OpenManage Switch Administrator interface. The left sidebar has a tree view with 'VLAN Membership' selected. The main content area is titled 'VLAN Membership'. It includes a dropdown for 'Select VLAN ID' set to 1, a 'Create VLAN' button, and a note '(2-4094)'. Below is a 'Remove VLAN' checkbox. A table shows port and LAG assignments across 16 ports and 6 LAGs. Port 1 is highlighted in yellow. A legend at the bottom defines symbols: 'Not Member' (white), 'Untag egress packets' (U), and 'Tag egress packets' (T).

Viewing VLANs on a Dell switch using the web management interface

From a security point-of-view, each VLAN can represent a separate security zone. These zones would typically be configured to protect the integrity and confidentiality of different departments within the organization. Any communication between VLANs needs to be channeled via a router. This means that in the event of a successful layer 2 attack (such as ARP poisoning) the scope of the attack is limited to the single VLAN rather than the whole network. VLANs may also help to contain the spread of viruses and worms to a smaller group of computers.

As well as representing organizational departments and/or overcoming physical barriers between different locations, it is common practice to isolate server-to-server traffic from client-server traffic and to isolate administration / management traffic; channels used for inbound management of appliances and servers. Another standard configuration option is to create a "null" VLAN that is non-routable to the rest of the network. This VLAN is used for any ports that do not have authorized connected equipment.

Trunks

On a large network, one switch will not provide enough ports for all the hosts that need to be connected to the network. This means that multiple switches must be interconnected to build the network fabric. Multiple switches may also be deployed to provide redundant links. The interconnections between switches are referred to as **trunks**.

When VLANs are also configured on the switches, trunking means that a VLAN can be configured across more than one switch device without having to manually configure the VLANs on each device. The protocol governing this data exchange would either be Cisco's **VLAN Trunking Protocol (VTP)** or **Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP)**.

Under VTP, switches can be grouped into **management domains**, identified by a domain name. Within these groups, switches are assigned the roles of either **VTP server** or **VTP client**. Modifications to the VLAN topology of the network can be made on any switch that has been assigned the VLAN server role and these changes are replicated to all switches in the management domain. In a small network with only a few switches, all switches may be configured as VTP servers. However, in a large network it is more efficient to limit the number of switches assigned this role.

Pruning refers to removing broadcasts related to particular VLANs from a trunk to preserve bandwidth. If a particular VLAN is not associated with a given trunk link, pruning it from the trunk reduces the amount of broadcast traffic passing over the link.

Switch Vulnerabilities and Exploits



Switches represent a powerful exploit if they can be compromised. Some typical attacks against switches include:

- MAC flooding - overloading the switch's MAC cache (referred to as the **Content Addressable Memory [CAM]** table) using a tool such as **Dsniff** or **Ettercap** to prevent genuine devices connecting and potentially forcing the switch into "hub" mode (facilitating eavesdropping).
- ARP poisoning - the attacker poisons the switch's ARP table with a false MAC-IP address mapping, typically allowing the attacker to masquerade as the subnet's default gateway.
- VLAN hopping – this exploits the native VLAN feature of 802.1Q. Native VLANs are designed to provide compatibility with non-VLAN capable switches. The attacker (using a device placed in the native VLAN) crafts a frame with two VLAN tag headers. The first trunk switch to inspect the frame strips the first header and the frame gets forwarded to the target VLAN.
- VLAN Trunking Protocol (VTP) attacks - VTP propagates the VLAN configuration from a "master" switch to other switches in the same domain. The attacker masquerades as a switch and tries to set itself up as a trunk by exploiting the VTP auto-negotiation process. This enables the attacker to channel all traffic through their computer or remove all the VLANs.
- Spanning Tree Attacks - the Spanning Tree Protocol (STP) is designed to provide loop protection. A loop could lead to a broadcast storm and crash the network. A DoS attack on STP tries to engineer this situation by masquerading as the root bridge.

Hardening Switches

In order to secure a switch, the following guidelines should be met:

- Configure port security (to restrict the number of MAC addresses that can be associated with a port) or port-based authentication, to ensure the integrity of devices connecting to the network.
- Disable unused ports by placing them in an otherwise unused VLAN with no connectivity to the rest of the network.
- Secure the switch's management console by renaming the administrative account (if possible) and setting a strong password.
- Use a secure interface to access the management console. Most switches can be operated using Telnet or HTTP, but these are not secure and transmit all information as plaintext. Use encrypted communications (such as SSL or SSH) or use the switch's console serial port. Switch administration traffic should be performed on a dedicated VLAN, separate from other types of traffic.



Using an access method other than the normal data network is referred to as Out-of-Band management.

- Disable unused management console access methods. For example, if you use SSH, disable the serial port, HTTP, HTTPS, and Telnet.
- Restrict the hosts that can be used to access the management console by enforcing an Access Control List (ACL); to restrict permitted hosts to a single IP address or subnet for instance.
- To mitigate VLAN hopping, do not use the default native VLAN (VLAN 1 or the "management VLAN") for any other purpose. This VLAN should be restricted to trunking protocol traffic.
- To mitigate VLAN trunking protocol exploits, only allow auto-negotiation of trunking protocols on ports legitimately used for trunking. Disable the protocols on all other ports. Enforce use of password authentication valid VTP packets.
- Install the latest firmware updates and review vendor security bulletins to be forewarned about possible exploits or vulnerabilities.
- Configure the SNMP interface on the switch to report only to an authorized management station or disable SNMP if it is not required.



SNMP is covered in [Unit 3.5](#).

- Enable features such as portfast, BPDU Guard, Root Guard, and Loop Guard to mitigate spanning tree attacks. These features prevent an attacker from injecting malicious STP traffic on a protected port or detect potential loops.

Network Separation



As most laptops and many desktops come with both LAN and wireless adapters, such computers can be configured as a bridge. Users may do this in the belief that it improves performance. In fact, it is likely to cause problems with broadcast traffic and looping on the enterprise network.

Also, if an attacker could then access the wireless link on the laptop (perhaps if the wireless adapter is configured in ad hoc mode with no connection security), s/he could gain access to the wider network.

Consequently many network admins scan for the presence of such bridges and disable the switch port if they are found. In Windows, it is possible to use group policy to prevent bridging network connections or to force the use of only one connection at a time.

More generally, it is important to verify the network infrastructure when connecting devices such as routers and wireless access points to a switch, especially if VLANs are configured. VLANs can be used to enforce network separation but they have to be configured correctly and made robust against the attacks described above.

A highly secure network or single host computer may have to be physically separated from any other network. This is also referred to as an **air gap**.



You can read more about some of the configuration issues surrounding air gapping on Bruce Schneier's blog (gtsgo.to/nmj9i).

Routers



A **router** is a device that connects multiple networks and routes packets from one network to another. The main features of a router include the following:

- Routers work at the **network (IP) layer**. Routers are able to identify source and destination network addresses within packets.
- A router is able to keep track of multiple active paths between any given source and destination network. This makes it **fault-tolerant**.
- Routers provide excellent traffic management using sophisticated path selection; they select the best routes based on traffic loads, line speeds, number of hops or administrator pre-set costs. The parameters used for determining routes for packets are known generically as **metrics**.
- Routers can share status and routing information with other routers and can listen to the network and identify which connections are busiest or not working. They then route network traffic avoiding slow or malfunctioning connections.

- Routers do not forward any information that does not have a correct network address. They also filter broadcast traffic by not routing broadcast packets. This means network broadcasts do not propagate throughout the internetwork and that broadcast storms are confined to a single subnet.

Devices Used for Routing

The relatively complex tasks performed by a router mean that they tend to be processing intensively. A router may be a dedicated appliance with a port to each of the networks or it may be a NOS server with multiple interface cards (**multi-homed**). Routers very often also support the functions of a firewall.

A router designed to connect a private network to the internet is called an **edge router** or **border router**. These routers can perform framing to repackage data from the private LAN frame format to the WAN internet access frame format. Edge routers designed to work with DSL or cable modems are called SOHO Routers (Small Office or Home Office).

Routers designed to service medium to large networks are complex and expensive appliances. They feature specialized processors to handle the routing and forwarding processes and memory to buffer data. Most routers of this class will also support plug-in cards for WAN interfaces.

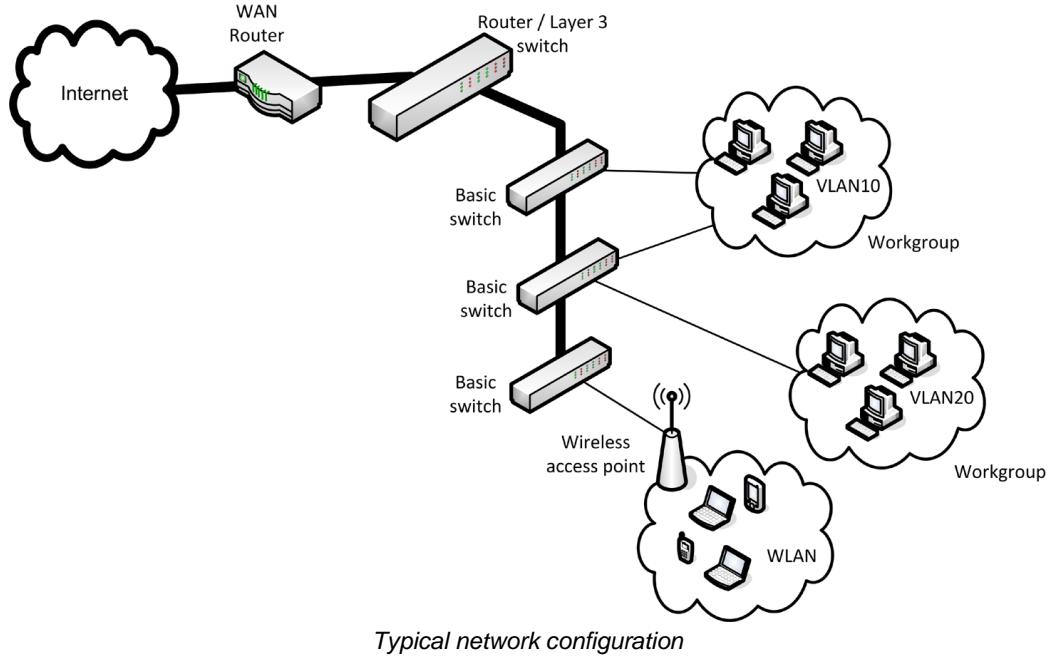


HP ProCurve router with 2xEthernet, ADSL, and T1 interfaces

Router Placement

As mentioned above, routers serve both to join physically remote networks and subdivide a single network into multiple subnets. Routers that join different types of network are called **border** or **edge** routers. These are typified by distinguishing external (internet-facing) and internal interfaces. These devices are placed at the network **perimeter**.

The graphic below shows a simplified example of a typical network configuration. Basic switches provide ports and Virtual LANs (logical groupings of clients) for wired and (via an access point) wireless devices. Traffic between logical networks is controlled by a router (or layer 3 switch). A WAN router provides access to the internet.



Routers are connected to a LAN network via switches. Each interface (LAN and WAN) must be configured with appropriate IP addressing information. Their function is typified by acting as the "default gateway" for hosts on the internal network. You should note however, that the function of subdividing a large network can also be performed more efficiently by Layer 3 Switches, which take on the functions of a router.

Static Routers

Static routers require the administrator to manually configure routes between each network. The administrator adds an entry to the routing table for each route that is supported. The routers do not communicate amongst themselves. If a route becomes unavailable, it must also be removed manually. This type of configuration is only possible with a small number of routers and does not provide the flexibility of dynamic routing. Its advantage is that complete control remains with the network administrator.

Dynamic Routers

Dynamic routers automatically discover routes by communicating with each other. They require minimal configuration since their routing tables are built and modified through these communications. This is a highly flexible approach that can quickly react to changes in the internetwork (such as router failure or broken links).

Dynamic routers exchange information about routes using **routing protocols** such as:

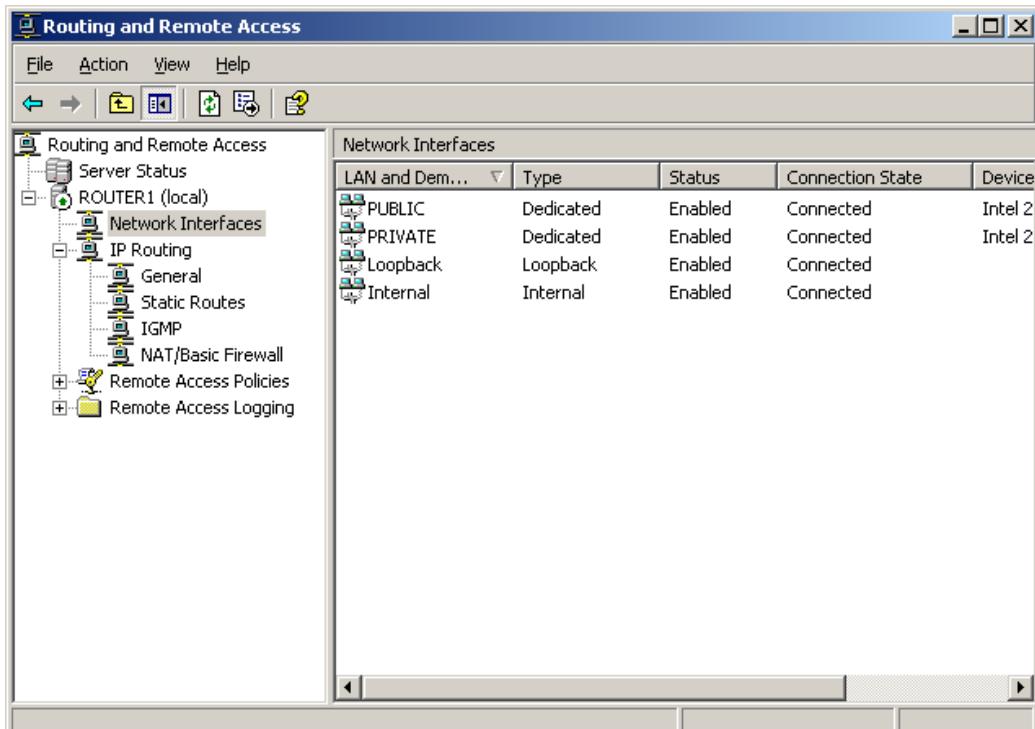
- **Open Shortest Path First (OSPF)** - uses a **link state** algorithm to calculate routes based on the number of hops, line speed, traffic and cost.
- **Routing Information Protocol (RIP)** - uses **distance vector** algorithms to determine routes. This is less efficient than a link state algorithm, especially on larger networks.

- **Border Gateway Protocol (BGP)** - the protocol used by the routers that support the major internet infrastructure.



Router Configuration

A hardware router is configured and secured in the same way as a switch (using a web or command line interface for instance). The main difference is that a router is likely to have an exposed public interface. This means that properly securing the router is all the more important. Routers are often more complex than switches and it is consequently easier to make mistakes. A software router is configured using the appropriate tools in the underlying NOS. As well as the configuration of the routing functions, the performance and security of the underlying server should be considered too.



Configuring Routing and Remote Access on Windows Server

Routing Attacks

Routing is subject to numerous vulnerabilities, including:

- Fingerprinting - port scanning using a tool such as nmap can reveal the presence of a router and which dynamic routing and management protocols it is running.



SOHO routers are particularly vulnerable to exploitation through unpatched vulnerabilities.

- Software exploits in the underlying operating system. Hardware routers (and switches) have an embedded operating system. For example, Cisco devices typically use the Internetwork Operating System (IOS). These do suffer from far fewer exploitable vulnerabilities than full network operating systems though. It has a reduced "attack surface" compared to a computer OS such as Windows.
- Spoofed routing information (route injection). Routing protocols that have no or weak authentication are vulnerable to route table poisoning. This can mean that traffic is misdirected to a monitoring port (sniffing) or sent to a blackhole (non-existent address) or continually looped around the network, causing DoS. Border routers should be configured never to accept routes that resolve to private IP addresses.
- Denial of Service (redirecting traffic to routing loops or blackholes or overloading the router).
- ARP poisoning or ICMP redirect - tricking hosts on the subnet into routing through the attacker's machine rather than the legitimate default gateway. This allows the attacker to eavesdrop on communications and perform replay or Man in the Middle attacks.
- Source routing - this uses an option in the IP header to pre-determine the route a packet will take through the network (strict) or "waypoints" that it must pass through (loose). This can be used maliciously to spoof IP addresses and bypass router / firewall filters. Routers can be configured to block source routed packets.
- There have also been various vulnerabilities associated with the way routing software processes miscalculated IP headers (to cause buffer overflows).

Network Address Translation



rf1sz

Network Address Translation (NAT) was originally devised as a way of freeing up scarce IP addresses for hosts needing internet access. It provides an addressing method for private networks connected to the internet. NAT is defined in [RFC 3022](#). A private network will typically use a private addressing scheme to allocate IP addresses to hosts. These addresses can be drawn from one of the pools of addresses defined in [RFC 1918](#) as non-routable over the internet:

- 10.0.0.0 to 10.255.255.255 (Class A private address range).
- 172.16.0.0 to 172.31.255.255 (Class B private address range).
- 192.168.0.0 to 192.168.255.255 (Class C private address range).

Essentially, NAT is a service translating between a **private (or local)** addressing scheme used by hosts on the LAN and a **public (or global)** addressing scheme used by an internet-facing device. NAT is configured on a border device, such as a router, proxy server, or firewall.

There are several types of NAT, including static, dynamic, overloaded, and destination NAT.

Static NAT

In a static (or basic) NAT configuration, a simple 1:1 mapping is made between the private ("inside local") network address and the public ("inside global") address. If the destination network is using NAT, it is described as having "outside global" and "outside local" addressing schemes.

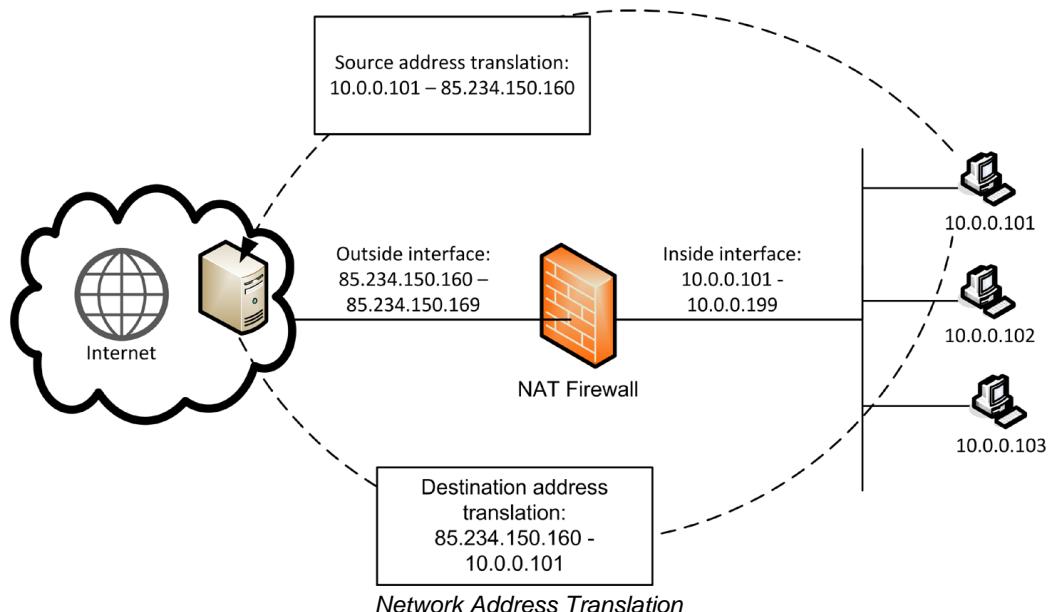
Static NAT is useful in scenarios where an inbound connection to a particular host must be supported. For example, you might position a web server behind a firewall running NAT. The firewall performs 1:1 address translation on the web server's IP address. This means that external hosts do not know the true IP address of the web server but are able to communicate with it successfully.



To support a server, the firewall must also perform port forwarding. This means that incoming requests for the service (port 80 for HTTP for instance) are passed on.

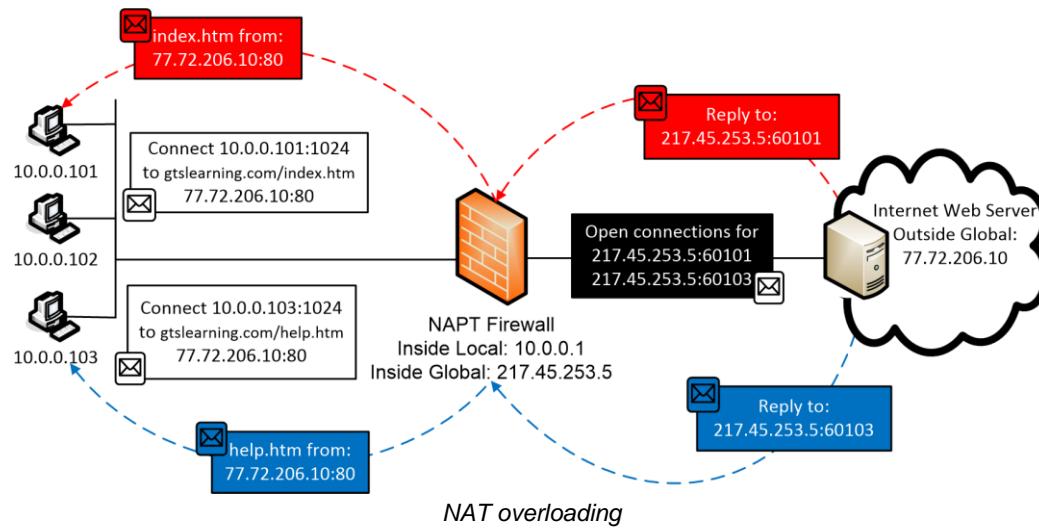
Dynamic NAT

Static NAT only supports one host, which is not very useful in most scenarios. Under dynamic NAT, the NAT device exposes a pool of IP addresses to the public internet. In order to support inbound and outbound connections between the private network and the internet, the NAT service builds a table of public to private address mappings. Each new connection creates a new public-private address binding in the table. When the connection is ended or times out, the binding is released for use by another host.



NAPT (Network Address Port Translation)

Dynamic NAT supports multiple simultaneous connections but is still limited by the number of available public IP addresses. Smaller companies may only be allocated a single or small block of addresses by their ISP. In this case, a means for multiple private IP addresses to be mapped onto a single public address would be useful. This function is provided by **Network Address Port Translation (NAPT)**. This can be referred to as **PAT (Port Address Translation)** or as **NAT overloading**.



NAPT works by allocating each new connection a high level TCP or UDP port. For example, say two hosts (192.168.0.101 and 192.168.0.102) initiate a web connection at the same time. The NAPT service creates two new port mappings for these requests (192.168.0.101:61101 and 192.168.0.102:61102). It then substitutes the private IP for the public IP and forwards the requests to the public internet. It performs a reverse mapping on any traffic returned using those ports, inserting the original IP address and port number, and forwards the packets to the internal hosts.

The screenshot shows the Windows Server Manager interface with the title "GATEWAY - Network Address Translation Session Mapping Table". The table lists the following session mappings:

Protocol	Direction	Private address	Private port	Public Address	Public Port	Remote Address	Remote Port
UDP	Outbound	10.1.0.1	63.456	10.0.0.1	63.456	192.168.1.254	53
UDP	Outbound	10.1.0.1	64.818	10.0.0.1	62.143	192.58.128.30	53
UDP	Outbound	10.1.0.1	64.818	10.0.0.1	62.143	192.203.230.10	53
UDP	Outbound	10.1.0.1	64.818	10.0.0.1	62.143	199.7.83.42	53
UDP	Outbound	10.1.0.1	64.818	10.0.0.1	62.143	192.5.5.241	53
UDP	Outbound	10.1.0.1	64.020	10.0.0.1	64.020	192.168.1.254	53
TCP	Outbound	10.1.0.11	1.079	10.0.0.1	62.144	10.0.0.2	80
TCP	Outbound	10.1.0.11	1.080	10.0.0.1	62.145	10.0.0.2	80

NAPT session mappings in Windows Server

Drawbacks

NAT (and NAPT) can disrupt communications for many protocols, especially those that use UDP. If the protocol embeds the source IP address in the payload, the fact that the IP address has been changed by NAT in the header but not in the payload will often break the protocol. Notably, FTP and IPsec are problematic when used with NAT.

In order to support such protocols, the NAT device may be installed with an **Application Layer Gateway**. This is a service that can inspect and modify the contents of packets. This is referred to as **NAT Traversal**.

Destination NAT / Port Forwarding

The types of NAT described above involve source addresses (and ports in the case of NAPT) from a private range being rewritten with public addresses. This type of address translation is called **source NAT**.

There are also circumstances where you may want to use the router's public address for something like a web server but forward incoming requests to a different IP. This is called **Destination NAT (DNAT) or port forwarding**.

Port forwarding means that the router takes requests *from* the internet for a particular application (say, HTTP / port 80) and sends them to a designated host and port on the LAN.

	LAN IP Address	Description	Protocol Type	LAN Port	Public Port	Enabled	
1	192.168.1.3	Web(http)	TCP	80	80	<input checked="" type="checkbox"/>	<input type="button" value="Clear"/>
2	192.168.1.3	Web(https)	TCP	443	443	<input checked="" type="checkbox"/>	<input type="button" value="Clear"/>
3	192.168.1.3	Email : SMTP	TCP	25	25	<input checked="" type="checkbox"/>	<input type="button" value="Clear"/>
4	192.168.1.3	Email : POP3	TCP	110	110	<input checked="" type="checkbox"/>	<input type="button" value="Clear"/>
5	192.168.1.3	Email : IMAP4	TCP	143	143	<input checked="" type="checkbox"/>	<input type="button" value="Clear"/>
6	192.168.1.3	FTP	TCP	21	21	<input checked="" type="checkbox"/>	<input type="button" value="Clear"/>
7	192.168.1.		TCP			<input type="checkbox"/>	<input type="button" value="Clear"/>

Configuring port forwarding for various applications



Review Questions / Module 3 / Unit 1 / Secure Network Design

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) Why is subnetting useful in secure network design?
- 2) What is the purpose of a DMZ?
- 3) How can a DMZ be implemented?
- 4) What technology would you implement to protect part of a network against packet sniffing?
- 5) True or false? Administration and configuration of a switch should be limited to the "default" or "management" VLAN.
- 6) How could you prevent a malicious attacker from engineering a switching loop from a host connected to a standard switch port?
- 7) What technology would you use to enable private addressing on the LAN and still permit hosts to browse the web?
- 8) What steps would you take to secure a network device against unauthorized reconfiguration?



If you have access to the Hands On Live Labs, complete the "Network Security / Routers" and "Network Security / Routing Protocols" labs now.

Module 3 / Unit 2

Security Appliances and Applications

Objectives

On completion of this unit, you will be able to:

- Know the types and features of network and application firewalls, proxies, gateways, and security appliances.
- Implement and configure security appliances and applications.
- Describe the types and features of Intrusion Detection Systems.
- Understand the importance of configuring and monitoring secure audit logs.

Basic Firewalls



Firewalls are the devices principally used to implement security zones, such as intranet, DMZ, and internet. The basic function of a firewall is **traffic filtering**. A firewall resembles a quality inspector on a production line; any bad units are knocked off the line and go no farther. The firewall processes traffic according to **rules**; traffic that does not conform to a rule that allows it access is blocked.

Types of Firewall

There are many types of firewall and many ways of implementing a firewall. One distinction can be made between firewalls that protect a whole network (placed inline in the network and inspecting all traffic that passes through) and firewalls that protect a single host only (installed on the host and only inspect traffic destined for that host). Another distinction is what parts of a packet a firewall can inspect and operate on.

Almost all firewalls implement NAT or NAPT, with the exception of personal software firewalls. NAT conceals information about the private network behind the firewall.

Packet Filtering Firewalls

Packet filtering describes the earliest types of firewall. All firewalls can still perform this basic function. A packet filtering firewall can inspect the **headers** of IP packets. This means that rules can be based on the information found in those headers:

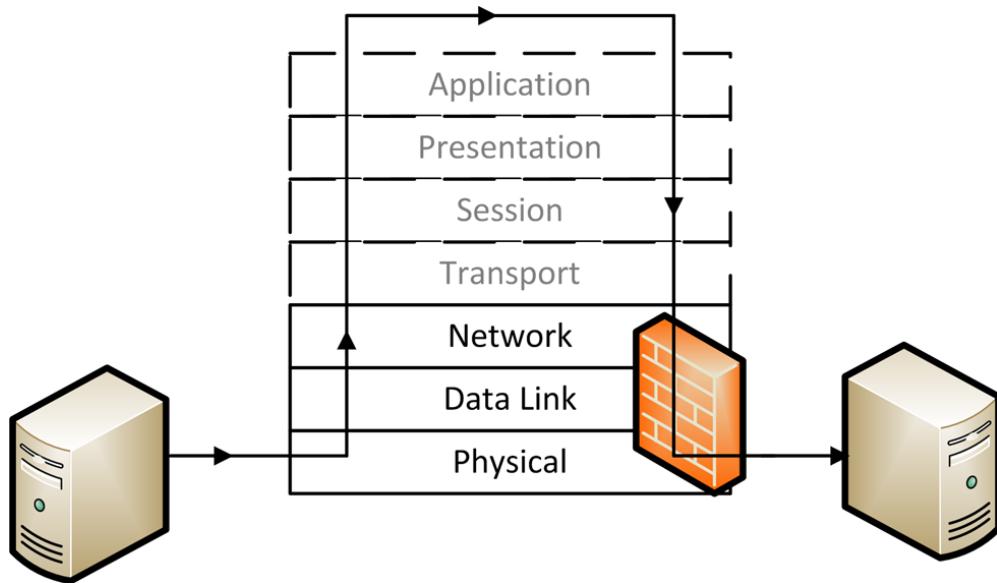
- IP filtering - accepting or blocking traffic on the basis of its source and/or destination IP address.

- Protocol ID / type (TCP, UDP, ICMP, routing protocols, and so on).
- Port filtering / security - accepting or blocking traffic on the basis of source and destination port numbers (TCP or UDP application type).

There may be additional functionality in some products, such as the ability to block some types of ICMP (ping) traffic but not others or the ability to filter by hardware (MAC) address. Packet filtering works mainly at Layer 3 (Network) of the OSI model.



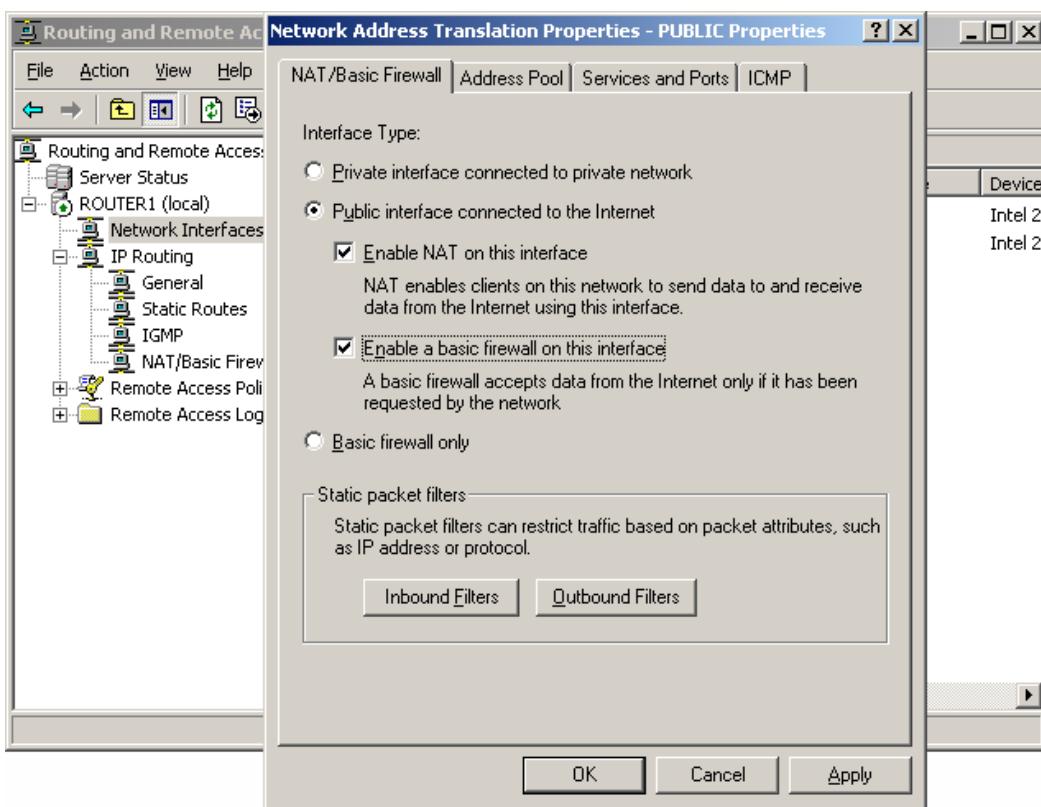
Port numbers are contained in TCP or UDP headers (layer 4) rather than the IP datagram header but packet filtering firewalls are still almost always described as working at layer 3. They can only inspect port numbers and not any other layer 4 header information.



Another distinction that can be made is whether the firewall can control only inbound traffic or both inbound and outbound traffic. This is also often referred to as "ingress" and "egress" traffic or filtering. Controlling outbound traffic is useful because it can block applications that have not been authorized to run on the network and defeat malware such as backdoors.

A packet filtering firewall is configured by specifying a number of rules, called an **Access Control List (ACL)**. An ACL is a list of rules, each of which defines a specific type of data packet and the appropriate action to take when a packet matches the rule. Actions can be either to **block** (drop the packet, and optionally log an event) or to **allow** (let the packet pass through the firewall).

Packet filtering firewalls are simple, fast, and inexpensive.



Configuring a packet filtering firewall under Windows Server



gpysv

Stateful Firewalls

A packet filtering firewall does not maintain **stateful** information about the connection between two hosts. Each packet is analyzed independently with no record of previously processed packets. For example, it cannot defend against the SYN flood Denial of Service attack that can be launched against a TCP/IP network.

Stateful Inspection Firewalls

A **circuit-level stateful inspection firewall** addresses this problem by maintaining stateful information about the session established between two hosts (including malicious attempts to start a bogus session). Information about each session is stored in a dynamically updated **state table**. It operates at Layer 5 (Session) of the OSI model. When a packet arrives, the firewall checks it to confirm whether it belongs to an existing connection. If it does not, it applies the ordinary packet filtering rules to determine whether to allow it. Once the connection has been allowed, the firewall allows traffic to pass unmonitored, in order to conserve processing effort.

A circuit-level firewall examines the TCP three-way handshake and can detect attempts to open connections maliciously (a **flood guard**). It also monitors packet sequence numbers and can prevent session hijacking attacks. It can respond to such attacks by blocking source IP addresses and throttling sessions.



Flood guards may also be required farther up the network stack. Initiating logon attempts to trigger lockout policies is one common DoS technique for instance. Any application may be vulnerable to different types of flooding techniques.



Application Aware Devices

An **application aware device** is one that can inspect the *contents* of packets at the application layer. For example, a web application firewall could analyze the HTML code present in HTTP packets to try to identify code that matches a pattern in its threat database. Application aware devices (and software firewalls) have many different names, including **application layer gateway**, **stateful multilayer inspection**, or **deep packet inspection**.

Application aware devices have to be configured with separate filters for each type of traffic (HTTP and HTTPS, SMTP/POP/IMAP, FTP, and so on).

When first introduced, this type of firewall was costly and required high specification hardware on which to run. Now all but the cheapest firewalls perform stateful multilayer inspection to some extent.

Name	Group
Active Directory Domain Controller - Echo R...	Active Directory Domain
Active Directory Domain Controller - Echo R...	Active Directory Domain
Active Directory Domain Controller - LDAP (T...	Active Directory Domain
Active Directory Domain Controller - LDAP fo...	Active Directory Domain
Active Directory Domain Controller - NetBIO...	Active Directory Domain
Active Directory Domain Controller - SAM/LS...	Active Directory Domain
Active Directory Domain Controller - SAM/LS...	Active Directory Domain
Active Directory Domain Controller - Secure ...	Active Directory Domain
Active Directory Domain Controller - Secure ...	Active Directory Domain
Active Directory Domain Controller - W32Tim...	Active Directory Domain
Active Directory Domain Controller (RPC)	Active Directory Domain
Active Directory Domain Controller (RPC-EP...	Active Directory Domain
BITS Peercaching (Content-In)	BITS Peercaching
BITS Peercaching (RPC)	BITS Peercaching
BITS Peercaching (RPC-EPMAP)	BITS Peercaching
BITS Peercaching (WSD-In)	BITS Peercaching
COM + Network Access (DCOM-In)	COM + Network Access
Core Networking - Destination Unreachable (...	Core Networking
Core Networking - Destination Unreachable ...	Core Networking
Core Networking - Dynamic Host Configurati...	Core Networking
Core Networking - Internet Group Managem...	Core Networking
Core Networking - IPv6 (IPv6-In)	Core Networking
Core Networking - Multicast Listener Done (I...	Core Networking

A stateful host firewall ships with Windows Server and Windows 7

Application aware firewalls are very powerful but they are not invulnerable. Their very complexity means that it is possible to craft DoS attacks against exploitable vulnerabilities in the firewall firmware. Also, the firewall cannot examine encrypted data packets.



The basic function of a packet filtering network firewall is to inspect packets and determine whether to block them or allow them to pass. Network traffic passes (or doesn't pass) through the firewall.

Proxy servers work on a "Store and Forward" model. Rather than inspecting traffic as it passes through, the proxy deconstructs each packet, performs analysis, then rebuilds the packet and forwards it on (providing it conforms to the rules). In fact, a proxy is a "Man in the Middle"; but a legitimate one! This is more secure than a firewall that only performs filtering because if the original packet had contained anything "suspicious" that a firewall had not noticed, a firewall might allow it through whereas the proxy, even if it did not directly identify the suspicious content, would erase it in the process of rebuilding the packet.

The drawback is that there is obviously more processing to be done than with a firewall.

Many firewalls are implemented as proxies. Not all proxies are firewalls however, as they can have other useful functions.

Proxy Servers

A basic proxy server provides for protocol-specific *outbound* traffic. For example, you might deploy a web proxy that enables client computers to connect to websites and secure websites on the internet. In this case, you have deployed a proxy server that services TCP ports 80 and 443 for outbound traffic.

Web proxies are often also described as **web security gateways** as usually their primary functions are to prevent viruses or Trojans infecting computers from the internet, block spam, and restrict web use to authorized sites.

The main benefit of a proxy server is that client computers connect to a specified point within the perimeter network for web access. This provides for a degree of traffic management and security. In addition, most web proxy servers provide **caching engines**, whereby frequently requested web pages are retained on the proxy, negating the need to re-fetch those pages for subsequent requests. Some proxy servers also **pre-fetch** pages that are referenced in pages that have been requested. When the client computer then requests that page, the proxy server already has a local copy.

Proxy servers can generally be classed as **non-transparent** or **transparent**. A non-transparent server means that the client must be configured with the server address to use it; a transparent (or "forced" or "intercepting") proxy intercepts client traffic without the client having to be reconfigured.

Reverse Proxy Servers

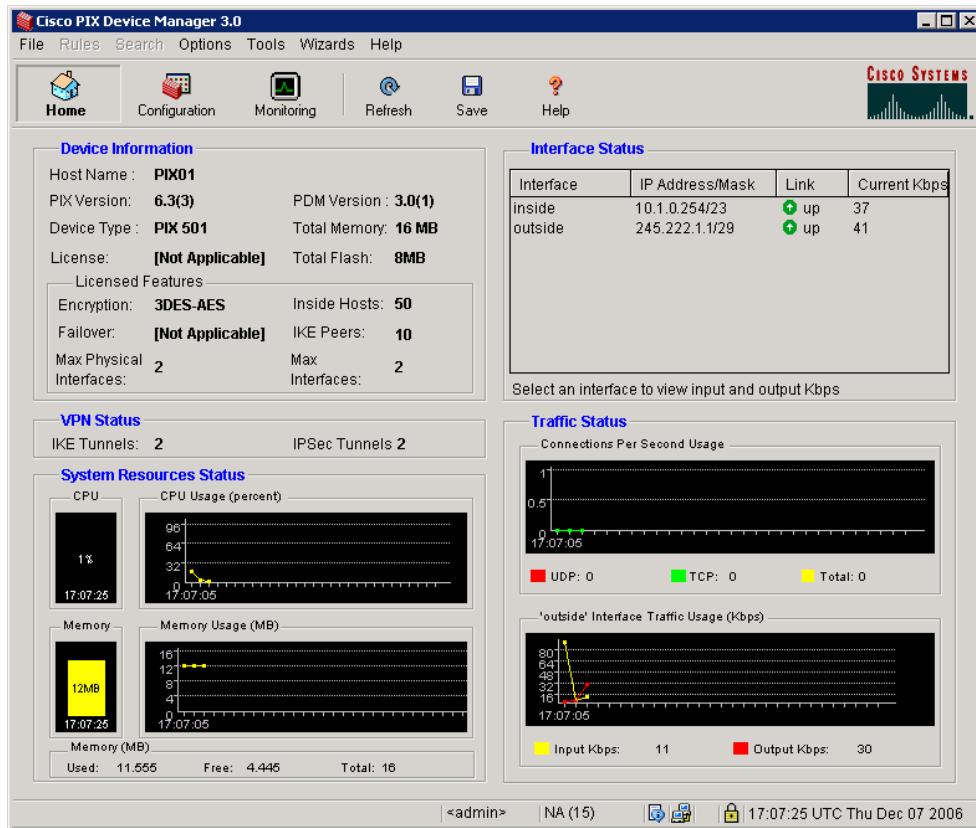
A **reverse proxy server** provides for protocol-specific *inbound* traffic. For security purposes, it is inadvisable to place application servers, such as messaging and VoIP servers, in the perimeter network, where they are directly exposed to the internet. Instead, you can deploy a reverse proxy and configure it to listen for client requests from a public network (the internet) and create the appropriate request to the internal server on the corporate network.

Reverse proxies can *publish* applications from the corporate network to the internet in this way. In addition, some reverse proxy servers can handle the encryption / decryption and authentication issues that arise when remote users attempt to connect to corporate servers, reducing the overhead on those servers. Typical applications for reverse proxy servers include publishing a web server, publishing IM or conferencing applications, and enabling POP/IMAP mail retrieval.

Implementing a Firewall or Gateway

There is no one way to implement a firewall. The following represent some of the most common technologies:

- Appliance firewall - a stand-alone firewall using dedicated hardware and firmware. Nowadays, this role is likely to be performed by an all-in-one or Unified Threat Management (UTM) security appliance, combining the function of firewall, intrusion detection, malware inspection, and web security gateway (content inspection and URL filtering).

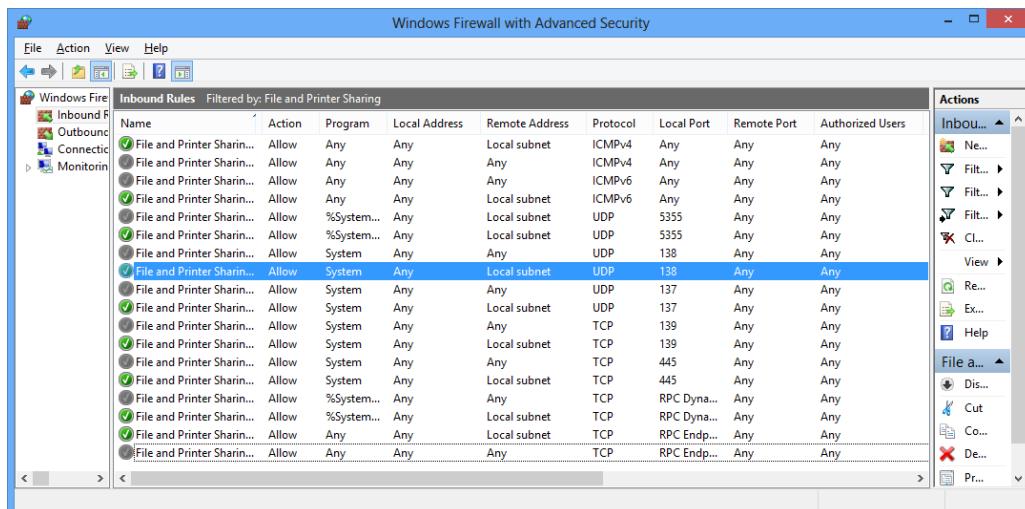


- Router firewall - the firewall functionality is built into the router firmware.
- Switch firewall - some layer 3 switches can perform packet filtering.
- NOS firewall - software designed to run under a network server. This could be a simple packet filtering firewall or an application aware firewall.
- Application firewall - software designed to run on a server to protect a particular application only (a web server firewall for instance or a firewall designed to protect an SQL Server database). This would typically be deployed in addition to a network firewall.
- Personal firewall - software designed to run on a single client computer.



Configuring a Firewall

A firewall is an example of **rule-based management**. Firewall rules are configured on the principle of **least access**. This is the same as the principle of least privilege; only allow the minimum amount of traffic required for the operation of valid network services and no more.



Sample firewall rule set

The rules in a firewall's ACL are processed top-to-bottom. If traffic matches one of the rules then it is allowed to pass; consequently the most important and specific rules are placed at the top. The final default rule is typically to block any traffic that has not matched a rule (**implicit deny**). Each rule can specify whether to block or allow traffic based on a number of parameters, often referred to as **tuples**. If you think of each rule being like a row in a database, the tuples are the columns. For example, in the screenshot above, the tuples include "Program", "Local Address", "Remote Address", "Protocol", "Local Port", "Remote Port", "Authorized Users", and so on.

Even the simplest packet filtering firewall can be complex to configure securely. It is essential to create a written policy describing what the firewall should do and to test the firewall configuration as far as possible to ensure that the ACLs you have set up work as intended. Also test and document changes made to ACLs. Some other basic principles include:

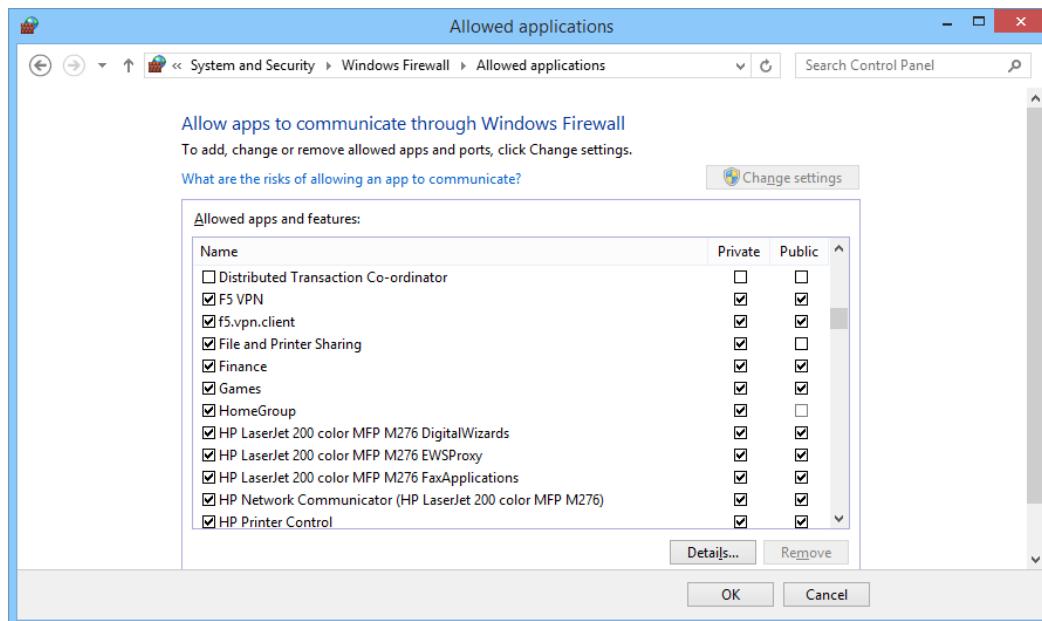
- Block incoming requests from internal or private IP addresses (that have obviously been spoofed).
- Block incoming requests from protocols that should only be functioning at a local network level, such as ICMP, DHCP, or routing protocol traffic.
- Use penetration testing to confirm the configuration is secure. Log access attempts and monitor the logs for suspicious activity.
- Take the usual steps to secure the hardware on which the firewall is running and use of the management interface.



Host-based Firewalls

A **host-based firewall** or **personal firewall** describes a firewall that is implemented as a software application running on a single host. The firewall is designed to protect that host only (as opposed to a network).

While they can perform basic packet filtering, to make them simpler for a user to configure, personal firewalls tend to be program- or process-based. When a program tries to initiate (in the case of outbound) or accept (inbound) a TCP/IP network connection, the firewall prompts the user to block, allow once, or allow always.



Windows Firewall

Advanced configuration options allow the user to do things such as specify ports or IP scopes for particular programs (to allow access to a local network but not the internet for instance), block port scans, and so on.

One of the main drawbacks of a personal firewall is that as software it is open to compromise by malware. For example, there is not much point in allowing a process to connect if the process has been contaminated by malicious code, but a basic firewall would have no means of determining the integrity of the process. Therefore the trend is for security suite software, providing comprehensive anti-virus and intrusion detection.



A growing malware trend is to target vulnerabilities or exploits in security software specifically.

When using a personal firewall on an enterprise network, some thought needs to be given as to how it will interact with network border firewalls. The use of personal firewalls can make troubleshooting network applications more complex.



or6rc

Web Application Firewall

A **Web Application Firewall (WAF)** is one specifically designed to block threats over HTTP. Its ruleset is designed to prevent specific attacks on web applications, such as Cross-site Scripting (XSS), SQL injection, and DDoS. It is capable of performing sophisticated analysis of HTTP sessions to detect whether an attack might be occurring. A WAF may also be capable of examining outbound traffic to ensure that confidential information such as credit card numbers is not being stolen.

A web application firewall could be implemented as software running on the web server itself or as a standalone network appliance.



See [Unit 4.4](#) for more information about web application threats and security measures.



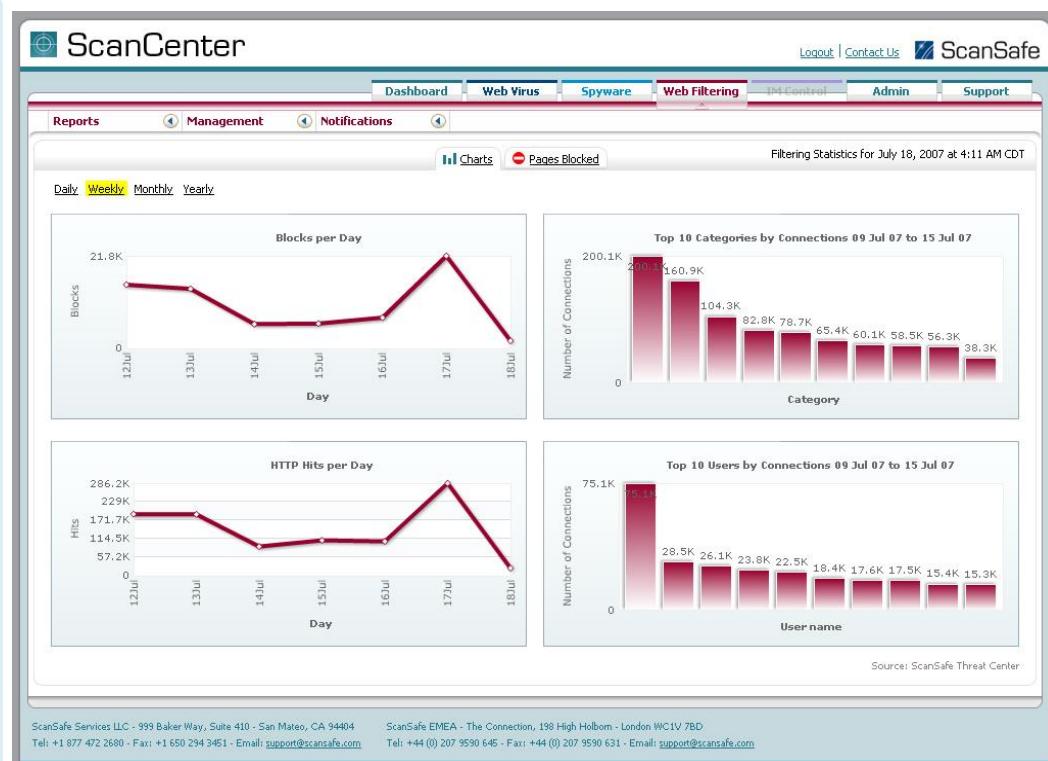
xtnew

Web and Email Security Gateways

As firewalls have become effective at blocking unwanted ports, configuring network applications to work with firewalls has become more difficult. Many network applications consequently package all their content as HTTP traffic and send it all over port 80. This means that allowing all HTTP traffic is not particularly secure, as it could be allowing all sorts of malicious applications or management interfaces, in addition to basic web pages.

A **web security gateway** is designed for corporate control over employees' internet use. It could be implemented as a standalone appliance or proxy server software. Many ISPs implement content filtering as part of their internet access packages.

Web security gateways would typically apply content restrictions to web, Instant Messaging, email, FTP, and P2P applications. Filtering can be applied to a mix of permitted / restricted URLs, keyword matching, web object matching (looking at usage of plug-ins), time of day use, total usage, and so on. The software may also allow the creation of profiles for different user groups and should feature logging and reporting capabilities.



ScanCenter web content filter from www.scansafe.com

As mentioned above, many security gateway software products and appliances perform an "all-in-one" role, combining the function of firewall, web and email content gateway / filter, malware scanner, and intrusion detection engine. This is also referred to as **Unified Threat Management (UTM)**.

Simple Mail Transfer Protocol (SMTP)

Electronic mail enables a person to compose a message and send it to another user on their own network (intranet) or anywhere in the world via the internet. The **Simple Mail Transfer Protocol (SMTP)** specifies how mail is delivered from one system to another. It is a relatively straightforward protocol that makes the connection from the sender's server to that of the recipient and then transfers the message.

The SMTP server of the sender discovers the IP address of the recipient SMTP server using the domain name part of the email address. The SMTP server for the domain is registered on the DNS using a **Mail Exchanger (MX)** record. SMTP communications take place over TCP port 25.

Post Office Protocol (POP3)

SMTP is only useful to deliver mail to hosts that are permanently available. Mail users require the convenience of receiving and reading their mail when they choose. The **Post Office Protocol v3 (POP3)** is designed to allow mail to be downloaded to the recipient's email client at his or her convenience.

A POP3 client application (such as Microsoft Outlook or Mozilla Thunderbird) establishes a TCP connection to the POP3 server over port 110. This is often a different service running on the *same machine* as the SMTP server. The user is authenticated (by username and password) and the contents of his or her mailbox are downloaded for processing on the local PC.

```
GNU nano 2.2.2          File: /etc/dovecot/dovecot.conf          Modified

protocols = imap imaps
#protocols = none

# A space separated list of IP or host addresses where to listen in for
# connections. "*" listens in all IPv4 interfaces. "[::]" listens in all IPv6
# interfaces. Use "*", "[::]" for listening both IPv4 and IPv6.
#
# If you want to specify ports for each service, you will need to configure
# these settings inside the protocol imap/pop3/managesieve { ... } section,
# so you can specify different ports for IMAP/POP3/MANAGESIEVE. For example:
protocol imap {
    listen = *:143
    ssl_listen = *:943
}
protocol pop3 {
    listen = *:10100
#
#
}
protocol managesieve {
    listen = *:12000
#
#
}
#listen = *

# Disable LOGIN command and all other plaintext authentications unless
[ Read 1280 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^T Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Configuring mailbox access protocols on a server

Internet Message Access Protocol (IMAP)

While POP3 is widely used, it does have limitations, some of which are addressed by the **Internet Message Access Protocol v4 (IMAP4)**. Clients connect over port 143 (993 for SSL). They authenticate themselves then retrieve messages from the designated folders. SMTP is still needed to support mail delivery. Like POP3, IMAP is a mail retrieval protocol only.

POP3 is primarily designed for dial-up access; the client contacts the server to download its messages then disconnects. IMAP supports permanent connections to a server and connecting multiple clients to the same mailbox simultaneously. It also allows a client to manage the mailbox on the server (to organize messages in folders and control when they are deleted for instance) and to create multiple mailboxes.



8j35a

Spam Filters and Mail Gateways

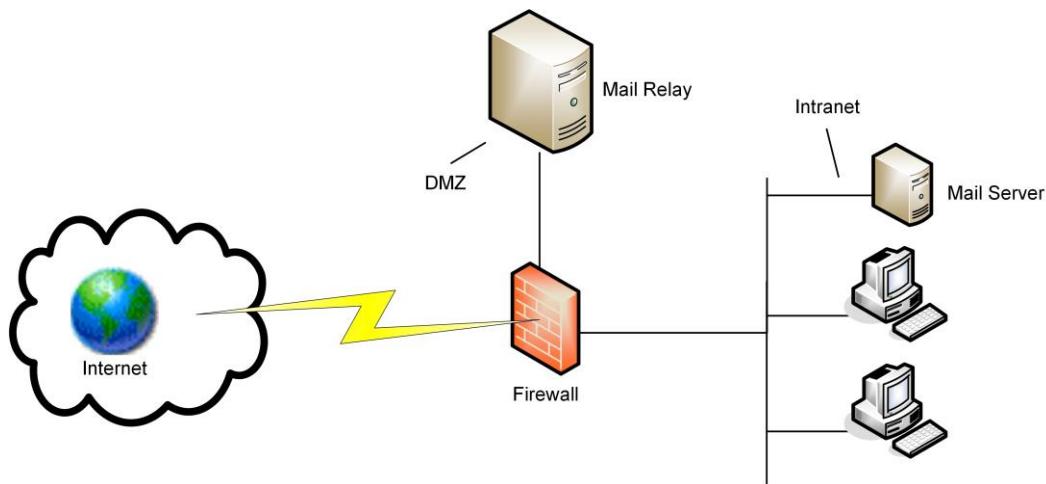
Spam is unsolicited email. Dealing with spam wastes resources (computer and people). Most new email application software has spam filtering built-in. This is an appropriate solution for home users but on enterprise networks, if spam has already reached the user's mailbox then it has already wasted bandwidth and taken up space on the server.

Consequently, most companies deploy a gateway server with spam filtering technology. This can either be installed in-house or leased from a provider such as MessageLabs.



Spam filtering can cause legitimate messages to be blocked. It needs careful configuration to provide the right balance between security and usability.

A secure configuration for email is to install an email relay server in a Demilitarized Zone (DMZ).



The mail relay can be installed with software to monitor and filter email traffic, checking for spam and infected file attachments.

MessageLabs mail filtering gateway

Apart from message-based filtering and using blacklists (to block mail servers or domains known to send spam), there are many other methods for trying to reduce spam. As with filters though, these can generate numerous "false positives" (that is, block legitimate traffic). Some examples include:

- Whitelist - if an organization only deals with a limited number of correspondents, they can set up a whitelist of permitted domains or use some sort of authentication between the mail servers.
- SMTP standards checking - rejecting email that is not strictly RFC-compliant can block some spam, but may also block legitimate traffic.
- rDNS (reverse DNS lookup) - rejecting mail from servers where the IP address does not match the domain in the message header or is a dynamically assigned address.
- Tarpitting - introducing a delayed response to the SMTP session. This makes the spammer's server less efficient; in many cases the spamming software will simply give up.
- Recipient filtering - block mail that is not addressed to a valid recipient email address.

Intrusion Detection Systems



An **Intrusion Detection System (IDS)** is a means of using software tools to provide *real-time* analysis of either network traffic or system and application logs. IDS is similar to anti-virus software but protects against a broader range of threats.

Network-based Intrusion Detection Systems

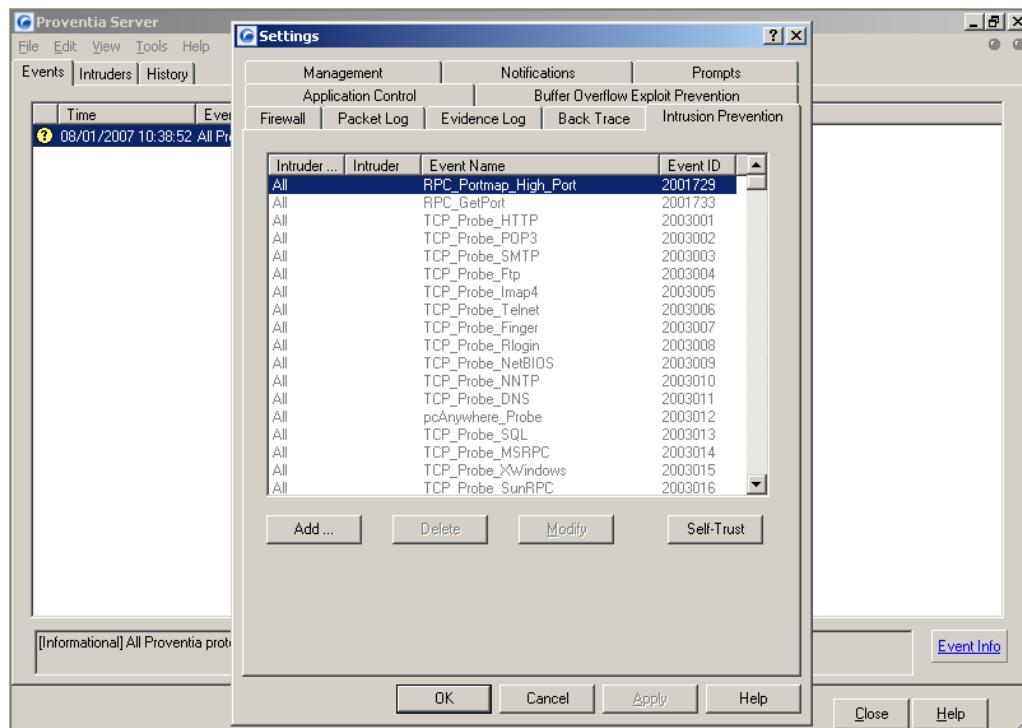
A **Network IDS (NIDS)** is basically a packet sniffer (referred to as a **sensor**) with an **analysis engine** to identify malicious traffic and a **console** to allow configuration of the system.

Typically, NIDS sensors are placed inside a firewall or close to some server of particular importance (the idea is to identify malicious traffic that has managed to get *past* the firewall). In a switched environment, the sensor must be connected to a spanning port on the switch in order to monitor traffic passing through the switch on other ports (also known as port mirroring). If the switch does not support spanning ports, another option is to install a tap. This is a device that connects directly to the network media.

The sensor does not slow down traffic and is undetectable by the attacker (it is not connected to the same logical network).

The basic functionality of NIDS is to provide **passive detection**; that is, to log intrusion incidents and to display an alert at the management interface or to email the administrator account. A NIDS will be able to identify and log hosts and applications, detect buffer overflow attacks, password guessing attempts, port scans, worms, backdoor applications, malformed packets or sessions, and policy violations (ports or IP addresses that are not permitted for instance).

Some NIDS have prevention capabilities however. These are classified as **active detection** (or **reactive** detection). One typical preventive measure is to end the TCP session (sending a spoofed TCP reset packet to the attacking host). This will not always succeed in preventing an attack however. Another option is for the sensor to apply a temporary filter on the firewall to block the attacker's IP address (shunning). Finally, the sensor may be able to run a script or third-party program to perform some other action not supported by the IDS software itself.



ISS Proventia Server Agent intrusion prevention software

The main disadvantages of NIDS are:

- If an attack is detected, without an effective active response option there can be a significant delay before an administrator is able to put countermeasures in place.
- Heavy traffic (such as a large number of sessions or high load) may overload the sensor or analysis engine, causing packets to pass through uninspected. A blinding attack is a DoS aimed at the IDS with the intention of generating more incidents than the system can handle. This attack is run in parallel with the "real" attack.
- Training and tuning are complex, resulting in high false positive and false negative rates, especially during the initial deployment.
- Encrypted traffic cannot be analyzed, though often the setup of an encrypted session can be monitored to ensure that it is valid.

Unified Threat Management

"All-in-one" or **Unified Threat Management (UTM)** appliances and applications merge the roles of firewall and IDS, creating **Intrusion Detection and Prevention Systems (IDP or IPS or NIPS)** that can provide an active response to network threats. Some can also provide inline, "wire-speed" anti-virus scanning. Their rulesets can also be configured to provide user content filtering, such as blocking URLs, applying keyword-sensitive blacklists or whitelists, or applying time-based access restrictions.

UTM appliances are positioned like firewalls at the border between two network zones. As with proxy servers, the appliances are "inline" with the network, meaning that all traffic passes through them (also making them a single point-of-failure if there is no fault tolerance mechanism). This obviously means that they need to be able to cope with high bandwidths and process each packet very quickly to avoid slowing the network down.

IDP software is capable of advanced measures, including throttling bandwidth to attacking hosts, applying complex firewall filters, and even modifying suspect packets to render them harmless.

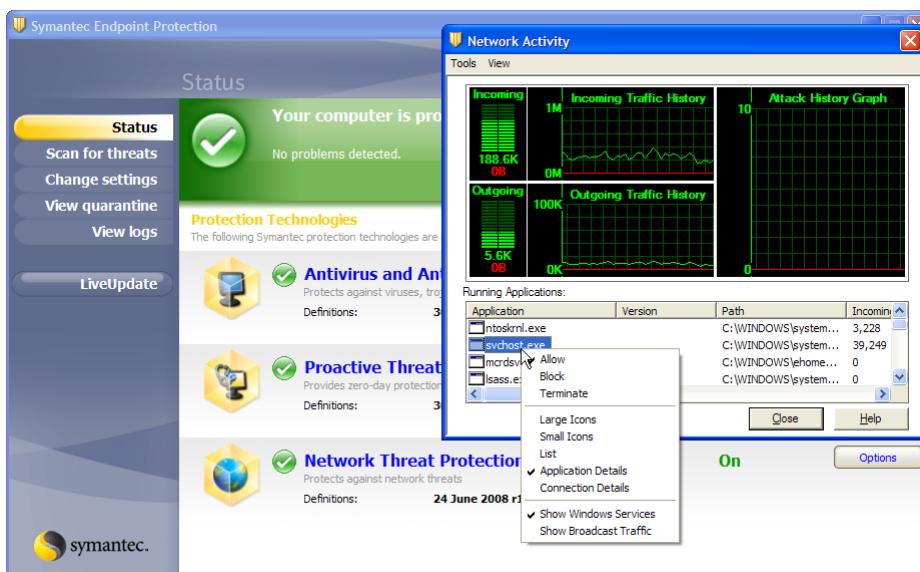


As well as preventing malicious content from coming in, some security appliances can prevent confidential data from going out. These can be used to implement Data Loss Prevention (DLP) - see [Unit 4.2](#) for more information on DLP.

Host-based IDS (HIDS)

A **Host-based IDS (HIDS)** captures information from a single host (a server, router, or firewall for instance).

HIDS come in many different forms with different capabilities. The core ability is to capture and analyze log files, but more sophisticated systems can also monitor OS kernel files, monitor ports and network interfaces, and process data and logs generated by specific applications (such as HTTP or FTP).



Monitoring services and intrusion attempts in Symantec Endpoint Protection security suite

Installing host-based IDS is simply a case of choosing which hosts to protect then installing and configuring the software. There will also normally be a reporting and management server to control the agent software on the hosts.



Ideally, an IDS host has two network interfaces; one to connect to the normal network; the other is a management interface to connect to a separate network containing the management server. This could be implemented as a physically separate network infrastructure or as a VLAN.

Host-based active response can act to preserve the system in its intended state. This means that the software can prevent system files from being modified or deleted, prevent services from being stopped, log off unauthorized users, and filter network traffic.

The main advantage of HIDS is that they can be much more application specific than NIDS. For example, HIDS can analyze encrypted traffic (once it has been decrypted on the host) and it is easier to train the system to recognize normal traffic.

The main disadvantages of HIDS are:

- The software is installed on the host and therefore detectable. This means that it is vulnerable to attack by malware.
- The software also consumes CPU, memory, and disk resources on the host.
- Depends on OS and application logs being configured properly.

IDS Analysis Engines



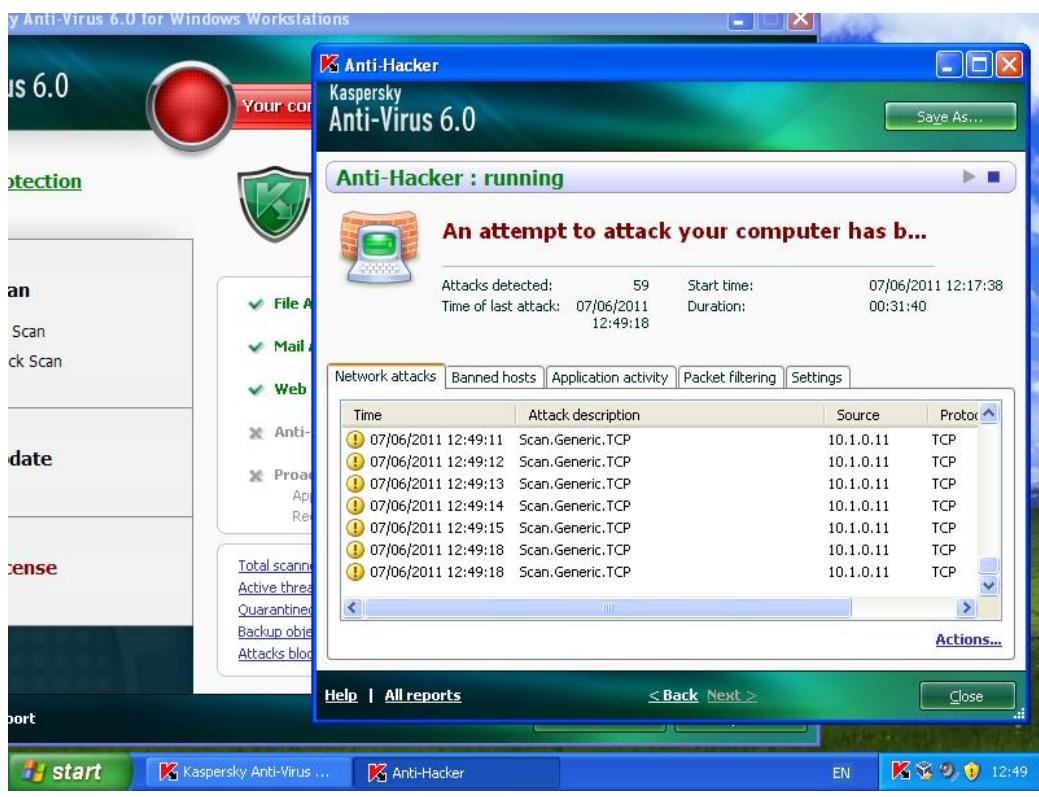
3m10d

In both network and host intrusion detection, the **analysis engine** is the component that scans and interprets the traffic captured by the sensor or agent with the purpose of identifying suspicious traffic. The analysis engine determines whether any given event should be classed as an **incident** (or violation of the security policy or standard).

There are several methods of doing this...

Signature-based Detection

Signature-based detection (or pattern-matching) means that the engine is loaded with a database of attack patterns or signatures. If traffic matches a pattern then the engine generates an incident.



Detecting a network scanning attack with Kaspersky Anti-Virus

Behavior-based Detection

Behavior-based detection (or statistical- or profile-based detection) means that the engine is trained to recognize baseline "normal" traffic or events. Anything that deviates from this baseline (outside a defined level of tolerance) generates an incident. The idea is that the software will be able to identify "zero-day" attacks (those for which the exploit has not been detected or published).

The engine does not keep a record of everything that has happened and then try to match new traffic to a precise record of what has gone before. It uses **heuristics** (meaning to learn from experience) to generate a statistical model of what the baseline looks like. It may develop several profiles to model network use at different times of the day. This means that the system generates false positive and false negatives until it has had time to improve its statistical model of what is "normal".

Anomaly-based Detection

Often behavior- and anomaly-based detection are taken to mean the same thing (in the sense that the engine detects anomalous behavior). Anomaly-based detection can also be taken to mean specifically to look for irregularities in the use of protocols. For example, the engine may check packet headers or the exchange of packets in a session against RFC standards and generate an alert if they deviate from strict RFC compliance.

Advantages and Disadvantages of Analysis Methods



9qxof

Most IDS now use a combination of these methods but there are advantages and disadvantages to each.

The two principal vulnerabilities of signature detection are that the protection is only as good as the last signature update and that no protection is provided against threats that cannot be matched in the pattern database. Another issue is that pattern matching often cannot detect attacks based on a complex series of communications.

These vulnerabilities are addressed by behavior-based detection, which is effective at detecting previously unknown threats. Heuristic, profile-based detection is usually harder to set up and generates more false positives and false negatives than 1:1 pattern matching.



A false positive is where legitimate behavior is identified as an incident. Conversely, a false negative is where malicious traffic is not identified. False positives disrupt ordinary users but false negatives mean that attacks are going undetected.

Signature matching can be tuned to the extent of disabling signatures that are not relevant to the network. For example, it would be appropriate to disable Windows-specific threat signatures on a Linux network. Behavior-based detection requires an intensive training period, during which there could be considerable disruption to the network in addition to requiring close monitoring by administrators. Also, re-training may be required as typical network use changes over time and the IDS starts to generate more false positives. Behavior-based detection also requires more processing resources.

Some IDS support dynamic profiles, which automatically adjust over time to match typical network behavior. These can be vulnerable to low-level attacks, during which only a small amount of malicious traffic is generated at any one time. Another vulnerability is for an administrator to allow malicious traffic through during the training period by mistake.



kljc9

Monitoring System Logs

Logs are one of the most valuable sources of security information. A log can record both authorized and unauthorized uses of a resource or privilege. Logs function both as an audit trail of actions and (if monitored regularly) provide a warning of intrusion attempts.



Logs typically associate an action with a particular user. This is one of the reasons that it is critical that users not share log on details. If a user account is compromised, there is no means of tying events in the log to the actual attacker.

Types of Log

All NOS and many software applications log system events automatically. However, many types of log may need to be enabled manually. For example, Windows does not log use of user account privileges or file access automatically. The following general types of log can be identified:

- Event log - records things that occur within an operating system (the System event log in Windows for instance) or a software application (Windows' Application log). These logs are used to diagnose errors and performance problems.
- Audit log - records the use of system privileges, such as creating a user account or modifying a file. Security logging needs to be configured carefully as over-logging can reduce the effectiveness of auditing by obscuring genuinely important events with thousands of routine notifications and consume disk resources on the server.
- Security log - this is another way of describing an audit log. The audit log in Windows Event Viewer is called the Security log.
- Access log - server applications such as Apache can log each connection or request for a resource. This log is typically called the access log.



NIST have published a guide to security log management (SP800-92) available at gtsgo.to/76c3m.



3o909

Establishing Baselines

A **baseline** establishes (in security terms) the expected pattern of operation for a server or network. As well as baselining the server configuration, you can also take a baseline performance measurement. Significant variation from the baseline could be an indicator of some kind of attack or other security breach.

Remember that server usage will change during the day and there may be known, expected events that cause utilization to go up (scanning for viruses or running Windows Update for instance). Your baseline should identify typical usage patterns so that it is easier to spot anything genuinely out-of-the-ordinary.

Most operating systems provide some tools for this process, and most server vendors ship equipment with their own monitoring software, or you can use third-party tools.

Changes to the system require a new baseline to be taken. Some examples when this should be done are:

- Hardware or software upgrade.
- Reconfiguration of software.
- Installation of new software.
- Changed user access volume or patterns.
- Changed server role.

Establishing Thresholds

Thresholds are points of reduced or poor performance or security-related events that generate an administrative alert. Examples include low disk space, high memory, CPU, or network utilization, server chassis intrusion, failed logins, and so on.

Setting thresholds is a matter of balance. On the one hand you do not want performance to deteriorate to the point that it affects user activity; on the other you do not want to be overwhelmed by performance alerts.

Some of the key performance counters to watch for in terms of detecting security-related intrusions or attacks are:

- Free disk space - rapid decreases in available disk space could be caused by malware or illegitimate use of a server (as a peer-to-peer file sharing host for instance).
- High CPU or network utilization - this could have many causes but could indicate the presence of a worm or Trojan or peer-to-peer file sharing software.
- Memory leak - a process that takes memory without subsequently freeing it up (look for decreasing Memory/Available Bytes and increasing Memory/Committed Bytes) could be a legitimate but faulty application or could be a worm or other type of malware.
- Page file usage - high page file utilization could be caused by insufficient physical memory but otherwise could indicate malware.
- Account activity - any unusual activity in the area of account creation, allocation of rights, logon attempts, and so on might be suspicious.
- Out-of-hours utilization - if you can discount scheduled activities such as backup or virus scanning, any sort of high utilization when employees are not working is suspicious.

Reporting Alerts and Alarms

If a threshold is exceeded, some sort of alert or alarm notification must take place. A low priority alert may simply be recorded in a log. A high priority alarm might make some sort of active notification, such as emailing a system administrator or triggering a physical alarm signal.

Secure Logging

For computer logs to be accepted as an audit trail, they must be shown to be tamper-proof. It is particularly important to secure logs against tampering by rogue administrative accounts as this would be a means for an insider threat to cover his or her traces.

Log files should be writable only by system processes or by secure accounts that are separate from other administrative accounts. Log files should be configured to be "append only" so that existing entries cannot be modified.

Another option is for the log to be written to a remote server over a secure communications link.

Maintaining Logs

If left unmonitored and set to append only, logs can grow to consume a large amount of disk space. Most logs are set to overwrite older events automatically to forestall this. The old events can be written to an archive log but obviously these must be moved to secure long-term storage to avoid filling up the server's disk.



Log Analysis and Reporting Trends

Not all security incidents will be revealed by a single event. One of the features of **log analysis** and reporting software should be to identify **trends**. A trend is difficult to spot by examining each event in a log file. Instead, you need software to chart the incidence of particular types of event and show how the number or frequency of those events changes over time. Examples could include:

- Increasing amounts of malware activity.
- Failure of hosts to obtain security patches.
- Increasing bandwidth usage / reducing performance.

Software designed to assist with security logging and alerting is often described as **Security Information and Event Management (SIEM)**.



Someone should be reviewing logs continually. Only referring to the logs following a major incident is missing the opportunity to identify threats and vulnerabilities early and to respond proactively.



Review Questions / Module 3 / Unit 2 / Security Appliances and Applications

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What is the advantage of a firewall that works above layer 3 of the OSI model?
- 2) What distinguishes a personal software firewall from a network firewall appliance?
- 3) Other than attempting to block access to sites based on content, what other security options might be offered by web security gateways?
- 4) True or false? Host-based IDS cannot be combined with network-based IDS?
- 5) What are examples of passive detection?
- 6) What sort of maintenance must be performed on signature-based monitoring software?
- 7) What is the best option for monitoring switched Ethernet traffic?
- 8) What feature of server logs makes them useful as an audit trail?
- 9) What difficulty is inherent in monitoring the way users exercise privileges granted to them (to access particular files for instance)?
- 10) You have configured perimeter security firewalls. What type of security control would provide defense-in-depth against insider threats?



If you have access to the Hands On Live Labs, complete the "Network Security / Firewall Rule Based Management", "Network Security / Firewall Rule Based Management" and "Network Security / Spam Filter" labs now.

Module 3 / Unit 3

Wireless Network Security

Objectives

On completion of this unit, you will be able to:

- Describe different types of wireless attacks.
- Configure and troubleshoot wireless network security (encryption, authentication, and site surveys).

Wireless LANs

A **wireless** system uses electromagnetic waves to carry data signals over the air. Wireless transmission methods are also referred to as "unguided media". These systems are often used in a hybrid environment comprising some cable and some wireless technology. From a security point-of-view, the problem with wireless is that signals are usually relatively simple to eavesdrop. The way some wireless standards were originally implemented also opened numerous security vulnerabilities, most of which have been addressed in the last few years.

Wi-Fi Topologies

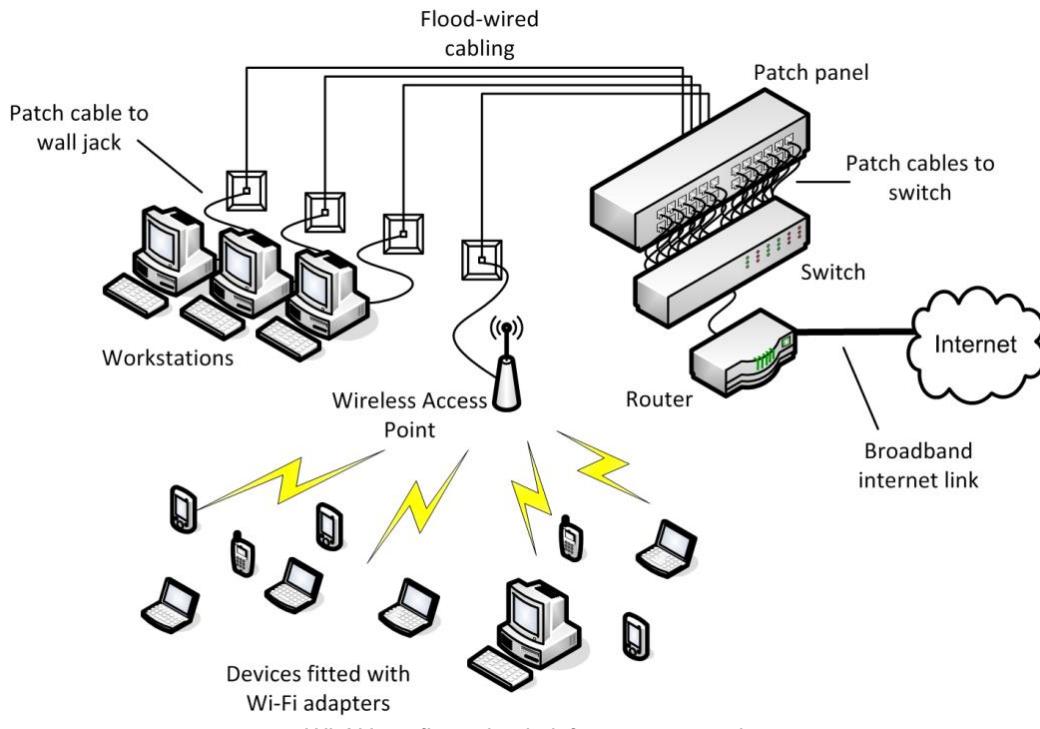
Wireless networks can be configured in one of two modes:

- Ad hoc - the wireless adapter allows connections to and from other devices (a peer-to-peer WLAN). In 802.11 documentation, this is referred to as an **Independent Basic Service Set (IBSS)**.
- Infrastructure - the adapter is configured to connect through an Access Point (AP) to other wireless and wired devices. In 802.11 documentation, this is referred to as a **Basic Service Set (BSS)**. The MAC address of the AP is used as the Basic Service Set Identifier (BSSID).

More than one BSS can be grouped in an **Extended Service Set (ESS)**.

The AP is normally attached to the LAN using standard cabling and transmits and receives network traffic to and from wireless devices. Each client device requires a wireless adapter compatible with the standard(s) supported by the AP.

All wireless devices operating on a WLAN must be configured with the same network name (**Service Set Identifier** or **SSID**). When multiple access points are grouped into an extended service set, this is more properly called the Extended SSID (ESSID). This just means that all the APs are configured with the same SSID.



WLAN configuration in infrastructure mode

Wireless connections require careful configuration to make the connection and transmissions over the connection secure. Some security problems and solutions are listed below.



Wireless Packet Sniffing

As *unguided media*, WLANs are subject to **data emanation**, or signal "leakage". A WLAN is a broadcast medium, like hub-based Ethernet. Consider how much simpler packet sniffing is on hub-based compared to switched Ethernet. Similarly, on a WLAN, there is no simple way to "limit" the signal within defined boundaries. It will propagate to the extent of the antenna's broadcast range, unless blocked by some sort of shielding or natural barrier. Data emanation means that packet sniffing a WLAN is trivially easy if you can get within range.



Many Windows wireless card drivers are not supported by wireless sniffing software. Much of this software is designed to run on Linux. The wireless adapter must support being placed in monitor mode.



War Driving and War Chalking

"War driving" is the practice of driving around with a wireless-enabled laptop scanning for insecure WLANs. "War chalking" is the practice of marking little symbols to advertise the presence of an open and exploitable AP.



War chalking is a bit of an urban legend. The symbols are more likely to be used by internet cafes than by "war drivers" but keep your eyes peeled...



WEP and WPA

Because it is so easy to eavesdrop on communications, for Wi-Fi networks to offer confidentiality and integrity, hosts must authenticate to join the network and the transmissions must be encrypted. There are two encryption schemes: **Wired Equivalent Privacy (WEP)** and **Wi-Fi Protected Access (WPA)**.

Wired Equivalent Privacy (WEP)

WEP is supported on old and new devices. However, the encryption system, based on the **RC4** cipher, is flawed.

WEP IV Attack



Under WEP version 1, you can select from different key sizes (64-bit or 128-bit). WEP version 2 enforces use of the 128-bit key, but is still not considered secure. The main problem with WEP is the 24-bit initialization vector (IV). The IV is supposed to change the key stream each time it is used. Problems with the IV are:

- It is transmitted in plaintext (not encrypted).
- It is not sufficiently large, meaning it is reused and subject to "brute force" attacks, where raw computing power is used to discover the encryption key and decrypt the confidential data.
- It is often not generated using a sufficiently random algorithm; again, assisting brute force or statistical analysis attacks.

```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
CH 5 || Elapsed: 16 mins || 2011-06-03 08:57 || WPA handshake: 00:26:44:00:14:7C:BA:DB:36
BSSID      PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER A1
00:14:7C:BA:DB:36 0 92 9802 35813 126 5 54 . WEP WEP OI
BSSID      STATION PWR Rate Lost Packets Probes
00:14:7C:BA:DB:36 00:16:E0:03:20:82 0 8 - 1 169169 181108

root@bt: ~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
Aircrack-ng 1.0 r1645
[00:00:12] Tested 123497 keys (got 29328 IVs)
KB depth byte(vote)
0 0/ 2 25(45056) 61(40704) 5B(38656) 5C(37776) 74(37128)
1 0/ 14 D(37192) 5D(39880) 26(38864) 4B(36088) 6C(36688)
2 1/ 15 50(46868) 52(39168) 54(37676) 4C(37376) F8(37128)
3 0/ 15 7C(48192) BA(38656) 46(38144) 18(37888) D1(36684)
4 48/ 43 EF(33792) 2C(33536) 2F(33536) 4C(33536) 9B(33536)

KEY FOUND! [ 25:D1:50:7C:60 ]
Decrypted correctly: 100%
root@bt: ~

root@bt: ~ - Shell - Konsole <4>
Session Edit View Bookmarks Settings Help
Wrote packet to: classroom-arp
root@bt: ~# airoplay-ng -interactive -r classroom-arp mon0
For information, no action required: Using gettimeofday() instead of /dev/rtc
No source MAC (h) specified. Using the device MAC (00:16:E0:03:20:82)

Size: 68, FromDS: 0, ToDS: 1 (WEP)
      BSSID = 00:14:7C:BA:DB:36
      Dest. MAC = FF:FF:FF:FF:FF:FF
      Source MAC = 00:16:E0:03:20:82

0x0000: 08:01 03:01 00:14 7C:ba d3:36 00:16 c0:03 2d:82 .A...|..6...
0x0010: ffff ffff ffff 8001 75a6 2a00 cbc1 5280 .u.*...R.
0x0020: c054 b5b5 977a ac89 44fd 57ce 0a5c ed58 .TKU.z..D.W.\.X
0x0030: 41d0 ae74 82a9 db4a bc65 8d71 c543 85dc A..t..J.e.q.C...
0x0040: cd00 810f

Use this packet ? y
Saving chosen packet in replay_src.0603-085243.cap
You should also start airodump-ng to capture replies.

Sent 17565 packets... (499 pps)

```

Aireplay sniffs ARP packets to harvest IVs while Airodump saves them to a capture, which Aircrack can analyze to identify the correct encryption key

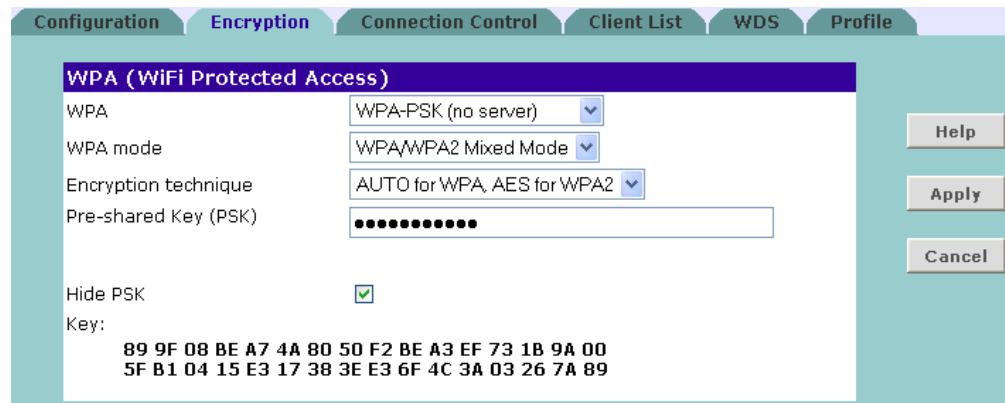
These flaws allow attackers using **WEP cracking** tools such as Aircrack-NG or AirSnort to decrypt and eavesdrop traffic. The IV attack is made more successful if the cracking software can obtain many examples of IVs. Consequently, a type of replay attack is used to make the access point generate lots of IV packets. WEP is not safe to use. If devices only support WEP, the best alternative is to enhance the connection security with another security application, such as L2TP / IPsec.



Wi-Fi Protected Access (WPA / WPA2)

WPA fixes most of the security problems with WEP and adds the ability to authenticate to a network using the 802.1X security model. WPA still uses the RC4 cipher but adds a mechanism called the **Temporal Key Integrity Protocol (TKIP)** to make it stronger. TKIP fixes the checksum problem in WEP (Message Integrity Check), uses a larger IV (48-bit), transmits it as an encrypted hash rather than in plaintext, adds a sequence counter to resist replay attacks, and ensures that keys are not reused.

WPA2 is fully compliant with the 802.11i WLAN security standard. The main difference to WPA is the use of **AES (Advanced Encryption Standard)** for encryption. AES is stronger than RC4 / TKIP. The only reason not to use WPA2 is if it is not supported by adapters, APs, or operating systems on the network. In many cases, devices will be compatible with a firmware or driver upgrade. AES is deployed within the **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)**. AES replaces RC4 and CCMP replaces TKIP.



Configuring encryption on an access point

WPA/WPA2 is much more secure than WEP and there are few known attacks against the protocol itself. When used in pre-shared key mode, an attacker can obtain the encrypted key by associating with the access point and then subject the key to brute force or dictionary-based password attacks. These may succeed if a weak password was used to generate the key. When enterprise authentication is deployed (see below), there are no known attacks that would enable an attacker to gain unauthorized access to the network.



There are some vulnerabilities in TKIP that can allow an attacker to decrypt individual packets but only with a low rate of recovery (that is, decrypting each packet takes minutes).

Wi-Fi Authentication

In order to secure a network, you need to be able to confirm that only valid users are connecting to it. WLAN authentication comes in three types.

Pre-shared Key

A **Pre-Shared Key (PSK)** is the key that is used to encrypt communications. It is also referred to as group authentication. It is generated from a passphrase, which is like a long password. In WPA-PSK, the user enters a passphrase of between 8 and 63 ASCII characters. This is converted to a 256-bit HMAC (expressed as a 64-character hex value) using the PBKDF2 key stretching algorithm.



It is critical that PSK passphrases be long (12 characters or more) and complex (contain a mixture of upper and lower case letters and digits and no dictionary words or common names). See [Unit 2.3](#) for more information on password security and PBKDF2.

The main problem is that distribution of the key or passphrase cannot be secured properly and users may choose insecure phrases. It also fails to provide accounting, as all users share the same key. The advantage is that it is simple to set up. Conversely, changing the key periodically (as would be good security practice) is difficult.

PSK is the only type of authentication available for WEP and is suitable for SOHO networks and workgroups using WPA.

802.1X

WPA can also implement 802.1X (or **EAP [Extensible Authentication Protocol]**) authentication. The AP passes authentication information to a RADIUS server on the wired network for validation. The authentication information could be a username and password or could employ smart cards or tokens. This allows WLAN authentication to be integrated with the wired LAN authentication scheme. This type of authentication is suitable for enterprise networks.

WPA (WiFi Protected Access)	
Security Mode	WPA (with Radius Server)
WPA mode	WPA2
Encryption technique	AES
RADIUS Server	10.0.0.101
Radius Port	1812
Radius Key	••••••••••••••••
Re-Key Interval	86400 Seconds

Configuring RADIUS authentication on an access point



EAP and RADIUS are discussed in more detail in [Unit 2.4](#). See [Unit 4.1](#) for more information about 802.1X.



Open Authentication and Captive Portals

Selecting "open" authentication means that the client is not required to authenticate. This mode would be used on a public AP (or "hotspot"). This also means that data sent over the link is unencrypted.

Open authentication may be combined with a secondary authentication mechanism managed via a browser. When the client associates with the open hotspot and launches the browser, the client is redirected to a **captive portal**. This will allow the client to authenticate to the hotspot provider's network (over HTTPS so the login is secure). The portal may also be designed to enforce terms and conditions and/or take payment to access the Wi-Fi service.



Enterprise networks can also use captive portals to ensure clients meet a security health policy. See the topic on Network Access Control in [Unit 4.1](#) for more information.



VPN over Open Wireless

Remote users may need to get an internet connection via an open Wi-Fi hotspot. Many of these are operated in towns and cities commercially. It is important to realize that unless communicating with a secure server, data sent over these links is unencrypted. It is also possible that an open hotspot has been setup maliciously to try to harvest confidential information from traffic passing through it.

When using open wireless, users must ensure they send confidential web data only over HTTPS connections and only use email and file transfer services with SSL / TLS enabled.

Another option is for the user to join a **Virtual Private Network (VPN)**. The user would associate with the open hotspot then start the VPN connection. This creates an encrypted "tunnel" between the user's computer and the VPN server. This allows the user to browse the web or connect to email services without anyone able to eavesdrop on the open Wi-Fi network being able to intercept those communications.

The VPN could be provided by the user's company or they could use a third-party VPN service provider. Of course, if using a third-party the user needs to be able to trust them implicitly.



See [Unit 3.4](#) for more information about remote links and VPNs.



Wi-Fi Protected Setup (WPS)

As setting up an access point securely is relatively complex for domestic consumers, vendors have developed a system to automate the process called **Wi-Fi Protected Setup (WPS)**. To use WPS, all the wireless devices (access point and wireless adapters) must be WPS-capable.

Typically the devices will have a push-button. Activating this on the access point and the adapter simultaneously will associate the devices using a PIN then associate the adapter with the access point using WPA2. The system generates a random SSID and PSK. If the devices do not support the push-button method, the PIN (printed on the AP) can be entered manually.

Unfortunately, WPS is vulnerable to a brute force attack. While the PIN is 8 characters, one digit is a checksum and the rest is verified as two separate PINs of 4 and 3 characters. These separate PINs are many orders of magnitude simpler to brute force, typically requiring just hours to crack.

On some models, disabling WPS through the admin interface does not actually disable the protocol or there is no option to disable it. Some APs can lock out an intruder if a brute force attack is detected but in some cases the attack can just be resumed when the lock out period expires. To counter this, the lock out period can be increased. However, this can leave APs vulnerable to a Denial of Service attack.

When provisioning an AP, it is essential to verify what steps the vendor has taken to make their WPS implementation secure and the firmware level required to assure security.

Additional Wi-Fi Security Settings

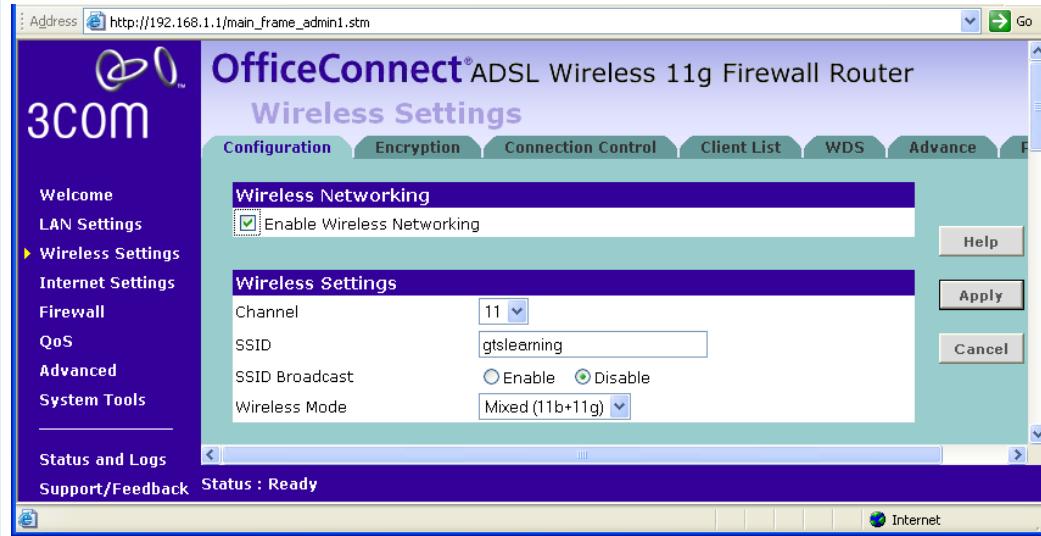
A number of options can provide marginally greater security, though the benefits are often offset by increased complexity of administration.



Disable SSID Broadcast

The 32-character SSID provides a "friendly" name for the WLAN. Vendors use default SSIDs for their products but this should generally be changed. You can use an SSID that clearly identifies your network or you can use a random or meaningless name to gain some measure of "security by obscurity".

Disabling broadcast of the SSID prevents any adapters not configured to connect to the name you specify from finding the network. This provides another layer of security by obscurity but does not actually prevent unauthorized access. Hiding the SSID does not secure the network; you must enable encryption. Even when broadcast is disabled, the SSID can still be detected using packet sniffing tools.



3Com wireless AP configuration

Firmware / Driver

Keep the firmware and driver for the AP and wireless adapters up-to-date with the latest patches. This is important to fix security holes and to support the latest security standards, such as WPA2.

Configuration Password

Vendors ship access points with a default management password (such as "admin" or "default"). Always change this password to something more secure when installing the equipment.



MAC Address Filtering

As with a switch, **MAC address filtering** means specifying which MAC addresses are allowed to connect to the AP. This can be done by specifying a list of valid MAC addresses but this "static" method is difficult to keep up-to-date and relatively error-prone. It is also easy for a wireless sniffer to discover valid MAC addresses and spoof them. Enterprise-class APs allow you to specify a limit to the number of permitted addresses and automatically learn a set number of valid MAC addresses.

Another option is to put a firewall behind the AP in order to filter traffic passing between the wired LAN and WLAN.

DHCP

Some extra security can be gained by disabling DHCP on the access point. Of course, this means that TCP/IP settings have to be allocated and configured manually on the devices, which adds a lot of administrative overhead.

Wi-Fi Site Security

As well as knowing the protocols and settings to configure a single access point securely, in a complex site you may need to consider additional issues to provide secure wireless access and resist wireless Denial of Service attacks.



7rvcz

Antenna Types

Most wireless devices have simple omnidirectional vertical **rod**-type antennas, which can receive and send a signal in all directions. To extend the signal range, you can use an antenna focused at a particular point (such as **Yagi** [a bar with fins] or **parabolic** [dish or grid] antennas). This is referred to as a unidirectional antenna. These are useful for point-to-point connections (a **wireless bridge**). A unidirectional antenna may also be useful to an eavesdropper, allowing them to snoop on a network from a greater distance than might be expected. The increase in signal strength obtained by focusing the signal is referred to as the **gain** and is measured in **dBi**.



Omnidirectional antennas on an HP ProCurve wireless access point



dwp5j

Site Surveys and Antenna Placement

The supported transfer rates and indicative ranges of the 802.11 standards are as follows:

	Rates / Stream (Mbps)	Indoor Range	Outdoor Range
a	6, 9, 12, 18, 24, 36, 48, 54	35m (115ft)	120m (390ft)
b	1, 2, 5.5, 11	35m (115ft)	140m (460ft)
g	6, 9, 12, 18, 24, 36, 48, 54	38m (125ft)	140m (460ft)
n	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 (Single Channel) 15, 30, 45, 60, 90, 120, 135, 150 (Bonded Channels)	70m (230ft)	250m (820ft)

Radio signals pass through solid objects, such as walls, but can be blocked by particularly dense or thick material and metal. Other radio-based devices can also cause interference. Bluetooth uses the same frequency range as Wi-Fi but a different modulation technique, so interference is possible but not common. Other examples are microwave ovens, cordless phones, and baby monitors.



Conversely the signal can also travel much further than the indicative range.

To minimize interference, position the AP as high as possible and set the channels of other nearby APs to different settings. On the device, point the antenna towards the AP if possible. If signals are particularly weak or the WLAN must cover a large area, you can obtain booster antennas or add multiple APs to the network. Placement of APs is worked out by performing a site survey. This will identify which locations require wireless access and the optimum location for each AP.

A site survey is performed first by examining the blueprints or floor plan of the premises to understand the layout and to identify features that might produce interference. This can be backed up by a visual inspection that may reveal things that are not shown on the blueprints (such as thick metal shelving surrounding a room that you want to have WLAN access). Each AP mounting point needs a network port and power jack, so it will help to obtain plans that show the locations of available ports.

The next step is to create a new plan on which you will mark the WLAN zones or cells and associated APs and booster antennas. A WLAN is organized in the same way as a cellular phone network. Each AP is its own "cell", supporting a number of users in a particular location. The idea here is to place APs close enough together to avoid "dead zones" (areas where connectivity is difficult or data transfer rates are below an acceptable tolerance level) but far enough apart that one AP does not interfere with another or that one AP is over-utilized and a nearby one under-utilized.



Surveying Wi-Fi networks using inSSIDer

The next step is to position an AP in the first planned location then use a laptop with a wireless adapter and some site survey software (such as Cisco Aironet) to record signal strength and supported data rate at various points in the intended WLAN zone. This step is then repeated for each planned location.

Next, you need to review the information gathered so far and determine whether the plan is fit for purpose: Are there enough APs? Are they in the best locations?

The final step is to install the APs and connect them to the network. In terms of the logical network topology, you may want to put the WLAN in a DMZ and use a firewall to filter traffic passing between the local network(s) and the WLAN. Another option is to configure wireless clients to connect via a VPN.

Then you should perform a final site survey and write up the baseline signal strength and transfer rates onto your WLAN plan.

This gives you resource documentation that will help with the design of any extensions or modifications to the WLAN and assist with troubleshooting (for example, technicians can easily find out whether a user is actually within a zone intended for WLAN access or get them to move to a spot where signal strength is known to be good).

From a security point-of-view, an additional step would be to use the plan of WLAN zones to identify areas where there is leakage of signals. Depending on the level of security required, you may then want to install shielding at strategic locations to contain the WLAN zones. For example, you might install shielding on external walls to prevent signals from escaping from the building. Of course, this will block incoming signals too (including cell phone calls). As ever, security is about finding a balance between accessibility and inaccessibility.



Remember that wireless signals travel horizontally and vertically.



rkt55

Rogue Access Points and Evil Twins

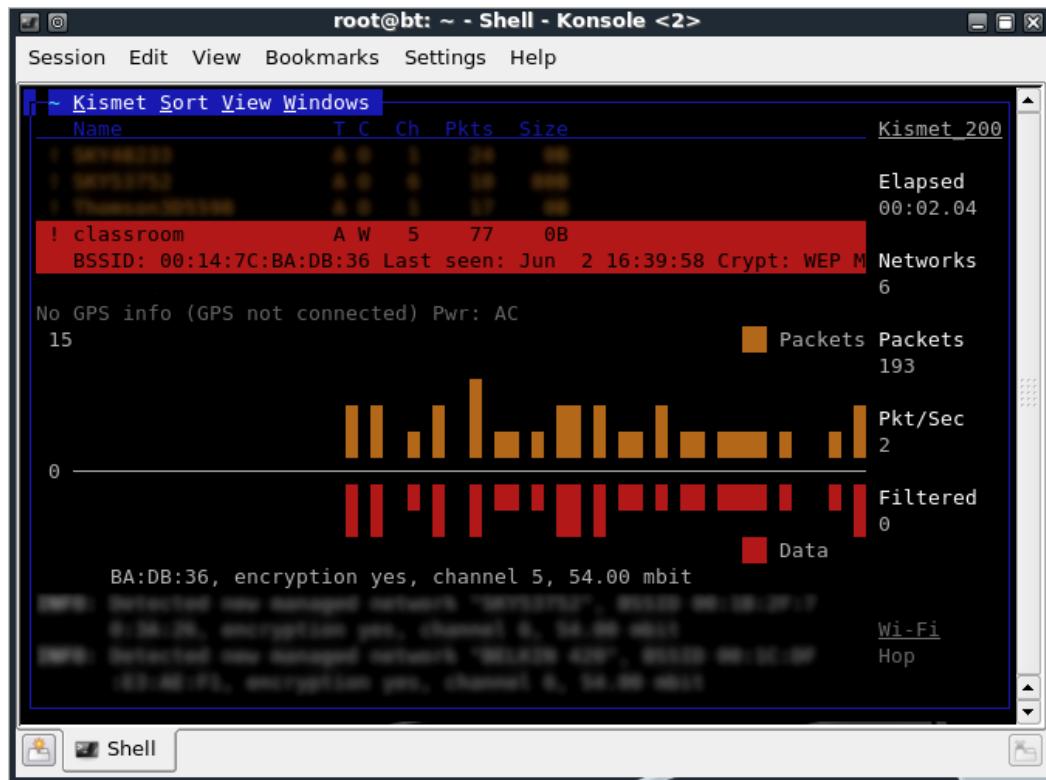
As with any service or device, if a wireless adapter is not being used, it is best to disable it or turn the device off, just to protect against the connection being misused. Most laptops have a button or **Fn** key shortcut to turn off the wireless adapter. Alternatively, you can use the adapter's configuration software, or just disable the device through Device Manager or CMOS Setup.



Follow this rule for any type of unused connection: IrDA, Bluetooth, wired LAN, and so on.

It is also vital to periodically survey the site to detect rogue APs ("white hat" war driving). If connected to a LAN without security, an unauthorized AP creates a very welcoming backdoor through which to attack the network. A rogue AP could also be used to capture user log in attempts.

A rogue AP masquerading as a legitimate one is called an "Evil Twin" or sometimes "Wiphishing". An evil twin might just have a similar name (SSID) to the legitimate one or the attacker might use some DoS technique to overcome the legitimate AP. This attack will not succeed if authentication security is enabled on the AP, unless the attacker also knows the details of the authentication method. However, the evil twin might be able to harvest authentication information from users entering their credentials by mistake.



Surveying Wi-Fi networks using Kismet

One solution is to use EAP-TLS security so that the authentication server and clients perform mutual authentication. There are also various scanners and monitoring systems that can detect rogue APs, including AirMagnet, inSSIDer, Kismet, and NetStumbler. Another option is a **Wireless Intrusion Detection System (WIDS)** or **Wireless Intrusion Prevention System (WIPS)**. As well as rogue access points, WIPS can detect and prevent attacks against WLAN security, such as MAC spoofing and DoS.



See [Unit 3.2](#) for more information about intrusion detection.



4r2gh

Jamming (Interference)

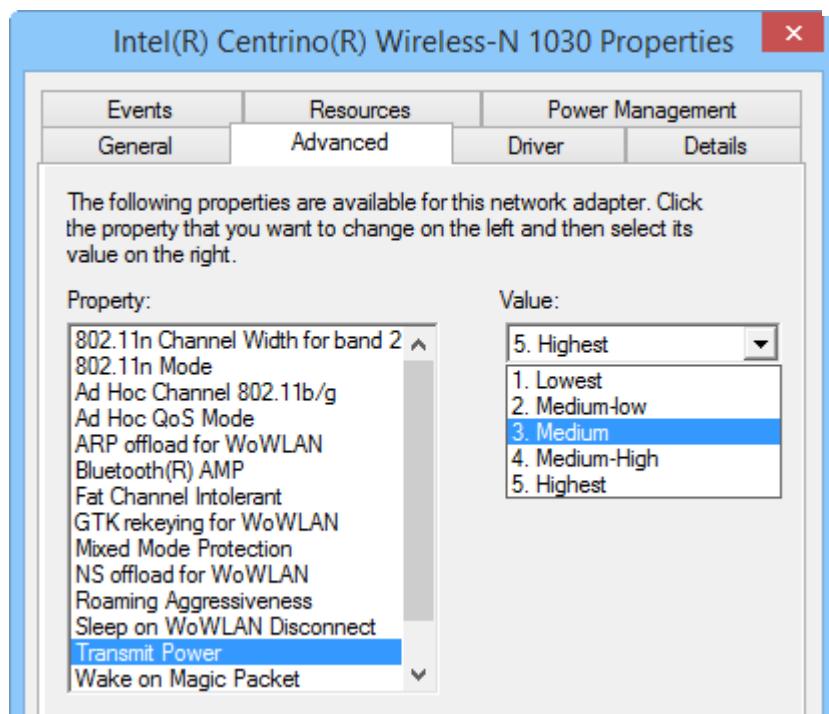
As mentioned above, a wireless network can be disrupted by interference from other radio sources. These are often unintentional but it is also possible for an attacker to purposefully jam an access point. This might be done simply to disrupt services or to position an "evil twin" AP on the network with the hope of stealing data.

A Wi-Fi jamming attack can be performed by setting up an AP with a stronger signal. Wi-Fi jamming devices are also widely available, though they are often illegal to use and sometimes to sell. Such devices can be very small but the attacker still needs to gain fairly close access to the wireless network.

The only ways to defeat a jamming attack are either to locate the offending radio source and disable it or to boost the signal from the legitimate equipment. AP's for home and small business use are not often configurable but the more advanced wireless access points, such as Cisco's Aironet series, support configurable power level controls.



Power Level Controls



Configuring power level on a Wi-Fi adapter

Simply increasing power output is not always reliable. As you increase power, you also increase the chance of the signal bouncing, causing more interference, especially if there are multiple APs. Also, the client radio power levels should match those of the AP or they may be able to receive signals but not transmit back. Consequently power levels are best set to autonegotiate. You should also be aware of legal restrictions on power output - these vary from country-to-country.

Conversely, you may want to turn the power output on an AP down and ensure careful AP device placement to prevent "war driving". The main problem with this approach is that it requires careful configuration to ensure that there is acceptable coverage for legitimate users. You also expose yourself slightly to "evil twin" attacks, as users may expect to find the network at a given location and assume that the rogue AP is legitimate.



Review Questions / Module 3 / Unit 3 / Wireless Network Security

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What are the security considerations when placing antennas to boost the range of a wireless network?
- 2) What is the main difference between WPA and WPA2?
- 3) What technologies exist to prevent the connection of rogue wireless access points to a network?
- 4) If WPA2 provides the strongest possible wireless encryption and authentication, why is it not deployed on all networks?
- 5) What is a pre-shared key?
- 6) Why is it best to disable the wireless adapter in a laptop if Wi-Fi is not being used?
- 7) Your company director wants the presence of the wireless network to be concealed. What measure could you take to comply with this?
- 8) You are constrained to operating a single wireless network that must provide access for both guests and employees. Consequently the network uses open authentication. What technology could you use to make the network secure for employee use?
- 9) Which provides stronger security: TKIP or CCMP?
- 10) You need to configure a wireless bridge between two sites. What type of wireless network technology will be most useful?

Module 3 / Unit 4

VPN and Remote Access Security

Objectives

On completion of this unit, you will be able to:

- Identify the components and security considerations of different remote access and VPN media and technologies.
- Identify the features and vulnerabilities of remote connection protocols, including PPTP, L2TP, IPsec, and SSH.
- Describe the functions and vulnerabilities of remote administration tools (Telnet, SSH, and Remote Desktop).
- Harden remote access services and clients.



c45n6

Remote Access

Remote access describes a situation where access to the network does not depend on the user being physically present. Typically, use is made of a public WAN, such as the telephone system, or a private link (a leased line).

Administering remote access is essentially the same job as administering the local network. Only authorized users should be allowed access to local network resources and communication channels.

Additional complexity comes about because it can be more difficult to ensure the security of remote workstations and servers and there is greater opportunity for remote logins to be exploited.

Remote Access Devices

In order to communicate with the outside world, an organization needs a connection to the telecommunications (telecoms) network. This worldwide network carries voice and data communications. It is operated in each country by one or more telecoms providers.

There are various connection technologies - dial-up, leased line, DSL, or cable for instance - offering various speeds. The local network is connected to the telecoms network via some kind of modem or router.

Analog modems are either internal or external, in which case they connect to the computer via a USB or serial port. The modem plugs into the phone system via an RJ-11 connector.

Many computers come with built-in modems. If these are not used, they should be disabled to prevent the chance that an attacker could gain access to the computer by dialing the modem. Alternatively, the modem can be configured not to answer incoming calls. Another problem is users making unauthorized connections using a modem. These could circumvent the organization's firewall and security procedures.



War dialing is the practice of using software to dial through a phone list in an attempt to find unsecured modems (or computer accounts secured with weak passwords).

Modems are also available for other technologies, such as ISDN, DSL, or cable. DSL modems are often incorporated into simple routers, for home and small office installations. So called "broadband" modems are an increased risk to home users, as the users' computer equipment remains connected to the internet for longer periods, making them more vulnerable to attackers. It is essential to install and configure firewall and anti-virus software on these connections and to keep the OS up-to-date with security patches.



The same security principles apply to "SOHO" router / DSL modems as apply to any other network appliance. Make sure the default administration password is changed and that exploits are patched by firmware upgrades. See [Unit 3.1](#) for more information.

The architecture of cable modem services makes them vulnerable to snooping. A cable service depends on the infrastructure designed to deliver cable TV. Subscribers connect to the same network segment (typically the area of a street), which makes the communications vulnerable to packet sniffing.

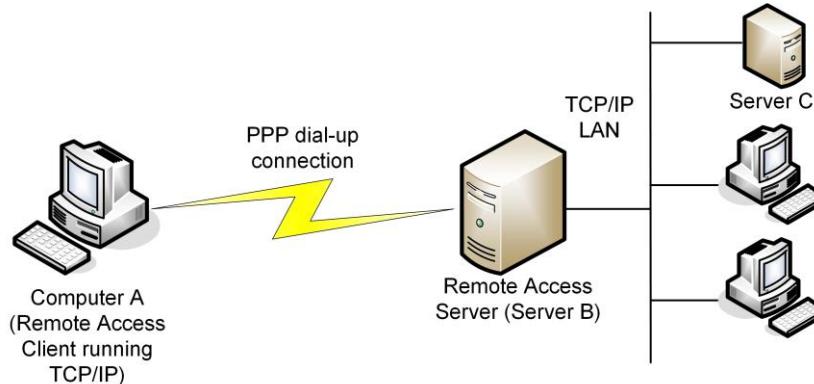
In order to secure the system, cable vendors developed the **Baseline Privacy Interface (BPI)**, part of the **Data Over Cable System Interface Specification (DOCSIS)**. This defines the use of DES to encrypt communications sent over the shared segment so that a modem only receives traffic it is supposed to. However, not all cable providers enable BPI, it uses a weak key (56-bit), and does not authenticate the cable modem. An updated specification (BPI+) uses stronger encryption (AES) and digital certificates for authentication (the certificate is tied to the cable modem's MAC address), but again this is not much use if the ISP has not enabled it.

Point-to-Point Protocol (PPP)

Legacy WAN communication links use point-to-point serial communications (such as dial-up, ISDN, or leased line). The remote server and client must agree a data link protocol to use to transport the network protocol, which will typically be IP.

The **Point-to-Point Protocol (PPP)** is the most widely used internet access and remote dial-in protocol. It provides encapsulation for IP traffic (amongst others) plus IP assignment, authentication, and a means for an internet Service Provider (ISP) to monitor a connection and bill for time used. PPP is known as an **encapsulation** protocol. This means that the protocol sits around other protocol data. This allows a virtual **tunnel** to be created. PPP works at the Data Link layer of the OSI model (layer 2).

Tunneling is a technology used when the source and destination computers are on the same *logical* network but connected via a different *physical* networks.



Tunneling (IP datagrams are tunneled via PPP)

- 1) **Computer A** is located at a user's home and requires remote access to information on **Server C** using the **TCP/IP** protocol.
- 2) **Computer A** uses its modem to dial the modem of **Server B** (a **Remote Access Service [RAS]** server) and establishes a physical connection.
- 3) The local protocol request (TCP/IP packets) generated by **Computer A** is encapsulated into **PPP** frames for transfer across the **dial-up** serial connection.
- 4) **Server B** receives the **PPP** frames and extracts the local protocol request.
- 5) The TCP/IP packets are placed onto the network in Ethernet frames for **Server C** to recognize and respond.

PPP allows the user to specify a means of authentication, for example, **Challenge Handshake Authentication Protocol (CHAP)** or **Extensible Authentication Protocol (EAP)**.



Details of authentication protocols are given in [Unit 2.3](#).

Most internet subscribers use "broadband" services, such as ADSL, to connect to an ISP. These use Ethernet as the data link protocol. **PPP over Ethernet (PPPoE)** is simply a means of creating PPP sessions over an Ethernet link. Some ISPs use **Point to Point Protocol over ATM (PPPoA)** rather than PPPoE.

The main drawback is that PPP provides no security for data transmissions. Other protocols have been developed to provide connection security.



Virtual Private Networks

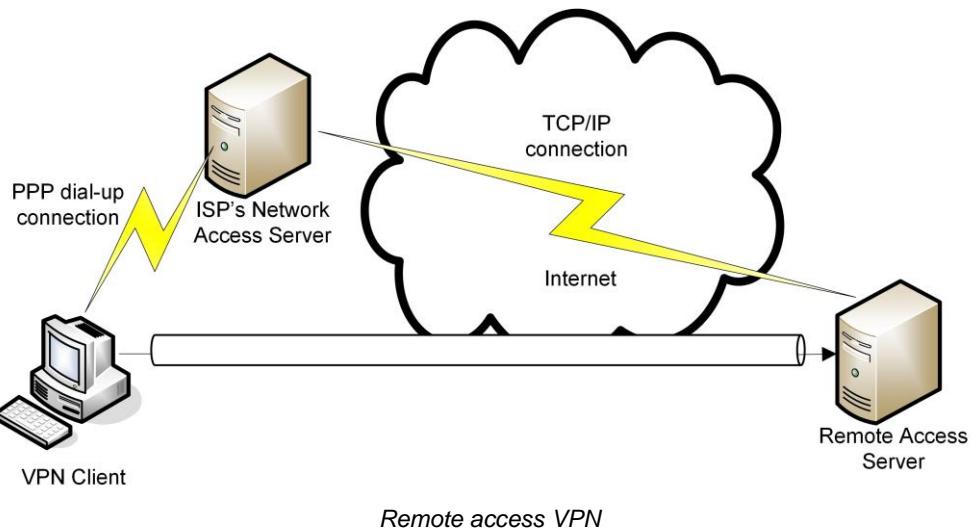
Providing secure leased lines or dial-up connections for remote access is difficult and expensive. A more practical solution is to use internet access infrastructure and set up a **secure tunnel** for private communications through the internet connection. This is referred to as a **Virtual Private Network (VPN)**. Most business and domestic sites have internet connectivity, so this solution is very efficient in terms of cost.

The main concerns are providing security for the transmissions that pass through the public network and preventing unauthorized users from making use of the VPN connection.

A VPN can be implemented in one of two topologies...

Remote Access VPN

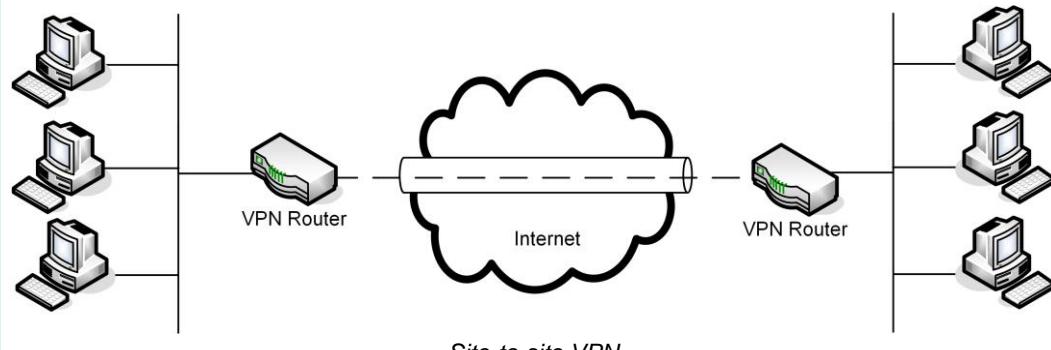
In this scenario, clients connect to a VPN gateway (a VPN-enabled router) on the local network. This is the "telecommuter" model, allowing home-workers and employees working in the field to connect to the corporate network. The VPN clients will connect over the internet.



Remote access VPN

Site-to-Site VPN

This model connects two or more local networks, each of which runs a VPN gateway (or router).



Site-to-site VPN

Another use for a VPN is to secure communications within a private network. For example, the department for product development might need to provide secure communications with the marketing department.

Point-to-Point Tunneling Protocol (PPTP)

The **Point-to-Point Tunneling Protocol (PPTP)**, developed by Cisco and Microsoft, runs on top of PPP to provide encryption, with TCP/IP providing the transport protocol. PPTP is documented in [RFC 2637](#). Like PPP, PPTP operates at Layer 2 of the OSI model.

The connection process for PPTP is as follows:

- 1) The client and server establish an IP connection. A control link is then established over TCP port 1723 on the server to negotiate connection parameters. This connection is not secured, and represents one of the weaknesses of PPTP.

It is possible to eavesdrop the unsecured connection to discover information about how the VPN works (such as client and server IP addresses, username, and hashed password). It also makes the server vulnerable to DoS attacks.
- 2) The client and server negotiate the establishment of a PPTP tunnel and the link is assigned a call ID.
- 3) The client and server exchange Link Control Protocol (LCP) messages to negotiate the creation of a PPP link (the most important point is the selection of an authentication protocol such as CHAP or EAP).
- 4) The client authenticates to the server (and if mutual authentication is configured the server also authenticates to the client).

No.	Time	Source	Destination	Protocol	Info
74	39.616634	10.0.0.5	10.0.0.205	PPP	CHAP Challenge (NAME=' SERVERS',
75	39.616971	10.0.0.5	10.0.0.205	PPP	CHAP Challenge (NAME=' SERVERS',
76	39.617853	10.0.0.205	10.0.0.5	PPP	CHAP Response (NAME=' CLASSROOMS',
77	39.617995	10.0.0.205	10.0.0.5	PPP	CHAP Response (NAME=' CLASSROOMS',
78	39.655015	10.0.0.5	10.0.0.205	GRE	Encapsulated PPP
79	39.655074	10.0.0.5	10.0.0.205	GRE	Encapsulated PPP

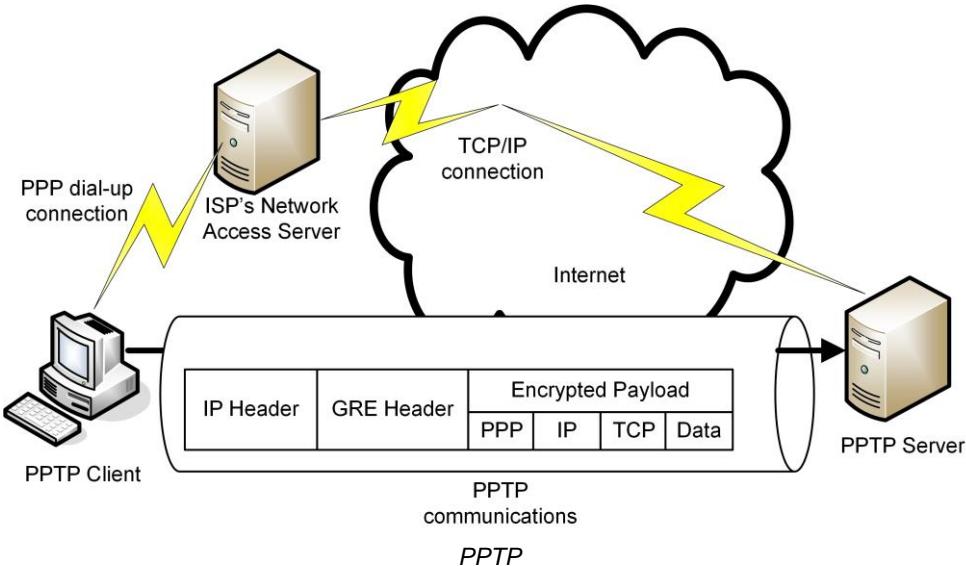
Generic Routing Encapsulation (GRE)
 ▾ Point-to-Point Protocol
 ▾ PPP Challenge Handshake Authentication Protocol
 Code: Response (2)
 Identifier: 0
 Length: 69
 ▾ Data (65 bytes)
 Value Size: 49
 Value: 6f99e7fbcd2d345d857395f61056ce48000000000000000000...
 Name: CLASSROOM5\sue2

PPTP session establishment

- 5) The client and server negotiate use of a network protocol (such as IP).
- 6) The client and server exchange PPP frames securely by re-packaging them using the Generic Routing Encapsulation Protocol (GRE). This payload can be encrypted using MPPE.

PPTP does not define an encryption mechanism itself but can use Microsoft Point-to-Point Encryption (MPPE). MPPE uses the RC4 cipher with 48-bit and 128-bit session keys. GRE is a layer 3.5 protocol - it is delivered at the IP layer (it has the IP protocol number 47) but also encapsulates IP traffic. Routers and firewalls must be configured to allow GRE traffic if they are to support PPTP.

- 7) On an IP network, the client will usually obtain an address from a DHCP server and register with DNS for name resolution. At this point the remote client is part of the local network (though limited by the bandwidth of the remote link).
- 8) The control link on TCP port 1723 remains open to manage the connection.



Layer 2 Tunneling Protocol (L2TP)

L2TP is based on PPTP and Cisco's L2F (Layer 2 Forwarding) protocol. It was published as [RFC 2661](#). The main advantage of L2TP over PPTP is interoperability. There is support for frame types other than PPP (Ethernet, ATM, and Frame Relay) plus support for different transport protocols (notably IPX [Netware] and SNA [IBM mainframes] in addition to IP).

As with PPTP, L2TP provides no authentication or confidentiality (encryption) in itself. L2TP is almost always used with IPsec (see below), which enables the encryption of the PPP negotiation messages from the start, making the link negotiation stronger than PPTP. Using IPsec, the client and server *machines* can authenticate using digital certificates or a pre-shared key. The *user* can then authenticate to the remote access server using whatever method is supported (CHAP, EAP, or RADIUS for instance).

The use of IPsec in conjunction with L2TP as a VPN solution is published as internet standard [RFC 3193](#).

L2TP uses UDP port 1701 for data and connection control. Message sequencing is used to ensure reliable delivery of packets.

SSL VPN

Secure Sockets Layer (SSL), or more technically going forward **Transport Layer Security (TLS)**, provides transmission encryption and (through digital certificates and PKI) authentication for application level TCP/IP services such as HTTP. Where authentication is integrated with the network user database, this can be thought of as a sort of VPN. As well as web applications, this can enable secure access to FTP and Terminal Services (applications running on a server).

Two advantages of an SSL VPN compared to L2TP/IPsec are that no special client software is required and that configuration is much simpler. Another is that access is restricted to defined services rather than the whole network, protecting the network in the event that remote access clients are compromised.

The main disadvantage of SSL VPNs is just that they do not extend the network to the remote user, which can make management of the remote client more complex and preventing direct access to software that cannot be deployed as a web application. OpenVPN is an open-source SSL VPN solution that does provide a VPN solution for all layers of the network stack. Another option is Microsoft's Secure Sockets Tunneling Protocol (SSTP), which works by tunneling PPP over an HTTPS session.

IPSec



z8dli

IPsec is a layer 3 protocol suite providing security for IP packets. Most TCP/IP security protocols operate at higher levels, so IPsec is flexible (that is, it can be used with a variety of applications). IPsec can provide both confidentiality (by encrypting data packets) and integrity/anti-replay (by signing each packet). The main drawback is that it is quite processor intensive, adding an overhead to data communications. IPsec can be used to secure communications on local networks and with remote access protocols, such as L2TP.

IPsec is published in [RFCs 4301](#) through 4309 (Security Architecture for IP). It was designed as an integral part of the next version of IP (IPv6) but adapted for the IPv4 protocol as worldwide adoption of IPv6 capable hardware and software has been slow.

IPsec works over TCP/UDP port 1293. IPsec can be used with a number of cryptographic algorithms. Algorithms that an implementation *must* support to be standards-compliant are defined in [RFC 4835](#). There are also some obsolete ciphers that the RFC deprecates. Vendors can support additional, perhaps proprietary, ciphers as they see fit.

There are two core protocols in IPsec, which can be applied singly or together.

Authentication Header (AH)

The **Authentication Header (AH)** protocol performs a cryptographic hash on the packet plus a shared secret key (known only to the communicating hosts) and adds this **HMAC** in its header as an Integrity Check Value (ICV). The recipient performs the same function on the packet and key and should derive the same value to confirm that the packet has not been modified. The payload is not encrypted so this protocol does not provide confidentiality.

IPsec datagram with AH (transport mode)



IPsec datagram using AH - the integrity of the payload and IP header is ensured by the Integrity Check Value (ICV) but the payload is not encrypted

MD5, SHA-1, or SHA-2 are the algorithms typically used by AH.

Encapsulation Security Payload (ESP)

This provides confidentiality and authentication by encrypting the packet rather than simply calculating an HMAC. ESP attaches three fields to the packet (a header, a trailer [providing padding for the cryptographic function], and an Integrity Check Value).

IPsec datagram with ESP (transport mode)



IPsec datagram using ESP - the TCP header and payload from the original packet is encapsulated within ESP and encrypted to provide confidentiality

HMAC-MD5, HMAC-SHA-1, or HMAC-SHA-2 and 3DES or AES (symmetric encryption ciphers) are the algorithms typically used by ESP.



The principles underlying IPsec are the same for IPv4 and IPv6 but the header formats are different. IPsec makes use of extension headers in IPv6 while in IPv4 ESP and AH are allocated new IP protocol numbers (50 and 51) and either modify the original IP header or encapsulate the original packet (see "Transport and Tunnel Modes" below).

Internet Key Exchange / ISAKMP

AH and ESP both use encryption technologies that depend on the idea of a **shared secret**; that is, a key known only to the two hosts that want to communicate. For this to happen securely, the secret must be communicated to both hosts and the hosts must confirm one another's identity (mutual authentication); otherwise the connection is vulnerable to Man-in-the-Middle and spoofing attacks.

The **Internet Key Exchange (IKE)** protocol is the part of the IPsec protocol suite that handles authentication and key exchange (referred to as **Security Associations [SA]**). IKE is also referred to as **Internet Security Association and Key Management Protocol (ISAKMP)**. In fact, ISAKMP is a protocol separate from IPSec; the IKE implementation combines features of ISAKMP and two other protocols (Oakley and SKEME). IKE negotiations use UDP port 500. The negotiations take place over two phases:

- Phase I establishes the identity of the two hosts and performs key agreement using the Diffie-Hellman algorithm to create a secure channel. Phase 1 is usually initiated in Main Mode, which involves 6 messages (two to propose an IKE SA, two to agree DH keys, and then two to exchange identifiers securely). The alternative is Aggressive Mode, which packs the information in these 6 messages into 3 messages. This is quicker but means that identifiers are exchanged in the clear. This may allow a snooper to perform a dictionary or brute-force password-guessing attack on the authentication information.

Diffie-Hellman key agreement establishes the shared secret used to sign the packets for message integrity. Diffie-Hellman does not authenticate the endpoints however. Several different methods of authenticating hosts are supported:

- PKI - the hosts use certificates issued by a mutually trusted Certificate Authority to identify one another. This is the most secure mechanism, but requires PKI architecture.
- Pre-shared Key (Group Authentication) - the same passphrase is configured on both hosts. A Pre-Shared Key (PSK) is also referred to as group authentication as a single password or passphrase is shared between all users. Obviously, this is not very secure as it is difficult to keep the pre-shared key a secret known only to valid users. It can also be difficult to change the key.
- Kerberos - this can be used on a Windows Domain to integrate with Active Directory security credentials.
- Phase II uses the secure channel created in Phase 1 to establish which ciphers and key sizes will be used with AH and/or ESP in the IPsec session.

Transport and Tunnel Modes

IPsec can be used in two modes:

- Transport mode - the IP header for each packet is not encrypted, just the data (or **payload**). This mode would be used to secure communications on a private network (an end-to-end implementation).

IPsec datagram with AH and ESP (transport mode)



IPsec datagram using AH and ESP in transport mode

- Tunnel mode - the whole IP packet (header and payload) is encrypted and a new IP header added. This mode is used for communications across an insecure network (creating a VPN). This is also referred to as a router implementation.

IPsec datagram with ESP (tunnel mode)

*IPsec datagram using ESP in tunnel mode*

Remote Access Servers

Most NOS support remote access. In Windows, the service is called **Routing and Remote Access**. Remote servers can be configured to allow access to the entire network or just to the server itself. In the first case, the remote server forwards requests to other servers on the network.



A Remote Access Server is also referred to as a Network Access Server. A related device is a Remote Access Concentrator, which can handle high call densities.

A remote access server can be configured in two ways:

Dial-in RAS

A dial-in server has a physical connection (a PSTN or leased line) to a dedicated WAN link and one or more modems.

VPN RAS

An RAS configured for VPN access is simply connected to the internet, using any appropriate media. The server is then configured to use the appropriate protocols and users are granted "dial-in" rights.

Once the client has been authenticated, it can be assigned a local network address. To all intents and purposes, the client becomes part of the local network.

Another option is to provide a hardware solution (a VPN-enabled router); this is generally more costly but provides better performance and security.



lrtq8

All the major NOS are bundled with software supporting VPNs. The drawbacks of using a software solution for VPN are security (the server is exposed to the internet) and performance (if the server is performing other tasks). A hardware or appliance-based solution overcomes these problems and a range of devices is available to meet different performance requirements at different price points.

Many SOHO routers support IPsec and / or SSL VPNs with tens of simultaneous connections. These are "all-in-one" type boxes combining the functions of VPN, internet router, firewall, and DSL "modem".

There are also dedicated SSL VPN concentrator appliances, such as those from Netgear, again aimed at the SME market. These are intended to be installed alongside a router / firewall / IPsec VPN to enable secure access to web applications on the corporate intranet or extranet. Heavyweight dedicated VPN concentrator appliances, such as Cisco's 3000 and 5000 series, provide scalable performance for hundreds or thousands of users. This type of product is no longer marketed however (both the 3000 and 5000 series have been discontinued) as the same functionality is more economically incorporated into enterprise-class routers.

Remote Administration Tools



979bv

Remote administration tools allow administrators to manage and configure a computer over a network. They can work over a local network, over a VPN, or even across the internet (if the appropriate ports are opened on the firewall).

Remote administration tools are enormously useful but they also represent a significant security exploit if their use is not secured.

Telnet

Telnet is terminal emulation software to support a remote connection to another computer. It does not support file transfer directly, but when you connect, your computer acts as if your keyboard is attached to the remote computer and you can use the same commands as a local user.

In order to support Telnet access, the remote computer must run a service known as the Telnet Daemon. Telnet uses TCP port 23 by default.

Telnet is not very secure. Telnet daemon software has exploitable vulnerabilities and Telnet communications are sent in plaintext (including password authentication information). One option would be to ensure Telnet is only used over a secure channel, such as an IPsec tunnel.

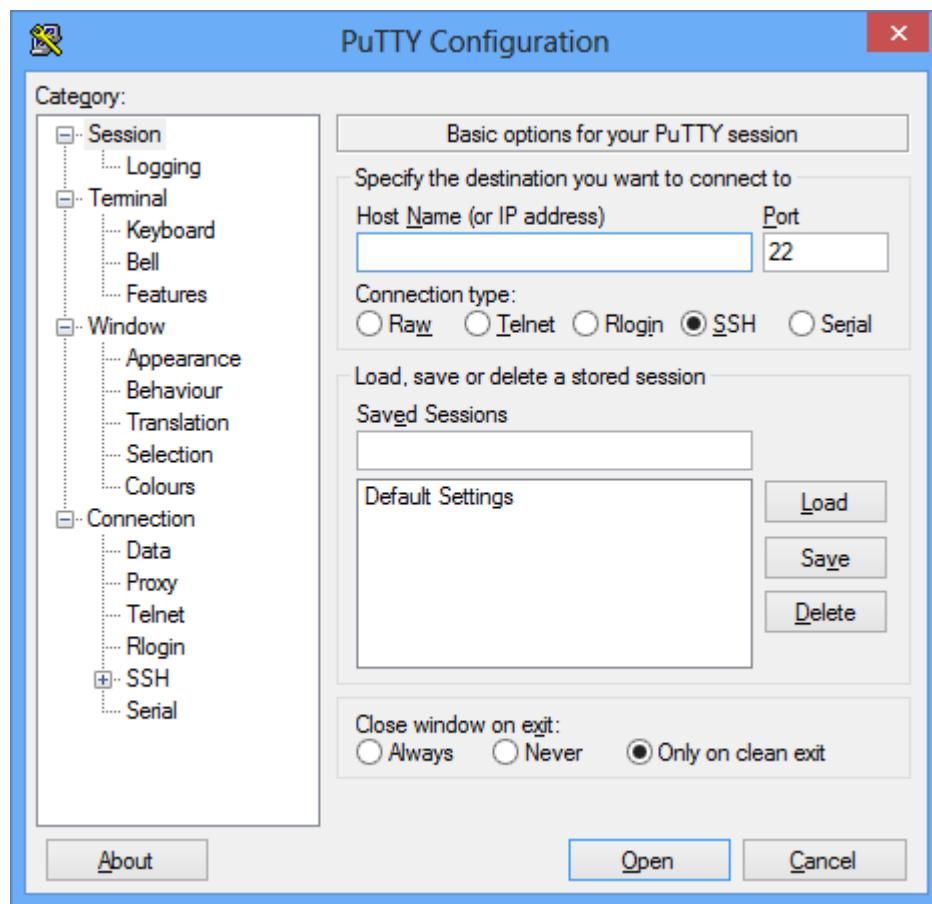
Secure Shell (SSH)

Secure Shell (SSH) is an improvement on the UNIX remote administration and file copy programs (rsh [Remote Shell], Telnet, rlogin, and FTP). The main uses of SSH are:

- Remote administration.
- Secure file transfer (SFTP).
- Secure file copy (SCP).

SSH also supports **port forwarding**, which can be used to implement a limited type of VPN. Port forwarding means that communications over a particular port are channeled through SSH, which provides authentication and encryption for that application. The advantage of SSH port forwarding over IPsec is that there is a lower overhead. If only data transmitted by certain applications needs to be encrypted, SSH may be a better option.

There are numerous commercial and open source SSH products available for all the major NOS platforms (UNIX, Linux, Windows, and Mac OS). The most widely used is OpenSSH.



PuTTY SSH client for Windows

SSH servers are identified by a private/public key pair. A mapping of host names to public keys can be kept manually by each SSH client or PKI and CAs can be used to establish trust relationships. Under OpenSSH, a secure session is established as follows:

- 1) An SSH client contacts an SSH server on TCP port 22 and identify a mutually supported version of the SSH protocol. SSH versions 1 and 2 are different; some servers can support clients using either version however. The process described here is for SSHv2.
- 2) The client and server exchange identification strings (including the server's public key). If a server key is not already within the client's keystore, there is a prompt whether to trust it or not.
- 3) The server and client then indicate their preferred cipher suites and the highest mutually compatible ciphers are selected. OpenSSH supports patent-free algorithms, such as AES, 3DES, Blowfish, Arcfour (RC4), MD5, and SHA-1.
- 4) The client and server generate a session key, typically using the Diffie-Hellman key agreement protocol. The D-H packets are signed by the server using its private key, authenticating the server to the client.



In SSHv1, the session key is configured on the server (and is called the server key). The server generates a new server key every hour.

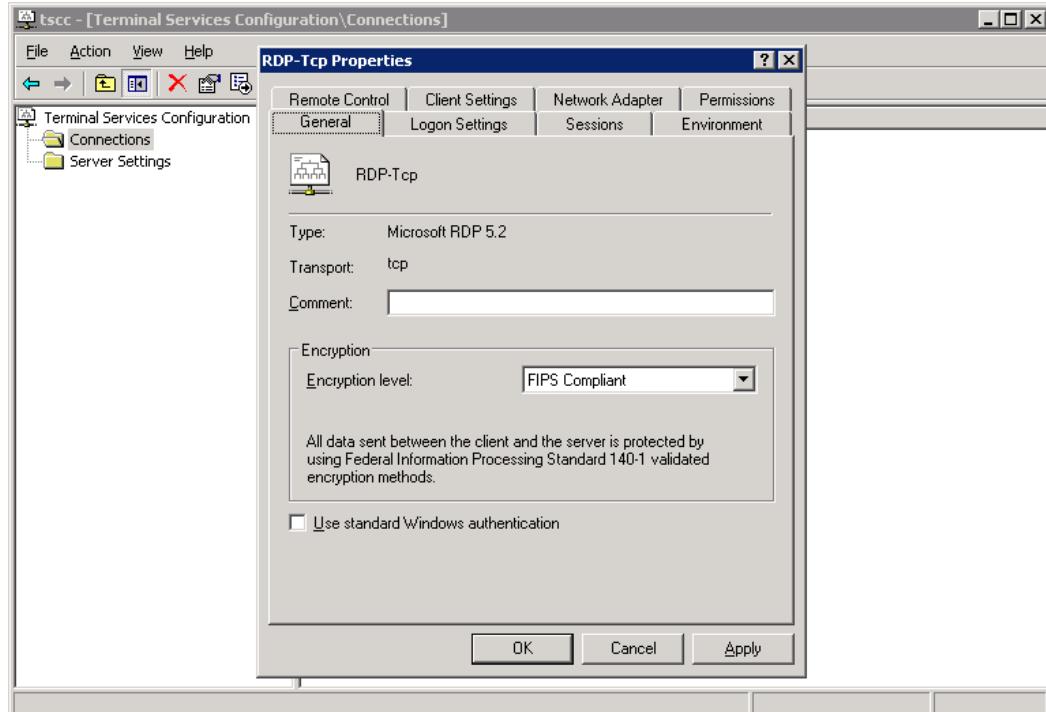
- 5) Once the session is established, all communications continue over server port 22. The user can request user authentication against network services (via the SSH User Authentication Protocol) and run commands from protocols such as FTP (sftp) or Secure Copy (scp) over this secure channel (the SSH Connection Protocol).

Remote Desktop Protocol (RDP)

There are also GUI remote administration tools. The programs send screen and audio data from the remote host to the client and transfer mouse and keyboard input from the client to the remote host. This means that the tools are accessible not just to experienced administrators but also to ordinary users (allowing a teleworker to access a desktop PC in the office for instance).

Remote Desktop Protocol (RDP) is Microsoft's protocol for operating remote connections to a Windows machine. Under Windows NT and 2000, these are referred to as Terminal Services but under later versions of Windows they are referred to as Remote Desktop. RDP uses TCP port 3389. The administrator can specify permissions to connect to the server via RDP and also configure encryption on the connection.

The version of RDP released with Windows Vista/7 and Windows Server 2008 introduces **Network Level Authentication (NLA)**. This requires the client to authenticate before a full remote session is started. An RDP server that does not enforce NLA can be subject to DoS attacks as the server uses resources to prepare for each requested session. It also sends information about the server to an attacker (such as the computer and domain names) regardless of whether they have valid authentication credentials.



Configuring terminal services on Windows Server

Hardening Remote Access Infrastructure

Remote access is a serious network security problem, mainly because control of the client computer often falls outside the reach of security mechanisms set up to protect the network.

Remote Client Security

The integrity of the client computer presents many issues:

- Malware protection - the computer may not be accessible to network systems used to update and enforce malware protection. This may have to be left to the end-user. If a worm or Trojan is installed, network security may be compromised. This is especially true as using a VPN connection will make traffic between the client and network invisible to network firewalls.
- Security information - authentication information may be stored on the client (saving a password for instance), making the network vulnerable if the computer is stolen.
- Data transfer - files copied to the client may no longer be properly secured, raising the potential that confidential information could be stolen along with the device.

- Local privileges - the user of a remote computer might be configured with administrative privileges but have no understanding of how such privileges can be exploited or misused. They might install unauthorized software on the machine or make it more vulnerable to malware by browsing the web using their administrative account.
- Weak authentication - relying on a username and password combination is simply not secure enough in a remote access scenario. Two-factor authentication using smart cards or biometric recognition in addition to a PIN or password should be enforced. If this is not an option, a strong password policy must be enforced and users made aware of the very real risks of writing down or sharing their password.

The principal solution to remote access security problems is to educate remote users about security risks and their responsibilities. Enforcement can be provided by having remote devices audited periodically to ensure that anti-virus, firewall, and OS/browser/application patches are being kept up-to-date and to check that unlicensed software has not been installed. It is also wise to limit what remote users can access on the local network and to severely restrict the rights of remote computer accounts. The principle of least privilege should be applied. Technologies such as Remote Desktop provide an opportunity to lock down the user's privileges more than they would have been in the past. Technicians can provide support and assistance without having to go offsite or conversely without the machine having to be brought onsite.

Remote Access Server Security

The most important point to make about remote access services is that they should only be running if they are required! The creation of a remote access server or remote administration interface should be accompanied by documentation describing the uses of the service, security risks and countermeasures, and authorized users of the service. There should also be authorization to run the service from the network manager.

The remote access policy should then implement the measures identified through compiling the documentation. Typical policy restrictions would be:

- Restricting access to particular users or groups.
- Restricting access to particular times of the day or week.
- Enforcing strong authentication.
- Restricting privileges on the local network (ideally, remote users would only be permitted access to a clearly defined part of the network).
- Logging and auditing access logons and attempted logons.
- Using callback for dial-up access.

In addition to this, a management plan should ensure that remote access servers and other hardware are kept up-to-date with the latest software or firmware updates. Administrative access to the devices should also be secured, using strong authentication.



Review Questions / Module 3 / Unit 4 / VPN and Remote Access Security

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) Which protocol is used in conjunction with L2TP to provide a secure access VPN?
- 2) What two protocols must a firewall allow to establish a PPTP link?
- 3) What are the two main advantages of L2TP over PPTP?
- 4) What IPsec mode would you use for data confidentiality on a private network?
- 5) What authentication methods are supported by IPsec?
- 6) Describe what role SSH might play in securing communications.
- 7) What protocol could you deploy to protect the management interface of a router that only accepts Telnet connections?
- 8) What is the main risk of using remote administration tools over a network without encryption?
- 9) Your firewall is configured with a rule allowing external hosts to connect to port 3389. What protocol is being permitted?
- 10) What bit of information confirms the identity of an SSH server to a client?



If you have access to the Hands On Live Labs, complete the "Protocols and Services / IPSec" lab now.

Module 3 / Unit 5

Network Application Security

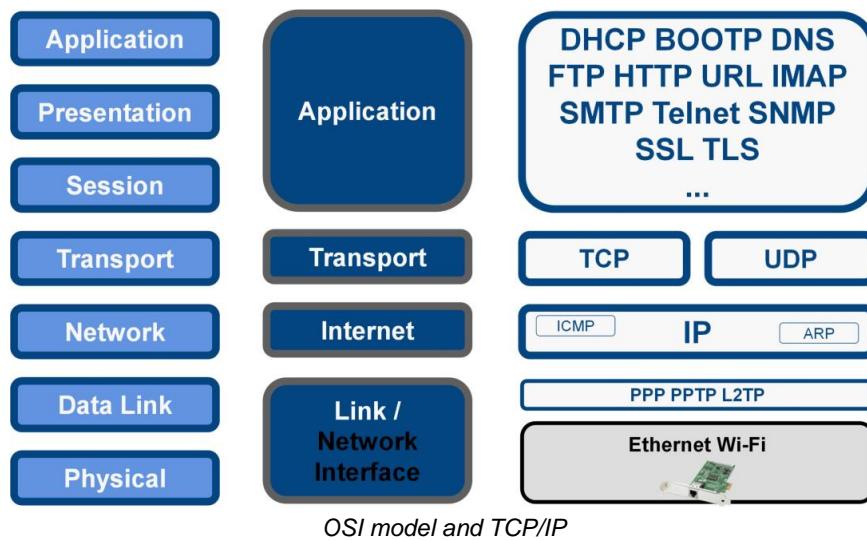
Objectives

On completion of this unit, you will be able to:

- Identify the features and vulnerabilities of NetBIOS, DHCP, DNS, and SNMP.
- Identify technologies used to implement Storage Area Networks.
- Identify the main security issues involved as networks transition from IPv4 to IPv6.
- Describe methods used to implement and secure voice communications (telephony).

Application Layer Security

Above the transport layer, the DoD model refers to the application layer. This contains client/server application protocols such as HTTP (web services), SMTP (email relay), and DNS (name resolution).



Eavesdropping, Replay, and Session Hijacking

Most TCP/IP application protocols are vulnerable to eavesdropping and spoofing / session hijacking as all information in the packets (including passwords) is transmitted as clear text and can easily be read in a protocol analyzer or modified using a hacking tool. A good example is the Telnet program and server, sometimes still used to configure switches or routers. Any authentication password entered through Telnet is sent in clear text and so can easily be intercepted by a packet sniffer.

Some protocols can work with an encryption protocol to make them secure. For example, HTTP can be secured using Secure Sockets Layer [SSL] encryption; used together they are referred to as the HTTPS protocol. Telnet has been replaced by remote administration tools that support secure authentication and encryption.

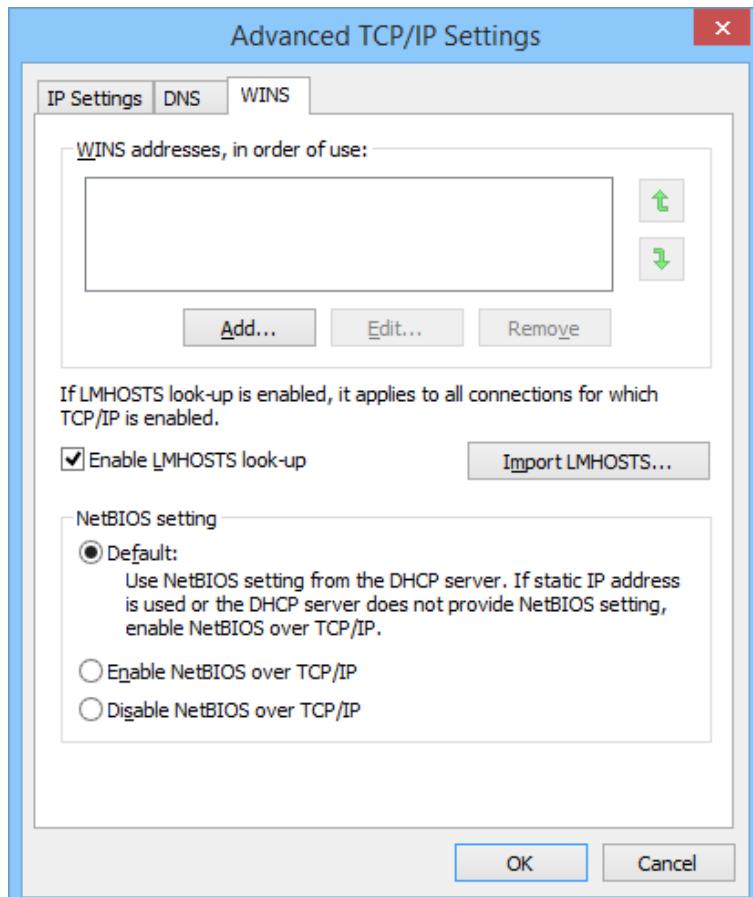
Bombing

Web applications are vulnerable to DoS attacks such as **bombing**, which is where an attacker generates a large number of HTTP requests or SMTP mail messages designed to overwhelm the server. Spam is also a sort of DoS attack, as it makes it difficult for users to distinguish legitimate from illegitimate messages. It also consumes disk space and resources on the target server plus network bandwidth.



NetBIOS

Windows networks may also need to take account of **NetBIOS**. This is a legacy Application Programming Interface (API) designed to provide programmers with an easy means of accessing and utilizing network resources over a Windows network, which originally ran on **NetBEUI (NetBIOS Extended User Interface)**. NetBIOS is still used for some Windows services and applications and therefore is configured to run over TCP/IP by default. The use of NetBIOS over TCP/IP is documented in RFCs 1001 and 1002. NetBIOS runs over ports 135, 137, 138, 139, and 445. These ports should be blocked on the public interface.



Enabling or disabling NetBIOS over TCP/IP

To enable or disable NetBIOS over TCP/IP, use the setting on the **WINS** tab in the **Advanced TCP/IP Settings** dialog (open the network adapter properties, select **TCP/IP** and click **Properties**, then click the **Advanced** button).

Remote Procedure Call

Remote Procedure Call (RPC) is used to implement distributed applications, where a client executes code on a remote server. Under UNIX, RPC programs open ephemeral ports using the **portmap** program, meaning that there is no list of standard port numbers for different programs. Well-known RPC programs can be identified by their program number. The list of program numbers is maintained by Sun and stored locally in /etc/rpc.

Port 111 is closely associated with RPC. This is the port used by portmap to enumerate the open RPC ports. This port should be blocked on the public interface if not offering RPC services over the internet. This prevents footprinting attacks and DoS or remote execution attacks on local network services from the internet.

The other problem with RPC is running unnecessary services that might suffer remote execution vulnerabilities. Some of these services may be set to run by default under a typical installation. If not required, they should be disabled using a startup script.

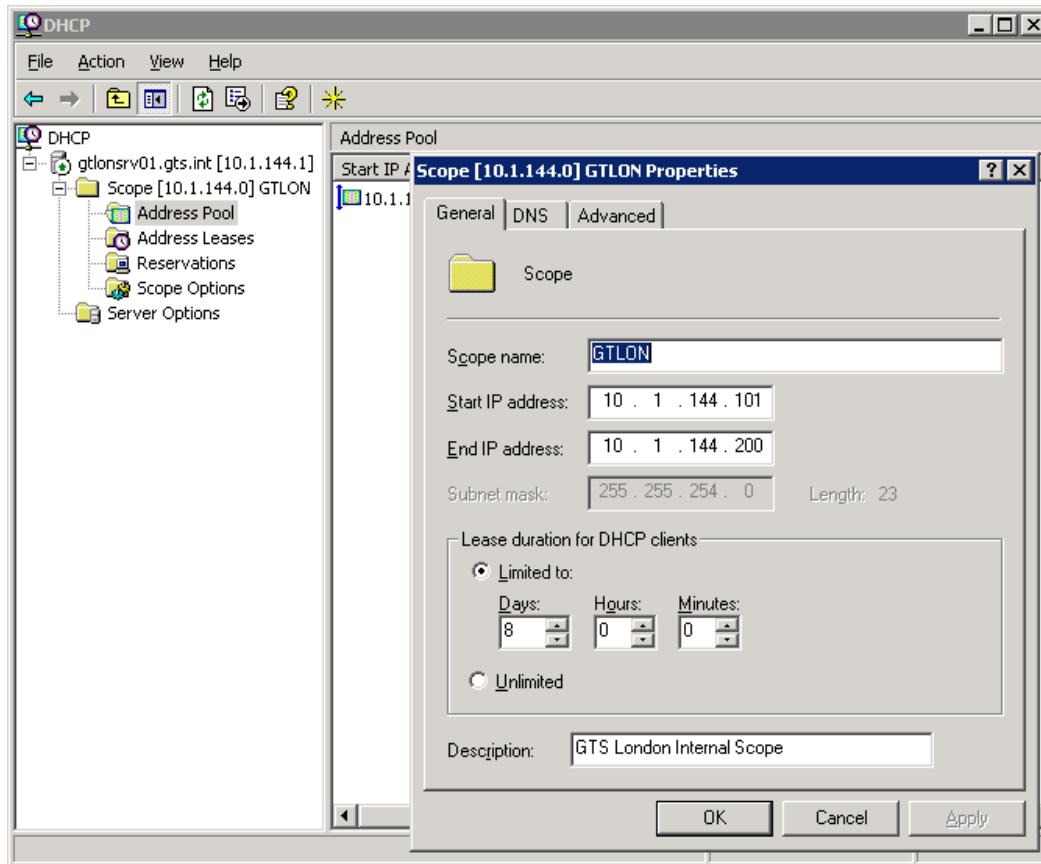
Windows also suffers from vulnerabilities through RPC (implemented as MSRPC) where faults in application software become vulnerable to remote code execution. The MSRPC portmapper works over port 135 or 445 by default but can also be configured to run over HTTP (80, 443, or 593). The general strategy for preventing these attacks is to monitor security bulletins and keep affected programs patched and updated.

DHCP Security

The **Dynamic Host Configuration Protocol (DHCP)** provides an automatic method for allocating IP addresses, subnet masks, and optional parameters, such as the default gateway, Domain Name Server (DNS) address, or NetBIOS name server address. This avoids the configuration errors that can occur if addresses are specified manually.

The key point about DHCP is that only one server should be running. DHCP broadcasts are typically limited to the local subnet. A router can be configured to forward the packets to another network, but this is not typical. More than one DHCP server may be running for fault tolerance, as long as they are all configured correctly and scopes don't overlap. If a rogue DHCP server is set up, it can perform DoS (as client machines will obtain an incorrect TCP/IP configuration) or be used to snoop network information. There are various tools that can be used to detect rogue DHCP servers, including Dhcplc for Windows and dhcp_probe. Windows DHCP servers in an AD environment automatically log any traffic detected from unauthorized DHCP servers.

Another DoS attack against DHCP is installing a rogue client; that is, one that repeatedly requests new IP addresses using spoofed MAC addresses, with the aim of exhausting the IP address pool. It is possible to configure a DHCP server to bind only to known MAC addresses (DHCP Registration), but this is time-consuming and quite easily subverted, as it is trivial to harvest and spoof valid MAC addresses.



Configuring DHCP on Windows Server

Administration of the DHCP server itself must be carefully controlled and the settings checked regularly. If an attacker compromises the DHCP server, he or she could point network clients to rogue DNS servers and use that as a means to direct users to spoofed websites. Another attack is to redirect traffic through the attacker's machine by changing the default gateway, enabling the attacker to snoop on all network traffic.

The best defenses against attacks on DHCP fall under the headings of general network security best practice:

- Use scanning and intrusion detection to pick up suspicious activity.
- Enable logging and review the logs for suspicious events.
- Disable unused ports and perform regular physical inspections to ensure that unauthorized devices are not connected via unused jacks.



Port security is discussed in [Unit 4.1](#); Intrusion Detection Systems are discussed in [Unit 3.2](#).



2s99h

DNS Security

The **Domain Name System (DNS)** is a distributed hierarchical system for resolving names to IP addresses. It uses a distributed database system that contains information on domains and hosts within those domains. The information is distributed among many name servers, each of which holds part of the database. The name servers work over port 53. The distributed nature of the system has the twin advantages that the maintenance of the system is delegated and the loss of one DNS server does not prevent name resolution from being performed.

DNS Spoofing / Client Redirection

DNS spoofing involves compromising the victim's DNS server. Typically, the attacker will replace the valid IP address for a trusted website such as **mybank.com** with the attacker's IP address. The attacker can then intercept all the packets directed to mybank.com and bounce them to the real site, leaving the victim unaware of what is happening (referred to as **pharming**). Alternatively, DNS spoofing could be used for a Denial of Service attack, by directing all traffic for a particular FQDN to an invalid IP address (a black hole).

There are two common means of corrupting the victim's DNS...

HOSTS File

Before DNS was developed (in the 1980s), name resolution took place using a text file named HOSTS. Each name-to-IP address mapping was recorded in this file and system administrators had to download the latest copy and install it on each internet client or server manually.

Despite the fact that all name resolution now *functions* through DNS, the HOSTS file is still *present* and most operating systems check the file before using DNS. Its contents are loaded into a cache of known name:IP mappings and the client only contacts a DNS server if the name is not cached. Therefore, if an attacker is able to place a false name:IP address mapping in the HOSTS file s/he will be able to redirect traffic.

The HOSTS file requires administrator access to modify. In UNIX and Linux systems it is stored as /etc/hosts while in Windows it is placed in %SystemRoot%\System32\Drivers\etc\hosts.

Spoofing

The attacker performs a Denial of Service attack on the victim's DNS server then uses ARP spoofing to respond to DNS lookups from the victim network.

Typosquatting / URL Hijacking



A number of attacks exploit the domain name registration process. Misspelt domains can be profitable depending on the frequency that users enter the misspelled name (for example, visiting amazoon.com or amazun.com). This is referred to as **typosquatting** or **URL hijacking**. Such domains can generate advertising revenue through Google or be used to host malware or launch pharming attacks.

- Kiting - a domain name can be registered for up to 5 days without paying for it. Kiting means that the name is continually registered, deleted, then re-registered.
- Tasting - this is the registration of a domain to test how much traffic it generates within the 5 day grace period; if the domain is not profitable, the registration is never completed.
- Hijacking - this means supplying false credentials to the domain registrar when applying for a new domain name or re-registering an existing one (a domain name must be re-registered every year).
- Cybersquatting - this means acquiring a domain for a company's trading name or trademark (or some spelling variation thereof). While there are often laws against doing this, companies need to be careful to renew domain names that they want to continue to use.

DNS Server Vulnerabilities

Many DNS services run on BIND (Berkley Internet Name Domain), distributed by the Internet Software Consortium (www.isc.org). There are known vulnerabilities in many versions of the BIND server so it is critical to patch the server to the latest version.

The same general advice applies to other DNS servers, such as Microsoft's. Obtain and check security announcements and then test and apply critical and security-related patches and upgrades.

Footprinting

Footprinting is obtaining information about a private network, in this case by using its DNS server to perform a zone transfer (all of the records in a domain) to a rogue DNS or simply by querying the DNS service, using a tool such as **nslookup** or **dig**.

To prevent this, you can apply an Access Control List to prevent zone transfers to unauthorized hosts or domains, to prevent an external server from obtaining information about the private network architecture.

Denial of Service

DoS attacks are hard to perform against the servers that perform internet name resolution, but if an attacker can target the DNS server on a private network it is possible to seriously disrupt the operation of that network. Active Directory (for instance) relies on DNS to work properly.

DNS Poisoning

DNS poisoning (or DNS cache pollution) is another redirection attack, but instead of trying to subvert the name service used by the client, it aims to corrupt the records held by the DNS server itself. The intention is to redirect traffic for a legitimate domain (such as **mybank.com**) to a malicious IP address.

DNS poisoning can be achieved by modifying query traffic. A typical attack would proceed as follows:

- 1) The server in grommet.com wants to find an address in widget.com. It queries the root and .com name servers and gets an address for the name server for widget.com.
- 2) The attacker spoofs the name server for widget.com. To do this, the attacker has to compromise the genuine widget.com name server through some sort of DoS attack. The attacker just needs to ensure that his malicious DNS responds to grommet.com's queries before the legitimate one.
- 3) The attacker spoofs responses to the grommet.com server and poisons its cache, meaning that traffic for widget.com from grommet.com gets directed to the attacker's IP address.

The latest DNS servers are protected against this type of tampering by randomizing the transaction ID and client port better, making it more difficult for the attacker to spoof responses.

Another attack involves getting the victim name server to respond to a recursive query from the attacker. A recursive query compels the DNS server to query the authoritative server for the answer on behalf of the client. In this case, the attacker's DNS, masquerading as the authoritative name server, responds with the answer to the query, but also includes a lot of false domain:IP mappings for other domains that the victim DNS accepts as genuine. To protect against this attack, local DNS servers should only accept recursive queries from local hosts (preferably authenticated local hosts) and not from the internet.



Queries between servers on the internet should be iterative. This means that the server responds with an appropriate record from its zone database or cache or with a referral to an authoritative server but does not "take up" the query itself.

```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
[ metasploit v3.5.1-dev [core:3.5 api:1.0]
+ --=[ 635 exploits - 316 auxiliary
+ --=[ 215 payloads - 27 encoders - 8 nops
    =[ svn r11089 updated 192 days ago (2010.11.22)

Warning: This copy of the Metasploit Framework was last updated 192 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
http://www.metasploit.com/redmine/projects/framework/wiki/Updating

msf > use auxiliary/spoof/dns/bailiwicked_host
msf auxiliary(bailiwicked_host) > set hostname www.classroom.com
hostname => www.classroom.com
msf auxiliary(bailiwicked_host) > set newaddr 10.1.0.101
newaddr => 10.1.0.101
msf auxiliary(bailiwicked_host) > set srcport 53
srcport => 53
msf auxiliary(bailiwicked_host) > set rhost 10.1.0.1
rhost => 10.1.0.1
msf auxiliary(bailiwicked_host) > check
[*] Using the Metasploit service to verify exploitability...
[-] ERROR: This server is not replying to recursive requests
msf auxiliary(bailiwicked_host) >

```

Secure servers against DNS record injection

You also need to ensure access control on the server, to prevent a malicious user altering records manually.

SNMP Security



c98xx

A network management system provides a proactive way to manage the network and help to identify problems.

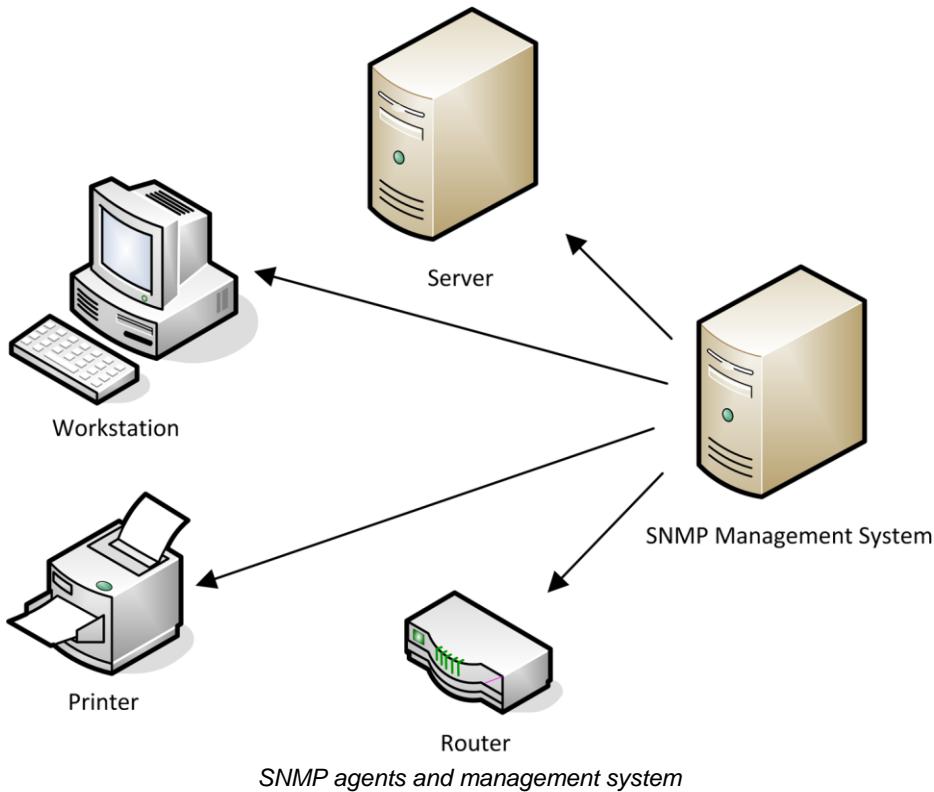
Simple Network Management Protocol (SNMP) is a widely used framework for management and monitoring. It is part of the TCP/IP protocol suite (operating at the Application layer of the OSI model).

SNMP consists of a **management system** and **agents**.

- The **agent** is a process (software or firmware) running on a switch, router, server, or other SNMP-compatible network device.

This agent maintains a database called a **Management Information Base (MIB)** that holds statistics relating to the activity of the device (for example, the number of frames per second handled by a switch). The agent is also capable of initiating a **trap** operation where it informs the management system of a notable event (port failure for instance). The threshold for triggering traps can be set for each value. Device queries take place over port 161 (UDP); traps are communicated over port 162 (also UDP).

- The **management system** (a software program) provides a location from which network activity can be overseen. It monitors all agents by polling them at regular intervals for information from their MIBs and displays the information for review. It also displays any trap operations as alerts for the network administrator to assess and act upon as necessary.



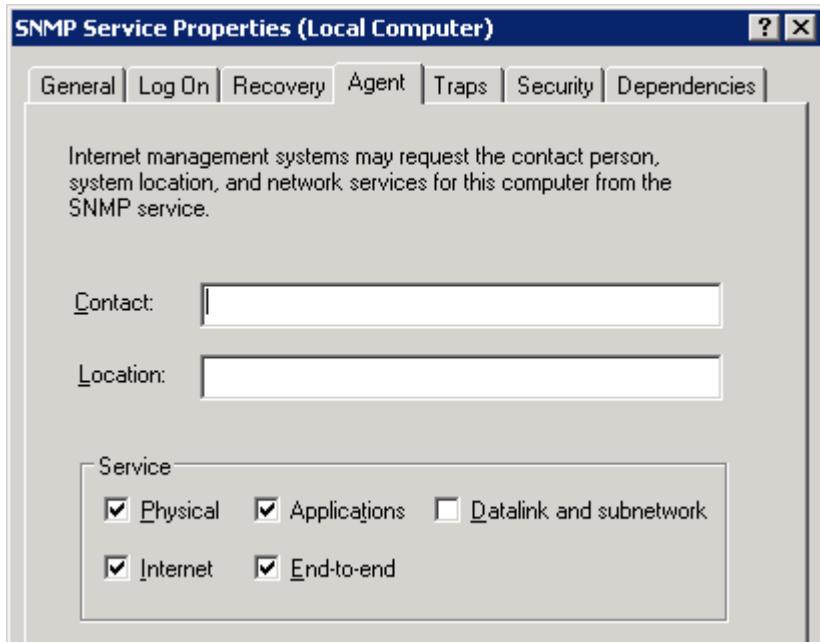
Examples of management systems include IBM's Tivoli software suite, HP's OpenView, Computer Associate's Unicenter, Novell's ZENworks, SolarWinds Orion, Microsoft's System Center, and Spiceworks.

The current SNMP specification is version 3.0 (see www.snmplink.org for details).

Configuring SNMP Agents

The method of configuring the SNMP Agent on a particular device or component depends on the software or firmware installed on the device. On a Windows Server, you configure the agent via **SNMP Service Properties** (open the **Services** applet from Computer Management, alt-click the **SNMP Service**, and select **Properties**). You can input a contact name and physical location for the computer and choose what services are running on the machine.

On the **Traps** tab, you should input the **Community Name** of the computers allowed to manage the agent and the IP address or host name of the server running the management system. The community name acts as a rudimentary type of password. An agent can only pass information to management systems configured with the same community name. There are usually two community names; one for read only access and one for read-write access (or privileged mode).



SNMP Service - Agent properties

On a device such as a hardware router, UPS, or RAID controller you would use the card's management interface to set agent properties.

Thresholds for triggering trap **alerts** are configured using the management system.

The screenshot shows the Dell OpenManage Server Administrator interface under the 'Alert Management' tab. On the left, there's a navigation tree with 'System' expanded, showing 'Main System Chassis', 'Software', and 'Storage'. The main panel is titled 'Set Alert Actions for Chassis Intrusion'. It lists four alert actions: 'Beep speaker on the server.', 'Display an alert message on the server.', 'Broadcast a message.', and 'Execute application.' Each action has a corresponding checkbox. To the right of the 'Execute application.' checkbox is a text input field labeled 'Absolute path to the application:' with a placeholder 'Local intranet'. At the bottom of the panel are 'Print', 'Email', 'Clear All', and 'Refresh' buttons.

Configuring SNMP traps using Dell OpenManage

SNMP Security

If SNMP is not used, you should remember to change the default configuration password and disable it on any SNMP-capable devices that you add to the network.

If you are running SNMP version 1, keep to the following guidelines:

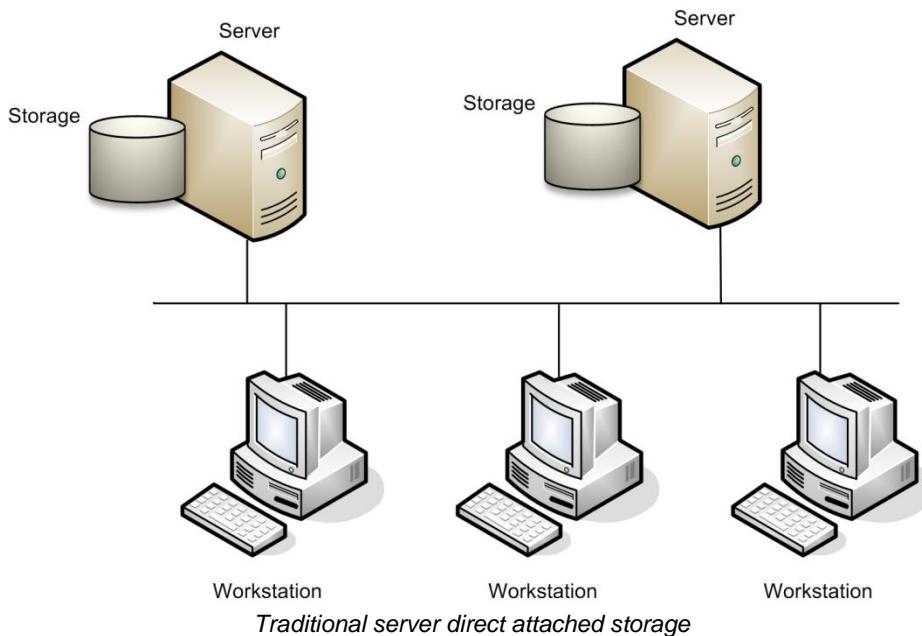
- SNMP community names are sent in plaintext and so should not be transmitted over the network if there is any risk that they could be intercepted.
- Use difficult to guess community names; never leave the community name blank or set to the default.
- Use Access Control Lists to restrict management operations to known hosts (that is, restrict to one or two host IP addresses).

SNMP v3 supports encryption and strong user- or group-based authentication.

Storage Area Network Security



Traditional server-based (or direct attached) storage means that the data a server hosts is stored on its internal hard drives or on a USB or eSATA external device connected only to that server.



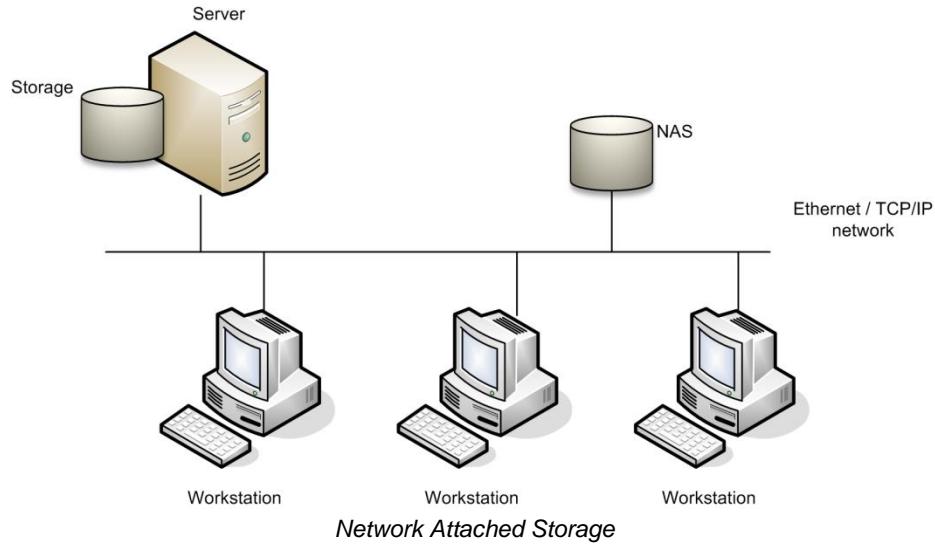
Such **direct attached storage** creates certain problems:

- It is resource inefficient because while some servers have space free, other may be running low on storage capacity.
- Traditional storage creates unplanned redundancy, because multiple instances of files may exist on multiple servers.
- There is little cross-platform sharing of data (for example, Linux and Windows) because the file system may only be accessible to one type of client.

Vendors have been coming up with methods for attaching storage devices to the network for shared use by servers and clients. These are usually divided into **Network Attached Storage (NAS)** solutions and **Storage Area Networks (SAN)** solutions.

Network Attached Storage

For a **Network Attached Storage (NAS)** solution, the vendor supplies a box, which essentially plugs into the network like any other device, but you won't need to attach it via a PC file server.



NAS devices share these characteristics:

- They are usually IP-based network devices.
- Clients attach directly to them (they provide file-level access).
- They support multiple network file access protocols (NFS [Unix / Linux] and SMB / CIFS [Windows] for instance).
- They contain an embedded, stripped down operating system such as a Linux kernel and file processor.
- Configuration is via a web browser interface.
- They are generally cheaper than PC file servers.
- Most support RAID 1 and some will support RAID 5 or 6 or nested RAID plus hot pluggable drives.

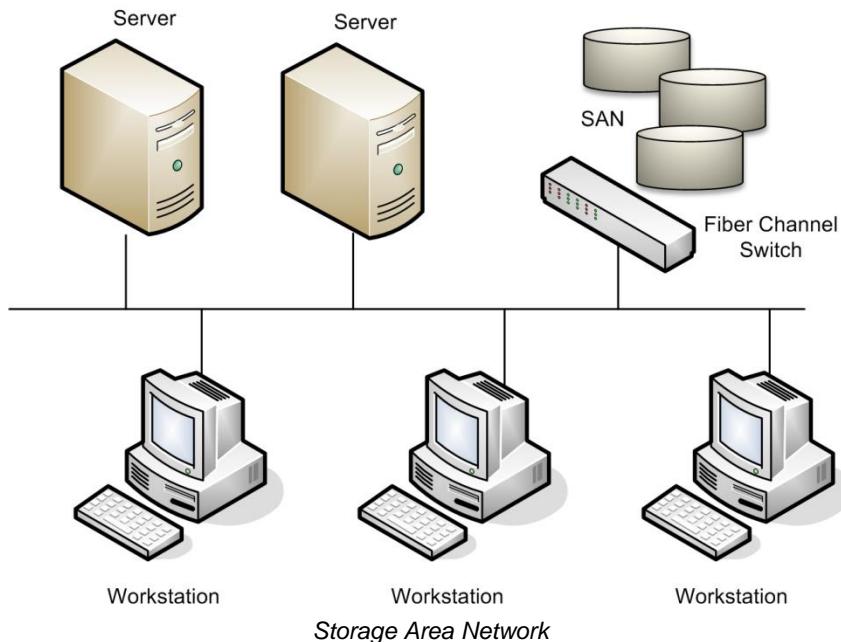
Storage Area Network (SAN)

NAS provides a cheap storage solution and is very easy to set up. NAS is typified as providing access to clients at **file level** (via the file name [File I/O]). In a **Storage Area Network (SAN)**, access is provided at **block level** (that is, the actual location of data on the media [Block I/O]). This is much more efficient for database applications, as it does not mean copying the whole file across the network to access a single record.

A SAN can integrate different types of storage technology - RAID arrays and tape libraries for instance. It can contain a mixture of high-speed and low cost devices, allowing for tiered storage to support different types of file access requirements without having to overprovision high-cost, fast drives.

A SAN can provide robust and extensible storage solutions for local networks and for remote storage but at greater cost than NAS. Consequently, SANs are typically deployed in enterprise networks and data centers while NAS is more of a small office or workgroup solution. Remote storage facilities generally leased from service providers rather than owned and maintained by the organization itself.

The SAN is isolated from the main network. It is only accessed by servers, not by client workstations. A SAN can be implemented using a variety of technologies, but the most popular are high bandwidth Fibre Channel and iSCSI fiber optic networks.



Fibre Channel Hardware

A SAN based on a **Fibre Channel (FC) Switched Fabric (FC-SW)** involves three main types of component:

- Initiator - this is a host bus adapter installed in the file or database server.
- Target - the network port for a storage device. Typical devices include single drives, RAID drive arrays, tape drives, and tape libraries. Space on the storage devices is divided into logical volumes, each identified by a 64-bit **Logical Unit Number (LUN)**. The initiator will use SCSI, SAS (Serial Attached SCSI), or SATA commands to operate the storage devices in the network, depending on which interface they support. Most devices have multiple ports for load balancing and fault tolerance.

The initiators and targets are identified by 64-bit **World Wide Names (WWN)**; similar to network adapter MAC addresses. Collectively, initiators and targets are referred to as **nodes**. Nodes can be allocated their own WWN, referred to as a WWNN (WorldWide Node Name). Also, each port on a node can have its own WorldWide Port Name (WWPN).

- FC switch - this provides the interconnections between initiators and targets. The switch topology and interconnections would be designed to provide multiple paths between initiators and targets, allowing for fault tolerance and load balancing. High performance FC switches are often referred to as directors.

Using fiber optic cabling, an FC fabric can be up to 10 km (6 miles) in length using single mode cable or 500m (1640ft) using multimode cable.

Fibre Channel is defined in the T11 ANSI standard. The spelling "fibre" is deliberately used to distinguish the standard from fiber optic cabling, which it often uses but on which it does not rely. The standard transfer rates are 1GFC (1 Gbps), 2GFC, 4GFC, 8GFC, and 16 GFC. Two other rates (10GFC and 20GFC) use different encoding and are incompatible with devices supporting only the standard rates.

Fibre Channel over IP (FCIP)

Fibre Channel over IP is a tunneling protocol allowing the transfer of frames of FC data over any IP-based network, such as the internet. This is a cost-effective way to link SANs in different geographic locations.

iSCSI

Internet SCSI (iSCSI) is also an IP tunneling protocol and enables the transfer of SCSI data over an IP-based network.

Unlike FC, iSCSI works with ordinary Ethernet network adapters and switches. It could be deployed with bonded Gigabit links or with Ethernet 10G adapters and switches.

iSCSI can be used to link SANs (as per FCIP) but is also seen as an alternative to Fibre Channel itself, as it does not require FC-specific switches or adapters.

Fibre Channel over Ethernet (FCoE)

Provisioning separate Fibre Channel adapters and cabling is expensive. As its name suggests, **Fibre Channel over Ethernet (FCoE)** is a means of delivering Fibre Channel packets over 10G Ethernet cabling, NIC/HBAs (referred to as Converged Network Adapters [CNA]), and switches. FCoE uses a special frametype, identified by the EtherType value 0x8096. The protocol maps WWNs onto MAC addresses.



FCoE does not quite run on standard Ethernet. It requires quality of service mechanisms to ensure flow control and guaranteed delivery. FCoE compliant products are referred to as lossless Ethernet, Data Center Ethernet, or Converged Enhanced Ethernet.



f85uf

Fibre Channel Security Issues

As with IP, all FC frames are transferred unencrypted, meaning that an attacker with access to the switch fabric could easily perform eavesdropping or Man-in-the-Middle modification attacks.

LUN Masking

One basic FC security technique is to use LUN masking. This could be configured on the HBA but is more typically implemented on the storage device. LUN masking means that the device is configured with an access control list of valid WWNs (or WWPNs). A server without a matching WWN will not be able to access the storage device.



It is possible to spoof a WWN (in a similar way to spoofing a MAC address). Consequently it is important to secure the management interfaces of HBAs and switches to prevent unauthorized changes or the attachment of rogue devices.

Zoning

Another option is to configure zoning. When implemented using an FC switch (hard zoning), a zone is somewhat similar to a VLAN. Each device is placed in a zone based on the switch port it is connected to and the switch determines whether they are allowed to communicate.

Fibre Channel Security Protocols (FC-SP)

Legacy FC security depends on the physical security of the network and the servers used to access it. A security protocol (FC-SP) was standardized in 2004. FC-SP allows for the use of encryption for authentication and confidentiality:

- **Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP)** - this allows initiators and targets to authenticate by configuring the same shared secret on each device or by configuring a RADIUS server to hold device authentication information.
- **Fibre Channel Authentication Protocol (FCAP)** - provides authentication through digital certificates installed on the devices.
- **Encapsulating Security Protocol (ESP)** - this provides message confidentiality and integrity (in the same sort of way as IPsec).



When used over IP (FCIP or iSCSI) native IP security mechanisms such as IPsec can be used directly.



IPv4 versus IPv6

IPv6 is the planned replacement for IPv4. It uses a 128-bit address space. On the internet, each host is identified by a 64-bit network prefix and a 64-bit host ID. The host ID is either generated randomly or derived from the adapter's MAC address (the 48-bit MAC address is padded to make it up to 64 bits). The network prefix is assigned by the ISP.

The prefix is hierarchical and ISPs can allocate different length prefixes according to need. Companies and individuals will receive prefixes of between /48 and /64. The number of bits remaining in the mask can be used by a company to subnet its internal network. For example, a company that receives a /48 network prefix has 16 bits available to subnet its network; a private individual with a /64 prefix would not be able to create subnets (but would not be likely to have any reason to do so anyway).

Some ISPs are starting to test their IPv6 readiness but IPv6 is still very far from being widely deployed.

While it has been in development for over a decade, additional security issues are certain to appear as more websites and subscribers start to use the IPv6 internet. Security issues can be grouped into three broad categories: vulnerabilities in the IPv6 protocol itself, vulnerabilities in transition mechanisms, and the different security model envisaged by IPv6.

Core Vulnerabilities

As IPv6 is deployed to more networks, more vulnerabilities may appear in the core protocol. Known or potential vulnerabilities are currently published in [RFC 4942](#).

On the other hand, IPv6 should make ARP and IP address spoofing attacks much more difficult and native support for IPsec could see many more networks deploy it as a matter of course, providing confidentiality and integrity.



ARP is not part of IPv6 at all. IPv6 uses the Neighbor Discovery (ND) and Secure Neighbor Discovery (SEND) protocols rather than ARP.

The larger address space also makes network mapping (port scanning for active hosts) more difficult. Also, IPv6 does not use broadcast traffic, eliminating many DoS attacks, though new attacks against IPv6 multicast protocols could arise.

IPv6 deployment is also likely to see the full implementation of DNSSEC, to prevent DNS spoofing.

Transition Mechanisms

Most networks are likely to have to support a mix of IPv4 and IPv6 traffic. There are two means of doing this:

- Dual-stack means that routers run both IPv4 and IPv6 side-by-side.
- Tunneling means that IPv6 is encapsulated within IPv4 packets by routers.

One significant problem is a lack of support in the market for IPv6 security products, such as firewalls, intrusion detection, and vulnerability scanners. Another is that the mix of architectures makes configuration complex and prone to error.

Another consideration is that while IPv6 is often enabled and running on networks (it is installed and enabled on Windows 7 and Server 2008 by default for instance), there are no security mechanisms deployed for it. IPv6 tunnels could be used as a means of bypassing firewalls that can only process IPv4 traffic for instance.

Security Model

IPv4 is very much based on perimeter security, enforced by firewalls. There are endpoint security products, designed to control which devices are allowed to connect to the network. These reflect the increasingly problematic nature of perimeter security solutions. The use of remote access and mobile IP-enabled devices makes the perimeter "fuzzy".

Technologies such as private (RFC 1918) addressing and Network Address Translation (NAT) are deprecated in IPv6. Hosts are supposed to establish transparent end-to-end links with security provided by IPsec. These end-to-end links should still be controlled by router and firewall policies so perimeter security is still important. However, the principle of IPv6 is that if a link can be established through the firewall, the endpoints should know one another's true IP addresses.

Endpoint security tools (802.1X authentication and IPsec) to control which hosts can attach to a network will continue to be very important in IPv6.



See [Unit 4.1](#) for more information about endpoint security and 802.1X.



Telephony

A domestic telephone installation would be serviced by a simple box providing a one or two line interface to the local exchange. A typical business requires tens or hundreds of lines for voice communications, let alone capacity for data communications. These connections will normally be facilitated by a PBX.

Private Branch Exchange (PBX)

A **Private Branch Exchanges (PBX)** is an automated switchboard providing a single connection point for the organization's voice and data lines. The PBX is connected to the telecoms provider (normally over a T-carrier link). It can support the multiple lines required and allows configuration of the internal phone system to direct and route calls and data.

Most PBX are digital machines with numerous customizable features. The increasing sophistication of PBX, especially the incorporation of **Voice over IP (VoIP)** functions, makes them a tempting target for attackers. Compromising the PBX can allow the attacker to perform a Denial of Service against the organization's voice and data lines.



Panasonic Hybrid IP PBX System

Another common attack is to dial into the PBX then place a call using the PBX, making the PBX owner liable for the call charges.

The PBX needs to be physically secured to prevent the attachment of snooping devices and other unauthorized access. Administrative features (such as access to configuration consoles) need to be locked down, especially remote access features. As with any computer system, unused features and ports should be disabled and operating system or firmware updates applied to fix any known security vulnerabilities.



Panasonic digital handset - most PBX can be configured via handsets



Most PBX allow remote administration by the telecoms provider. These features should either only be activated when the telecoms provider requires it or protected by strong authentication.



As with any network device, do not leave a PBX configured with the default administration passwords or PINs.

Voice over IP (VoIP)

Voice over IP (VoIP) packages voice communications as data packets, transmits them over the network, then reassembles the packets to provide two-way, real-time voice communication. A significant advantage (notably for call center operations) is that data from calls can be recorded, tracked, routed, and analyzed much more easily.

There are numerous different ways of implementing VoIP, each with different protocols, which are often proprietary to a particular VoIP software vendor.

To implement VoIP to make calls from a computer in a typical Peer-to-Peer configuration, you need software (such as Skype) an internet connection, and usually a handset (more convenient than using PC microphone and speakers). VoIP calls can be placed from computer-to-computer or from computer-to-PSTN / cell phone. Calls can also be made from PSTN-to-computer, if a suitable access number is set up. Software such as Skype can also function as an IM client.

On an enterprise level, many organizations have implemented VoIP using fully digital PBX.

Convergence refers to the collapsing of the various means of communicating over networks (PSTN, email, IM, and VoIP). For example, products are appearing that allow IM conversations to be "escalated" to voice and smart clients that let (for instance) an IM caller know if the recipient is currently on the telephone.

Implementing internet telephony brings its own raft of security concerns. Each part of the VoIP network infrastructure needs to be evaluated for threats and vulnerabilities. This includes protocols, servers, handsets, and software.

The main protocols used to implement VoIP are as follows:

- Session control - there are a number of open and proprietary protocols for establishing a session between two VoIP devices that want to communicate. The Session Initiation Protocol (SIP) and H.323 are the most popular open standards while Skype is one of the best established proprietary mechanisms.
- Data transport - the RTP (Real-time Transport Protocol) is designed to deliver packets in real time over IP. Secure RTP provides encryption and authentication for connections.
- Quality of Service (QoS) - the Real-time Control Protocol (RTCP) provides information about the connection to a QoS system, which in turn ensures that voice or video communications are free from problems such as dropped packets, delay, or jitter.

One of the main concerns is that of eavesdropping. Hackers could exploit unencrypted VoIP communications to try to intercept passwords, credit card details, and so on. Without strong mutual authentication, connections are also vulnerable to Man-in-the-Middle attacks (redirection, replay, and hijacking). The drawback is that poorly implemented encryption adds a substantial processing overhead and can significantly reduce call quality. Fully secure VoIP infrastructure is likely to add substantially to costs!

The organization is also particularly vulnerable to DoS, which could cripple voice communications as well as data. Another threat that could possibly evolve is unsolicited calls or SPIT (SPAM over Internet Telephony), a direct descendant of auto-dialers.



Review Questions / Module 3 / Unit 5 / Network Application Security

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What risk might IPv6 pose to a network that does not have an IPv6 management plan?
- 2) What vulnerabilities does a rogue DHCP server expose users to?
- 3) Why is it vital to ensure the security of an organization's DNS service?
- 4) True or false? The contents of the HOSTS file are irrelevant so long as a DNS service is properly configured.
- 5) What is DNS cache poisoning?
- 6) If anonymous access to an IPC\$ share is required by a Line of Business application, what steps can be taken to prevent remote exploitation of RPC?
- 7) What steps should you take to secure an SNMPv2 service?
- 8) What access control measures could you deploy on a Fibre Channel SAN to restrict which servers can access certain storage devices?
- 9) True or false? The management console of a PBX can often be accessed from outside the organization.
- 10) Why is it difficult to encrypt VoIP?



If you have access to the Hands On Live Labs, complete the "Protocols and Services / DNS", "Threats / DNS Poisoning", "Protocols and Services / SNMP" and "Protocols and Services / iSCSI" labs now.

Module 3 / Summary

Network Security

In this module, you learned about network designs and appliances and their vulnerabilities plus network security appliances and software. You also learned about wireless, VPN, and remote security and about implementing typical network applications.

Module 3 / Unit 1 / Secure Network Design

- A security zone is an area of the network with the same security configuration. Different zones (such as intranet, extranet, internet, and DMZ) are required to provide a different balance between confidentiality / integrity to availability, depending on user requirements.
- VLANs, NAT, firewalls, routers, and switches can be used to define security zones and implement network access control.
- A perimeter security model is often not adequate. Defense-in-depth ensures that network endpoints are equally well protected as zone borders.
- Network hardening involves creating secure configuration baselines for devices such as switches, routers, and firewalls. Firmware for devices such as routers and switches should be kept up-to-date.

Module 3 / Unit 2 / Security Appliances and Applications

- A packet filtering firewall accepts or rejects traffic on the basis of IP addresses and port numbers (an Access Control List).
- More advanced firewalls can track sessions (stateful inspection) and inspect the payloads of packets (application layer / stateful multilayer).
- Firewalls are often implemented as proxy servers. Rather than monitor the link between two hosts, a proxy server inspects and forwards requests on the client's behalf. Other typical web proxy functions include caching resources locally and prefetching pages to reduce bandwidth and performing content / usage / spam filtering. Reverse proxies can be deployed to publish server applications.
- Intrusion Detection Systems (IDS) identify suspicious behavior. They can be either network- or host-based. Detection can be via pattern matching (signature-based) or heuristic analysis of behavior and anomalies (or both).
- Passive detection means that incidents are logged or generate alerts; active detection means that the system can take action to prevent attacks. These systems are also referred to as Intrusion Prevention Systems (IPS).
- Logs provide an audit trail of network and system activity. Baseline configuration and performance levels help to identify suspicious deviations. Thresholds can be configured to provide automatic alerting. Logs must be made tamper-proof.

Module 3 / Unit 3 / Wireless Network Security

- WEP is a legacy security protocol for Wi-Fi. Because WEP is flawed, a new standard (Wi-Fi Protected Access [WPA/WPA2]) has been introduced.
- Clients can be authenticated against a WEP or SOHO WPA network using a Preshared Key. With WPA and EAP, the client can authenticate against a RADIUS accounts server.
- When planning wireless access, a site survey is performed to find the optimum placement of access points and booster antennas. Shielding can be used to prevent eavesdropping of wireless signals.

Module 3 / Unit 4 / VPN and Remote Access Security

- Most networks must now support remote access. Traditionally, this was accomplished using modems and dial-up access. This infrastructure has been replaced by VPN technologies.
- Tunneling protocols enable two networks using one protocol to be connected via an intermediate network using a different protocol. Secure tunneling protocols can be used to establish a VPN.
- A VPN can be established using a layer 2 tunneling protocol (such as L2TP/IPsec or PPTP) or by encrypting higher layer traffic (using technologies such as SSL or SSH).
- Remote management applications such as Telnet, SSH, and Remote Desktop must be used securely.

Module 3 / Unit 5 / Network Application Security

- DHCP services require careful configuration and monitoring to ensure they are set up securely.
- DNS is a critical service for the internet and most local networks. It is vulnerable to footprinting, spoofing, and DoS attacks at the client and server level.
- SNMP can be used for performance monitoring and network management but v3 supports security mechanisms.
- Storage Area Networks based on technologies such as Fibre Channel provide high volume storage solutions for enterprises and data centers.
- Networks might start to transition to IPv6 over the next few years and while the protocol has security improvements, new attacks are likely to arise and the transition process needs to be carefully managed.
- Telephony systems such as PBX and VoIP may be exploitable or vulnerable to DoS or eavesdropping. Make sure the management interfaces of these devices are secured.

Module 4 / Host, Data, and Application Security

The following CompTIA Security+ domain objectives and examples are covered in this module:

Domain Objectives/Examples	Refer To
1.2 Given a scenario, use secure network administration principles <i>Port security • 802.1X</i>	Unit 4.1 Host Security
1.3 Explain network design elements and components <i>NAC</i>	
2.9 Given a scenario, select the appropriate control to meet the goals of security <i>Availability (Patching)</i>	
3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques <i>Hardening (Disabling unnecessary services • Protecting management interfaces and applications) • Network security (MAC limiting and filtering, 802.1X, Disabling unused interfaces and unused application service ports, Rogue machine detection)</i>	
3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities <i>Assessment technique (Baseline reporting)</i>	
4.1 Explain the importance of application security controls and techniques <i>Application configuration baseline (proper settings) • Application hardening • Application patch management</i>	
4.3 Given a scenario, select the appropriate solution to establish host security <i>Operating system security and settings • OS hardening • Patch management • Whitelisting vs. blacklisting applications • Trusted OS • Host software baselining</i>	
5.2 Given a scenario, select the appropriate authentication, authorization or access control <i>Authentication (Trusted OS)</i>	
2.3 Given a scenario, implement appropriate risk mitigation strategies <i>Enforce policies and procedures to prevent data loss or theft • Enforce technology controls (Data Loss Prevention [DLP])</i>	Unit 4.2 Data Security
2.6 Explain the importance of security related awareness and training <i>Personally identifiable information • Information classification (High, Medium, Low, Confidential, Private, Public) • Data labeling, handling and disposal • User habits (Data handling)</i>	
2.8 Summarize risk management best practices <i>Disaster recovery concepts (Backup plans/policies, Backup execution/frequency)</i>	

Domain Objectives/Examples	Refer To
4.4 Implement the appropriate controls to ensure data security <i>Handling Big Data • Data encryption (Full disk, Database, Individual files, Removable media, Mobile devices) • Hardware based encryption devices (TPM, USB encryption, Hard drive) • Data in-transit, Data at-rest, Data in-use • Permissions/ACL • Data policies (Wiping, Disposing, Retention, Storage)</i>	<u>Unit 4.2</u> <u>Data Security</u>
1.1 Implement security configuration parameters on network devices and other technologies <i>Load Balancers</i>	<u>Unit 4.3</u> <u>Web Services Security</u>
1.4 Given a scenario, implement common protocols and services <i>Protocols (TLS, SSL, FTPS, HTTPS, FTP, SFTP, TFTP, HTTP) • Ports (21, 80, 443)</i>	<u>Unit 4.3</u> <u>Web Services Security</u>
6.2 Given a scenario, use appropriate cryptographic methods <i>Use of algorithms/protocols with transport encryption (SSL, TLS, HTTPS)</i>	
3.2 Summarize various types of attacks <i>Privilege escalation • Transitive access • Client-side attacks</i>	<u>Unit 4.4</u> <u>Web Application Security</u>
3.5 Explain types of application attacks <i>Cross-site scripting • SQL injection • XML injection • Directory traversal/command injection • Buffer overflow • Integer overflow • Zero-day • Cookies and attachments • Malicious add-ons • Session hijacking • Header manipulation • Arbitrary code execution / remote code execution</i>	<u>Unit 4.4</u> <u>Web Application Security</u>
3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities <i>Assessment technique (Code review • Determine attack surface • Review architecture, Review designs)</i>	
4.1 Explain the importance of application security controls and techniques <i>Fuzzing • Secure coding concepts (Error and exception handling, Input validation) • Cross-site scripting prevention • Cross-site Request Forgery (XSRF) prevention • NoSQL databases vs. SQL databases • Server-side vs. Client-side validation</i>	
1.3 Explain network design elements and components <i>Virtualization • Cloud Computing (Platform as a Service, Software as a Service, Infrastructure as a Service, Private, Public, Hybrid, Community)</i>	<u>Unit 4.5</u> <u>Virtualization and Cloud Security</u>
2.1 Explain the importance of risk related concepts <i>Risks associated with Cloud Computing and Virtualization</i>	
4.3 Given a scenario, select the appropriate solution to establish host security <i>Virtualization (Snapshots, Patch compatibility, Host availability/elasticity, Security control testing, Sandboxing)</i>	
4.4 Implement the appropriate controls to ensure data security <i>Cloud storage</i>	

Module 4 / Unit 1

Host Security

Objectives

On completion of this unit, you will be able to:

- Understand the concepts of hardening, baseline configurations, and host management.
- Understand the use of group policies to apply security settings in a Windows Server network.
- Apply operating system and application software patches and firmware updates.
- Understand the role of Network Access Control (NAC) in maintaining host security.

Computer Hardening

The process of securing a PC, operating system, or application for use is called **hardening**. For an OS functioning in any given role, there will usually be a fairly standard series of steps to follow to configure it to perform securely in that role.

It is also important to establish a maintenance cycle for each device and keep up-to-date with new security threats and responses for the particular software products that you are running.



Common Criteria and Trusted OS

Common Criteria (CC) is an ISO standard (ISO 15408) defining security frameworks. It evolved from separate standards developed by the USA (TCSEC or "Orange Book"), Canada (CTCPEC), and Europe (ITSEC).

The CC security framework for a given **Security Target (ST)** has the following components:

- Security environment - organizational policies and threats.
- Security objectives - the measures that are intended to support policies and counter threats.
- Target of Evaluation (TOE) - a specific part of the security system that is being put under evaluation.

- TOE security requirements - this is the "high-level" design or statement of intentions for the TOE
- TOE security specifications - this is a detailed design specification for the TOE
- TOE implementation - realization of the TOE security functions

Another concept of CC is the **Protection Profile (PP)**. This is an implementation-independent set of security requirements and objectives for different functional components. CC defines eleven functional component categories, including Cryptography, Auditing, User Data Protection, Communications, and Identification and Authentication. This provides backwards compatibility with the DoD's C1, C2, B1, B2, B3, and A1 security ratings.

Products and security implementations can be rated to one of seven **Evaluation Assurance Levels (EAL)**, with EAL7 being the most exacting. It is crucial to recognize the distinction between a product and the way the product is used or configured. A product may conform to a certain EAL but its deployment on the network might not.

Product reports can be checked at www.commoncriteriaportal.org.



Common Criteria certificate (EAL4) for Microsoft Windows 2000 SP3

An operating system can be evaluated to a given EAL for a given number of protection profiles. An OS that meets the criteria can be described as a **Trusted OS (TOS)**. In very general terms, a trusted OS provides:

- Trusted Computing Base (TCB) - the kernel and associated hardware and processes must be designed to support the enforcement of a security policy (an access control model). This means it should be tamper-resistant, resistant to vulnerabilities, and not able to be bypassed (it provides complete "mediation" between users and resources). The TCB should be as small as possible, in order to facilitate better analysis and understanding.
- Security features - such as support for multilevel security (Mandatory Access Control). A problem for many OS is the means of restricting root or Administrator access to classified data. The process for patching security vulnerabilities is also critical.
- Assurance - such as secure design principles, availability of code reviews and audits, and so on.

Commercial operating systems are simply too complex to achieve anything over EAL4+. Examples of EAL4+ products include Windows Server 2008, RedHat Enterprise Linux v5.3 on Dell 11G servers, and VMWare ESXi Server 3.5 and Virtual Center 2.5.

All this means that the computing environment is trusted not to create security issues. For example, when a user authenticates to a network using a computer running a trusted OS, there is (or should be) assurance that the system itself has not compromised the authentication process (by allowing snooping, session hijacking, or other such attacks).



t18j0

Baseline Operating System Security and Settings

A **baseline** is a snapshot of the typical activity on your network or on any given host. Baselines are most useful for performance monitoring (you cannot tell whether performance has improved or degraded unless you know the starting point) and for security monitoring (both manually and using Intrusion Detection Systems).



Intrusion Detection Systems are covered in [Unit 3.2](#).

Another use of "baseline" is to mean a system in the minimum working configuration that is also secure. This can also be described as **host software baselining**. The essential principle is that a system should run only the protocols and services required by legitimate users and no more. This reduces the potential **attack surface**. If a particular configuration deviates from the baseline set, that can be taken as suspicious and the variations investigated.

- **Interfaces** provide a connection to the network. Some machines may have more than one interface. For example, there may be wired and wireless interfaces or a modem interface. Some machines may come with a management network interface card. If any of these interfaces are not required, they should be explicitly disabled rather than simply left unused.

- **Services** provide a library of functions for different types of application. Some services support local features of the OS and installed applications. Other services support remote connections from clients to server applications. Unused services should be disabled.
- **Application service ports** allow client software to connect to the application. Again, these should be closed if remote access is not required. Also consider that an application may use multiple ports. For example, there may be a "standard" user port and another port for management functions. Finally, be aware that a server might be configured with a non-standard port. For example, an HTTP server might be configured to use 8080 rather than 80.

Any service or interface that is enabled through the default installation and left unconfigured should be considered a vulnerability.

In the last few years, vendors have started shipping devices and software in secure configurations. This means that the default installation is (theoretically) secure but minimal. Any options or services must explicitly be enabled by the installer. This is not the case for older devices and software though; these would often be shipped with all the "Bells and Whistles" activated to make set up easier.



2m990

Host Software Baselining Security Checklist

The following checklist shows the sort of steps that are required to harden the OS of a workstation PC:

- 1) Remove (or disable) devices that have no authorized function. These could include a legacy modem or floppy disk or standard optical disk drives, USB ports, and so on.
- 2) Install OS and application patches and driver / firmware updates (when they have been tested for network compatibility) according to a regular maintenance schedule. Patches for critical security vulnerabilities may need to be installed outside the regular schedule
- 3) Uninstall all but the necessary network protocols.
- 4) Uninstall or disable services that are not necessary (such as local web server or file and print sharing) and remove or secure any shared folders.
- 5) Enforce Access Control Lists on resources, such as local system files and folders, shared files and folders, and printers.
- 6) Restrict user accounts so that they have "least privilege" over the workstation (especially in terms of installing software or devices).
- 7) Secure the local administrator or root account by renaming it and applying a strong password.
- 8) Disable default user and group accounts (such as the Guest account in Windows) and verify the permissions of system accounts and groups (removing the Everyone group from a folder's ACL for instance).

- 9) Install anti-virus software (or malware protection software) and configure it to receive virus definition updates regularly. Anti-virus software should also be configured so that the user cannot disable it and so that it automatically scans files on removable drives, that have been downloaded from the internet, or received as email/IM file attachments.



9ku02

Server and Application Hardening

Much the same procedure applies to servers and web applications, only "more so". Obviously a server will host more shares and services than a client, but the same principle of running only services (or application features) that are required applies.

The other side of running services and protocols is availability. You may need to consider the likelihood of Denial of Service (DoS) attacks against a particular service and provide alternative means for clients to access it. This could mean providing multiple network links, redundant servers, configuring separate physical servers for different server applications, and so on.



b8wf4

Execution Control (Whitelisting / Blacklisting)

Execution control is the process of determining what additional software may be installed on a client or server beyond its baseline. Execution control can be implemented as either as a whitelist or a blacklist:

- Whitelist control means that nothing can run if it is not on the approved "whitelist".
- Blacklist control means that anything not on the prohibited "blacklist" can run.

Anti-virus works on the basis of a blacklist. Malware known to the anti-virus software is recorded in its signature database. It blocks any process matching a malware signature from executing. For consumers, most smartphones and tablets work on the basis of whitelists; apps can only be selected from those approved by the OS vendor to be listed in a store.

Corporate execution control software might use a mixture of approaches. Whitelisting will inevitably hamper users at some point and increase support time and costs. For example, a user might need to install a particular conferencing application at short notice. Blacklisting is vulnerable to software that has not previously been identified as malicious (or capable of or vulnerable to malicious use).

Host Security Management Plan

A **management plan** for all network servers, devices, and workstations is the central plank in ensuring a secure, efficient, and well-documented network. A management plan should indicate what tasks are to be performed, when, and by whom. Tasks would include monitoring performance and hardware status, performing backups, resolving and recording errors, cleaning and environmental checks, identifying security threats and measures, detecting and resolving security breaches and intrusions, and so on.

It is essential that the plan sets out clear responsibilities and procedures for auditing action items (that is, ensuring that tasks are carried out properly and securely). Technicians responsible for maintenance may have different levels of access to the system. For example, administrators may have access to all configuration options on a server but backup operators can only access backup software and media.

The results of management activities should be reported back and fed into development plans, to identify upgrade requirements. In the event that a problem is discovered during routine maintenance, a proper change management procedure should be followed to ensure that the solution is tested and verified without further impacting performance, reliability, or security.

Thought needs to be given to implementing and protecting management interfaces and applications. There are two ways of managing a device: locally and remotely. *Some* tasks can *only* be performed locally (such as cleaning or upgrading hardware). *Most* tasks can be performed locally *if necessary*, by logging on to the device at the console. However, most software tasks can be performed *remotely* more efficiently.

Remote management has significant advantages in terms of saving time and personnel. The advantages for managing geographically separate locations should be obvious, but even within a building, remote management can simplify administration and if correctly configured, can enhance security (by restricting personnel needing to access the server room). Proper configuration and security measures are essential however, if the network is not to be made vulnerable to attack via abuse of the remote management interface.

Remote management tools are available in two different classes:

- In-band tools use the ordinary network connection to manage the device. These are the tools commonly used for basic management tasks. Examples include Telnet, SSH, and GUI utilities such as Remote Desktop.

With in-band tools, a careful consideration needs to be made of the security implications. Thought also needs to be given to the impact on the network of running the remote management software.

- Out-of-band tools access the device via an alternative connection, such as a dial-up modem, serial port, or non-standard network link (often implemented as a different VLAN). These are used when the network is not available or when the server is not available to ordinary software tools (such as during power off and on, in the early stages of OS setup routines, or if the server has crashed).

A **Baseboard Management Controller (BMC)** enables an administrator to access a server when mains power is off. The BMC contains a battery that keeps the controller and an out-of-band network interface active.

As with in-band management, the connection must be properly secured to prevent unauthorized access.

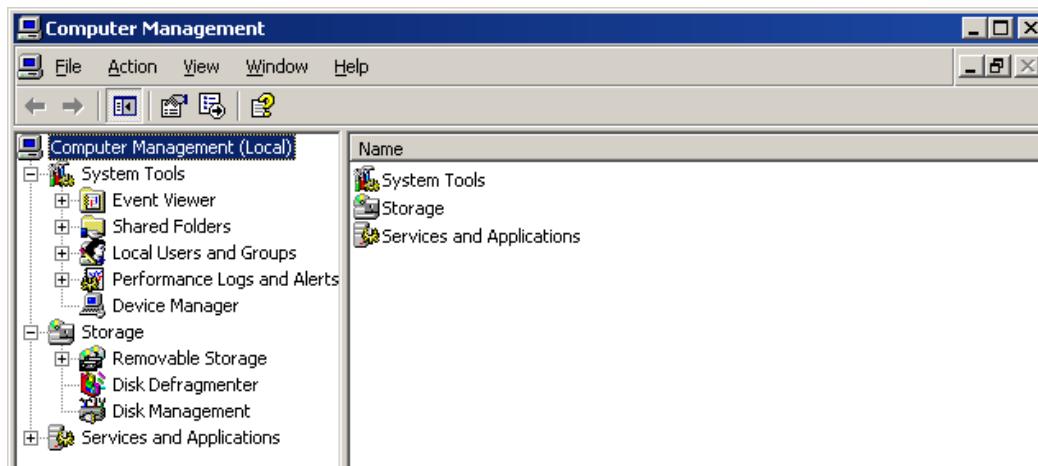
OS Hardening



OS hardening is a mixture of applying general steps, such as installing patches and service packs, and understanding the specific security issues of a particular OS.

Windows Administration and Management Tools

Windows has gone through a number of different versions over the years in terms of both server NOS (Network Operating System) and desktop client software. Each version has delivered improved security compared to its predecessor. The main administration tools for Windows are the **Control Panel, Management Consoles, and Administrative Tools**. A management console can contain snap-in tools for such things as Disk Management, Services, and User and Group Management.



Computer Management console

On a Windows Server network, most user rights and security settings are configured through **Group Policy Objects (GPO)**, controlled via a management console. For a standalone workstation, the **Local Security Policy** is used.

Configuration of Windows Server is made easier by the **Server Management** wizard, which leads the administrator step-by-step through adding and configuring server roles (such as File and Print, DNS, DHCP, Certificate Services, Routing and Remote Access, and so on).

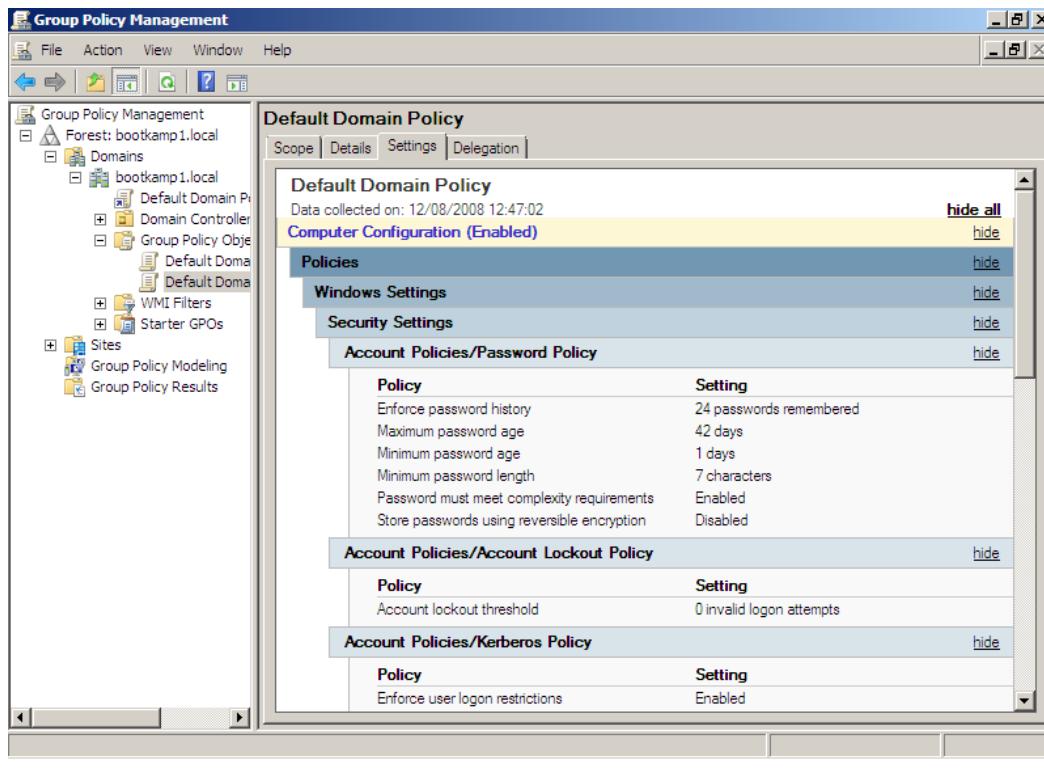
Group Policies, Security Templates, and Configuration Baselines

Group Policy Objects (GPO) are a means of applying security settings (as well as other administrative settings) across a range of computers. GPOs are linked to network administrative boundaries in Active Directory, such as sites, domains, and Organizational Units (OU).

GPOs can be used to configure software deployment, Windows settings, and (through the use of **Administrative Templates**) custom Registry settings. Settings can also be configured on a per-user or per-computer basis.

A system of inheritance determines the **Resultant Set of Policies (RSoP)** that apply to a particular computer or user. GPOs can be set to override or block policy inheritance where necessary.

Windows ships with a number of default **security templates** to provide the basis for GPOs. These simplify the configuration of the proper settings in **application configuration baselines**. The templates can be modified using the Group Policy Editor or Group Policy Management Console.



Group Policy Management

With Windows Server 2003 SP1, Microsoft introduced the **Security Configuration Wizard (SCW)** tool to better facilitate modelling, editing, testing, and deploying GPOs.

Baseline Reporting

The **Microsoft Baseline Security Analyzer (MBSA)** can be used for **baseline reporting** in small and medium size enterprises. Baseline *reporting* means testing the actual configuration of clients and servers to ensure that they are patched and that their configuration settings match the baseline template. MBSA can also be used to scan for weak passwords.

The **Security Compliance Manager (SCM)** (first released in 2011) wraps a number of security tools into one interface. SCM also links with Microsoft's enterprise compliance management product; the **Desired Configuration Management (DCM)** service in **System Center Configuration Manager (SCCM)**.



For more information about these and other free Microsoft security tools, view the Technet blog series at gtsgo.to/sg5tp.

Hardening UNIX and Linux

While Windows enjoys a huge installation base for both clients and servers, a number of other operating systems are very widely deployed on enterprise and campus networks and the internet.

UNIX predates Windows by a good long while. Almost forty years of development has produced a fast, stable, and very secure operating system. It is capable of providing file and print services as well as acting as an application server.

Configuration and management is mostly performed using a command line interface and scripts (UNIX is not renowned for being "user friendly") though there is a GUI interface for UNIX (X Window).

UNIX is available from a variety of vendors and is also available freely as open source software. Some of the main implementations of UNIX are:

- System V - developed by AT&T and then sold to Novell, who then sold the rights on again. It has spawned Sun Solaris and SCO's OpenServer and UnixWare.
- BSD (including NetBSD, OpenBSD, and FreeBSD) - based on the version of UNIX developed at the University of California at Berkley. Apple has based Mac OS X on BSD UNIX.

Linux is also based on the UNIX operating system. In recent years it has gained a significant following amongst not only enthusiasts, but major software vendors, such as Sun, Oracle, and Novell. There are many versions and editions of Linux (notably SUSE, Red Hat, Mandriva, Fedora Core, Debian, SimplyMEPIS, PCLinuxOS, and Ubuntu). Broadly speaking, the operating system does not require a graphical interface, though most versions provide one.

UNIX and Linux (or *nix) are considered to be particularly strong operating systems but relatively difficult to configure. One of the problems is the sheer number of different UNIX and Linux distributions and utilities.

The basic way of modifying configuration files, installing applications (packages), and configuring services is to modify the configuration files from a command line. Most versions of UNIX and Linux are shipped with GUI utilities to make these operations a bit easier.

Patch Management



Software updates resolve issues that a vendor has identified in the initial release of their product, based on additional testing or customer feedback. The updates are usually provided free-of-charge. Many updates address security vulnerabilities. In this sense, patching tools are a type of security control used to improve **availability**.

There are two approaches to applying updates:

- Apply all the latest patches to ensure the system is as secure as possible against attacks against flaws in the software.
- Only apply a patch if it solves a particular problem being experienced.

The second approach obviously requires more work, as the administrator needs to keep up-to-date with security bulletins. However, it is well recognized that updates (particularly service releases) can cause problems, especially with software application compatibility, and so the second approach is wisest.



Some applications may require the operating system to be patched to a certain level.

It makes sense to trial an update, especially a service release, on a test system to try to discover whether it will cause any problems. Approach the update like a software installation or upgrade (make a backup and a rollback plan). Read the documentation accompanying the update carefully. Updates may need to be applied in a particular order and there may be known compatibility issues or problems listed in the ReadMe.

Most operating systems and applications now support automatic updates via a vendor website.

Windows Update

Microsoft make the following distinctions between different types of software patch:

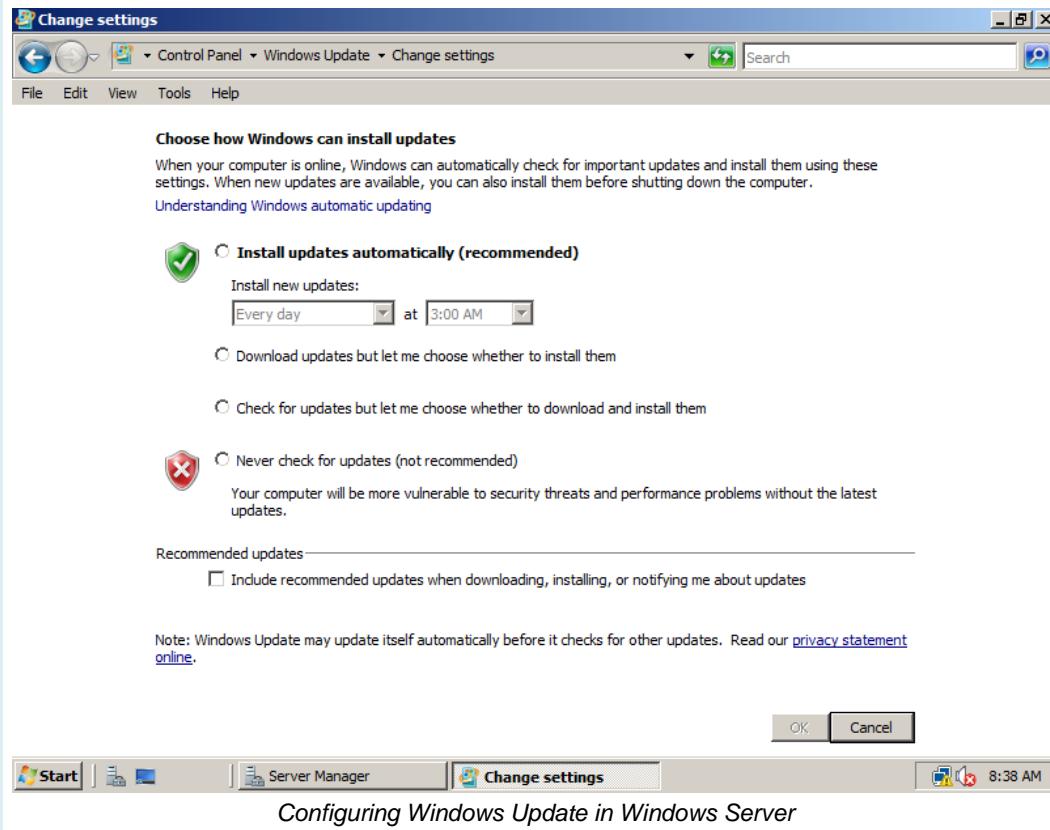
- **Updates** are widely released fixes for bugs. **Critical** updates address performance problems while **security** updates address vulnerabilities and can be rated by severity (critical, important, moderate, or low). There are also **definition** updates for software such as malware scanners and junk mail filters and **driver** updates for hardware devices.



Microsoft release most patches on "Patch Tuesday"; the second Tuesday in the month.

- **Hotfixes** are patches supplied in response to specific customer troubleshooting requests. With additional testing these may later be developed into public release updates.
- **Feature packs** add new functionality to the software.
- **Service packs** and **update rollups** form a tested collections of updates and hotfixes that can be applied in one package.

Patches, driver updates, and service packs for Windows (and other Microsoft software) can be installed using the **Windows Update** client. This client can be configured to obtain and install updates automatically. The settings used for automatic updates are often configured in Group Policy.



Windows Server Update Services (WSUS)

Connecting each client directly to the Windows Update website to download patches can waste a lot of bandwidth. On a network with a lot of computers, it can make more sense to deploy an **update server**. The update server for Windows networks is called **Windows Server Update Services (WSUS)**.



Another benefit of using a local update server is that some versions of Windows have been very vulnerable to attack if allowed to connect to the internet unpatched. Using a local server mitigates that risk.

The WSUS server works as a proxy. It scans the network to identify clients and determines what updates they require. An administrator can review the list of required updates and choose whether to apply or decline them. The server then downloads the updates from Microsoft's website and clients connect to it to obtain the patches.

Computers can be placed into pools, each with different update settings. For example, you could have a pool of test clients and servers and a pool of production computers. Updates could be applied to the test pool and then only applied to the production pool if the update is shown not to cause compatibility issues.

Update Services

Updates

This view shows a summary of the status of your updates by update view.

Overview

All Updates	Critical Updates
Updates with errors: 0	Updates with errors: 0
Updates needed by computers: 0	Updates needed by computers: 0
Updates installed/not applicable: 0	Updates installed/not applicable: 0
Updates with no status: 0	Updates with no status: 0

Security Updates	WSUS Updates
Updates with errors: 0	Updates with errors: 0
Updates needed by computers: 0	Updates needed by computers: 0
Updates installed/not applicable: 0	Updates installed/not applicable: 0
Updates with no status: 0	Updates with no status: 0

Actions

Updates

- Search...
- New Update Vie...
- Import Updates...
- View
- New Window fro...
- Refresh
- Help

Web Management Interface for WSUS

Linux Patch Management

Linux is very much based on **distributions**. A distribution contains the Linux kernel plus any other software packages the distribution vendor or sponsor considers appropriate. Copies of these packages (including any updates) will be posted to a **software repository**. Often the vendor will maintain different repositories (for example, one for officially supported package versions, one for beta / untested versions, and one for "at own risk" unsupported packages).



The integrity of a package is usually tested by making an MD5 hash of the compiled package. The MD5 value is published on the package vendor's site. When you download a package, you can run md5sum on the package file and compare the output with the published value. If they do not match, you should not proceed with the installation.

Linux software is made available both as source code and as pre-compiled applications. A source code package needs to be run through the appropriate compiler with the preferred options. Pre-compiled packages can be installed using various tools, such as **rpm** (RedHat), **apt-get** (Debian), or **yum** (Fedora). Many distributions also provide GUI package manager front-ends to these command-line tools.

The package manager needs to be configured with the web address of the software repository (or repositories) that you want to use. It can then be used to install, uninstall, or update the software.

```
GNU nano 2.2.6          File: /etc/apt/sources.list

#
# deb cdrom:[Ubuntu-Server 11.04 _Natty Narwhal_ - Release i386 (20110426)]/ na$#
#deb cdrom:[Ubuntu-Server 11.04 _Natty Narwhal_ - Release i386 (20110426)]/ nat$#
# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
# newer versions of the distribution.
deb http://gb.archive.ubuntu.com/ubuntu/ natty main restricted
deb-src http://gb.archive.ubuntu.com/ubuntu/ natty main restricted

## Major bug fix updates produced after the final release of the
## distribution.
deb http://gb.archive.ubuntu.com/ubuntu/ natty-updates main restricted
deb-src http://gb.archive.ubuntu.com/ubuntu/ natty-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team. Also, please note that software in universe WILL NOT receive any
## review or updates from the Ubuntu security team.
deb http://gb.archive.ubuntu.com/ubuntu/ natty universe
deb-src http://gb.archive.ubuntu.com/ubuntu/ natty universe
deb http://gb.archive.ubuntu.com/ubuntu/ natty-updates universe
deb-src http://gb.archive.ubuntu.com/ubuntu/ natty-updates universe

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
[ Read 64 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit    ^J Justify ^W Where Is ^V Next Page ^U UnCut Text^T To Spell
```

Configuring package manager sources in Ubuntu

Updates to the Linux kernel and a distribution's software tools and applications can be obtained via the package manager.

For example, you can edit a configuration file in the unattended-packages package to allow apt to obtain different types of updates. In the example below, only security updates are being obtained - the other types are commented out.

```
GNU nano 2.2.6  File: /etc/apt/apt.conf.d/50unattended-upgrades

// Automatically upgrade packages from these (origin, archive) pairs
Unattended-Upgrade::Allowed-Origins {
    "${distro_id} ${distro_codename}-security";
//    "${distro_id} ${distro_codename}-updates";
//    "${distro_id} ${distro_codename}-proposed";
//    "${distro_id} ${distro_codename}-backports";
};

// List of packages to not update
Unattended-Upgrade::Package-Blacklist {
//    "vim";
//    "libc6";
//    "libc6-dev";
//    "libc6-i686";
};

// This option allows you to control if on a unclean dpkg exit
// unattended-upgrades will automatically run
// dpkg --force-confold --configure -a
// The default is true, to ensure updates keep getting installed
//Unattended-Upgrade::AutoFixInterruptedDpkg "false";

// Split the upgrade into the smallest possible chunks so that
// they can be interrupted with SIGUSR1. This makes the upgrade
// a bit slower but it has the benefit that shutdown while a upgrade
[ Read 50 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is ^V Next Page ^U UnCut Text ^I To Spell
Configuring update types
```

Having configured automatic updates, another configuration file sets options for the frequency of updates, cleaning out temporary files, and so on. Finally, you would use an executable update task for scheduling by the `cron` tool.

```
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *    root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo$ 
47 6    * * ?    root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo$ 
52 6    1 * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo$ 
#
[ Read 17 lines ]

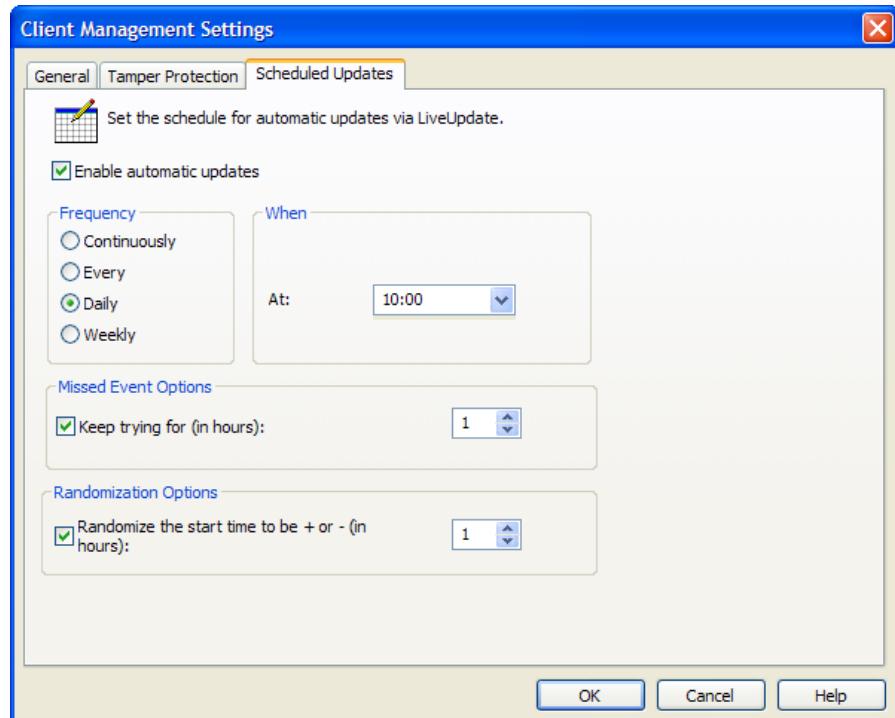
lms-admin@lms:/etc/cron.daily$ ls
apache2  apt      bsdmainutils  logrotate  mlocate  popularity-contest
apport   aptitude  dpkg       man-db     passwd  standard
lms-admin@lms:/etc/cron.daily$
```

The apt script runs as a daily task to install updates as per the configuration files

You could set up a local update server along the lines of WSUS to conserve internet bandwidth.



Application Patch Management



Configuring Symantec LiveUpdate to schedule automatic updates

As with operating system updates, applications should be kept current in terms of fixes and security patches. Most also support an automatic mechanism, as shown above for the Symantec LiveUpdate client updater for anti-virus and intrusion protection definitions.

Firmware Updates

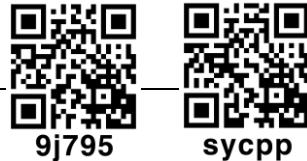
As well as software updates, it is also important to keep hardware up-to-date with the latest patches. There are two main types of updates for hardware devices:

- Driver - this is software that provides an interface between the operating system and the device.
- Firmware - this is software instructions stored on a ROM chip or (more usually) flash memory. This type of chip does not require a power supply so the data does not have to be moved in and out of disk storage.

The firmware on a device such as a router/firewall may be a very sophisticated piece of software. It is quite common for such software to have known vulnerabilities, so it is vital to use a secure version.

Updating firmware is known as "flashing" the chip. This is generally done via a vendor-supplied setup program. It is important to make a backup of the system configuration (especially for a firewall) before performing a firmware update or upgrade.

Endpoint Security



Endpoint security is a set of security procedures and technologies designed to restrict network access at a device level. Endpoint security contrasts with the focus on perimeter security established by topologies such as DMZ and technologies such as firewalls. Endpoint security does not replace these but adds **defense in depth**.

The portability of devices such as removable storage, wireless access points, VoIP phones, cell phones, smartphones, and laptop computers, makes penetrating network perimeter security more straightforward. The security of these devices is often heavily dependent on good user behavior. There is also the circumstance of providing guests with network facilities, such as web access and email. While training and education can mitigate the risks somewhat, new technologies are emerging to control these threats.

Physical Port Security

With wired ports, access to the physical switch ports and switch hardware should be restricted to authorized staff, using a secure server room and/or lockable hardware cabinets. To prevent the attachment of unauthorized client devices, a switch port can be disabled using the management software or the patch cable can be physically removed from the port. Completely disabling ports in this way can introduce a lot of administrative overhead and scope for error. Also, it doesn't provide complete protection as an attacker could unplug a device from an enabled port and connect their own PC. Consequently, more sophisticated methods of ensuring port security have been developed.

MAC Limiting and Filtering

MAC filtering means specifying which MAC addresses are allowed to connect to a particular port. This can be done by specifying a list of valid MAC addresses but this "static" method is difficult to keep up-to-date and relatively error-prone. Some switch models allow you to specify a **limit** to the number of permitted addresses and automatically learn a set number of valid MAC addresses. For example, if port security is enabled with a maximum of two MAC addresses, the switch will record the first two MACs to connect to that port but then drop any traffic from machines with different network adapter IDs that try to connect.

802.1X

The **IEEE 802.1X** standard defines a **Port-based Network Access Control (PNAC)** mechanism. PNAC means that the switch (or router) performs some sort of authentication of the attached device before activating the port.

Under 802.1X, the device requesting access is the **suplicant**. The switch, referred to as the **authenticator**, enables the **Extensible Authentication Protocol over LAN (EAPoL)** protocol only and waits for the device to supply authentication data. Using EAP, this data could be a simple username / password (EAP-MD5) or could involve using a digital certificate or token.

The authenticator passes this data to an **authenticating server**, typically a RADIUS server, which checks the credentials and grants or denies access. If access is granted, the switch will configure the port to use the appropriate VLAN and enable it for ordinary network traffic. Unauthenticated hosts may also be placed in a "guest" VLAN with only limited access to the rest of the network.

Rogue Machine Detection

Rogue machine detection refers to a process of identifying (and removing) machines on the network that are not supposed to be there. You should be aware that "machine" could mean several different types of device (and software):

- Wired clients (PCs, servers, laptops, appliances).
- Wireless clients (PCs, laptops, mobile devices).
- Software (rogue servers and applications, such as malicious DHCP or DNS servers).
- Virtual machines.

There are a number of techniques available to perform rogue machine detection:

- Visual inspection of ports / switches will reveal any obvious unauthorized devices or appliances. It is however possible to imagine a sophisticated attack going to great lengths to prevent observation however, such as creating fake asset tags.
- Network mapping / host discovery - unless an OS is actively trying to remain unobserved (not operating when scans are known to be run for instance), network mapping software should identify hosts. Identifying a rogue host on a large network from a scan may still be difficult.
- Wireless monitoring can reveal the presence of unauthorized or malicious access points and stations.
- Network monitoring can reveal the use of unauthorized protocols on the network or identify hosts producing an unusual volume of network traffic.
- NAC and intrusion detection - security suites and appliances can combine automated network scanning with defense and remediation suites to try to prevent rogue devices accessing the network.



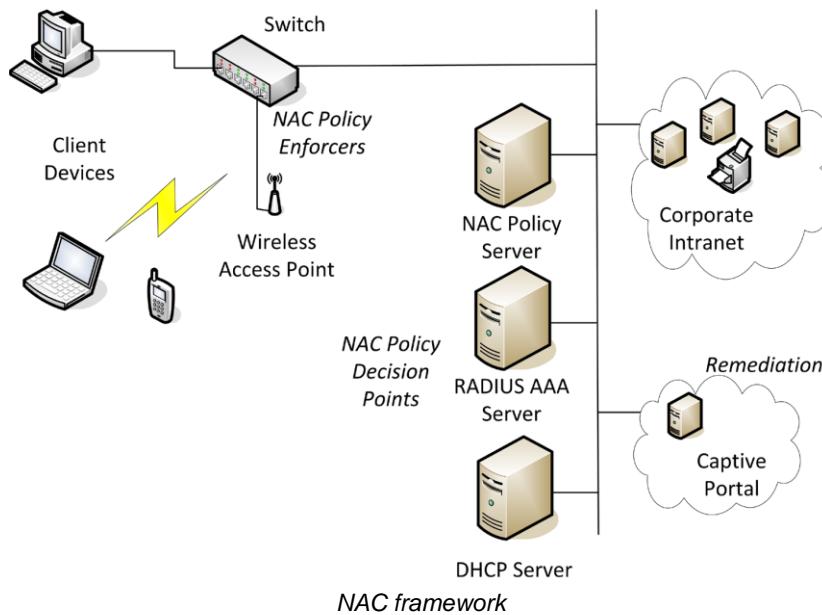
Network Access Control

As well as authenticating users, **Network Access Control (NAC)** allows administrators to devise policies or profiles describing a minimum security configuration that devices must meet to be granted network access. This is called a **health policy**. Typical policies check things such as malware infection, firmware and OS patch level, personal firewall status, and presence of up-to-date virus definitions. A solution may also be able to scan the registry or perform file signature verification. Some of the key features of NAC solutions are:

- Gathering data - information can be collected from a device either by installing an agent or by polling the device.
- Remediation - this refers to what happens if the device does not meet the security profile. A non-compliant device may be refused connection completely or put in a quarantined area (VLAN) or captive portal (a web application), from which there is the option to install the required patches or malware definitions.
- Management - the system for defining policies and reporting and logging.
- Pre- and post-admission control - most NAC solutions work on the basis of pre-admission control (that is, the device must meet the policy to gain access). Post-admission control involves subsequently polling the device to check that it remains compliant. Some solutions only perform post-admission control; some do both.
- Integration - many agent-based solutions are integrated with other client software, such as anti-virus and intrusion detection.

Implementing Network Access Control

The general architecture of a NAC solution would contain the following elements.



Supplicant client devices connect to the network via a NAC Policy Enforcer, such as a switch, router, or wireless access point. Other options for the location of the policy enforcer include a VPN remote access gateway or a specially-configured DHCP server. The policy enforcer checks the client credentials with the NAC Policy Server and performs machine and user authentication with a RADIUS AAA Server. The client is allocated a suitable IP address by a DHCP server and assigned to a VLAN by the switch; depending on whether the policy was met, this would allow access to the network or to a quarantined area or captive web portal only.

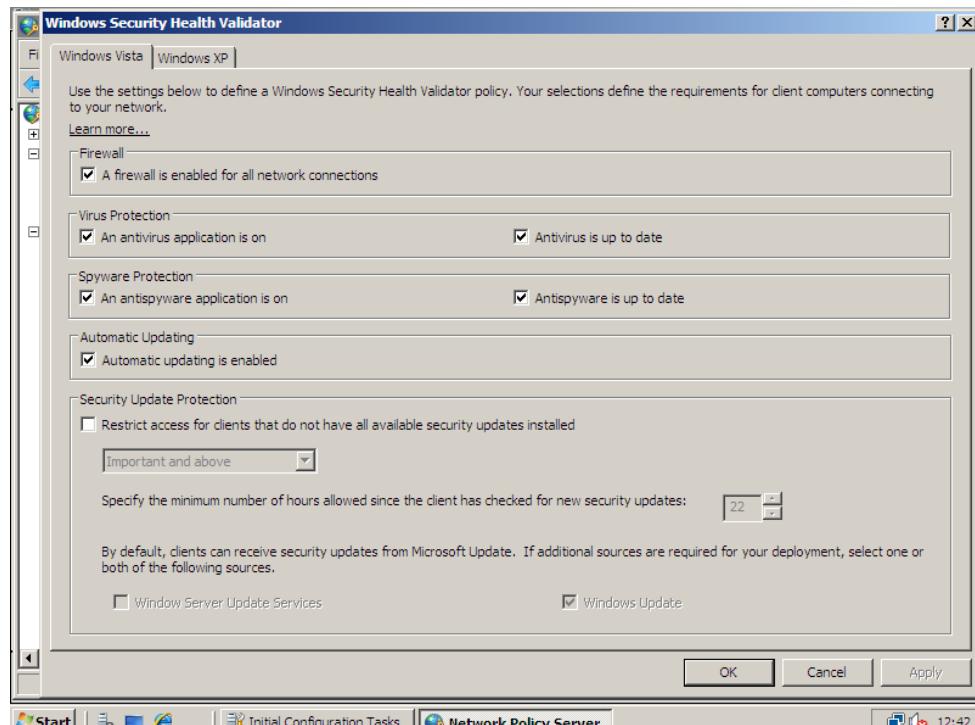


A RADIUS server provides Authentication, Authorization, and Accounting services for simpler connectivity devices, such as switches and access points. RADIUS is discussed in [Unit 3.4](#).

NAC Products and Frameworks

There are three main frameworks for NAC:

- **Cisco Network Admission Control (CNAC)** - device health status is provided by an agent, which can run on Windows and Linux as well as Cisco's IOS router and switch firmware.
- **Network Access Protection** from Microsoft - this is a solution for Windows Server networks.
- **Trusted Network Connect** from Trusted Computing Group - this is a standards-based approach to NAC focusing on use of a Trusted Platform Module chip (see below).



Configuring NAP on Windows Server

There are also numerous NAC software and hardware solutions from vendors such as Symantec, Juniper, ForeScout, McAfee, Sophos, and so on.

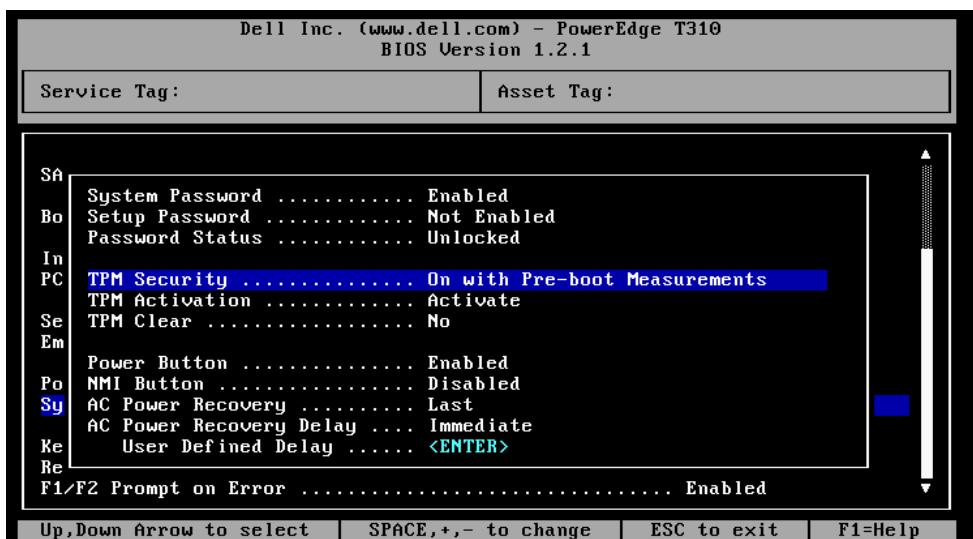
NAC often requires more than one product, as the range of possible devices that can connect to a network means that no one vendor can offer a completely comprehensive solution. NAC policy configuration is an extremely complex task. Poorly configured NAC can cause network support incidents to multiply rapidly.



When rolling out NAC, it is vital to run a test deployment with a limited user base first.

Trusted Platform Module

Trusted Platform Module (TPM) is a specification for hardware-based storage of digital certificates, keys, hashed passwords, and other user and platform identification information. Essentially it functions as an embedded smart card. Each TPM microprocessor is hard-coded with a unique, unchangeable key (the **endorsement key**). During the boot process, the TPM compares hashes of key system state data (BIOS, boot loader, and OS kernel) to ensure they have not been tampered with. A TPM can also store and transmit a NAC health status report securely (attestation).



Configuring a Trusted Platform Module



TPM can also be used for whole disk encryption (see [Unit 4.2](#)).

NAC Security Risks

If implemented as a primarily software-based solution, NAC can suffer from the same sort of exploits as any other software. There have been instances of exploits to evade the NAC admission process or submit false scan results. One fruitful line of attack is to use virtual machines to evade the initial admission policy; one VM is created that complies with the policy and when access is granted the user switches to a second non-compliant VM. This is why post-admission control is an increasingly important requirement for NAC solutions.

These attacks can also be mitigated by using a Trusted Platform Module, though attacks against TPM itself are likely to develop.



Review Questions / Module 4 / Unit 1 / Host Security

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What is a "security-enabled" configuration?
- 2) Why is it essential to create a baseline when setting up a system for the first time?
- 3) What are the management options and security considerations for network clients?
- 4) What first step must you take when configuring automatic updates on a Linux server?
- 5) True or false? Only Microsoft's operating systems and applications require security patches.
- 6) What is meant by "remediation" in the context of NAC?
- 7) What use is made of a Trusted Platform Module for NAC attestation?
- 8) IT administrators in your company have been abusing their privileges to install computer games on company PCs. What technical control could you deploy to prevent this?
- 9) You are managing a huge site with large numbers of network ports spread across many floors. You are considering implementing a Network Access Control system but what interim measures could you take to identify rogue machines?
- 10) Why is a trusted OS necessary to implement file system access control measures?



If you have access to the Hands On Live Labs, complete the "Threats / Mitigation and Deterrent Techniques" and "Compliance / Patching" labs now.

Module 4 / Unit 2

Data Security

Objectives

On completion of this unit, you will be able to:

- Understand the importance of policies and information classification in preventing data loss and theft.
- Understand the use of encryption to secure data.
- Use Data Loss Prevention software to manage secure information.
- Describe backup strategies and technologies.
- Apply policies and controls to dispose of data and hardware securely.



54hh1

Data Handling

Data handling or document management is the process of managing information over its lifecycle (from creation to destruction). At each stage of the lifecycle, security considerations are vital. A **data policy** describes the security controls that will be applied to protect data at each stage of its lifecycle. Data policies and procedures are important in reducing the risk of data loss or theft.



Information management is a massive task in any organization. Most schemes focus on structured data (that is, information that is stored in a directory hierarchy and subject to administrative access control). Managing and classifying unstructured data (emails, chat sessions, telephone calls, and so on) is an even more daunting task, though software solutions designed to tackle the problem are emerging.



jyv1g

Information Classification and Access Control

Most documents go through one or more draft stages before they are published. As a draft, a document will be subject to a **workflow**, which describes how editorial changes are made and approved. The workflow will specify who are the authors, editors, and reviewers of the document.

As part of the creation process, the document must be classified depending on how sensitive it is. Classification restricts who may see the document contents. Classification (or labeling) is generally divided into several levels, following military usage:

- Unclassified (public) - there are no restrictions on viewing the document.
- Classified (private / restricted / internal use only / official use only) - viewing is restricted to the owner organization or to third-parties under a Non-Disclosure Agreement (NDA).
- Confidential (or low) - the information is highly sensitive, for viewing only by approved persons within the organization (and possibly by trusted third-parties under NDA).
- Secret (or medium) - the information is too valuable to permit any risk of its capture. Viewing is severely restricted.
- Top-Secret (or high) - this is the highest level of classification.

Classified, confidential, secret, and top-secret information should be securely protected (encrypted) for storage and transmission.



Data labeling applies both to soft copy (computer data) and hard copy (printed) documents.

Information may change in sensitivity, typically becoming less sensitive over time. A document may be downgraded to a lower security level or eventually declassified. In this circumstance, there needs to be a clear process of authorization and notification, so that confidentiality is not breached.

As discussed earlier, information classification lends itself to the Mandatory Access Control model. However, even where a document is subject to DAC or RBAC, it is still wise to label the document with its sensitivity level, especially when it is transmitted in a form that is not subject to the access control system (such as printed copies).

Publication and Distribution

When a draft has been finalized, the document is published. A published document should always show information such as the author(s), date of publication, version number, and classification.

At this point in the lifecycle, document management needs to specify the following:

- Storage and retrieval - where is the document to be stored and what mechanisms exist for retrieving it?
- Distribution - what restrictions are there on making copies of the document? In what formats may it be distributed and to whom?
- Security - what is the process of notification if the security of the document is compromised? Are the security mechanisms for storage and distribution working?



Data States

Thought needs to be given to all the ways that information could potentially be intercepted. This means thinking beyond the simple concept of a data file stored on a disk. Data can be described as being in one of three states:

- Data at-rest - this state means that the data is in some sort of persistent storage media. In this state, it is usually possible to encrypt the data, using techniques such as whole disk encryption, database encryption, and file- or folder-level encryption. It is also possible to apply permissions (Access Control Lists [ACL]), to ensure only authorized users can read or modify the data. This requires that access to the data is fully mediated through a trusted OS.
- Data in-transit (or data in-motion) - this is the state when data is transmitted over a network. In this state, data can be protected by transport encryption, such as TLS or IPsec.



With data at-rest, there is a greater encryption challenge than with data in-transit as the encryption keys must be kept secure for longer. Transport encryption can use ephemeral (session) keys.

- Data in-use - this is the state when data is present in volatile memory, such as system RAM or CPU registers and cache. In this state, the data will typically be decrypted so a malicious intruder with rootkit access to the computer may be able to access it. New technologies may emerge to encrypt data in-use.



Retention, Storage, and Destruction

When a document reaches the end of its lifecycle (that is, when it is no longer applicable or required for reference), there are two further stages to consider in the management process:

- Retention - this is a period that the document must be kept in an archive following its "active" lifecycle. Most documents are retained for regulatory reasons; others because the historical data is valuable to the organization. With this option, the challenge is to provide secure long-term storage.
- Destruction - some documents may be retained in archives in perpetuity; others may be destroyed to free up storage space or because the cost of keeping them in secure archives exceeds the value of the information. Data protection legislation is also a vital consideration for retention and destruction processing. For example, personal data may only be stored for as long as is necessary.

Destruction is also relevant to controlling the distribution of copies of sensitive information.

Personally Identifiable Information (PII)



The rise in consciousness of **identity theft** as a serious crime and growing threat means that there is an increasing impetus on government, educational, and commercial organizations to take steps to obtain, store, and process PII more sensitively and securely.

Personally Identifiable Information (PII) is data that can be used to identify, contact, or locate an individual (or in the case of identity theft, to impersonate them). A social security number is a good example of PII. Others include names, date of birth, email address, telephone number, street address, biometric data, and so on.

Some types of information *may* be PII depending on the context. For example, when someone browses the web using a static IP address, the IP address is PII. An address that is dynamically assigned by the ISP may not be considered PII. These are the sort of complexities that must be considered when laws are introduced to control the collection and storage of personal data.

Staff should be trained to identify PII and to handle personal or sensitive data appropriately. This means not making unauthorized copies or allowing the data to be seen or captured by any unauthorized persons. Examples of treating sensitive data carelessly include leaving order forms with customers' credit card details on view on a desk or putting a credit card number in an unencrypted notes field in a customer database.



In the European Union (EU), personal data is subject to Data Protection laws, which make data handlers responsible for compliant collection and storage of personal information. The US does not have comparable legislation though it does operate a "safe harbor" scheme for US companies exchanging data with EU ones.



Data Encryption

When data is hosted on a file system, it can be protected by the operating system's security model. Each file or folder can be configured with an Access Control List (ACL), describing the permissions that different users (or user groups) have on the file. Files often have to be stored outside of the OS's file system and there is also the chance that a disk could be physically removed. To protect data at-rest against these risks, the information stored on a disk can be **encrypted**.

File / Folder Encryption

One approach to encrypting data at-rest is to apply encryption to individual files or folders. The **Encrypting File System (EFS)** under NTFS supports file and folder encryption under professional and server versions of Windows.

- Windows 2000 uses the expanded Data Encryption Standard (DESX) algorithm (with 56-bit or 128-bit key strength).
- Windows XP uses DESX or 3DES (with 128-bit key strength).
- Windows XP SP1 or later, Windows Vista / 7 / 8, and Windows Server 2003 / 2008 / 2012 can use DESX or 3DES (with 128-bit key strength) but default to AES (with 256-bit key strength).
- Windows 7/8 and Server 2008 R2 / 2012 also support Elliptic Curve Cryptography (ECC).

Without strong authentication, encrypted data is only as secure as the user account. If the password can be compromised then so can the data.

There are also many third-party encryption products.

Full Disk Encryption

Another option is to use a **Full Disk Encryption (FDE)** product. This is built into the Enterprise version of Windows Vista / 7 / 8 (BitLocker) and is a feature of Mac OS X. It can also be enabled using a third-party product, such as TrueCrypt (now discontinued) or Symantec Drive Encryption.

Disk encryption carries a processing overhead but modern PCs usually have processing capacity to spare. It is particularly useful for mobile devices, such as laptops, and removable drives. The main advantage is that it does not depend on the user to remember to encrypt data so mitigates the risk of data loss in the case of the theft or loss of the device. Disk encryption also encrypts the swap file, print queues, temporary files, and so on.

Hardware-based Encryption Devices

Some disk encryption products, including BitLocker and PGP, can make use of a **Trusted Platform Module (TPM)** chip in the computer to tie use of a hard disk to a particular motherboard. The TPM is used as a secure means of storing the encryption key and to ensure the integrity of the OS used to boot the machine. Alternatively the key could be stored on a USB stick or smart card.

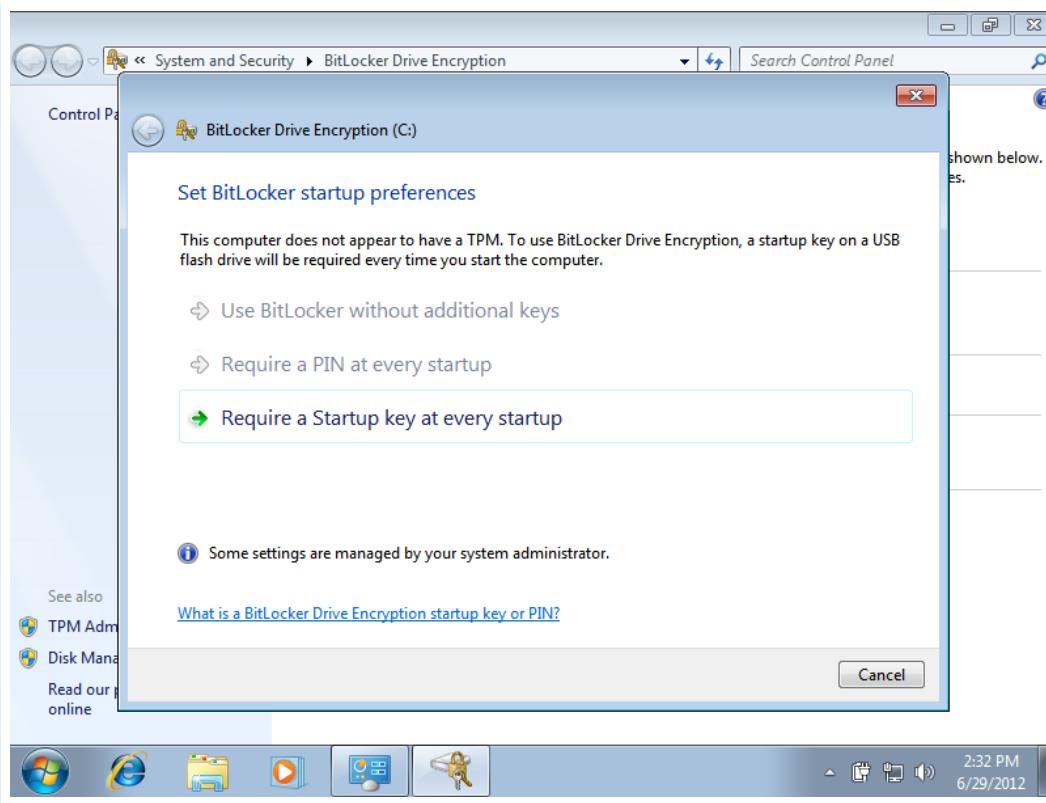


TPM is covered in more detail in [Unit 4.1](#).

Hardware-based FDE products are also being marketed by Seagate and Hitachi. The drives perform encryption at the controller level, removing the load from the CPU. These products depend on the presence of a secure boot password or **Pre-boot Authentication** environment.



Full device encryption is also an option on mobile devices such as smartphones and tablets based on the iOS and Android operating systems. Mobile device security is covered in more detail in [Unit 5.2](#).



Configuring BitLocker in Windows 7 - rather than using a TPM this system is being configured with a startup key; a USB stick that must be present at boot-time

Removable Media Encryption

Most full disk encryption products can also be used to encrypt the contents of USB media. The version of BitLocker provided with Vista cannot encrypt removable drives but the version provided with Windows 7 / 8 / Server 2008 / 2012 can. You can also purchase USB drives that come with pre-loaded encryption software. These drives are usually OS-specific so a Windows drive will not work with OS X for instance. The drive presents itself as a CD/DVD to the OS and is accessed using the encryption tool stored in the drive root, such as TotalLock.exe in the example from Integral below:



Total Lock USB encryption tool from Integral

The user configures personal information and a password. Thereafter, so long as the drive is being used in locked mode, the user must log in with a password to access files on it.

Database Encryption

For most end-user software, encryption at the disk or file level is usually sufficient. Encrypting client/server databases is more complex as the data must usually be accessible from multiple client devices. Encryption can also cause significant performance overheads. Consequently database security tends to focus more on access control than on encryption per se.

A multi-user database would not usually be encrypted using the sort of file or disk encryption products provided with the OS (though these could be used on backup copies of the database or on copies made to removable media). Instead, the **Database Management System (DBMS)** would come with its own encryption technology or you may select a specialist third-party product for use with a particular database technology.

Encryption is generally applied at the column (or field) level. For example, a customer's name and address might be stored in plaintext but their credit card number would be encrypted. This type of encryption is primarily deployed against malicious insider threats (database administrators who would normally be able to access any information in the database). The primary key of a table (the column used to uniquely identify each record) should never be encrypted.



x1pt3

Data Loss Prevention

In a workplace where mobile devices with huge storage capacity proliferate and high bandwidth network links are readily available, attempting to prevent the loss of data by controlling the types of storage device allowed to connect to PCs and networks can be impractical. Another option is to use policies or software to prevent data "leakage" or loss by focusing on the data files.

Users must of course be trained about document confidentiality and make sure that they are aware of the insecurity of unencrypted communications. This should also be backed up by HR and auditing policies that ensure staff are trustworthy. "Soft" measures such as these do not protect against user error or insider threats however.

Data Loss (or Leakage) Prevention (DLP) products, such as Symantec's DLP suite or the open source MyDLP, scan content in structured formats (such as a database with a formal access control model) or unstructured formats, such as email or word processing documents. These products use some sort of dictionary database or algorithm to identify confidential data. The transfer of content to removable media (or by email or IM or even social media) can then be blocked if it does not conform to a predefined policy.

Such solutions will usually consist of the following components:

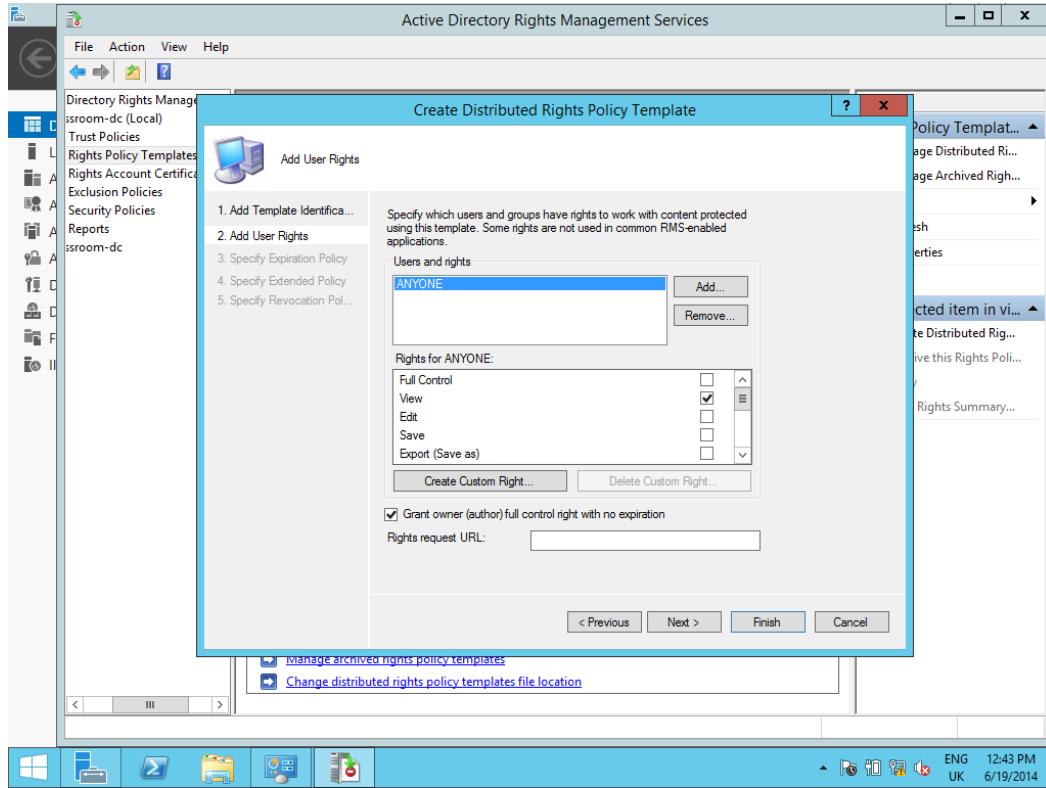
- Policy server - to configure confidentiality rules and policies and secure storage for information plus log incidents and compile reports.
- Endpoint agents - to enforce policy on client computers, even when they are not connected to the network.
- Network agents - to scan communications at network borders and interface with web and messaging servers to enforce policy.

Rights Management Services

As another example, Microsoft introduced an **Information Rights Management (IRM)** feature into their Office productivity suite coupled with Windows' **Rights Management Services (RMS)**. This provides administrators with the following functionality:

- Assign file permissions for different document roles (such as author, editor, or reviewer).
- Restrict printing and forwarding of documents, even when sent as file attachments.
- Restrict printing and forwarding of email messages.

Rights management is also being built into other secure document solutions, such as Adobe Acrobat.



Rights Management Services in Windows Server



Handling Big Data

"Big Data" refers to an unstructured data set. These are increasingly being used as backend databases for high-volume websites and as a means of analyzing huge datasets, such as web and network traffic logs and metadata. In addition to volume, big data is often high velocity. This means that a stream of information is captured continuously. Another characteristic of big data is variety; information from different sources and formats may be pooled together for analysis.

Like any other data, big data is just information stored in files. That said, a big datastore is likely to use a specialized server and file system architecture optimized for streaming and high availability, such as the Hadoop Distributed File System (HDFS) running on a server cluster.

The uses of big data make it more difficult to apply access controls however. It may be straightforward to apply access controls to the whole repository, but it can be more difficult to restrict access to certain types of information within it. The concept of big data analysis does not fit comfortably with the principle of "need to know". In order to find interesting patterns in a data set, the analysis software or its user is likely to be granted access to the whole dataset. Identifying and restricting access to certain bits of information within a high volume, high velocity dataset can be extremely challenging.

In terms of privacy for example, a big data set may go through a depersonalization process to try to remove Personally Identifiable Information (PII) before it is submitted for analysis. It can however be quite easy to continue to identify individuals within a dataset through analysis of metadata. Any queries designed to extract such information might be considered suspicious.

The volume of data may make it difficult to enforce auditing principles, such as recording who has accessed a certain bit of information within a dataset. Analysis software may be able to log the queries that have been performed however. Data Loss Prevention software is also of use, as it can automatically block the transfer of information matching its protection profile.



It is also likely that big data storage and analysis might involve a cloud provider. See [Unit 4.5](#) for more notes on cloud computing security issues.

Backup Plans and Policies

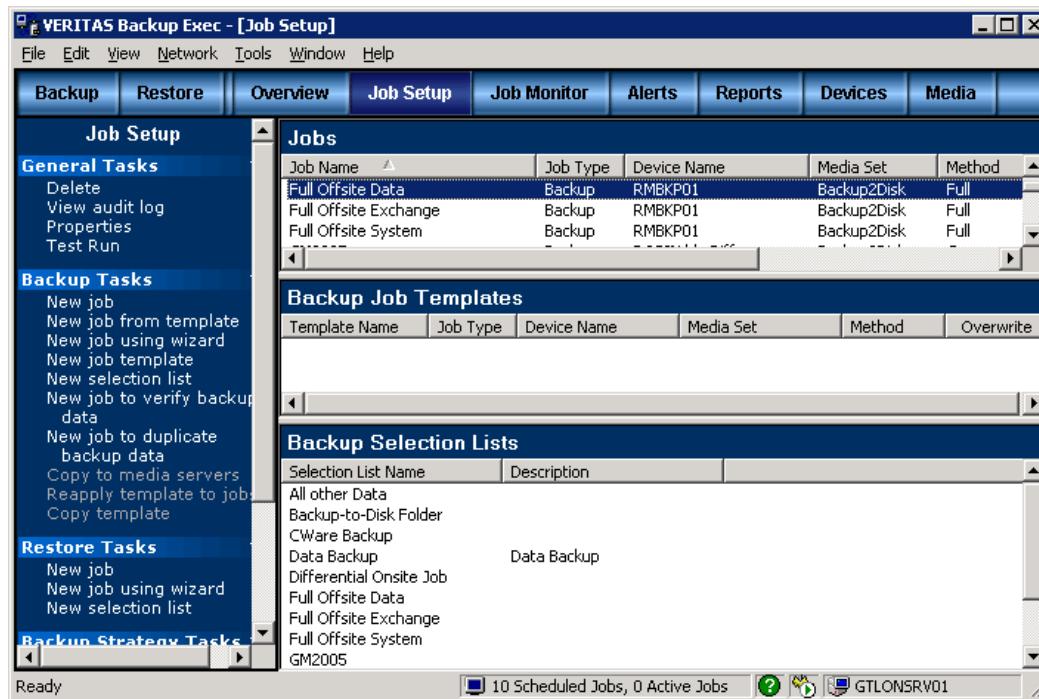
One of the most important operations in a data security is the creation of a secure backup. The execution and frequency of backups must be carefully planned and guided by policies.

Archiving and Backups

You should be aware of a distinction between **archiving** and **backup**:

- A backup is made for security - it is a second (or third or fourth) copy of data made with the intention of being able to restore the original should it be lost or damaged.
- Archive material is data that has passed its immediate usefulness and does not need to be accessed "live" but cannot be deleted. It may need to be retained for historical, regulatory, or legal reasons. Generally this means that it is moved from an immediately available storage area, such as a file server, to tape or optical media. An archive therefore is not a *copy*. It is likely to be important to continue to maintain additional security copies of archive material however, that is, to back up the archive.

Roughly speaking, a backup is a copy operation and archiving is a move operation.

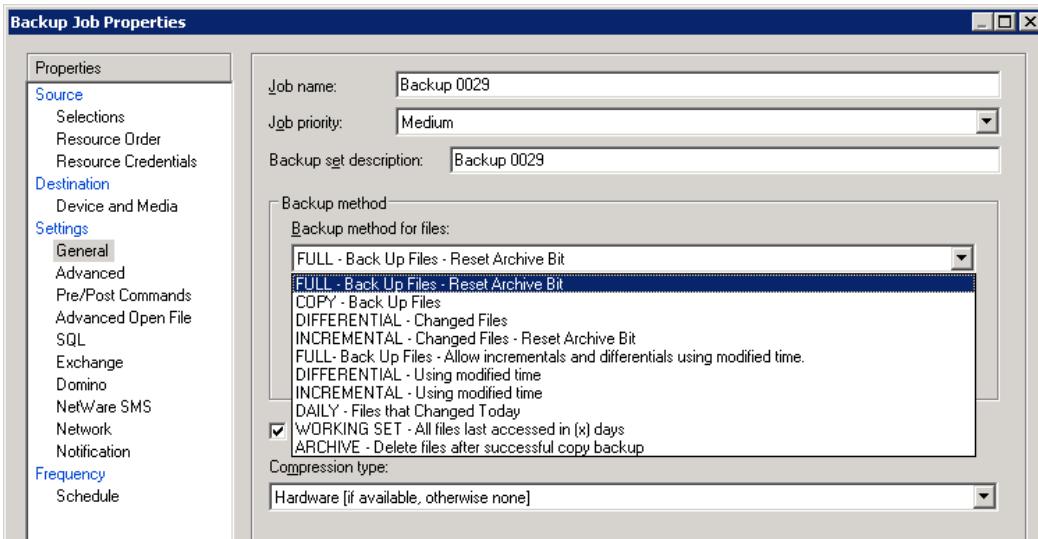


Performing a backup using Veritas BackupExec

Backup Types

When considering a backup made against an original copy of data, the backup can usually be performed using one of three main types:

- Full
- Incremental
- Differential



Choosing the backup type

In Windows, a **full** backup includes all selected files and directories while **incremental** and **differential** backups check the status of the **archive attribute** before including a file. The archive attribute is **set** whenever a file is modified. This allows backup software to determine which files have been changed and therefore need to be copied.



Linux doesn't support a file archive attribute. Instead, a date stamp is used to determine whether the file has changed.

The following table summarizes the three different backup types:

Type	Data Selection	Backup / Restore Time	Archive Attribute
Full	All selected data regardless of when it has previously been backed up	High / low (one tape set)	Cleared
Incremental	New files and files modified since the last backup	Low / high (multiple tape sets)	Cleared
Differential	All data modified since the last full backup	Moderate / moderate (no more than 2 sets)	Not Cleared

The criteria for determining which method to use is based on the time it takes to **restore** versus the time it takes to **back up**. Assuming a backup is performed every working day, an incremental backup only includes files changed during that day, while a differential backup includes all files changed since the last full backup.

Incremental backups save backup time but can be more time-consuming when the system must be restored. The system must be restored from the last full backup set and then from each incremental backup that has subsequently occurred. A differential backup system only involves two tape sets when restore is required.

Doing a full backup on a large network every day takes a long time. A typical strategy for a complex network would be a **full weekly backup** followed by an **incremental** or **differential** backup at the **end of each day**.

- The advantage of using a **full daily backup** is that one tape set is only required to restore the system.
- The advantage of an **incremental backup** is that it takes less time to back up but several tape sets may need to be restored before the system is operational.
- The advantage of a **differential backup** is the balance of time for both restoring and backing up.



Do not combine differential and incremental backups. Use full backups interspersed with differential backups, or full backups interspersed with incremental backups.



*Most software also has the capability to do **copy** backups. These are made outside the tape rotation system (ad hoc) and do not affect the archive attribute.*



Retention Policy

Data retention needs to be considered in the short and long term:

- In the short term, files that change frequently might need retaining for version control. Short term retention is also important in recovering from virus infection. Consider the scenario where a backup is made on Monday, a file is infected with a virus on Tuesday, and when that file is backed up later on Tuesday, the copy made on Monday is overwritten. This means that there is no good means of restoring the uninfected file.

Short term retention is determined by how often the youngest media sets are overwritten.

- In the long term, data may need to be stored to meet legal requirements or to comply with company policies or industry standards. Any data that must be retained in a particular version past the oldest sets should be moved to archive storage.

For these reasons, backups are kept back to certain points in time. As backups take up a lot of space, and there is never limitless storage capacity, this introduces the need for storage management routines and techniques to reduce the amount of data occupying backup storage media while giving adequate coverage of the required **recovery window**. The recovery window is determined by the **Recovery Point Objective (RPO)**, which is determined through business continuity planning.



Business Continuity Planning is covered in [Unit 5.3](#).

A retention policy can either be based on redundancy (the number of copies of each file that should be retained) or on a recovery window (the number of days into the past that should be retained). Advanced backup software can prevent media sets from being overwritten in line with the specified retention policy.

Database Backups

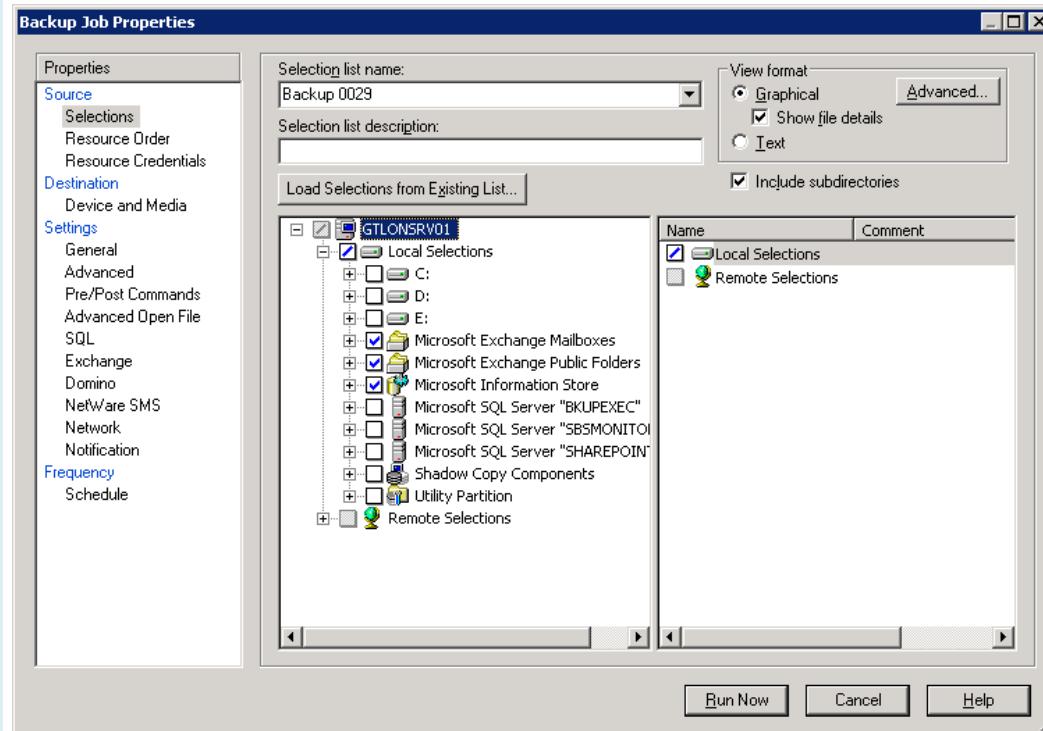
If the data that you're considering backing up is part of a database, such as SQL data or a messaging system, such as Exchange, then the data is probably being used all the time. Often copy-based mechanisms will be unable to backup open files. Short of closing the files, and so the database, a copy-based system will not work. To get round this, most databases support two useful features: replication and online backups.

Most modern RDBMS (Relational Database Management Systems) support **transactional** updates, and in most situations, the transactions can be posted to multiple replicas of the database, providing redundancy.

This doesn't protect you from accidentally deleting a record, however, because it is a valid transaction which will be propagated amongst all the replicas at the next scheduled replication interval. Therefore you should also provide **online** backups of database systems.

The problem with backing up at the database level is that to restore a record (or in Exchange terms, a message or perhaps a mailbox) is tricky. In fact, you generally have to restore the entire database. For example, the recovery scenario for Exchange typically involves a non-production server being used to restore the data and then the required messages/mailboxes being copied into the production system.

Some backup software allows for the backup of a database in a more targeted way. Staying with our Exchange scenario, both the third-party systems mentioned above support backup and restore at different *granular* levels - server, database, mailbox, or message.



Online backups with Exchange Server

The disadvantage with backing up at the mailbox level is that it is more time consuming. However, in the event of a problem, the system is more readily recoverable to the desired state.

Snapshots

Snapshots are another means of getting round the problem of open files. A snapshot is a point-in-time copy of data. A backup program can use the snapshot rather than the live data to perform the backup.

In Windows, snapshots are provided for on NTFS volumes by the **Volume Shadow Copy Service (VSS)**. They are also supported on Sun's ZFS file system, and under some enterprise distributions of Linux. Virtual system managers can also usually take snapshot copies of VMs.

System Backups

A system backup makes a copy of the OS and installed applications so that a server can be recovered without having to manually reinstall software and reconfigure settings.

Older methods of system backup could involve lengthy recovery procedures. Typically the operating system would have to be reinstalled then the backup applied to the new OS to recover the old configuration.

A **bare metal** backup is one that can be applied directly to a partitioned drive without the separate step of reinstalling the OS. Bare metal backups typically work by making an **image**. The backup software provides a recovery boot disk which enables the system to connect to the recovery media (an external hard drive or network drive for instance).

The only drawback of this method is that system images typically require multi-gigabyte storage media.

A system image can also be quite time-consuming to create, so this method works best if the system configuration is kept fairly static and user data is stored separately from the OS volume.

Virtual machines can be backed up and restored in the same way (in fact, most VMs are deployed using images in the first place).

Backout Contingency Plan

Another reason for making a backup is to support a **backout contingency plan**. Backout plans are most closely associated with rolling back OS updates (in the event that they cause some sort of problem with legacy hardware or software). A backout plan should be formulated for any sort of software or hardware upgrade though.

A backout plan allows the system to be restored to the state it was in prior to applying the patch or upgrade. As a *scheduled* backup may not be able to reverse *only the specific change* made during the upgrade, it may be necessary to perform a *specific* backup before performing the upgrade.

Backup Execution and Frequency

A backup is executed by selecting the files and folders for backup and setting the schedule (frequency) and the backup media.

There is no "best" media type for backups and archiving. Different media have different characteristics that make them more or less suitable for different storage tasks. Technologies and costs also change over time. The nature of storage means there is as much "looking back" to support older technologies as there is looking forward to opportunities that new or cheaper technologies may bring.

Hard Disk and SANs

"Disk-to-disk" backup now predominates much of the storage and backup market. Hard disks support very large and (with RAID) easily extensible capacity at quite low cost. The disks do not need to be high performance so cheap 5K rpm units can be specified. Even low-speed drives are far faster than tape solutions. A set of portable hard disks could be used to backup most small business servers and allow for onsite and offsite storage.

A NAS (Network Attached Storage) device or SAN (Storage Area Network) could be used as a backup or archive solution for larger networks. The main drawback of a networked-disk solution is that there is no offsite storage (unless the backup takes place over a WAN). Consequently, many enterprise storage architectures use a tiered solution:

- "Online" storage is provided by a high-performance server RAID array (15K SAS drives or SSDs for instance).
- "Nearline" storage and security backup is provided by a SAN, probably using cheaper and slower RAID components (5K SATA drives for instance).
- "Offline" and offsite storage and archiving is provided by tape or optical media.

Data is transitioned through the storage system (disk-to-disk-to-tape) according to data retention policies.

Tape

Magnetic tape drives provide a low cost per byte method of creating security backups and archiving data. They may be internal or external units, supplied with SATA, SAS, USB, or Firewire interfaces (or ATA/EIDE or SCSI in the case of legacy drives).

A **tape library** is a high-end backup solution in which an **AutoLoader** is pre-loaded with tapes, which it then auto-changes, allowing for fully-unattended backups. This minimizes the chance of human error (forgetting to change the tape or inserting the wrong tape for instance). It also allows for much larger capacities. Unless a backup operator is on-hand to change the tape, the capacity of a stand-alone system is limited to the capacity of a single tape.

The other advantage is that a greater number of restore points are available online (that is, a technician does not have to locate and load the cartridge on which the required data are stored).



HP StorageWorks tape library

Media (Tape) Rotation

Once a suitable backup method and media type has been determined, a **tape rotation** method must be established to minimize the number of tapes required for maintaining an adequate history of the backup jobs.



"Tape" could really be any media set - you could rotate a set of portable hard drives for instance.

A commonly used tape rotation method is known as **Grandfather-Father-Son**. This method uses **three sets** of media in which **monthly**, **weekly**, and **daily** tapes correspond to the generations. Before starting the system, a **full backup** of all media should be made. The system then proceeds as follows:

- 1) Daily backups, which may be incremental **or** differential, use the **son** tapes. These are **reused** each week and remain the youngest in the rotation.
- 2) Weekly full backups are written to the **father** tapes. A father tape set is required for each week of the month except the last.
- 3) The **final weekly** backup is written to the monthly grandfather tape set.

Assuming a network is operational five days per week, the following tape sets are required:

Type	Frequency	Number of Sets
Son	Daily	4 sets
Father	Weekly	4 sets (plus one to be held off site)
Grandfather	Monthly	12 sets



In any sort of tape rotation scheme, labeling the tapes and using the correct tape at the correct time is critical.

Storage Issues

Backed up and archived data needs to be stored as securely as "live" data. It is likely to have the same confidentiality considerations.

One critical problem is planning for events that might compromise both the live data *and* the backup set. Natural disasters such as fire, earthquake, flood plus theft could leave an organization without a data backup, unless they have kept a copy **offsite**. Offsite storage is obviously difficult to keep up-to-date.



There is a discussion of some of the issues impacting site-to-site data replication in [Unit 5.4](#).

Without a network that can support the required bandwidth, the offsite media must be physically brought onsite (and if there is no second set of offsite media, data is at substantial risk at this time), the latest backup performed, and then removed to offsite storage again. Quite apart from the difficulty and expense of doing this, there are data confidentiality and security issues in transporting the data.



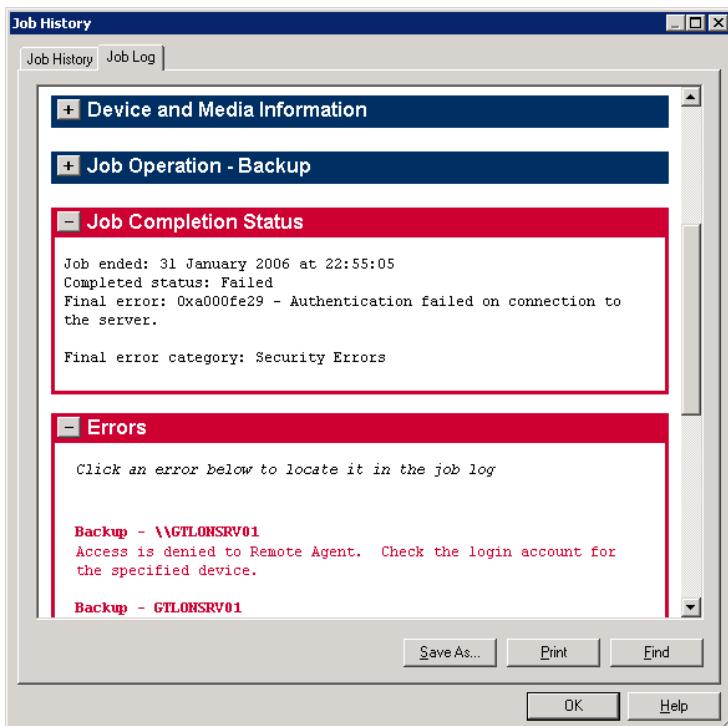
As internet bandwidth improves, remote offline backup becomes less dependent on leased lines. There are more and more "cloud"-based remote backup solutions, principally targeted at small and medium size enterprises.

Backup media is typically physically secured against theft or snooping by keeping it in a restricted part of the building, with other server and network equipment. Many backup solutions also use encryption to ensure data confidentiality should the media be stolen.

Restoring Data and Verifying Backups

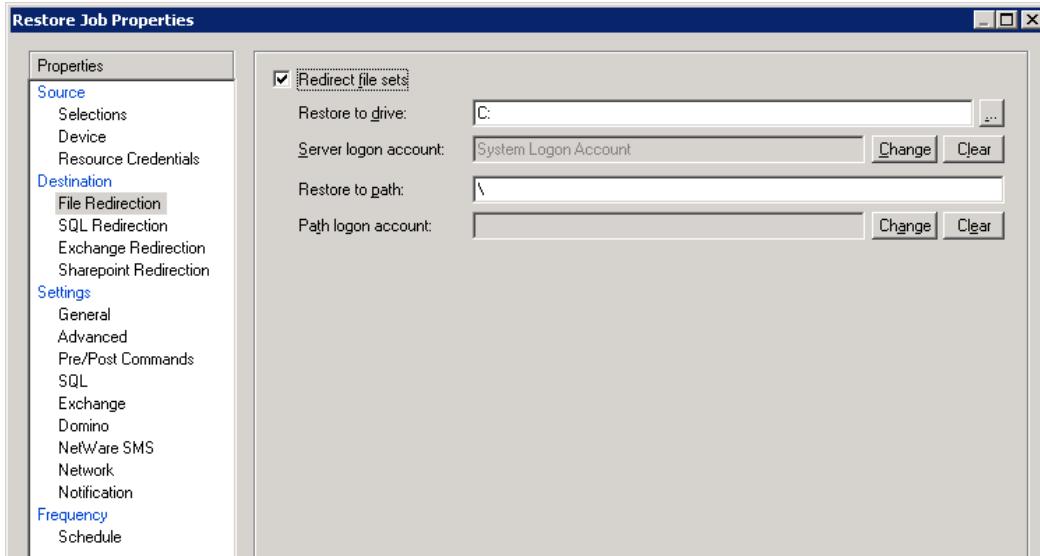
It is *critical* to test that backup operations work properly. There can no worse feeling in IT support than turning to the backup media you have been happily writing to and rotating for the last 8 months only to discover that a critical data folder has never been included in the job!

- **Compatibility** - a tape backup is useless without a drive capable of reading the media. Most drives can read from tape formats from the previous generation (or more). If a legacy drive fails and there is no replacement available, there is a very real risk to the security of the organization's data.
- **Error detection** - problems with the tape or configuration can cause backup jobs to fail. Depending on the error, the whole job may be cancelled or some data may not get backed up. Backup software usually has the facility to verify a backup (obviously this makes the backup operation longer though), report errors to a log, and send alerts by email.



Viewing failed backup job log under Veritas BackupExec

- **Configuration** - when setting up a new job (and periodically thereafter), it is wise to check the media catalog to ensure that all the expected data has been backed up.
- **Test restore** - another option is to test that a restore operation can be performed successfully. This is important when using new backup software, to test old tapes, to check a new job, and to carry out random spot checks. When you do a test restore, you **redirect** the data to a different folder, to avoid overwriting live data.



Redirecting file output for a restore operation

Data Wiping and Disposal



c9t88

A wiping / disposing policy refers to the procedures that the organization has in place for disposing of obsolete information and equipment.

Disposing of Paper Records

One of the less salubrious social engineering techniques is "dumpster diving", referring to combing through an organization's waste to discover documents containing useful information.



Shred documents before disposal

Generally speaking, all paper documents should be shredded before disposal. This is because even quite innocuous information (such as employee telephone lists, diary appointments, and so on) can help an attacker with impersonation attacks.

Confidential or secret documents should be marked as such. Such documents may be treated to special disposal methods, such as finer cross-shredding or even incineration. There are a number of types of shredder. They can be classified to a certain security level, based on the size of the remnants they reduce a sheet to. Level 1 is 12mm strips while Level 6 is 0.8x4mm particles.

Hard Drive Sanitation

Hard drive sanitation refers to fully erasing hard disks. More generally, **remnant removal** refers to decommissioning various media, including flash drives, tape media, CD and DVD ROMs, and so on. The problem has become particularly prominent as organizations recycle their old PCs, either by donating them to charities or by sending them to a recycling company, who may recover and sell on parts. The problem also applies to network printers, which often have installable hard disks to use to cache print jobs.

There are at least three reasons that make remnant removal critical:

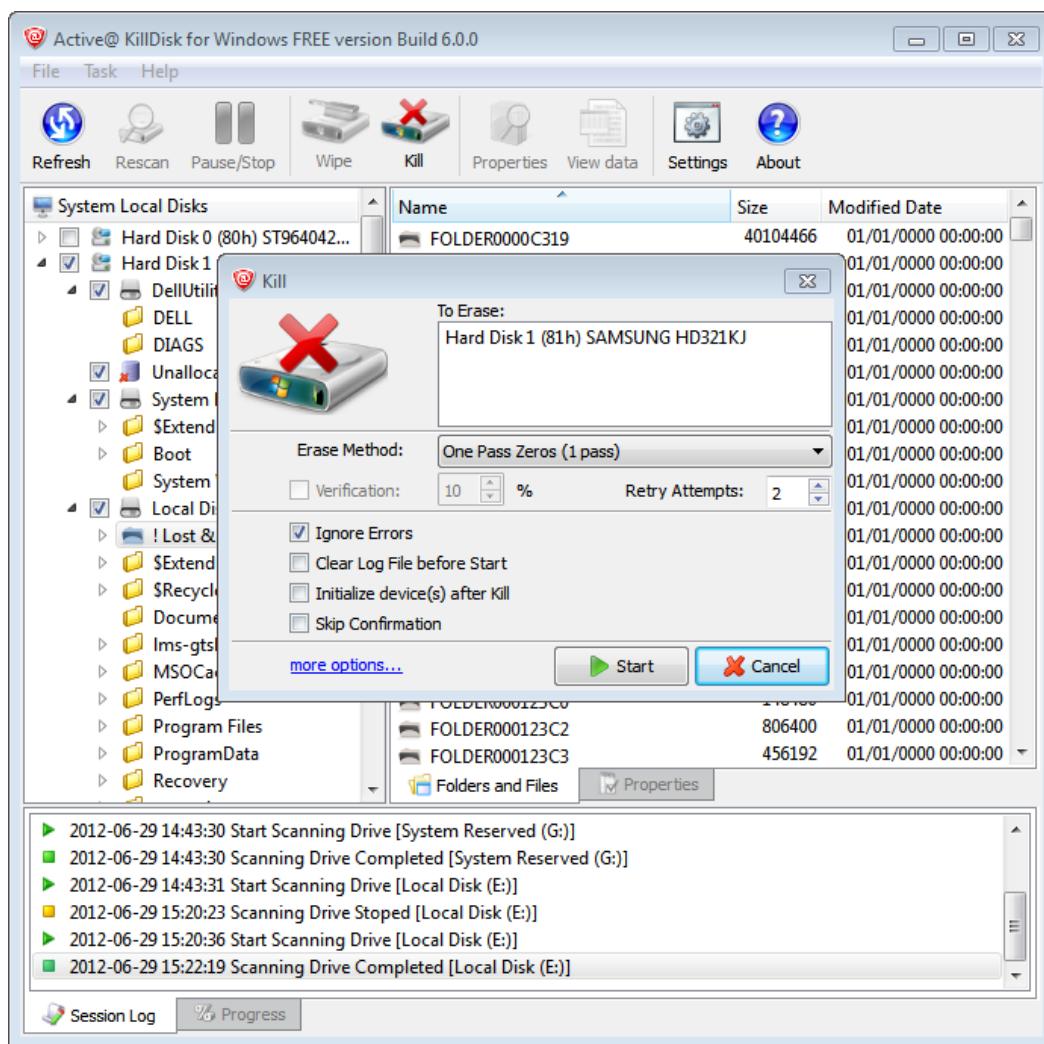
- An organization's own confidential data could be compromised.
- Third-party data that the organization processes could be compromised, leaving it liable under Data Protection legislation (in addition to any contracts or Service Level Agreements signed).
- Software licensing could be compromised.

The main issue is understanding the degree to which data on different media types may be recoverable. Data "deleted" from a magnetic-type disk (such as a hard disk) is not erased. Rather, the sectors are marked as available for writing and the data they contain will only be removed as new files are added.

Similarly, using the standard Windows format tool will only remove references to files and mark all sectors as useable. In the right circumstances and with the proper tools, any deleted information from a drive could be recoverable.

There are several approaches to the problem of data remnants on magnetic disks:

- Overwriting / disk wiping - disk wiping software ensures that old data is destroyed by writing to each location on the media, either using zeroes or in a random pattern. This is suitable for all but the most confidential data, but is time consuming and requires special software.
- Low Level Format - most disk vendors supply tools to reset a disk to its factory condition. These are often described as low level format tools and will have the same sort of effect as disk wiping software. Technically speaking a low level format creates cylinders and sectors on the disk. This can generally only be done at the factory. The disk utilities just clean data from each sector; they don't re-create the sector layout.



Active KillDisk data wiping software

- Destruction - a magnetic disk can be mechanically shredded or degaussed (exposing the disk to a powerful electromagnet disrupts the magnetic pattern that stores the data on the disk surface) in specialist machinery. Obviously, this sort of machinery is costly and will usually render the disk unusable, so it cannot be reused.

A less expensive method is to destroy the disk with a drill or hammer - do be sure to wear protective goggles. This method is not appropriate for the most highly confidential data as it will leave fragments that could be analyzed using specialist tools.

- Disk encryption - as discussed above, this method encrypts *all* the information in a volume, so that any remnants could not be read without possession of the encryption key.

Optical media cannot be reformatted. Discs should be destroyed before discarding them. Shredders are available for destroying CD and DVD media.



Review Questions / Module 4 / Unit 2 / Data Security

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What are the main management issues for a confidential document that has been published?
- 2) What are satisfactory ways of protecting confidential data stored on a hard disk for disposal of the disk?
- 3) What technology protects data in the event of the loss or theft of a computer or mobile device?
- 4) What sort of software prevents unauthorized copying of data onto removable media?
- 5) What term is used to describe data stored on the flash drive memory of a smartphone?
- 6) What range of information classifications could you implement in a data labeling project?
- 7) What is meant by PII?
- 8) What use is a TPM when implementing full disk encryption?
- 9) Why is the "velocity" of a big data dataset a problem for data handling procedures?
- 10) Why might an organization implement backups using incremental sets along with full sets rather than just full sets?



If you have access to the Hands On Live Labs, complete the "Application Data / Data Encryption" and "Compliance / Backup Execution and Frequency" labs now.

Module 4 / Unit 3

Web Services Security

Objectives

On completion of this unit, you will be able to:

- Describe how SSL/TLS is used to secure HTTP communications.
- Harden web servers.
- Identify vulnerabilities in FTP and peer-to-peer file sharing software.

HyperText Transport Protocol

The foundation of web technology is the **HyperText Transfer Protocol (HTTP)**. HTTP enables clients (typically web browsers) to request resources from an HTTP server. A client connects to the HTTP server using an appropriate TCP port (the default is port 80) and submits a request for a resource, using a **Uniform Resource Identifier (URI)**. The server acknowledges the request and returns the data.



URI is the preferred term. The use of URL (Uniform Resource Locator) is deprecated in standards documentation though still widely used by the public.

HTTP is usually used to serve HTML web pages, which are plain text files with coded tags (HyperText Markup Language) describing how the page should be formatted. A web browser can interpret the tags and display the text and other resources associated with the page, such as binary picture or sound files linked to the HTML page.

As with other early TCP/IP application protocols, HTTP communications are not secured.

HTTP also features a forms mechanism (POST) whereby a user can submit data from the client to the server. HTTP is a **stateless protocol**; this means that the server preserves no information about the client during a session. However, the basic functionality of HTTP servers is also often extended by support for scripting and programmable features (web applications). Technologies such as Java, ASP, and integration with databases increase flexibility and interactivity but also significantly increase security risks.

The popularity of the web has made it and related technologies (such as browsers and plug-ins) a popular target for different attacks.



SSL / TLS

Secure Sockets Layer (SSL) was developed by Netscape and released as version 3.0 in 1996 to address the problems with the security of HTTP. SSL proved very popular with the industry and is still in widespread use. **Transport Layer Security (TLS)** was developed from SSL and ratified as a standard by IETF.

SSL/TLS works as a layer between the application and transport layers of the TCP/IP stack (in OSI terms, at the session layer). It can be used to encrypt TCP connections (but not UDP). It is typically used with the HTTP application (referred to as HTTPS or HTTP Over SSL or HTTP Secure) but can also be used to secure other TCP application protocols, such as Telnet, FTP, NNTP, SMTP, or LDAP.

Essentially, a server is assigned a **digital certificate** by some trusted **Certificate Authority**. The certificate proves the identity of the server (assuming that the client trusts the Certificate Authority). The server uses the digital certificate and the SSL/TLS protocol to encrypt communications between it and the client. This means that the communications cannot be read or changed by a third party.



HTTPS operates over port 443 by default. HTTPS operation is indicated by using https:// for the URI and by a padlock icon shown in the browser.



SSL padlock icon

It is also possible to install a certificate on the client so that the server can trust the client. This is not often used on the web but is a feature of VPNs and enterprise networks.

SSL/TLS Operation

The initial connection is governed by the **SSL/TLS Handshake** sub-protocol:

- 1) The client makes a connection request (CLIENT_HELLO) listing the highest protocol version, cipher suites, and compression algorithm(s) supported. The client also sends the date and time plus a random number (ClientRandom), which is used to generate the secret key. The client may also specify a session ID, allowing resumption of an existing session without re-generating keys (which is processor intensive).



In this context, SSL 3.1 is used to mean TLS. Most implementations do not actually support any compression technologies.

- 2) The server responds with SERVER_HELLO, selecting the highest protocol version and strongest cipher suite supported by both and its own randomly generated number (ServerRandom), along with any session information.
- 3) If client and server support compatible versions and ciphers, the server sends its X.509 certificate to the client (CERTIFICATE command) followed by the SERVER_DONE command.



A server can optionally request a certificate from the client, providing mutual authentication. More commonly, the client is untrusted.

- 4) The client checks the server's certificate and if verified responds with CERTIFICATE_VERIFY. It then performs key exchange to create the secret session key for use with the confidentiality cipher (such as AES). This process can be completed using either RSA or Diffie-Hellman. If using RSA, the client generates a pre-master secret, encrypts it using the server's public key, and sends it to the server.
- 5) The server and client then follow the same steps to derive a shared master secret from the pre-master secret plus the ClientRandom and ServerRandom values.
- 6) Client and server then exchange the CHANGE_CIPHER_SPEC command, to indicate that subsequent communications will be encrypted, and the FINISHED command, which contains a digest of the command exchange that is used to verify that the handshake process has not been tampered with.
- 7) Once the session is established, client and server exchange encrypted data in SSL/TLS records, which are placed into transport layer packets for delivery.



The Alert sub-protocol defines error messages (such as "CERTIFICATE_EXPIRED").

Perfect Forward Secrecy



8zm4t

A transport encryption protocol such as SSL/TLS makes use of a different key for each session or each transaction. This type of key is often referred to as an **ephemeral key**. The key is used once then destroyed. This improves security because even if an attacker can obtain the key for one transaction, the other transactions will remain confidential. This massively increases the amount of "cracking" that an attacker would have to perform to recover an entire "conversation".

In standard SSL/TLS (using RSA key exchange), each session key is signed by the server's private key. The RSA key pair is used for *both* authentication and key exchange. This raises the possibility that if a session has been captured by a packet sniffer and at some point later the server's private key is compromised, the session could be decrypted.

This risk is mitigated by **Perfect Forward Secrecy (PFS)**. PFS uses Diffie-Hellman key agreement to create session keys without using the server's private key. PFS can be implemented using either the Diffie-Hellman Ephemeral mode (DHE or EDH) or Elliptic Curve Diffie-Hellman Ephemeral mode (ECDHE) cipher. Because the D-H key is truly ephemeral, even if the encrypted session is recorded there will be no way of recovering a key to use to decrypt it at a later date.



Refer back to [Unit 2.1](#) for more information about session keys and key exchange.

However, to use PFS the server and client must negotiate use of a mutually supported cipher suite. A browser will usually try to select a PFS-compatible suite but may not support one supported by the server. Also, the server is able to "dictate" use of a preferred cipher suite and may not be set to prefer a PFS one. Use of Diffie-Hellman key exchange is likely to reduce server performance though as use of PFS becomes more prevalent, faster implementations of the cipher suites are likely to be developed.



In 2014, a "Heartbleed" bug was discovered in the way some versions of OpenSSL works that allows remote users to grab 64K chunks of server memory contents. This could include the private key, meaning that any communications with the server could be compromised. The bug had been present for around 2 years. This illustrates the value of PFS but ironically many servers would have been updated to the buggy version of OpenSSL to enable support for PFS.

Supported Ciphers

SSL/TLS supports most of the major symmetric and asymmetric ciphers.

- Asymmetric ciphers (key exchange and authentication) - RSA, DSA/DSS, and Diffie-Hellmann.
- Symmetric ciphers (confidentiality) - RC4, RC2, DES, 3DES, IDEA, AES.
- Hashed Message Authentication Code (HMAC) function - MD5 or SHA.



Some of the ciphers (RC4, DES/3DES, and MD5 for instance) would no longer be supported by production servers as they are no longer considered secure enough.

Along with the cipher, client and server also need to negotiate the key strength. Up until 1999 the US government prevented the export of keys over 56-bit. Following the relaxation of this restriction, most sites will use 128-bit or better keys.

A cipher suite is written in the following form:

ECDHE-RSA-AES128-GCM-SHA256

This means that the server can use Elliptic Curve Diffie-Hellman Ephemeral mode (and supports PFS) for session key exchange, RSA for authentication, 128-bit AES-GCM for block symmetric encryption confidentiality (Galois/Counter Mode [GCM] is a high-performing variant of AES), and 256-bit SHA for HMAC functions. Suites the server prefers are listed earlier in its supported cipher list; the cipher above is currently the preferred option for OpenSSL.



Note that 128-bit AES is preferred over 256-bit AES. This is because the better security of AES256 is not perceived to be worth the performance trade-off. On a server where security is the overriding concern, the stronger version would be preferred.

SSL / TLS Versions

TLS is now the version in active development but SSL 3.0 is still very widely supported; SSL 2.0 contains known weaknesses and should not be used. SSL 1.0 was never used commercially.

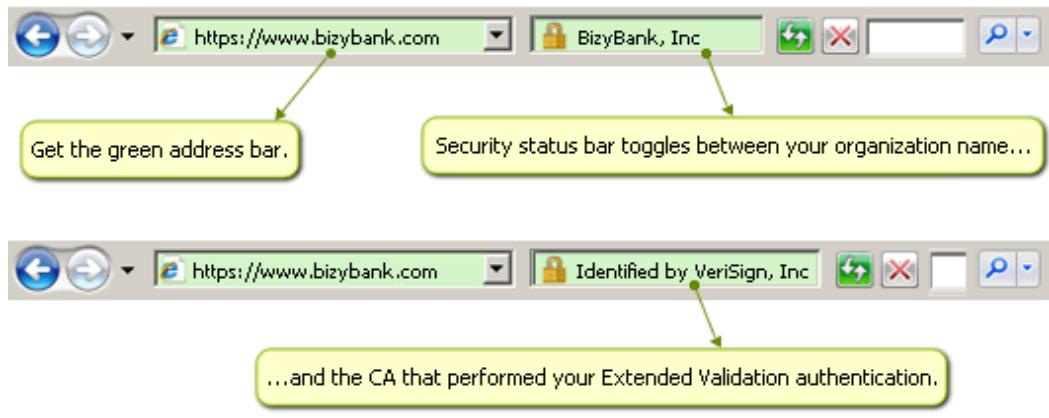
TLS 1.0 is also widely supported now but versions 1.1 and 1.2 are not so well adopted. The most notable changes between TLS 1.0, 1.1, and 1.2 are improvements to the cipher suite negotiation process (the means by which server and client agree to use the strongest ciphers available to both) and protection against known attacks. TLS 1.2 also adds support for the strong SHA-256 cipher.

SSL and TLS versions are not interoperable; that is, a client supporting only SSL 3.0 could not connect to a server supporting only TLS 1.0. A server *can* provide support for legacy clients, but obviously this is less secure. For example, a TLS 1.2 server could be configured to allow clients to downgrade to TLS 1.1 or 1.0 or even SSL 3.0 if they do not support TLS 1.2.

High Assurance SSL

One of the problems with SSL is that anyone can set up a PKI infrastructure. It is also simple to register convincing sounding domain names (such as **my-bank-server.com** where the "real" domain is **mybank.com**). If users choose to trust a certificate in the naïve belief that simply having a certificate makes a site trustworthy, they could expose themselves to fraud. There have also been cases of disreputable sites obtaining certificates from third-party CAs that are automatically trusted by Internet Explorer that apparently validate their identity as financial institutions.

To counter this, VeriSign (the major provider of third-party certificates) and Microsoft introduced Extended Validation Certificates (or High Assurance SSL). EV standards are now maintained by the CA / Browser forum (cabforum.org). EV certificates have been tagged as having undergone vigorous (or even more vigorous than usual; depending on your point-of-view) identity checking and assurance. Such certificates are recognized in the browser by a green highlight in the Address bar and by showing the "friendly" name of the organization associated with the URI plus the CA that performed the extended validation.



Web Servers

Most organizations have an online presence, represented by a website. In order to run a website, it must be hosted on an HTTP server connected to the internet. Typically, an organization will lease a server or space on a server from an ISP. Larger organizations or SMEs with good technical skills may host websites themselves.

When using an ISP, the degree to which the server may be customized, responsibility for security, and amount of technical support will all vary according to the contract terms. Greater flexibility may mean greater responsibility for securing the server.



As with any third-party service, analyze the Service Level Agreement (SLA) to confirm what the ISP is contracted to do and satisfy yourself that these obligations are being met (for example, demand reports of backup operations, security patch management, effective account management, and so on).

Running your own website gives complete control over the configuration of the server but also complete responsibility for its security (and the security of the private network behind it).

The main web server platforms are:

- **Apache** - open source software and powerful, robust features combine to make this server the most popular. It is available for UNIX, Linux, Mac OS X, and Windows but is most widely deployed on Linux. Apache accounts for about 50% of the most active websites.
- **Microsoft Internet Information Server (IIS)** - bundled with Windows Servers (and client versions of Windows). IIS accounts for about 12% of busy sites.
- **nginx** - an open source web server and load balancer specially designed to cope with very high traffic. nginx ("Engine X") accounts for about 17% of the active sites.

Web Server Hardening

As with any application, a web server must be kept up-to-date with service patches and fixes.



Apply patches to the server before connecting it to the internet!

Access Control

Most web servers have to allow access to guests (that is, unauthenticated users). The guest account must be secured so that it cannot be used to modify any data on the server (that it has read-only or browse permissions only). The guest account on IIS is called IUSR_ServerName; an account named httpd or apache is typically configured for guest access to Apache. The guest account should have no permissions outside the directory set up for browsing.



Guests may require execute permissions on scripts and applications that you want them to be able to run and these may be stored in a directory outside the root of the website.

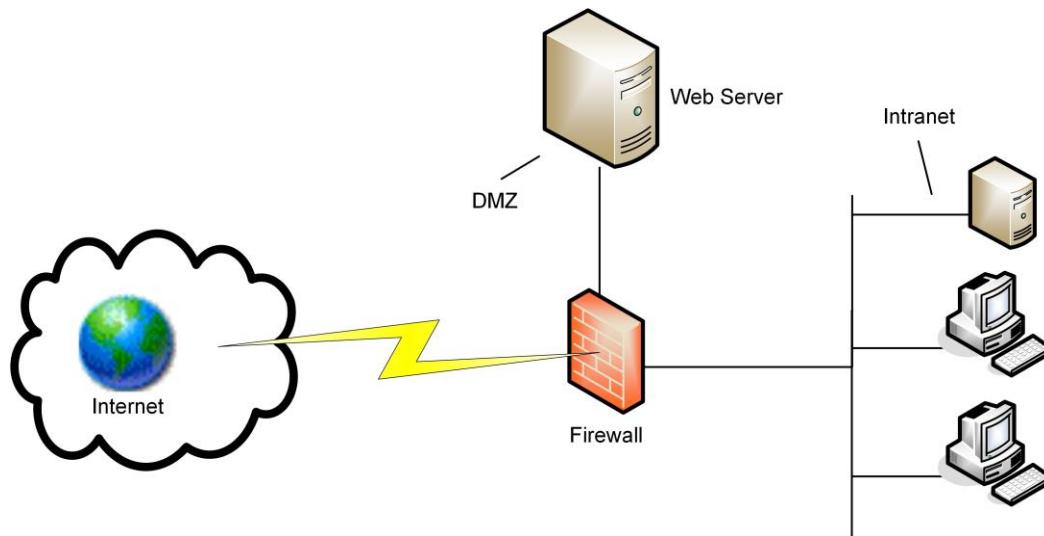
Similarly, passwords to administrative accounts must be strong, securely stored, and changed periodically. Do not re-use passwords used for private network administrative accounts on a publicly accessible machine.

Where confidential information needs to be exchanged, the web server should be configured to use a secure method, such as HTTPS.

Where a web server is leased, a secure means of uploading files and configuration changes needs to be used (SSH for example). Remember that ordinary FTP connections are *not* secure (critically, authentication information is transmitted in plaintext).

Where a web server is connected to a private network, the location of the server should be carefully considered so as not to expose the private network to attack from the public one through the web server. This is typically achieved by placing a firewall between the web server and the local network, creating a **Demilitarized Zone (DMZ)**.

Additionally, it is wise to configure a firewall between the web server and the internet. This can be used to reduce the impact of DoS attacks on the server.



You should also check that users do not install unauthorized web servers on their PCs (a **rogue server**). For example, a version of IIS is shipped with client versions of Windows, though it is not installed by default.

Directory and File Management

Think carefully about the directory structure and placement of files in designing the website. You should organize directories so that it is easy to apply access control and document the structure of the site so that it is easy for page authors, graphic designers, application/script developers, and administration staff to create a secure site in a collaborative environment.

It is also wise not to use virtual directories. A virtual directory is one that is located outside the web server's root directory, unless their use is critical and well-documented and understood. Scripts and executables should be stored in a single directory. Prevent code from being executed in any other directory.

Sample Files

Web servers are typically installed with sample pages (and even scripts) plus help documentation. These samples sometimes contain vulnerabilities and should be removed from a production server.

Directory Browsing

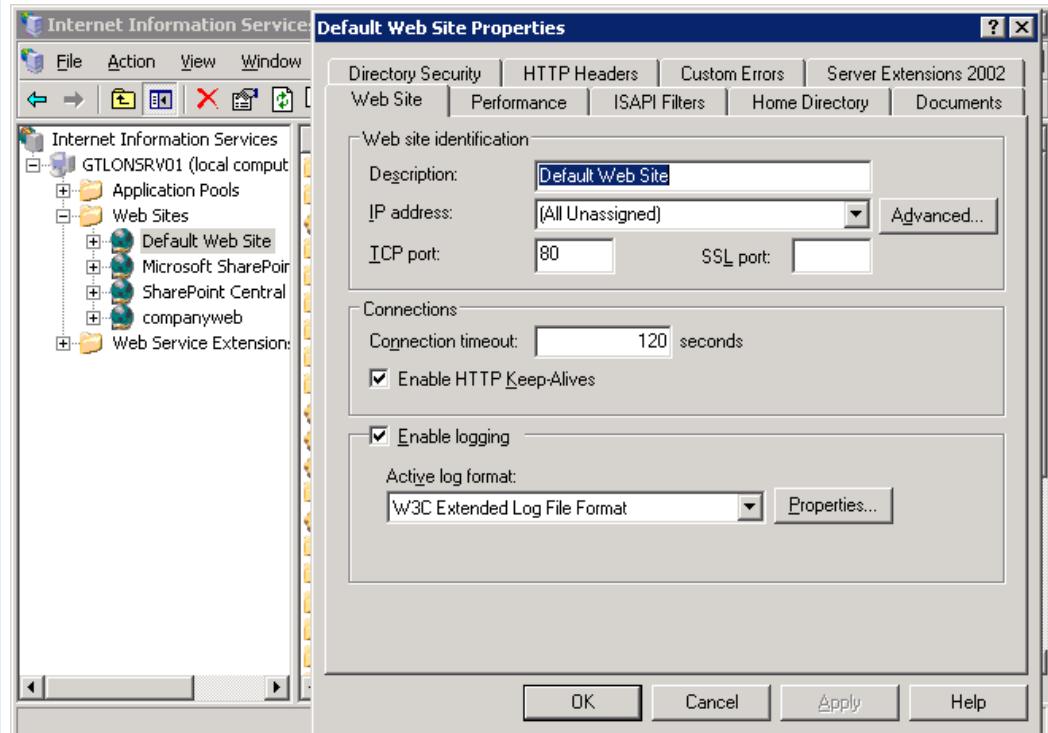
Enabling directory browsing displays a list of all files and folders in the published directory, in the form of hyperlinks. Files can be displayed and folders opened by clicking on the appropriate hyperlink. This has the advantage that pages are readily available and quick to set up. There are also disadvantages; users must understand filenames, directory browsing is unattractive in appearance, and allowing file names and folders to be visible raises security issues.

Throttling

If bandwidth to a server is limited, throttling can be used to limit the number of simultaneous connections that are allowed, guaranteeing a minimum performance level to those that can connect. The problem here of course is that the website will be unavailable to additional users once the limit is reached. Another use of throttling is to prevent Denial of Service attacks (or at least to limit their effectiveness) by limiting the number of requests allowed by any one IP address within a given time frame. As with other security measures, throttling needs to be configured sensitively to avoid disrupting ordinary use of the website.

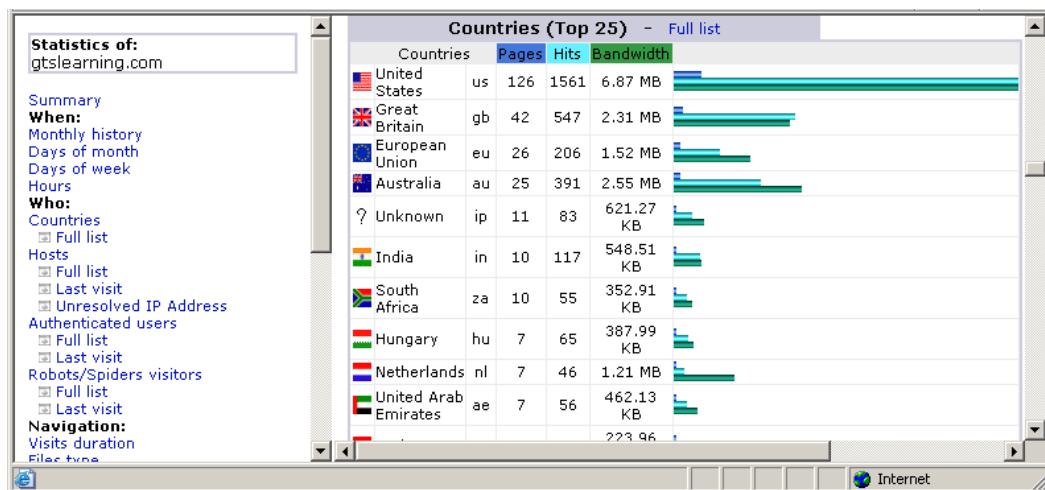
Logging

Servers provide facilities to log the web server activity. **Logging** provides the web administrator with valuable information regarding the use of the website, provide alerts of any unusual or suspicious behavior, and audit changes made to pages and settings.



Configuring IIS on Windows Server 2003

Applications can analyze these log files and generate statistics on who uses the site and how it is used.



Viewing logged information through awstats Linux utility



Microsoft provide the Security Compliance Manager toolkit to help to identify common misconfigurations and other security problems in IIS (and other Windows servers). The use of templates to configure application baselines is discussed in [Unit 4.1](#).



ladhx

Load Balancers

A **load balancer** provides for a higher throughput or to support more connected users. You might implement a server farm and place a load balancer in front of the farm. The load balancer distributes client requests across available server nodes in the farm. Clients use the single name/IP address of the load balancer to connect to the servers in the farm.

A load balancer also provides stateless fault tolerance. If there are multiple servers available in a farm, all addressed by a single name/IP address via a load balancer, then if a single server fails, client requests can be routed to another server in the farm.

Load balancing can only provide for *stateless* fault tolerance, as by itself it cannot provide a mechanism for transferring the state of data. If you need fault tolerance of *stateful* data, you must implement a **clustering** technology, whereby the data residing on one server (or group of servers) is made available to another server (or group of servers) quickly, seamlessly and transparently in the event of a server failure.

Most load balancers need to be able to provide for some or all of the following features:

- **Configurable load** - the ability to assign a specific server in the farm for certain types of traffic, or a configurable proportion of the traffic.
- **TCP offload** - the ability to group HTTP packets from a single client into a collection of packets assigned to a specific server.
- **SSL offload** - when you implement SSL / TLS to provide for secure connections, this imposes a load on the web server (or other server). If the load balancer can handle the processing of authentication and encryption/decryption, this reduces the load on the servers in the farm.
- **Caching** - as some information on the web servers may remain static, it is desirable for the load balancer to provide a caching mechanism to reduce load on those servers.
- **Prioritization** - to filter and manage traffic based on its priority.
- **Content switching** - a mechanism that routes traffic based on its header and/or payload.

You can use a load balancer in any situation where you have multiple servers providing the same function. Examples include web server farms, front-end e-mail servers, and web conferencing, A/V conferencing, or streaming media servers.

In terms of security, deploying a load balancer provides better fault tolerance and redundancy. The server will be more resilient to DoS attacks.



File Transfer

There are many means of transferring files across networks. A network operating system can host shared folders and files, enabling them to be copied or accessed over the local network or via remote access (over a VPN for instance).

Email and IM applications allow file transfer using attachments to messages. HTTP supports file download (and uploads via various scripting mechanisms). The TCP/IP FTP protocol and various peer-to-peer file sharing products can be used to transfer files more quickly and efficiently however.

File Transfer Protocol

An **FTP (File Transfer Protocol)** server is typically configured with a number of public directories, hosting files, and user accounts. Each user account can be configured with different permissions over files and directories. Most HTTP servers also function as FTP servers and FTP services, accounts, and directories may be installed and enabled by default when you install a web server.

FTP is more efficient compared to file attachments or HTTP file transfer, but has no security mechanisms. All authentication and data transfer is communicated as plain text.



Plain text is vulnerable to packet sniffing (that is, using a protocol analyzer to read the contents of data packets). Do not re-use secure passwords (such as Windows authentication passwords) for FTP applications. Any password used for FTP should be regarded as insecure.

FTP can actually perform more operations than just transfer a file from a server to a client. It allows a user to upload files to a server, delete files on the server, and create and remove directories on the server.

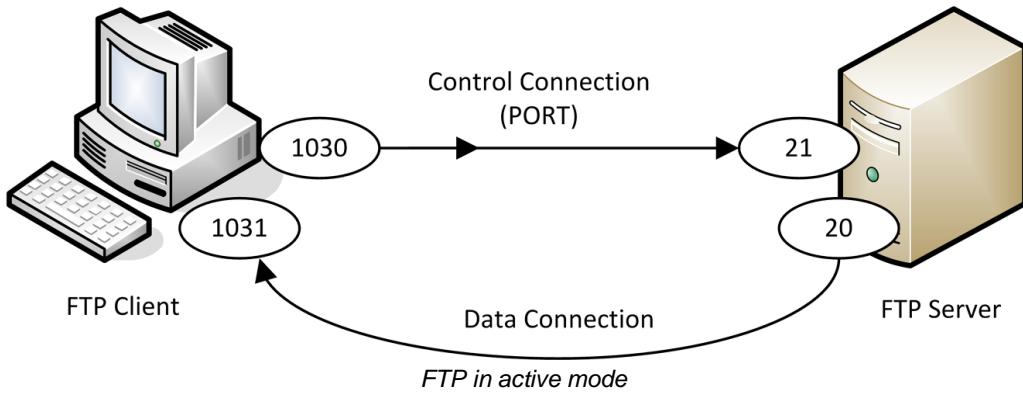
FTP clients usually have GUIs to help the user, though FTP can be performed over a command line as well. Most web browsers can function as basic FTP clients.

Active Versus Passive FTP

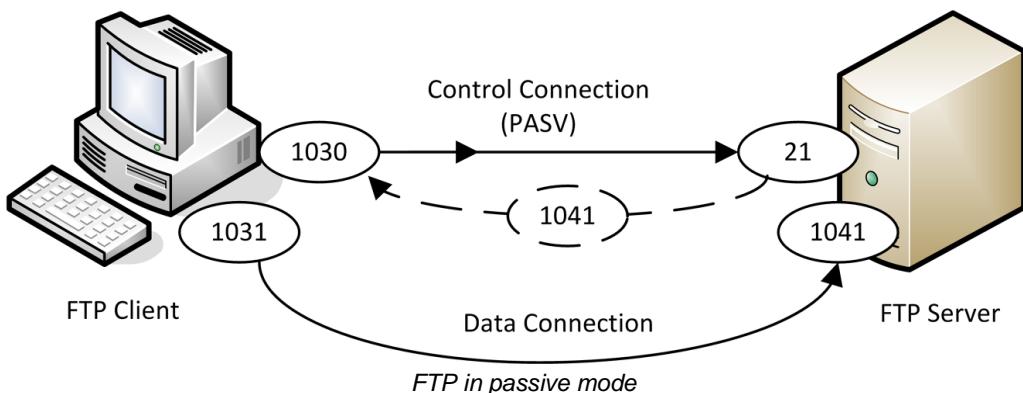
A client connects to TCP port 21 on an FTP server from a dynamically chosen dynamic port number (N) on the client. This **control port** is used to transfer commands and status information, but not for data transfer.

Data transfer can operate in one of two modes: active or passive.

In active mode, the client sends a PORT command specifying its chosen **data connection** port number (typically N+1) and the server opens the data connection between the chosen client port and port 20 on the server.



In passive mode, the *client* opens a data port (again, typically N+1) and sends the PASV command to the server's control port. The server then opens a random high port number and sends it to the client using the PORT command. The *client* then initiates the connection between the two ports.



Active FTP poses a configuration problem for some firewalls, as the server is initiating the inbound connection but there is no way of predicting which port number will be utilized. However, not all FTP servers and clients can operate in passive mode. If this is the case, check that firewalls installed between the client and server can support active FTP (stateful inspection firewalls).



Another problem is that the control connection can remain idle when the data connection is in use, meaning that the connection can be "timed out" by the firewall (or other routing device).



*You should check that users do not install unauthorized servers on their PCs (a **rogue server**). For example, a version of IIS that includes HTTP, FTP, and SMTP servers is shipped with client versions of Windows, though it is not installed by default.*

SSH FTP

SFTP (or "Secure FTP") addresses the privacy and confidentiality issues of FTP by encrypting the authentication and data transfer between client and server.

In SFTP, a secure link is created between the client and server using Secure Shell (SSH) over TCP port 22. Ordinary FTP commands and data transfer can then be sent over the secure link without risk of eavesdropping or Man-in-the-Middle attacks.



SSH is discussed in more detail in [Unit 3.4](#).

This solution requires a SSH server that supports SFTP and SFTP client software.



Do not confuse SFTP with the Simple File Transfer Protocol, a defunct version of FTP.

FTP over SSL (FTPS)

Another means of securing FTP is to use it with a secure lower layer protocol, such as SSL. This type of solution is often quite tricky to configure, especially when the connections are protected by firewalls.

Trivial File Transfer Protocol (TFTP)

Trivial File Transfer Protocol (TFTP) is a **connectionless** protocol (utilizing UDP port 69) that also provides file transfer services. It does not provide the guaranteed delivery offered by FTP and is therefore only suitable for transferring small files. Also, it only supports reading (GET) and writing (PUT) files not directory browsing, file deletion, or any of the other features of FTP. An example of the usage for TFTP might be a switch or router automatically downloading configuration files.



j4ywq

P2P File Sharing

In recent years, the use of peer-to-peer file sharing software, such as BitTorrent, has rocketed. Unfortunately, use of this type of software has often concentrated on illegal access to copyrighted material, such as music and film. This poses a legal problem for an organization hosting file sharing software on its computers (whether knowingly or not), as it may become a target for copyright owners seeking damages.

The software and file sharing archives are also popular targets for attackers to place viruses and spyware. File sharing software can also consume a lot of bandwidth and storage space.

Controlling use of consumer P2P file sharing software is very important, but quite difficult. Intrusion detection can be used to reveal its use but there should also be a firm policy against users installing this type of software, with strong penalties to enforce it!



Review Questions / Module 4 / Unit 3 / Web Services Security

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) How does SSL accomplish the secure exchange of session keys using certificates?
- 2) What general principles should be followed when setting up user accounts on a public web server?
- 3) What is throttling?
- 4) What application is typically used to secure FTP?
- 5) What cipher(s) can be selected to enable Perfect Forward Secrecy when configuring TLS?
- 6) A client and server have agreed the use of the cipher suite ECDHE-ECDSA-AES256-GCM-SHA384 for a TLS session. What is the key strength of the symmetric encryption algorithm?
- 7) You are implementing a new e-commerce portal with multiple web servers accessing data on a SAN. Would you deploy load balancers to facilitate access by clients to the web servers or by the web servers to the SAN?
- 8) What ports would you have to configure to allow client access to an FTP server in either active or passive mode?
- 9) You are configuring SSH on your web server to allow for secure management access. You want to allow the use of SFTP to transfer files. What port must you open on the server?



If you have access to the Hands On Live Labs, complete the "Cryptography / Transport Encryption" and "Network Security / Load Balancers" labs now.

Module 4 / Unit 4

Web Application Security

Objectives

On completion of this unit, you will be able to:

- Describe the technologies used to implement web applications.
- Understand typical attacks that can be made against web applications.
- Identify secure coding concepts for web applications.
- Harden web browser software and usage.

Web Application Technologies

A basic web server hosts static web pages. However, not many websites are content to use plain HTML anymore and a number of APIs (Application Programming Interface) are used to extend the functionality of web servers.

The use of this scripting makes secure configuration of a web server far more complex. The danger is that an attacker will be able to exploit vulnerabilities in the script or the parser (the application that interprets scripts). This could allow the attacker to damage the server in some way or even install a malicious script to compromise other users visiting the site.

The following languages and products are commonly used to implement web applications.

CGI (Common Gateway Interface)

The **Common Gateway Interface (CGI)** is a scripting mechanism allowing a web server to process data supplied by a client. CGI server-side scripting typically works as follows:

- 1) The client browser requests an HTML page containing a form from the HTTP server. The user completes the form and clicks the Submit button.
- 2) The form uses either the POST or GET method to transfer the data entered by the user to the server.
- 3) The server calls the executable program or a script referenced by the URI and passes the user input to the program.
- 4) The program processes the input and creates suitable output, which it passes back to the web server.

- 5) The web server uses the output to return a page to the client.

CGI programs are typically compiled C applications, scripts written in Perl or JavaScript, or shell scripts (those that use functions of the underlying OS). Poorly designed applications written in C or C++ are most susceptible to buffer overflow vulnerabilities. The CGI programs or scripts are typically located in a directory named **cgi-bin**.

ASP (Active Server Pages)

ASP originally ran on IIS 4.0 (shipped with Windows 2000). It offered similar functionality to CGI. The ASP process works as follows:

- 1) The browser requests a page with an ASP extension.
- 2) The web server recognizes that the page contains scripts because of the ASP extension and sends the page to ASP.DLL for processing.
- 3) The scripts are executed and dynamic content is incorporated into the page.
- 4) The resultant page is sent to the browser for display.

ASP.NET

The latest versions of ASP (ASP.NET 2.0 and 3.0) are considerably different. It is integrated into Microsoft's .NET web application platform. .NET allows the use of different programming languages and tools (including Microsoft's C# or Visual Basic as well as JavaScript, Perl, or PHP) to create web applications running on IIS.

ASP.NET files have .ASPX extensions.

PHP (PHP Hypertext Preprocessor)

PHP is a powerful and hugely popular application for creating dynamic websites. It is particularly effective at tying into back-end databases. It is associated with Linux/Apache-based sites but can also be used with Windows/IIS. A website running PHP generally serves .PHP files. These are HTML files with embedded PHP scripts. The PHP parser runs the script then passes the web server the resultant HTML code for delivery to the browser.



You will often see the acronym LAMP used - this refers to a web server running Linux, Apache, MySQL, and PHP.

Java

Java is a programming language developed by Sun Microsystems. It has several different implementations for web applications:

- JSP - Java Server Pages works like ASP.
- J2EE - this is a web application architecture, providing functionality similar to ASP.NET.
- Java Applets - these are client-side applications (see below).



Do not confuse Java with JavaScript. While some of elements of the languages are similar, they are different things.

Web Application Databases



ktjo4

Most web-based applications serve content from some sort of database.

Databases (SQL and NoSQL)

Structured Query Language (SQL) is a programming language used for the maintenance of **Relational Database Management Systems (RDBMS)**. Information must be entered into a relational database according to the rules of its **schema**. The schema defines things such as the fields that make up a record and what type of data is allowed in them. It will also define the relationship between different tables of data. For example, you might have one table of customer records and another table of orders. The orders table would contain a customer field related to a record stored in the customers table.

Where the database is accessible over the web, a copy of the live database should be used. This means that transactions can be fully verified before they are permitted on the local copy.

NoSQL refers to non-relational database stores. These are often based around **documents** rather than tables and records, though a NoSQL database can include relational databases within it. NoSQL can be expanded as "Not Only" SQL in recognition of this fact. Another NoSQL database type is based on **key-value stores**. In a key value store, the key identifies each "record", such as a user. The key can be associated with multiple values, or bins, which do not need to be defined in advance or have fixed data types or lengths.



You will often see the term JSON (JavaScript Object Notation) used. JSON refers to the use of attribute=value pairs. Each bin in a key-value store can be defined in terms of attribute=value pairs.

A third type in the NoSQL "family" is a columnar or wide-column database. In this type of database, field values are stored by column rather than by row. For example, the values for all rows in column 1 appear first, then those for column 2, and so on. This speeds up queries. A fourth important type is the graph store; this defines information in terms of the properties of nodes and the relationships between nodes.

The selection of a particular NoSQL type will depend on the needs of the application but in general terms NoSQL addresses several limitations of RDBMS:

- Ability to scale to meet peak demand requirements easily. Relational databases tend to run into problems if too many users try to access them simultaneously; "too many" being a function of the hardware underlying the database. NoSQL databases scale better because there is less work to do per user.
- Ability to analyze large, unstructured data sets. This is often referred to as **big data**. Organizations accumulate huge amounts of information that cannot easily be recorded in a pre-defined schema. NoSQL databases provide a means of accessing and analyzing data stored in these unstructured documents.

XML, Web Services, and SOAP

Extensible Markup Language (XML) is a means of describing information so that it can be transferred between different applications.

One of the features of complex web applications is that the applications (or **web services**) can communicate with one another. A web application exposes an Application Programming Interface (API). Other web applications can call functions in the API to perform operations on the remote web server, such as transferring customer information collected by a quote retrieval service to the merchant chosen by the customer. The **Simple Object Access Protocol (SOAP)** is a means for web services to exchange information in XML format.



"Simple Object Access Protocol" is the origin of the acronym but W3C have now decided that it shouldn't stand for anything; that is, SOAP is the thing that underpins web services.

Web Content Management System

Very few websites are produced from static HTML files these days. Most sites are designed using a **Web Content Management System (WCMS)** such as WordPress, Joomla!, or Drupal. A WCMS allows multiple authors to write web page copy and add images, which are uploaded to a database and then served using PHP (or similar). The appearance of the site can easily be customized using templates. A WCMS will also support the use of plug-ins, to facilitate tasks such as Search Engine Optimization (SEO) and traffic analysis or implement blogs or an e-commerce webstore.

A WCMS (and its plug-ins) needs to be updated to patch against security vulnerabilities like any other software. The risk is particularly high as a vulnerable WCMS is a valuable target for hackers. A severe vulnerability could allow an attacker to install "drive-by" download malware that could infect the site's visitors.

Web Application Exploits

Software exploitation means an attack that targets a **vulnerability** in OS or application software. Applications such as web servers, web browsers, email clients, and databases are often targeted. A vulnerability is a design flaw that can cause the application security system to be circumvented or that will cause the application to crash.

Typically, vulnerabilities can only be exploited in quite specific circumstances but because of the complexity of modern software and the speed with which new versions must be released to market, almost no software is free from vulnerabilities.

There are various vulnerability exploit kits, such as Mpack and Neosploit, that can be installed to a website and actively try to exploit vulnerabilities in clients browsing the site. These kits may either be installed to a legitimate site without the owner's knowledge (by compromising access control on the web server) and load in an iFrame (invisible to the user) or the attacker may use phishing / social engineering techniques to trick users into visiting the site, using Google search results, ads, "typosquatting", or clicking an email link.



Zero-day Attack

Most vulnerabilities are discovered by software and security researchers, who notify the vendor to give them time to patch the vulnerability before releasing details to the wider public. A vulnerability that is exploited before the developer knows about it or can release a patch is called a "zero-day" exploit. These can be extremely destructive, as it can take the vendor a lot of time to develop a patch, leaving systems vulnerable for days, weeks, or even years.

Input Validation

Most software accepts user input of some kind, whether the input is typed manually or passed to the program by another program (such as a browser passing a URI to a web server). Good programming practice dictates that input should be tested to ensure that it is valid (that is, the sort of data expected by the program).

An **input validation** (or format string) attack passes invalid data to the application and because the error handling on the routine is inadequate, it causes the application or even the OS to behave unusually. The following effects are possible:

- The application crashes.
- The OS crashes.
- The attacker is able to execute code on the system.



Buffer Overflow

A particular type of input validation attack is called **buffer overflow**. The attacker passes data that deliberately overfills the buffer (an area of memory) that the application reserves to store the expected data. There are three principal exploits:

- Stack overflow - the stack is an area of memory used by a program subroutine. It includes a return address, which is the location of the program that called the subroutine. An attacker could use a buffer overflow to change the return address, allowing the attacker to run arbitrary code on the system. Two examples of this are the Code Red worm, which targeted Microsoft's IIS web server (version 5) and the SQLSlammer worm, which targeted Microsoft SQL Server 2000.
- Heap overflow - a heap is an area of memory allocated by the application during execution to store a variable of some sort. A heap overflow can overwrite those variables, with unexpected effects. An example is a known vulnerability in Microsoft's GDI+ processing of JPEG images.
- Array index overflow - an array is a type of variable designed to store multiple values. It is possible to exploit insecure code to load the array with more values than it expects, creating an exception that could be exploited.

Integer Overflow

An integer is a positive or negative number with no fractional component (a whole number). Integers are widely used as a data type, where they are commonly defined with fixed lower and upper bounds. An integer overflow attack causes the target software to calculate a value that exceeds these bounds. This may cause a positive number to become negative (changing a bank debit to a credit for instance). It could also be used where the software is calculating a buffer size; if the attacker is able to make the buffer smaller than it should be, s/he may then be able to launch a buffer overflow attack.



Privilege Escalation

An application or process must have privileges to read and write data and execute functions. Depending on how the software is written, a process may run using a system account, the account of the logged on user, or a nominated account. If a software exploit works, the attacker may be able to execute their own process (a worm or Trojan for instance) with the same privilege level as the exploited process.

Arbitrary / Remote Code Execution



7zja0

The purpose of the attacks described above is to allow the attacker to run his own code on the system. This is referred to as **arbitrary code execution**.

Where the code is transmitted from one machine to another, it is sometimes referred to as **remote code execution**. The code would typically be designed to install some sort of Trojan or to disable the system in some way (Denial of Service).



55m1s

SQL Injection / XML Injection

As the name suggests, this attack attempts to insert an SQL query as part of user input. The attack can either exploit poor input validation or unpatched vulnerabilities in the database application.

If successful, this could allow the attacker to extract or insert information into the database or execute arbitrary code on the remote system using the same privileges as the database application.

XML injection is fundamentally the same thing but targeted against web servers using XML applications rather than SQL.



nq3ej

Directory Traversal / Command Injection

Directory traversal is another common input validation attack. The attacker submits a request for a file outside the web server's root directory by using the command to navigate to the parent directory (..). This attack can succeed if the input is not filtered properly and access permissions on the file are the same as those on the web server root.

A **command injection** attack attempts to run OS shell commands from the browser. As with directory traversal, the web server should normally be able to prevent commands from operating outside of the server's directory root and to prevent commands from running with any other privilege level than the web "guest" user (who is normally granted only very restricted privileges). A successful command injection attack would find some way of circumventing this security (or find a web server that is not properly configured).



lxigu

Transitive Access

Transitive access describes the problem of authorizing a request for a service that depends on an intermediate service.

For example, say a user orders an ebook through some ecommerce application on a merchant site. The merchant site processes the order and then places a request to a publisher site to fulfil the ebook to the user.

Designing the trust relationships between these three parties is complicated:

- The merchant site could impersonate the end user to obtain publisher site services fraudulently.
- The end user could exploit weaknesses in the merchant site to obtain unauthorized services from the publisher site.

Web Application Browser Exploits

The attacks described above mostly target weaknesses of server-side application code or security measures. There are also many attacks against the browser (client-side code and security measures).



7v6lx

Cross-Site Scripting

Cross-Site Scripting (XSS) is one of the most powerful input validation exploits. XSS involves a trusted site, a client browsing the trusted site, and the attacker's site.



The abbreviation XSS is used to avoid confusion with CSS (Cascading Style Sheets), which is used to format web pages.

A typical attack would proceed as follows:

- 1) The attacker identifies an input validation vulnerability in the trusted site.
- 2) The attacker crafts a URI to perform a code injection against the trusted site. This could be coded in a link from the attacker's site to the trusted site or a link in an email message.



The key to a successful XSS attack is making the link seem innocuous or trustworthy to the user. There are various ways of encoding a link to conceal its true nature.

- 3) When the user clicks the link, the trusted site returns a page containing the malicious code injected by the attacker. As the browser is likely to be configured to allow the site to run scripts, the malicious code will execute.
- 4) The malicious code could be used to deface the trusted site (by adding any sort of arbitrary HTML code), steal data from the user's cookies, try to intercept information entered into a form, or try to install malware. The crucial point is that the malicious code runs in the client's browser with the same permission level as the trusted site.



A common technique is to leverage iFrames to disguise the presence of malicious code. An iFrame is a legitimate HTML coding technique that can be used to embed one site within another. A malicious iFrame could either overlay a site with a fake login or host malicious code in an "invisible" 1x1 pixel frame. iFrame attacks can also be launched simply by compromising the web server security and uploading compromised code.

The attack is particularly effective not only because it breaks the browser's security model but also because it relies only on scripting, which is generally assumed by browsers to be safe. The vast majority of sites use some sort of scripting and so will not display correctly without it.

The attack described above is a **reflected** or **non-persistent** XSS attack. A **stored** (or **persistent**) XSS attack aims to insert code into a back-end database used by the trusted site. For example, the attacker may submit a post to a bulletin board with a malicious script embedded in the message. When other users view the message, the malicious script is executed.

Both the attacks described above exploit *server-side* scripts. A third type of XSS attack exploits vulnerability in *client-side* scripts. Such scripts often use the **Document Object Model (DOM)** to modify the content and layout of a web page. For example, the "document.write" method enables a page to take some user input and modify the page accordingly. An attacker could submit a malicious script as input and have the page execute the script. Such exploits can be very powerful as they run with the logged in user's privileges of the local system.



Cookies, Session Hijacking, and XSS

HTTP is a stateless protocol, meaning that the server preserves no information about the client. As most web applications depend on retaining information about clients, various mechanisms have been used to preserve this sort of stateful information. A **cookie** is one of those methods.

A cookie is created when the server sends an HTTP response header with the cookie. Subsequent request headers sent by the client will usually include the cookie. Cookies are either non-persistent (or session) cookies, in which case they are stored in memory and deleted when the browser instance is closed, or persistent, in which case they are stored on the hard drive until deleted by the user or pass a defined expiration date.

Normally a cookie can only be used by the server or domain that created it but this can be subverted by a cross-site scripting attack. Another weakness is where cookies are used to establish sessions in an application or for user authentication. Session IDs are often generated using predictable patterns (such as IP address with the date and time), making the session vulnerable to eavesdropping and possibly hijacking.

A **Cross-site Request Forgery (XSRF)** can exploit applications that use cookies to authenticate users and track sessions. To work, the attacker must convince the victim to start a session with the target site. The attacker then has to pass an HTTP request to the victim's browser that spoofs an action on the target site (such as changing a password or an email address). This request could be disguised in a number of ways (as an image tag for instance) and so could be accomplished without the victim necessarily having to click a link.

If the target site assumes that the browser is authenticated (because there is a valid session cookie) and doesn't complete any additional authorization process on the attacker's input (or if the attacker is able to spoof the authorization), it will accept the input as genuine. This is also referred to as a **confused deputy** attack (the point being that the user and the user's browser are not necessarily the same thing).



If cookies are used to store confidential information, the web application should encrypt them before sending them to the client. If using SSL, information in a cookie would be secure in transit but reside on the client computer in plaintext, unless it had been separately encrypted.

HTTP Header Manipulation

HTTP headers are information processed by the server and browser but not necessarily displayed to the user. One of the headers is the action (GET or POST for instance). Other headers may contain the user-agent (the type of browser) or custom information.

Some applications may use headers to encode some user data, such as setting a cookie or returning the value of a cookie. If this is the case, as with forms and URLs, an attacker could try to inject code to perform a malicious action on the target server or client if the web application does not process the header correctly.

The best known HTTP header manipulation attack is **HTTP Response Splitting** or **CRLF injection**. The attacker would craft a malicious URI and convince the victim to submit it to the web server. This could be encoded in something like an image tag so the user may not have to choose to click a link.

The URI contains extra line feeds, which may be coded in some non-obvious way. Unless the web server strips these out, when processing the URI it will be tricked into displaying a second HTTP response, containing content crafted by the attacker. This content could deface the genuine page, overlay a fake authentication form, perform some sort of XSS injection attack, and so on.

Secure Web Application Design

Security must be a key component of the application design process. Even a simple form and script combination can make a web server vulnerable if the script is not well written.



3abfo

Secure Coding Concepts

The security considerations for new programming technologies should be well understood and tested before deployment. One of the challenges of web application development is that the pressure to release a solution often trumps any requirement to ensure that the application is secure.

Some of the most important coding practices are input validation, error handling, and implementing proper authentication and authorization of sessions.



8xj02

Input Validation

As discussed above, the primary vector for attacking web applications is to exploit faulty **input validation**. Input could include user data entered into a form or URLs passed by another web application or link. Firstly, to reduce the attack surface, all input methods should be documented. Secondly, any input must be checked and anything that does not conform to what is required must be rejected.

Fuzzing is a means of testing that an application's input validation routines work well. Fuzzing means that the test or vulnerability scanner generates large amounts of deliberately invalid and / or random input and records the responses made by the application. This is a form of "stress testing" that can reveal how robust the application is.



38wt9

Server-side versus Client-side Validation

A web application (or any other client-server application) can be designed to perform input validation locally (on the client) or remotely (on the server). Applications may use both techniques for different functions.

The main issue with client-side validation is that the client will always be more vulnerable to some sort of malware interfering with the validation process. The main issue with server-side validation is that it can be time-consuming, as it may involve multiple transactions between the server and client.

Consequently, client-side validation is usually restricted to informing the user that there is some sort of problem with the input before submitting it to the server. Even after passing client-side validation, the input will still undergo server-side validation before it can be posted (accepted). Relying on client-side validation only is very poor programming practice.

Error and Exception Handling

A well-written application must be able to handle errors and exceptions "gracefully". This means that the application performs in a more-or-less expected way when something unexpected happens.

An exception means that the current procedure cannot continue. An exception could be caused by invalid user input, by a loss of network connectivity, by another server or process failing, and so on. Ideally, the programmer will have written an error or exception **handler** to dictate what the application should then do. Each procedure can have multiple error handlers. Some handlers will deal with anticipated errors and exceptions; there should also be a "catch-all" handler that will deal with the unexpected.

The main goal must be for the application not to fail in a way that allows the attacker to execute code or perform some sort of injection attack. Another issue is that an application's interpreter will default to a standard handler and display default error messages when something goes wrong. These may reveal the inner workings of code to an attacker. It is better for an application to use custom error handlers so that the developer can choose the amount of information shown when an error is caused.

XSS / XSRF Prevention

Input validation should be enough to defeat most cross-site style attacks. The other consideration is for the application to use secure authentication and authorization procedures. Naive methods of recording sessions (such as unencrypted cookies) should be deprecated. Even if a user has authenticated, any actions the user attempts to perform should be properly authorized using some sort of secure token that an attacker cannot guess or spoof.

Auditing Web Applications



5xcot

A new web application should be audited to ensure that it meets the goals of confidentiality, integrity, and availability critical to any secure computer system.

Test any new or updated web applications thoroughly before deploying them to a production server. Use pentest methods to try to discover and exploit any weaknesses in the application's design or implementation. Web application vulnerability scanners automate the process of testing for known vulnerabilities and insecure coding practice. Trial and monitor typical user behavior (beta testers) to find out if the application could be used in ways that the developers might not have expected.

As well as testing the application in production, submit new applications for architecture, design, and code reviews. These should take place when the application is first commissioned and when it is upgraded or at regular intervals thereafter (to ensure that the application is not vulnerable to new threats).

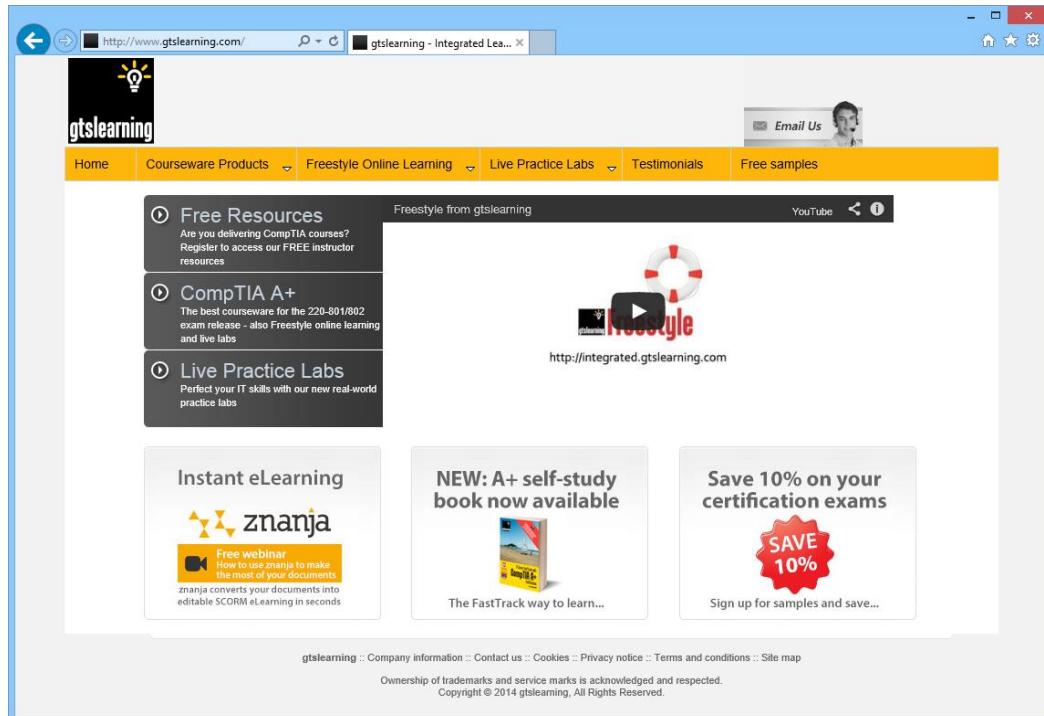
- A **design review** will ensure that security is one of the requirements for the application.

One of the design goals of a secure application should be to reduce the **attack surface**. The attack surface is all the ways that a user (including malicious users) can interact with the application. This includes ways that the application designer has foreseen (such as form fields and APIs - methods other applications can call) and those that they have not. As well as simplifying the application, it is also important to reduce the attack surface of the host OS and network. These should be set at the minimum configuration required to run the application.

- A **code review** is an in-depth examination of the way the application is written to ensure that it is well written and does not expose the application to known input validation or injection attacks.
- An **architecture review** will analyze the systems on which the web application depends. This could include things like the underlying OS and database application, programming language and development environment, client browsers and plug-ins, and so on.

Web Browser Security

Internet Explorer is by far the most popular PC web browser, but that popularity means that it is targeted ruthlessly by security researchers and attackers. This attention has led to a continual stream of security updates and patches to fix bugs and vulnerabilities.



Internet Explorer web browser

Other web browsers, notably Firefox, Opera, Safari, and Chrome, are growing in popularity. However, inconsistent standards support in IE for things like CSS and Dynamic HTML mean that many websites only support IE and using a different browser causes formatting problems. Most browsers incorporate other functions than simple web browsing, such as working as an email, newsgroup, or FTP client.



Note that a browser might also be used by other types of software. For example, Outlook's email preview pane uses a browser (either IE or Word, depending on the version) to render HTML messages.

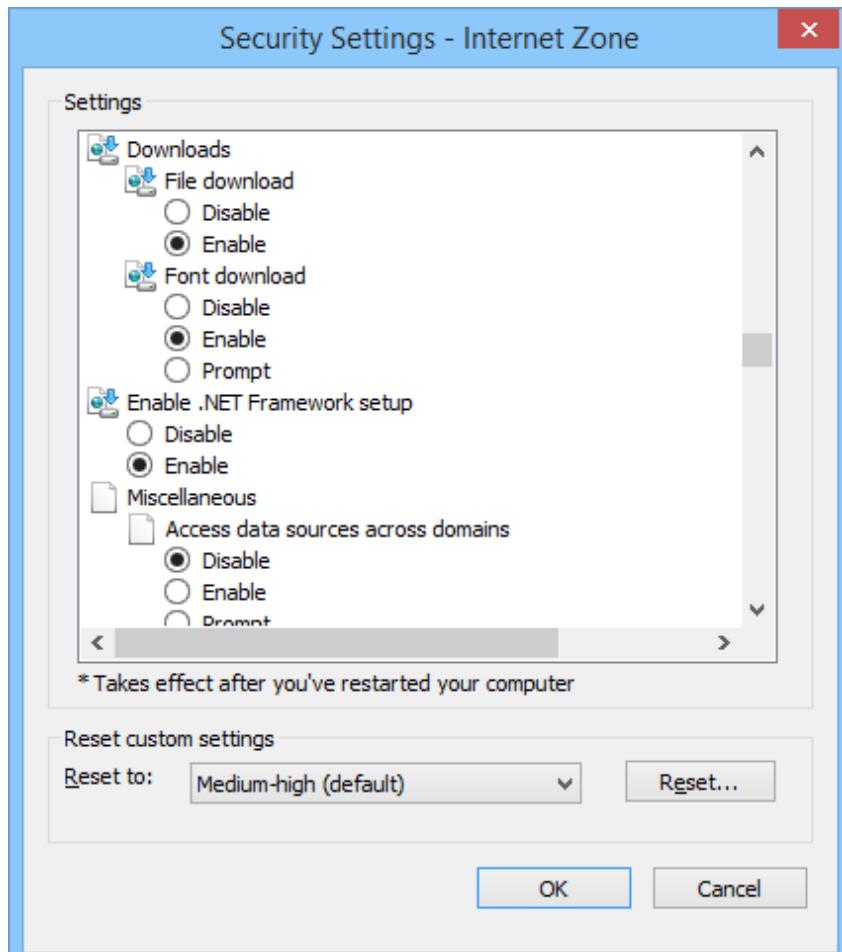
Configuring browser security is complex, but some of the main issues are discussed in the following topics.



97rr9

File Downloads and Attachments

Browsers automatically download files used to display a page from the web server to a local cache. Each browser has its own cache; IE calls it the Temporary Internet Files folder. Some websites may make other files available for user-initiated download, by providing a link to a file. Most browsers can be configured to prevent this type of file download. Files could also be delivered to a user's PC via an email or Instant Messaging file attachment. The risk is that downloadable files or message attachments could be infected with executable or macro viruses.



IE web browser file download security settings

Modern versions of Windows are protected by User Account Control (UAC). This will block executable code that is not digitally signed from running or warn the user that the code is potentially unsafe.



When downloading software from an archive where the developer is not using signed setup files, the software will typically be accompanied by a secure checksum, calculated using MD5 or similar. After downloading the file, you can calculate the file's checksum and verify that it matches. This will prove that the version has not been tampered with. It does not prove that the software was trustworthy in the first place though.

JavaScript / VBScript

Client-side scripts are designed to run within the browser "instance", which means that they are only supposed to perform actions that the user's web browser can perform. Unfortunately, there are numerous security vulnerabilities in JavaScript, meaning that scripts should only be enabled on sites that have been confirmed as safe for scripting. This is not helped by the warning message displayed by IE to the user when prompting them to enable scripts. This message suggests that enabling scripting is typically safe to do, which isn't really the case. The vulnerabilities include being able to send email, "spawn" pop-up windows, conceal URIs, read, add or modify files on local drives, and so on. Users should not be permitted to run browsers while logged on with administrative privileges for the OS.



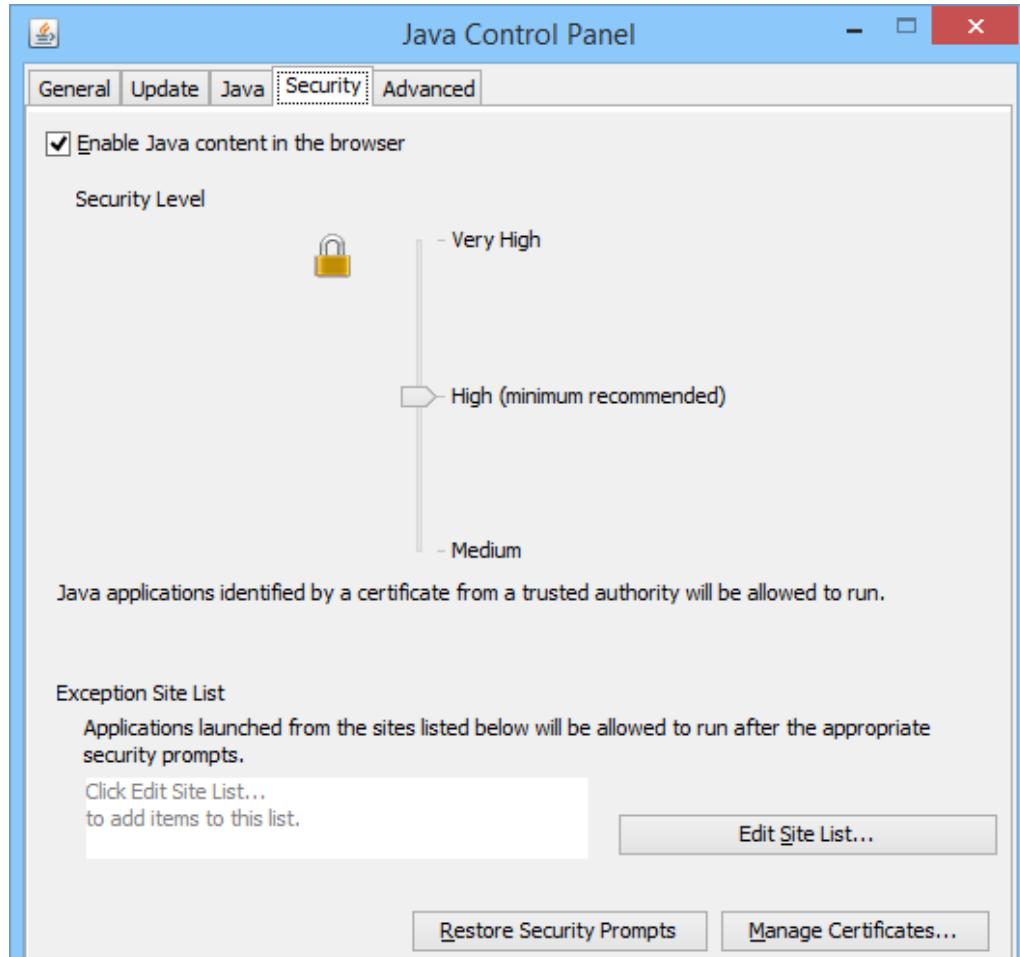
Under Windows Vista / 7, IE runs in a "sandbox" mode where the permissions for the browser are less than those of the logged-on user (User Account Control). Third-party products are also available to run the browser in a restricted virtual machine environment (for example GreenBorder Pro).

Plug-ins / Add-ons

For some years, web application developers have been keen to provide users with an "experience" that resembles that of locally-installed desktop software. One of the principal means of doing this is by installing desktop-like software in the form of a browser plug-in. There are many different types of plug-in, but some of the major ones are as follows:

- ActiveX - this is Microsoft's API for providing interactive, "rich media" content over the web. ActiveX controls are extremely powerful (for example, ActiveX enables a Windows PC to download and install operating system updates from Microsoft's website).
- Browser Helper Objects (BHO) - Dynamic Link Library (DLL) modules for Internet Explorer that extend the functionality of the browser (such as installing an additional toolbar).

- Java Applets - these are programs that run within the Java Virtual Machine (Java VM), which must also be downloaded and installed. Due to licensing disagreements, Windows no longer ships with a copy of the Java VM. It can be obtained from www.java.com. There are also versions for Linux, Solaris, and Mac OS.
- Shockwave / Flash / Authorware - these are plug-ins to play content developed in various Adobe (previously Macromedia) applications. This type of application is very popular with web developers as a means of providing "desktop-style" interactive content through a web page.
- Silverlight - a plug-in providing support for the Microsoft Silverlight framework. Silverlight is intended to provide a similar environment to Flash (for web applications using video, animation, and so on) and better cross-platform support than ActiveX.
- PDF - Portable Document Format files are a platform-independent means of distributing documents for viewing and printing. A browser plug-in enables PDFs to be shown in the browser window.



Under Windows, configure Java settings via the Control Panel

Plug-ins are essentially applications and so require administrative privileges to install. As with any application, an add-on may not be all it seems and might actually have been designed with some sort of malicious purpose. One means of reassuring users about the validity of a plug-in is to use a code-signing certificate. This uses PKI to show who developed the application and verify that it has not been modified in any way.

As software, plug-ins are vulnerable to exploits such as buffer overflow. To protect against these, the plug-ins should be kept up-to-date with security patches and upgrades.

Configuring Browser Security

Protecting a computer against malicious use of web content means deactivating the use of such content on web pages or at least warning that some level of threat is present. However, this means that some websites may not display correctly.



This section focuses on Internet Explorer to illustrate the sort of options that can be set. Browsers such as Opera, Firefox, and Safari offer similar (or stronger) security options.

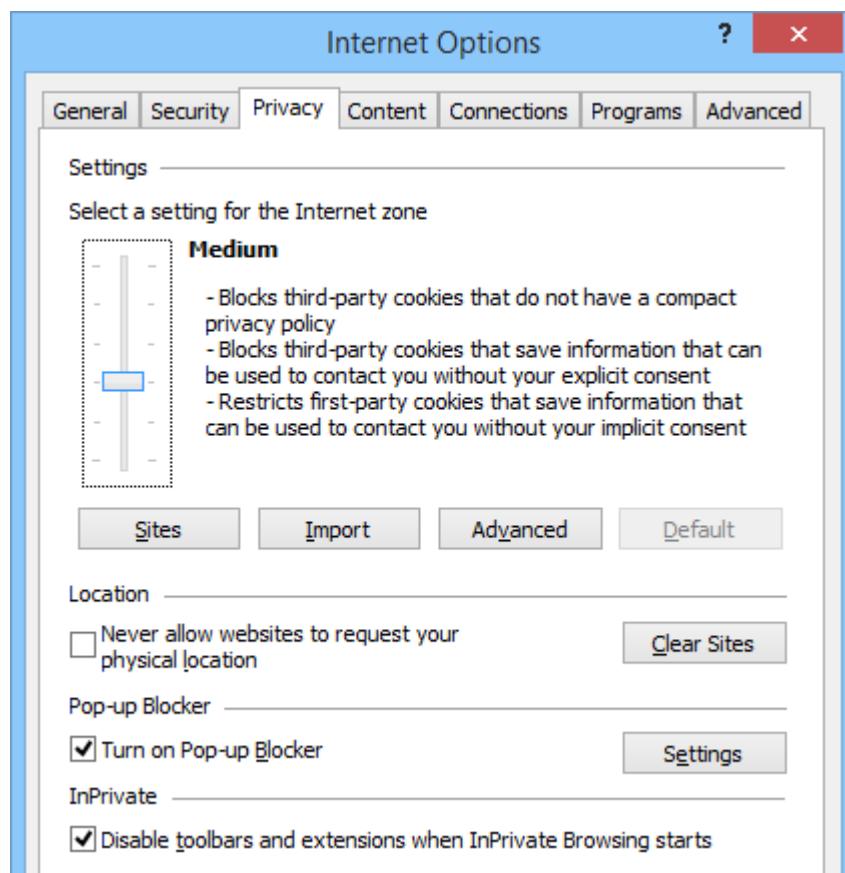
Internet Explorer has a system of zones, for which you can set different security levels. You can then enable the use of active web content and file downloading on trusted sites, so that you can browse them without interruption. The four security zones are as follows:

Use This Zone	To
	Internet Browse safely with warnings when sites contain potentially unsafe content.
	Trusted Sites Set minimum or no security protection.
	Restricted Sites Set the highest level of security and prevent any active content from running.
	Local Intranet Browse safely on a company intranet, with warnings when pages contain potentially unsafe content.

The settings for a particular zone can be customized to allow specific actions, such as downloading files or executing scripts, if they are not permitted by default. By default, all pages outside the local subnet appear in the **Internet** zone. You have to add sites to the **Trusted** and **Restricted** zones. On a domain network, the same settings can be configured and applied to a group of users through GPO (**User Configuration > Windows Settings > Internet Explorer Maintenance**):

Cookies

Browsers such as Internet Explorer usually have configurable cookie policies. This allows the user to (for instance) block all cookies or to block third-party cookies (those that are created by or send data to a site other than the one you are viewing), which may be used to track web browsing.



Internet Options dialog box - Privacy tab

Privacy

Internet Explorer can be set to store information typed into forms, including passwords, and retains a history of browsed pages. Any user using a publicly accessible computer should be trained to check these settings and to clear the browser cache before logging off. Internet Explorer also supports in **inPrivate** privacy mode, which suppresses cookies, browsing history, and autocomplete information.



Flash Player and Flash Cookies

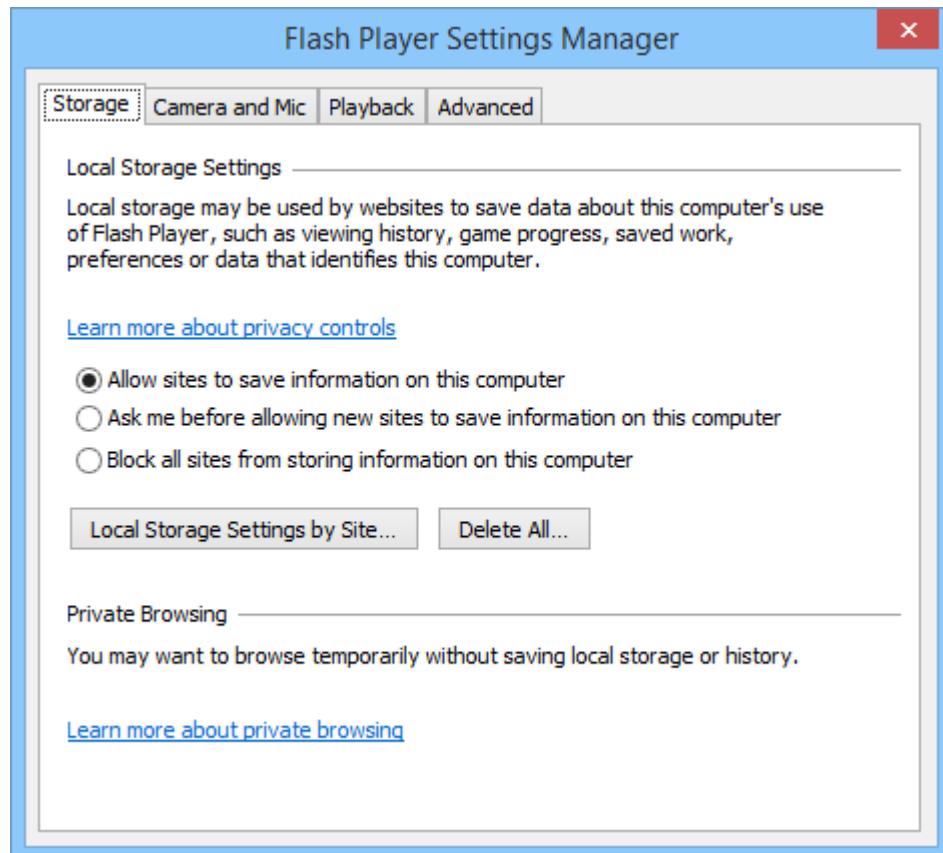
As mentioned above, Adobe's **Flash Player** is one means web developers have used to provide "rich interaction" on websites. A Flash object (packaged as an SWF file) can run from a web page to show video or implement a game, elearning, or any other type of interactive software. The SWF file runs within Flash Player's sandbox, which is supposed to prevent the object from gaining access to the wider file system without the user's consent. Unfortunately, Flash Player has been subject to numerous vulnerabilities and exploits over the years. It is critical to keep Flash up-to-date, if it is installed.



Flash is not supported by Apple's iOS devices and recent versions of Android have also dropped support for it.

Apart from security vulnerabilities, Flash objects also have privacy issues. Flash can be used to store its own **Flash cookies** or **Local Shared Objects (LSOs)**. LSOs are text files stored within the Flash object's sandbox. While these have legitimate uses (such as saving progress through a game or elearning course), Flash cookies can provide websites with an alternative means of tracking access, as originally they were not affected by the browser's cookie or security settings.

The latest versions of Flash (from around 2011) are more compliant and are likely to integrate with the browser to allow the user to select "privacy mode" or delete all types of local cookies. The user can control flash cookies and other local content using the Flash Player applet in Control Panel or by alt-clicking a particular Flash object.



Managing Flash cookies and local storage using the Flash Player applet in Control Panel

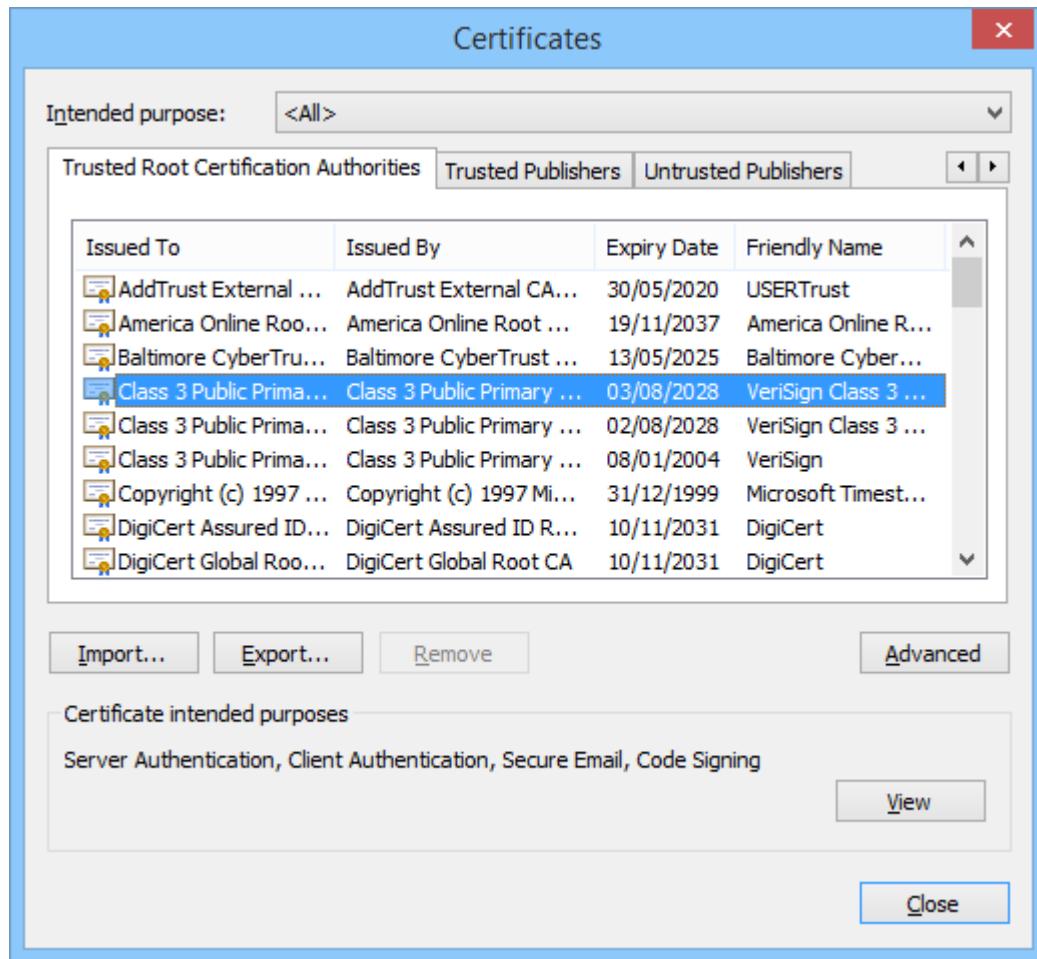
Digital Certificates

When a web browser communicates with a secure (HTTPS) server, it installs the server's certificate to use its public key to encrypt communications. Remember that the public key cannot be used to decrypt a message. Only the linked private key can be used to do that. The private key must be kept secret. Having a certificate is not in itself any proof of identity however. The browser and server rely upon a third-party - the Certificate Authority (CA) - to vouch for the server's identity.



This framework is called Public Key Infrastructure (PKI). See [Unit 2.2](#) for more information.

Internet Explorer is pre-installed with a number of **root certificates** that are automatically trusted. These represent the commercial CAs that grant certificates to most of the companies that do business on the web. When the user browses a site containing a new certificate (or attempts to run an application that has been signed using a code-signing certificate), Windows displays the certificate information and prompts the user whether to trust the certificate or not. If the certificate is trusted, it is added to the certificate store. You can view, add, and remove certificates from the store using Internet Explorer. From the **Internet Options** dialog, click the **Content** tab, then select the **Certificates** button.



Managing certificates in Internet Explorer

From here you can view (double-click), import, and remove certificates. They are grouped by category using the tabbed headings (use the arrow buttons to navigate left and right). Note that the **Untrusted Publishers** tab is populated with any certificates that the user has chosen not to trust.



Certificates can also be managed at a Management Console using the Certificates snap-in.

As well as commercial third-party CAs, a Windows network might be set up with its own CA for issuing certificates for network use (smart card authentication, code-signing, and so on). A PC that is part of Active Directory will install certificates automatically but a computer outside AD might need them installing manually.



Review Questions / Module 4 / Unit 4 / Web Application Security

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What is a persistent XSS attack?
- 2) What methods should be used to protect a web server against XSS exploitation?
- 3) Why would a NoSQL database format be selected for backend storage for a website?
- 4) Why might an integer overflow exploit in a web application lead to data loss?
- 5) What type of programming practice defends against injection-style attacks, such as inserting SQL commands into a database application from a site search form?
- 6) What type of security controls or programming practice defends against transitive access attacks?
- 7) Your company is developing a web application that will be deployed primarily to Apple iPads. What part of the auditing process will determine the security requirements for deployment on the tablets?
- 8) What vulnerabilities might default error messages reveal?
- 9) How does Internet Explorer choose whether to trust certificates?
- 10) What restriction should you enforce to prevent infection by malicious browser plug-ins?

Module 4 / Unit 5

Virtualization and Cloud Security

Objectives

On completion of this unit, you will be able to:

- Describe different technologies and uses of virtualization.
- Identify the security issues involved in virtualization.
- Understand the use and security implications of cloud computing.

Virtualization Technologies



yw17h



eico7

For most of the history of the microcomputer, a single computer has been able to run a single operating system at any one time. This makes multiple applications available on that computer (whether it be a workstation or server) but the applications must all share a common environment.

Virtualization means that multiple operating systems can be installed and run simultaneously on a single computer. There are many different ways of implementing this and many different reasons for doing it.

A virtual platform requires at least three components:

- Computer(s) - the platform that will host the virtual environment. Optionally, there may be multiple computers networked together.
- Hypervisor (or Virtual Machine Monitor [VMM]) - manages the virtual machine environment and facilitates interaction with the computer hardware and network.
- Guest operating systems (or Virtual Machines [VM]) - operating systems installed under the virtual environment. The number of operating systems is generally only restricted by hardware capacity.

The presence of other guest OS can be completely transparent to any single OS. Each OS "thinks" it is working with a normal CPU, memory, hard disk, and network link. The guest OS can be networked together or they may be able to share data directly through the hypervisor, though this is not commonly done for security reasons.

Hypervisor

Some of the main functions of the hypervisor are as follows:

- Assign resources to each guest OS. For example, in a desktop VM, if the host computer has 4 GB memory, at least 1 GB will be required by the host OS, leaving 3 GB to assign to each guest OS; you could have three guests, each configured with 1 GB for instance.
- Configure disk images and snapshots - a guest OS is stored in an image file. The single file represents all the data stored on the guest OS's hard disk. Disk images can be used as templates to set up new VMs quickly. A snapshot (or differencing disk) is a copy of the disk image at a certain point-in-time. Snapshots can be used to rollback changes made during a session.



Each hypervisor solution uses different hard disk image file formats. Some formats can be converted however.

- Configure networking - a hypervisor will be able to create a virtual network environment where all the guest OS can communicate. It will also be able to create a network shared by the host and by guest OS on the same host and on other hosts. Enterprise virtual platforms allow the configuration of virtual switches and routers.
- Security - ensure that guest OS are "contained" or "sandboxed" and cannot access other guest OS or the host except through authorized mechanisms. This is important to prevent data "leaking" from one VM to another, to prevent one compromised VM from compromising others, and to prevent malware from spreading between VMs or from a VM to the host.

Host versus Bare Metal Hypervisors

One basic distinction that can be made between virtual platforms is between host and bare metal methods.

In a **host-based (or desktop)** system, the hypervisor is itself installed onto a **host operating system**. Examples of host-based hypervisors include VMware Workstation, Oracle VirtualBox, and Parallels Workstation. The hypervisor software must support the host OS (for example, VMware Workstation can be installed under Windows or Linux while Microsoft's Virtual PC can only be installed under Windows).

A **bare metal** virtual platform means that the hypervisor is installed directly onto the computer. Examples include VMware ESX Server, Microsoft's Hyper-V, and Citrix's XEN Server. The hardware need only support the base system requirements for the hypervisor plus resources for the type and number of guest OS that will be installed.



If the hypervisor is running in a 64-bit environment, 32-bit guest OS can still be installed (providing the hypervisor supports them). 32-bit hypervisors will not support 64-bit OS however.

Processor Support

As virtualization solutions have become more popular, CPU vendors have built special instruction sets to facilitate running virtualization. The Intel technology for this is called VT (Virtualization Technology) while AMD call it AMD-V.

Some virtualization software *requires* a CPU with virtualization support enabled and performance of the VMs will be severely impaired if virtualization is not supported in hardware. Some cheaper CPU models ship without the feature and sometimes the feature is disabled in the BIOS. If specifying a computer that will be used, check the CPU specification carefully to confirm that it supports Intel VT or AMD-V.

Virtual Platform Applications

Any type of OS can be virtualized. This includes client OS and server NOS. Some hypervisors have limited support for certain operating systems. For example, Microsoft Virtual PC does not provide any official support for installing Linux as a guest OS.

There are also many different reasons for deploying a virtual platform.

Desktop Virtual Platforms

Desktop virtual platforms, based on some sort of host-based hypervisor, are unlikely to provide good performance. They are typically used for testing and development:

- Virtual labs - create a research lab to analyze viruses, worms, and Trojans. As the malware is contained within the guest OS, it cannot infect the researcher's computer or network. This is also referred to as a **sandbox**.
- Support legacy software applications - if the host computers have been upgraded, software may not work well with the new operating system. In this scenario, the old OS can be installed as a VM and the application software accessed using the VM.
- Development environment - test software applications under different OS and resource constraints. A VM can also be used to test **patch compatibility** to ensure an OS or application vendor's updates do not cause problems with other applications.
- Security control testing - use the VM environment to test security controls, such as firewalls, IDS, anti-malware, network access control, and data loss prevention.
- Training - lab environments can be set up so that students can practice using a live operating system and software without impacting the production environment. At the end of the lab, changes to the VM can be discarded so the original environment is available again for the next student to use.

Server Consolidation

Bare metal platforms or server-class host-based hypervisors can fill the same functions as desktop virtual platforms but their main use is better **hardware utilization** through **server consolidation**. In this scenario, a single physical server will host multiple virtual machines, each running a server OS. A virtual machine functioning as a server is known as a **virtual server**.

A typical hardware server may have resource utilization of about 10%. This implies that you could pack the server computer with another 9 server software instances and obtain the same performance.

Virtual Desktop Infrastructure (VDI)

To date, use of virtual platforms has mostly focused on test environments and consolidating server software. **Virtual Desktop Infrastructure (VDI)** refers to using a VM as the "main" environment for corporate desktops.

In a typical VDI, desktop computers are replaced by low-spec, low-power **thin client** computers.

When the thin client starts, it boots a minimal OS allowing the user to log on to a VM stored on the company server infrastructure. The user makes a connection to the VM using some sort of remote desktop protocol (Microsoft Remote Desktop or Citrix ICA for instance). The thin client has to find the correct image and use an appropriate authentication mechanism. There may be a 1:1 mapping based on machine name or IP address or the process of finding an image may be handled by a connection broker.

All application processing and data storage is performed by the server. The thin client computer only has to be powerful enough to display the screen image, play audio, and transfer mouse / key commands and video / audio information over the network.

All data is stored on the server so it is easier to back up and the desktop VMs are easier to support and troubleshoot. They are better "locked" against insecure user practices because any changes to the VM can easily be overwritten from the template image. With VDI, it is also easier for a company to completely off-load their IT infrastructure to a third-party services company.

The main disadvantage is that in the event of a failure in the server and network infrastructure, users have no local processing ability so downtime events may be more costly in terms of lost productivity.

Application Virtualization

Application virtualization is a more limited type of VDI. Rather than run the whole client desktop as a virtual platform, the client either accesses a particular application **hosted** on a server or **streams** the application from the server to the client for local processing.

Most application virtualization solutions are based on Citrix XenApp (formerly MetaFrame / Presentation Server) though Microsoft has developed an App-V product with its Server 2008 range and VMware have their ThinApp product.

Terminal Services

Terminal Services is the "old", pre-virtual platform way of providing hosted applications. A terminal server can host multiple connections from clients to one or more published applications running on the server. Clients can either be ordinary desktops or thin clients. Terminal services architecture is also referred to as **Server Based Computing (SBC)**.

Storage Virtualization

Another element in a virtual platform is **storage virtualization**. In a virtual storage platform, a software layer is inserted between client operating systems and applications and the physical storage medium (a **Storage Area Network [SAN]**). This abstraction makes it easier to expand or shrink storage capacity allocated to any particular client without having to reconfigure the client. It can also simplify operations such as backup, replication, and migration by consolidating data storage in one physical location.

One of the problems in data storage is data duplication. This refers to the way a single data file may get duplicated in multiple locations, through user file copy actions, attaching the file to email, and making backups. Each instance of the file takes up a chunk of storage space.

Data de-duplication refers to techniques to consolidate multiple copies of the same file in a single location. Data de-duplication is greatly facilitated by storage virtualization, as each user reference to a file can point to the same physical file location (without the user having to track where this might be).

Storage virtualization also assists the implementation of tiered storage hierarchies. The principle here is of where to store archived information. An **offline** storage medium might require physical interaction to access the data (such as putting a tape into a drive). **Nearline** storage refers to technology such as tape loaders or "slow" hard disk media that can operate in low-power states.

Virtual Networks

Where multiple virtual machines are running on a single platform, virtualization provides a means for these VMs to communicate with each other and with other computers on the network (both physical and virtual) using standard networking protocols.

The operating system running in each virtual machine is presented with an emulation of a standard hardware platform and for the most part is unaware that it is *not* running on an actual physical machine. Among the hardware devices emulated will be one or more network adapters. The number of adapters and their connectivity can typically be configured within the hypervisor.

Within the virtual machine, the network adapter will look exactly like a real NIC, and will be configurable in exactly the same way. For example, protocols and services can be bound to it and it can be assigned an IP address. However, as the adapter does not actually exist, it is clearly impossible to connect a patch cable directly to it. Instead, the configuration of the hypervisor determines how it is connected.

Typically, a hypervisor will implement network connectivity by means of one or more **virtual switches**. These perform exactly the same function as layer 2 physical switches, except that they are implemented in software rather than hardware. As the virtual machines and the virtual switch are all contained within a single hardware platform, no actual network traffic is generated; instead, data is moved from buffers in one virtual machine to another.

In the hypervisor, it is usually possible to configure the connectivity between the virtual network adapters in the VMs and the virtual switches. This is analogous to connecting patch cables between real computers and real switches. Multiple virtual machines may be connected to the same virtual switch or to separate switches. The number of virtual switches supported varies from one hypervisor to another.

It is also possible to configure connectivity between the host computer's physical network adapters and the virtual switches. This provides a bridge between the virtual switches within the host platform and the physical switches on the network, allowing frames to pass between physical and virtual machines, and between the virtual machines and the host.



When the VMs are allowed to interact with a "real" network, the host must support a high bandwidth, high availability network link. Any failure of the physical link will affect multiple VMs.

Virtualization Best Practices and Risks

Secure and efficient use of virtual platforms is an evolving discipline. Some of the pros and cons and best practices and risks are presented below.

Pros and Cons

As described above, some of the "pros" of server virtualization are better **hardware utilization** and **reduced infrastructure**. Fewer physical servers means less space required to house them, less electricity to run and cool them, and less waste when they are decommissioned. Desktop virtualization allows companies to deploy much lower power **thin clients**, with much lower running costs and environmental impact (though a substantial investment cost).

Virtualization also allows more **centralized administrative control** over IT infrastructure, which should reduce downtime and troubleshooting incidents. It also makes the enforcement of security policies simpler.

Locating the entire IT infrastructure within a single physical "space" can also make **disaster recovery** easier. Providing the VM images have been backed up at an appropriate point and there is no underlying hardware problem, system state can be restored simply by re-applying the backed up image.

One of the advantages of using virtual platforms for research, development, and training is the reduced cost of deploying new applications. Conversely, switching to a virtual desktop infrastructure or complex virtualized server environment may involve substantial investment costs, in terms of hardware, software, and training.

The other cons of deploying virtual machines mostly affect performance and security.

Performance and Host Elasticity

Virtualization only offers more efficient performance if the original server was *underutilized* in the first place. The use of a hypervisor and running an application within a virtual environment will always compare unfavorably to running the application on physical hardware. VMs tend to be used for a single, simple applications, such as web servers, rather than trying to run multiple web servers, messaging servers, and database applications within each guest OS.

If the shared hardware resources on the host are underspecified, because you have multiple servers or desktops contending for the same resources, performance problems will be multiplied across many more servers and desktops than would be the case in a physical network infrastructure. In project management terms, there is less "slack" or "elasticity" available to cope with unforeseen events.

As well as the resources of the server computer, also consider the resources available to the network. Network links, switches, and routers that were previously managing traffic for one server may suddenly have to cope with ten.

As mentioned above, the whole network infrastructure connecting guest OS can also be virtualized, but this still requires substantial processing power and creates an even more vulnerable single point of failure if all this infrastructure is running within a single physical server.

Host Security and Availability

Another key security vulnerability in a virtual platform is that if the host is compromised, then nn guest servers have also been compromised. Host availability represents a **single point of failure**. For example if the CPU on the host crashes, nn guest OS will suddenly go offline.

Another point is that running the host at a constantly high level of utilization could decrease the **Mean Time Between Failure (MTBF)** of its components. The MTBF is the number of hours the manufacturer expects that a component will run before experiencing some sort of hardware problem. If hardware is subjected to greater than expected loads, it may fail more often than expected.

A successful **Denial of Service (DoS)** attack on a host machine, host OS, or hypervisor will cause far more damage to the server infrastructure than a DoS on a single web server. As an example, the undo disks feature of some hypervisors (allowing the user to revert to the saved image after making changes) can be misused to perform DoS (by causing the undo file to grow to the point where it consumes all the available disk space on the host).

These sorts of vulnerability can be mitigated by duplicating the guest OS on a redundant physical server that can be used as a fail-over. This is costly however and keeping the redundant server up-to-date and ready to be deployed can be complex.



Another solution to the problem of host availability and elasticity is to use a cloud computing environment to provide the virtualization services. Cloud computing is discussed later in this unit.

Hypervisor Security

Apart from ensuring the security of each guest OS and the host machine itself, a virtual platform introduces an additional layer for the attention of security analysts; that of the hypervisor.

At the time of writing, there are no known significant exploits but hypervisor software is subject to patches and security advisories like any other software. As the use of virtual platforms grows, hypervisors will increasingly be the target of attacks. This becomes even more complex when the network infrastructure - switches and routers - is also virtualized. Where the network infrastructure is implemented in software, it may not be subject to inspection and troubleshooting by system administrators, who would have to rely entirely on the hypervisor developer for security.

Another issue is **VM escaping**. This refers to malware running on a guest OS jumping to another guest or to the host. To do this, the malware must identify that it is running in a virtual environment, which is usually simple to do. One means of doing so is through a **timing attack**.

The classic timing attack is to send multiple usernames to an authentication server and measure the server response times. An invalid username will usually be rejected very quickly but a valid one will take longer (while the authentication server checks the password). This allows the attacker to harvest valid usernames. Malware can use a timing attack within a guest OS to detect whether it is running in a VM (certain operations may take a distinctive amount of time compared to a "real" environment). There are numerous other "signatures" that an attacker could use to detect the presence of virtualized system hardware.

The next step in VM escaping is for the attacker to compromise the hypervisor. There are not many known instances of successful hypervisor attacks. There have been successful vulnerability exploits in hypervisors, but they were developed against the hypervisors running in the gaming machines Xbox 360 and the PlayStation 3. However, the more mechanisms the hypervisor exposes for sharing data with the host (via a "Shared Folders" feature or access to a disc image for instance) or with other guest OS, the more chances there are for an attack to succeed.

One serious implication of VM escaping is where virtualization is used for hosted applications. If you have a hosted web server, apart from trusting the hosting provider with your data, you have no idea what other applications might be running in other customers' VMs.

For example, consider a scenario where you have an e-commerce web server installed on a virtual server leased from an ISP. If a third-party installs another guest OS with malware that is able to subvert the virtual server's hypervisor, they might be able to gain access to your server or to data held in the memory of the physical server. Having compromised the hypervisor, they could make a copy of your server image and download it to any location.

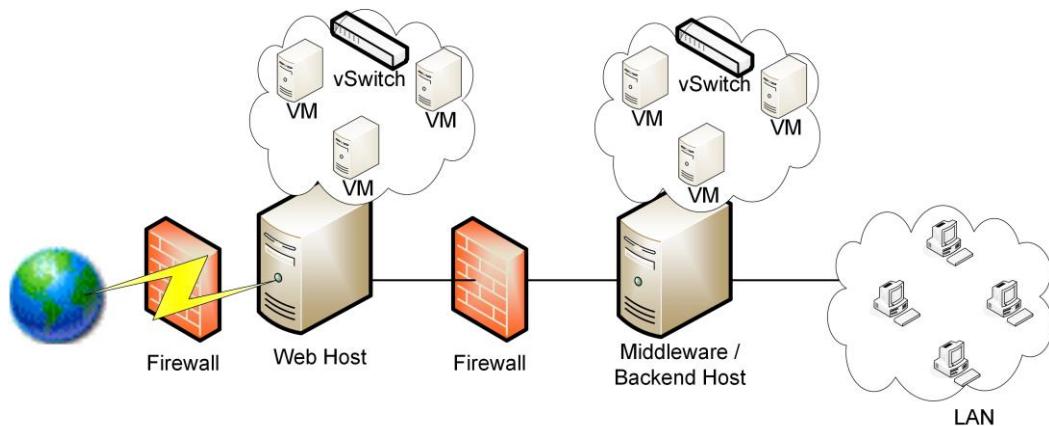
This would allow the attacker to steal any unencrypted data held on the e-commerce server. Even worse, it could conceivably allow them to steal encrypted data, by obtaining the private encryption keys stored on the server or by sniffing unencrypted data or a data encryption key from the physical server's memory.

Physical and Virtual Network Boundaries

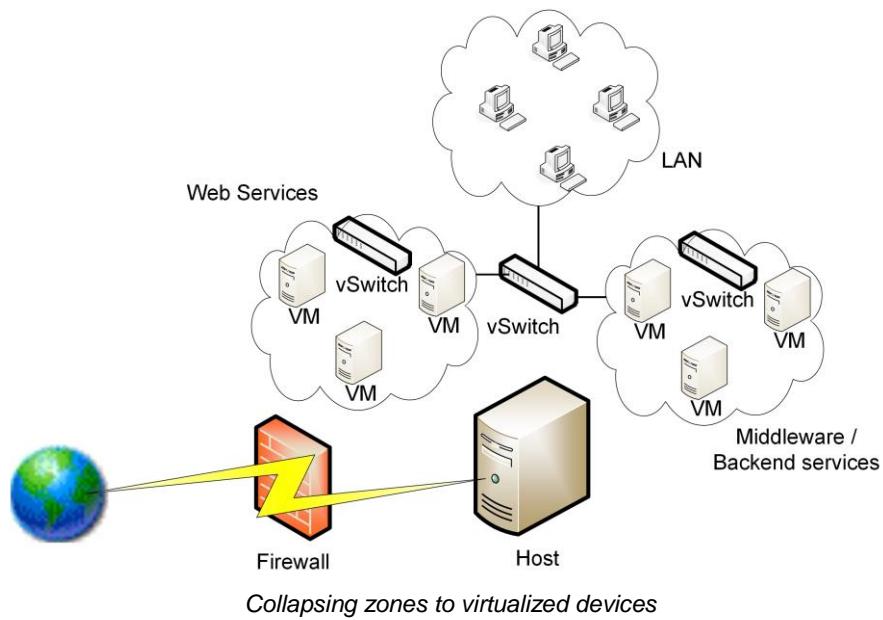
Where front-end and back-end web application servers are deployed on virtual platforms, thought needs to be given to placement of services within or without a DMZ.



Depending on your confidence on the virtual network infrastructure, different services and data that should logically be placed inside and outside a DMZ should not be placed together as VMs on the same hardware (or at least, not on the same physical network adapter).



Isolating VMs in different zones on separate hardware



Guest OS Patch Compatibility and Management

Each guest OS must be patched and protected against viruses and Trojans like any other OS. Patching each guest OS individually has performance implications, so in most environments a new image would be patched and tested then deployed to the production environment. You also need to verify **patch compatibility** with the virtual environment. The hypervisor may use drivers that are not so well supported by the guest OS vendor. The effect of running in a virtual environment may also have an impact on the guest OS and applications so it is even more vital to perform a test deployment of new patches before authorizing them for use in the production network.

Guest OS Security

Running security software (anti-virus and intrusion prevention) on each guest OS can cause performance problems. Solutions for running security applications through the host or hypervisor are developing though.



Ordinary anti-virus software installed on the host will NOT detect viruses infecting the guest OS. Scanning the virtual disks of guest OS from the host will cause serious performance problems.

The process of developing, testing, and deploying images brings about another security concern with virtual platforms. This is the problem of **rogue VMs**; installing unauthorized VMs (in the manner of a Trojan Horse). The uncontrolled deployment of more and more VMs is referred to as "VM Sprawl". It's a lot easier to add a guest OS image to a server than it is to plug a new hardware server into the network!

Virtual system management software can be deployed to detect rogue builds. More generally, the management procedures for developing and deploying machine images need to be tightly drafted and monitored. VMs should conform to an application-specific template with the minimum configuration needed to run that application (that is, not running unnecessary services). Images should not be run in any sort of environment where they could be infected by malware or have any sort of malicious code inserted. One of the biggest concerns here is of rogue developers or contractors installing backdoors or "logic bombs" within a machine image. The problem of criminal or disgruntled staff is obviously one that affects any sort of security environment but concealing code within VM machine images is a bit easier to accomplish and has the potential to be much more destructive.

Cloud Computing



Cloud computing has lots of different definitions but generally refers to any sort of IT infrastructure provided to the end user where the end user is not aware of or responsible for any details of the procurement, implementation, or management of the infrastructure. Its internal workings are a "cloud"; the end user is only interested and pays for the services provided by the cloud.

Among other benefits, cloud computing provides **elasticity**. This means that the cloud can scale to meet peak demand. For example, a company may operate a single web server instance for most of the year but provision additional instances for the busy Christmas period and then release them again in the New Year. This example also illustrates the principle of **pay-per-use**, another key feature of a cloud service (as opposed to a hosted service).

Cloud Deployment

In most cases, the "cloud" (that is, the hardware and/or software hosting the service) will be **offsite** relative to the organization's users, who will require an internet link to access the cloud services.

There can be different ownership and access arrangements for clouds, which can be broadly categorized as follows:

- Public (or multi-tenant) - hosted by a third-party and shared with other subscribers. This is what many people understand by "cloud computing". As a shared resource, there are risks regarding performance and security.
- Hosted Private - hosted by a third-party for the exclusive use of the organization. This is more secure and can guarantee a better level of performance but is correspondingly more expensive.
- Private - cloud infrastructure that is completely private to and owned by the organization. In this case there is likely to be one business unit dedicated to managing the cloud while other business units make use of it.

This type of cloud could be onsite or offsite relative to the other business units. An onsite link can obviously deliver better performance and is less likely to be subject to outages (loss of an internet link for instance). On the other hand, a dedicated offsite facility may provide better shared access for multiple users in different locations.

- Community - this is where several organizations share the costs of either a hosted private or fully private cloud.

There will also be cloud computing solutions that implement some sort of hybrid public / private / community / hosted / onsite / offsite solution. For example, a travel organization may run a sales website for most of the year using a private cloud but "break out" the solution to a public cloud at times when much higher utilization is forecast.

Flexibility is a key advantage of cloud computing but the implications for data risk must be well understood when moving data between private and public storage environments.

Infrastructure as a Service

Infrastructure as a Service (IaaS) is a means of provisioning IT resources such as servers, load balancers, and Storage Area Network (SAN) components quickly. Rather than purchase these components and the internet links they require you rent them on an as-needed basis from the service provider's data center.

Network as a Service (NaaS)

Cloud computing is often thought of as providing server-side solutions (especially CRM and ecommerce). However, as noted above, with VDI pretty much the whole IT desktop infrastructure can be provided on a serviced / leased basis rather than being fully owned.

VDI allows for the complete separation of the user interface from the processing of the operating system and applications. While all input and output occur on the user's desktop, all processing is done on a virtual machine hosted on a server, with input/output data being transferred via the network.

While generally the server hosting the OS and applications will be elsewhere on the corporate LAN, it is also possible for the virtual infrastructure to be hosted by a third party on a server outside the corporate network and the connection to be made via a secured connection across the internet. In this scenario, the organization would not need any onsite IT, apart from thin client devices and the basic network infrastructure required to provide internet connectivity. Such a situation is known as **Network as a Service (NaaS)**.

The advantage of this to the organization is that much less investment in IT hardware is required. The disadvantages are that the internet connection represents a potential single point of failure of the entire IT infrastructure and that a high level of trust must be placed in the third party providing the service.

Software as a Service

Software as a Service is a different model of provisioning software applications. Rather than purchasing software licenses for a given number of seats, a business would access software hosted on a supplier's servers on a pay-as-you-go or lease arrangement (on-demand). Virtual infrastructure allows developers to provision on-demand applications much more quickly than previously. The applications can be developed and tested within the cloud without the need to test and deploy on client computers.

Platform as a Service

Platform as a Service (PaaS) provides resources somewhere between SaaS and IaaS. A typical PaaS solution would provide servers and storage network infrastructure (as per IaaS) but also provide a multi-tier web application / database platform on top. This platform could be based on Oracle or MS SQL or PHP and MySQL.

As distinct from SaaS though, this platform would not be configured to actually do anything. Your own developers would have to create the software (the CRM or ecommerce application) that runs using the platform.

The service provider would be responsible for the integrity and availability of the platform components but you would be responsible for the security of the application you created on the platform.

Operating Systems and Software

Operating Systems

Amazon Machine Images (AMIs) are preconfigured with an ever-growing list of operating systems. We work with our partners and community to provide you with the most choice possible. You are also empowered to use our bundling tools to upload your own operating systems. The operating systems currently available to use with your Amazon EC2 instances include:

Operating Systems		
Red Hat Enterprise Linux	Windows Server	Oracle Enterprise Linux
OpenSolaris	Amazon Linux AMI	Ubuntu Linux
Fedora	Gentoo Linux	Debian
	SUSE Linux Enterprise	

Software

Amazon EC2 enables our partners and customers to build and customize Amazon Machine Images (AMIs) with software based on your needs. We have hundreds of free and paid AMIs available for you to use. A small sampling of the software available for use today within Amazon EC2 includes:

Databases	Batch Processing	Web Hosting
IBM DB2	Hadoop	Apache HTTP
IBM Informix Dynamic Server	Condor	IIS/Asp.Net
Microsoft SQL Server Standard	Open MPI	IBM Lotus Web Content Management
MySQL Enterprise		IBM WebSphere Portal Server
Oracle Database 11g		

Application Development Environments	Application Servers	Video Encoding & Streaming
IBM sMash	IBM WebSphere Application Server	Wowza Media Server Pro
JBoss Enterprise Application Platform	Java Application Server	Windows Media Server
Ruby on Rails	Oracle WebLogic Server	

Amazon's EC2 offers IaaS (Linux or Windows machine images) and PaaS (database and application development environments)

Risks of Cloud Computing



As with any contracted service, cloud computing is a means of transferring risk. As such, it is imperative to identify precisely which risks you are transferring; to identify which responsibilities the service provider is undertaking and which remain with you. This should be set out in a Service Level Agreement (SLA).

For example, in an SaaS solution, the provider may be responsible for the confidentiality, integrity, and availability of the software. They would be responsible for configuring a fault tolerant, clustered server service, for firewalls the servers and creating proper authentication, authorization, and accounting procedures, for scanning for intrusions and monitoring network logs, applying OS and software patches, and so on. You might or might not be responsible for some or all of the software management functions though - ensuring that administrators and users practice good password management, configuring system privileges, making backups of data, and so on.

Where critical tasks are the responsibility of the service provider, you should try to ensure that there is a reporting mechanism to show that these tasks are being completed, that their disaster recovery plans are effective, and so on.

Another proviso is that your company is likely to still be directly liable for serious security breaches. If customer data is stolen for instance or if your hosted website is hacked and used to distribute malware. The legal and regulatory "buck" still stops with you; you might be able to sue the service provider for damages, but your company would still be the point of investigation. You may also need to consider the legal implications of using a cloud provider if their servers are located in a different country.

You also have to consider the risk of insider threat, where the insiders are administrators working for the service provider. Without effective security mechanisms such as separation of duties and M of N control, it is highly likely that they would be able to gain privileged access to your data. Consequently, the service provider must be able to demonstrate to your satisfaction that they are prevented from doing so. There is also the risk described above that your data is in proximity to other, unknown virtual servers and that some sort of attack could be launched on your data from another virtual server.

As with any contracted service, with any *aaS solution you place a large amount of trust in the service provider. The more important the service is to your business, the more risk you are investing in that trust relationship.



Review Questions / Module 4 / Unit 5 / Virtualization and Cloud Security

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What is a hypervisor?
- 2) What methods can be used to allow communications between VMs and the host?
- 3) What term is used to describe a computing architecture where thin clients are used to access images of client operating systems stored on a server?
- 4) What is server consolidation?
- 5) Why might virtualization support faster deployment of applications?
- 6) What is the risk of VM escaping?
- 7) What is a snapshot?
- 8) What is meant by a public cloud?
- 9) What type of cloud solution would be used to implement a SAN?
- 10) Describe some key considerations that should be made when hosting data or systems via a cloud solutions provider.



If you have access to the Hands On Live Labs, complete the "Network Security / Cloud Computing" lab now.

Module 4 / Summary

Host, Data, and Application Security

In this module, you also learned about hardening clients and servers and enforcing data security. You also learned about web and file transfer protocols and the risks involved in implementing web applications and cloud services.

Module 4 / Unit 1 / Host Security

- OS hardening means configuring services, protocols, file system (access control), and updates.
- Networks and servers should only run essential services and protocols. Unused but enabled and overlooked services are potential vulnerabilities.
- Software configuration baselines and templates can be used to deploy new servers securely.
- Network Access Control can be deployed to verify the security status of hosts (patch level, anti-virus and firewall configuration, and so on) before or while they are connected to the network.

Module 4 / Unit 2 / Data Security

- Information should be classified and labeled and handled in accordance with policies, procedures, and guidance.
- Encryption can be used to protect data in different states (at-rest, in-transit, and in-use). Encryption can be applied at disk/device or file/database level or to network transports.
- DLP software can prevent the unauthorized use of confidential data by matching sensitive information to a protection profile, which could restrict users from copying or printing it.
- Backups are an essential part of data security. Backups are made according to a schedule to balance backup and restore time with availability and cost of media. The backup schedule should also account for offsite storage of critical data.

Module 4 / Unit 3 / Web Services Security

- HTTP services can be secured using SSL / TLS, which relies on PKI certificates for authentication and confidentiality.
- Web servers are popular targets for attack. Correct configuration and placement on the network is vital.
- FTP is used for file transfer over the internet but only supports secure transfer in conjunction with another protocol, such as SSH or SSL.

Module 4 / Unit 4 / Web Application Security

- Application and scripting technologies can be used to enhance websites but create security vulnerabilities if not designed and implemented properly.
- Web browsers are popular targets for attack. Security settings should be configured to prevent scripting exploits and application updates should be applied promptly.

Module 4 / Unit 5 / Virtualization and Cloud Security

- Virtualization offers hardware cost savings and simplified deployment but significant management and monitoring challenges.
- Cloud computing allows the lease of infrastructure and software on an as-needed basis but carries the same risks as other contracted services.

Module 5 / Operational Security

The following CompTIA Security+ domain objectives and examples are covered in this module:

Domain Objectives/Examples	Refer To
2.7 Compare and contrast physical security and environmental controls <i>Environmental controls (HVAC, Fire suppression, EMI shielding, Hot and cold aisles, Environmental monitoring, Temperature and humidity controls) • Physical security (Hardware locks, Mantraps, Video Surveillance, Fencing, Proximity readers, Access list, Proper lighting, Signs, Guards, Barricades, Biometrics, Protected distribution [cabling], Alarms, Motion detection)</i>	Unit 5.1 Site Security
2.9 Given a scenario, select the appropriate control to meet the goals of security <i>Safety (Fencing, Lighting, Locks, CCTV, Escape plans, Drills, Escape routes, Testing controls)</i>	
3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques <i>Detection controls vs. prevention controls (Camera vs. guard)</i>	
4.3 Given a scenario, select the appropriate solution to establish host security <i>Hardware security (Cable locks, Safe, Locking cabinets)</i>	
3.4 Explain types of wireless attacks <i>Bluejacking • Bluesnarfing • Near Field Communication</i>	Unit 5.2 Mobile / Embedded Device Security
4.2 Summarize mobile security concepts and technologies <i>Device security (Full device encryption, Remote wiping, Lockout, Screen-locks, GPS, Application control, Storage segmentation, Asset tracking, Inventory control, Mobile device management, Device access control, Removable storage, Disabling unused features) • Application security (Key management, Credential management, Authentication, Geotagging, Encryption, Application whitelisting, Transitive trust/authentication) • BYOD concerns (Data ownership, Support ownership, Patch management, Antivirus management, Forensics, Privacy, On-boarding/off-boarding, Adherence to corporate policies, User acceptance, Architecture/infrastructure considerations, Legal concerns, Acceptable use policy, On-board camera/video)</i>	
4.5 Compare and contrast alternative methods to mitigate security risks in static environments <i>Environments (SCADA, Embedded (Printer, Smart TV, HVAC control), Android, iOS, Mainframe, Game consoles, In-vehicle computing systems) • Methods (Network segmentation, Security layers, Application firewalls, Manual updates, Firmware version control, Wrappers, Control redundancy and diversity)</i>	
2.1 Explain the importance of risk related concepts <i>Risk calculation (Likelihood, ALE, Impact, SLE, ARO, MTTR, MTTF, MTBF) • Quantitative vs. qualitative • Probability / threat likelihood • Risk-avoidance, transference, acceptance, mitigation, deterrence • Recovery time objective and recovery point objective</i>	Unit 5.3 Risk Management
2.2 Summarize the security implications of integrating systems and data with third parties <i>On-boarding/off-boarding business partners • Social media networks and/or applications • Interoperability agreements (SLA, BPA, MOU, ISA) • Privacy considerations • Risk awareness • Unauthorized data sharing • Data ownership • Data backups • Follow security policy and procedures • Review agreement requirements to verify compliance and performance standards</i>	

Domain Objectives/Examples	Refer To
<p>2.3 Given a scenario, implement appropriate risk mitigation strategies <i>Change management • Perform routine audits</i></p>	Unit 5.3 Risk Management
<p>2.8 Summarize risk management best practices <i>Business continuity concepts (Business Impact Analysis, Identification of critical systems and components, Business continuity planning and testing, Risk assessment, Continuity of operations, High availability)</i></p>	
<p>3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques <i>Security posture (Initial baseline configuration, Continuous security monitoring, Remediation)</i></p>	
<p>3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities <i>Risk calculations (Threat vs. Likelihood) • Assessment types (Risk • Threat • Vulnerability)</i></p>	
<p>2.8 Summarize risk management best practices <i>Business continuity concepts (Removing single points of failure, Disaster recovery, IT contingency planning, Succession planning, Redundancy, Tabletop exercises) • Fault tolerance (Hardware, RAID, Clustering, Load balancing, Servers) • Disaster recovery concepts (Cold site, Hot site, Warm site)</i></p>	Unit 5.4 Disaster Recovery
<p>2.9 Given a scenario, select the appropriate control to meet the goals of security <i>Availability (Redundancy, Fault tolerance)</i></p>	
<p>2.3 Given a scenario, implement appropriate risk mitigation strategies <i>Incident management</i></p>	Unit 5.5 Incident Response
<p>2.4 Given a scenario, implement basic forensic procedures <i>Order of volatility • Capture system image • Network traffic and logs • Capture video • Record time offset • Take hashes • Screenshots • Witnesses • Track man hours and expense • Chain of custody • Big Data analysis</i></p>	Unit 5.5 Incident Response and Forensics
<p>2.5 Summarize common incident response procedures <i>Preparation • Incident identification • Escalation and notification • Mitigation steps • Lessons learned • Reporting • Recovery/reconstitution procedures • First responder • Incident isolation (Quarantine, Device removal) • Data breach • Damage and loss control</i></p>	
<p>2.1 Explain the importance of risk related concepts <i>Importance of policies in reducing risk (Privacy policy, Acceptable use, Security policy, Mandatory vacations, Job rotation, Separation of duties)</i></p>	Unit 5.6 Security Policies and Training
<p>2.6 Explain the importance of security related awareness and training <i>Security policy training and procedures • Role-based training • Compliance with laws, best practices and standards • User habits (Password behaviors, Clean desk policies, Prevent tailgating, Personally owned devices) • New threats and new security trends/alerts (New viruses, Phishing attacks, Zero-day exploits) • Use of social networking and P2P • Follow up and gather training metrics to validate compliance and security posture</i></p>	
<p>5.2 Given a scenario, select the appropriate authentication, authorization or access control <i>Authorization (Separation of duties)</i></p>	

Module 5 / Unit 1

Site Security

Objectives

On completion of this unit, you will be able to:

- Describe the use of physical security controls in planning and implementing site security.
- Identify the key features of environmental and fire suppression systems that impact security.

Site Layout and Access



6nu4x

Physical access controls depend on the same access control fundamentals as network or operating system security:

- Authentication - create access lists and identification mechanisms to allow approved persons through the barriers.
- Authorization - create barriers around a resource so that access can be controlled through defined access points.
- Accounting - keep a record of when access points are used and detect security breaches.

Physical security mechanisms are expensive. The cost of controls needs to be balanced against risk.

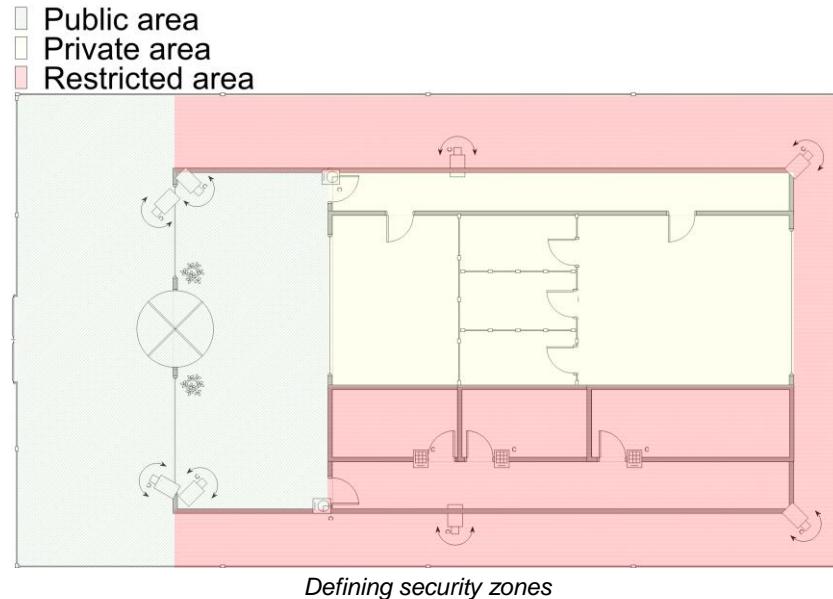
Security Zones

Physical security can be thought of in terms of **zones**. Each zone should be separated by its own **barrier(s)**. **Access points** through the barriers need to be controlled by one or more security mechanisms. Progression through each zone should be progressively more restricted.

The number of zones will depend on the size of the site and the type of operations that take place there, but you could categorize the following general areas:

- External - the areas outside the premises. It may be difficult to control these areas, with security mechanisms limited to surveillance.

- Perimeter - for a single site, this will be the walls of the building itself. A large site with many buildings will have an outer perimeter (fencing) and then inner perimeters for each building. Many businesses will share premises with other companies, in which case access to the building and monitoring of common parts is likely to be the responsibility of the landlord or building management company. A critical point in the perimeter is any location where voice and data cabling enter.
- Public - these are areas of the building where guests are invited, deliveries accepted, and so on. Public zones are typically high traffic (that is, people move through them frequently).
- Restricted - these are areas where most employees work. Guests may be invited into these zones, if they are subject to the proper controls. Depending on the level of security, it may or may not be appropriate to control the movement of employees between restricted zones.
- Secure - these are areas where access is strictly limited because they contain critical systems or confidential data.



You can also think of the access control models (discretionary, mandatory, and role-based) in terms of thinking how access to zones should operate. You may also think of access to zones operating in terms of security clearance levels and secure domains.

ID Badges and Access Lists

A photographic **ID badge** showing name and (perhaps) access details is one of the cornerstones of building security. Anyone moving through secure areas of a building should be wearing an ID badge; anyone without an ID badge should be challenged.

An **access list** held at each secure gateway records who is allowed to enter. This might be enforced by a security guard. As another option, badges can also be combined with passcode, smart card, or biometric information to authenticate at gateways.

Barricades and Access Points

A **barricade** is something that prevents access. As with any security system, no barricade is completely effective; a wall may be climbed or a lock may be picked, for instance. The purpose of barricades is to channel people through defined **access points**. Each access point should have an **authentication** mechanism so that only authorized persons are allowed through. Effective **surveillance** mechanisms ensure that attempts to penetrate a barricade by other means are detected.



Sites where there is a risk of terrorist attack will use barricades such as bollards and security posts to prevent vehicles from approaching to closely to a building.

Site Layout and Signs

In existing premises, there will not be much scope to influence site layout. However, given constraints of cost and existing infrastructure, try to plan the site using the following principles:

- Locate secure zones as deep within the building as possible, avoiding external walls, doors, and windows.
- Position public access areas so that guests do not pass near secure zones. Security mechanisms in public areas should be high visibility, to increase deterrence. Use signs and warnings to enforce the idea that security is tightly controlled. Conversely, access points to secure zones should be discreet. Do not allow an intruder the opportunity to inspect security mechanisms protecting such zones (or even to know where they are).
- Try to minimize traffic having to pass between zones. The flow of people should be "in and out" rather than "across and between".
- Make high traffic public areas high visibility, so that covert use of gateways, network access ports, and computer equipment is hindered and surveillance is simplified.
- In secure zones, do not position display screens or input devices facing towards pathways or windows. Alternatively, use one-way glass so that no-one can look in through windows.

Fencing

The exterior of a building may be protected by **fencing**. Security fencing needs to be transparent (so that guards can see any attempt to penetrate it), robust (so that it is difficult to cut), and secure against climbing (which is generally achieved by making it high and possibly by using razor wire).

Fencing is generally effective but the drawback is that it gives a building an intimidating appearance. Buildings that are used by companies to welcome customers or the public may use more discreet security methods.

Gateways and Locks

One of the oldest types of security is a wall with a door in it (or a fence with a gate). In order to secure such a **gateway**, it must be fitted with a **lock** (or **door access system**).

Gateway Locks

Locks can be categorized as follows:

- Conventional - a conventional lock prevents the door handle from being operated without the use of a key. More expensive types offer greater resistance against lock picking.
- Deadbolt - this is a bolt on the frame of the door, separate to the handle mechanism.
- Electronic - rather than a key, the lock is operated by entering a PIN on an electronic keypad. This type of lock is also referred to as cipher, combination, or keyless.



CodeLock keyless digital lock

- Token-based - a smart lock may be opened using a magnetic swipe card or feature a proximity reader to detect the presence of a wireless key fob or one-time password generator (physical tokens) or smart card.



Panasonic Iris Recognition Camera System

- Biometric - a lock may be integrated with a biometric scanner.
- Multifactor - a lock may combine different methods (for example, smart card with PIN).



See [Unit 2.4](#) for a full description of token-based, smart card, and biometric recognition technologies.

A secure gateway will normally be self-closing and self-locking, rather than depending on the user to close and lock it.

Turnstiles and Mantraps

Apart from being vulnerable to lock picking, the main problem with a simple door or fence as an entry mechanism is that it cannot accurately record who has entered or left an area. Multiple people may pass through the gateway at the same time; a user may hold a door open for the next person; an unauthorized user may "tailgate" behind an authorized user.

This risk may be mitigated by installing a **turnstile** (a type of gateway that only allows one person through at a time). The other option is to add some sort of surveillance on the gateway. Where security is critical and cost is no object, a **mantrap** could be deployed. A mantrap is where one gateway leads to an enclosed space protected by another barrier. Mantraps can operate in a number of modes:

- All doors normally unlocked - opening one door causes the other to lock.
- All doors normally locked - unlocking one door prevents the other from being unlocked.
- One door locked / other unlocked - when one door is open the other cannot be unlocked.

Another consideration is how secure the construction of a wall, fence, or door is. It may be necessary to use materials that can withstand determined attack (bulletproof glass or doors with reinforced hinges for instance).

As well as authorized gateways (such as gates and doors) consider the security of entry points that could be misused, such as emergency exits, windows, hatches, grilles, and so on. These may be fitted with bars, locks, or alarms to prevent intrusion. Also consider pathways above and below, such as false ceilings and ducting.

Fail-safe and Fail-secure Locks

A traditional mechanical lock is operated using a key. An **electromagnetic** lock requires a power-source to operate. Some locks are battery-powered but most run from mains power.

Electromagnetic locks may be designed to be either **fail-safe** (or fail-open) or **fail-secure**. A fail-safe lock means that the gateway will be open if the lock fails; a fail-secure lock means that the gateway will not be openable. For example, if the power fails, then a door with a fail-safe lock will become open.

An example of a fail-secure lock is that of a safe that "deadlocks" in the event of an alarm being triggered or the power being lost. This should not present any hazard to human health as the safe should not be occupied. Gateways for any sort of occupied area of a building can only be made one-way fail-secure (that is, they may prevent entry but they must not prevent egress) as otherwise they would be lethal in the event of an emergency such as fire, flood, or earthquake. Fail-secure locks for occupied areas (designed for use on fire doors etc) would come with a **manual bypass** on the inside. Of course, in an emergency fire teams need to be able to access all areas of a building safely so fail-secure locks must still be deployed with care. The use of locks must conform to local fire codes and expert advice should be sought when designing the building security system.

Alarm Systems

Alarms are another fairly standard type of security. There are three main types:

- Circuit - a circuit-based alarm sounds when the circuit is opened or closed, depending on the type of alarm. This could be caused by a door or window opening or by a fence being cut. A closed-circuit alarm is more secure because an open circuit alarm can be defeated by cutting the circuit.



Motion detector

- Motion detection - a motion-based alarm is linked to a detector triggered by any movement within a largish area, such as a room. These detectors are either radio reflection (similar to radar) or passive infrared.
- Duress - this type of alarm is triggered manually by staff if they come under threat. There are many ways of implementing this type of alarm, including wireless pendants and concealed sensors or triggers. Some electronic entry locks can also be programmed with a duress code that is different to the ordinary access code. This will open the gateway but also alert security personnel that the lock has been operated under duress.

Circuit-based alarms are typically suited for use at the perimeter and on windows and doors. These may register when a gateway is opened without using the lock mechanism properly or when a gateway is held open for longer than a defined period. Motion detectors are useful for controlling access to spaces that are not normally used. Duress alarms are useful for exposed staff in public areas.

An alarm might simply sound an alert or it may be linked to a monitoring system. Many alarms are linked directly to local law enforcement or to third-party security companies. A **silent alarm** alerts security personnel rather than sounding an audible alarm.

Alarms can be defeated by sophisticated methods of breaking and entering. The other main problem is the incidence of false alarms, where the alarm is either triggered by mistake or activates mistakenly (for example, a motion detector triggered by an air conditioning system). Usability and accessibility needs to be balanced against security and sensitivity.



Surveillance

Surveillance is typically a second layer of security designed to improve the resilience of perimeter gateways. Surveillance may be focused on perimeter areas or within security zones themselves.

Guard Dogs



Guard dog

Dogs have long been an effective means of intrusion detection and deterrence. The drawback is expense; good guard dogs need experienced trainers and handlers. The use of guard dogs may also give visitors an intimidating impression of the company, which may or may not be useful, depending on the type of business.

Security Guards

Again, the visible presence of guards is a very effective intrusion detection and deterrence mechanism, but is correspondingly expensive. It may also not be possible to place security guards within certain zones because they cannot be granted an appropriate security clearance. Training and screening of security guards is imperative.

Video Surveillance and CCTV

CCTV (Closed Circuit Television) is a cheaper means of providing surveillance than maintaining separate guards at each gateway or zone, though still not cheap to set up if the infrastructure is not already in place in the premises. It is also quite an effective deterrent.



Panasonic mini-dome CCTV

The other big advantage is that movement and access can be recorded. The main drawback is that response times are longer and security may be compromised if not enough staff are in place to monitor the camera feeds.

A camera is either fixed or can be operated using Pan-Tilt-Zoom (PTZ) controls. The main properties of cameras are:

- Focal length - shorter focal length gives a wider angle.
- Depth of field - the portion of the image that is in focus. A long depth of field gives an image of a larger area but may not capture sufficient detail (faces). A camera with zoom control allows the depth of field to be changed by the operator.
- Illumination requirements - a camera may not be able to record clear images if there is no light source (or very low light). If the ambient light changes, the camera exposure must be adjustable (some cameras can automatically adjust for exposure level). Most types of digital CCTV sensors can detect infrared (IR) light so an area could be illuminated using IR lamps rather than conventional lighting.

Different cameras suit different purposes. If you want to record the image of every person entering through a door, a fixed, narrow focal length camera positioned on the doorway will be perfectly adequate. If you want to survey a large room and pick out individual faces, a camera with PTZ is required.

Modern CCTV cameras use either CCD or CMOS sensors; the same type as are used in digital cameras and camcorders.

The cameras in a CCTV network are typically connected to a multiplexer using coaxial cabling. The multiplexer can then display images from the cameras on one or more screens, allow the operator to control camera functions, and record the images to tape or hard drive. Newer camera systems may be linked in an IP network, using regular data cabling.



If you consider control types, a security guard is a preventive control, as the guard can both discover and act to prevent an attack. A camera is a detective control only.

Lighting

Security lighting is enormously important in contributing to the perception that a building is safe and secure at night. Well-designed lighting helps to make people feel safe, especially in public areas or enclosed spaces, such as car parks. Security lighting also acts as a deterrent by making intrusion more difficult and surveillance (whether by camera or guard) easier.

The lighting design needs to take account of overall light levels (illuminance), the lighting of particular surfaces or areas (allowing cameras to perform facial recognition for instance), and avoiding areas of shadow and glare.

Physical Access Logs / Lists

An electronic lock may be able to log access attempts or a security guard can manually log movement. At the lowest end, a sign-in and sign-out sheet can be used to record authorized access.

Staff

The cheapest form of surveillance is to leverage ordinary employees to provide it. Security policies should explain staff responsibilities and define reporting mechanisms.

One of the most important parts of surveillance is the **challenge** policy. This sets out what type of response is appropriate in given situations and helps to defeat **social engineering** attacks. This must be communicated to and understood by staff. Challenges represent a whole range of different contact situations. For example:

- Challenging visitors who do not have ID badges or are moving about unaccompanied.
- Insisting that proper authentication is completed at gateways, even if this means inconveniencing staff members (no matter how senior!)
- Intruders and/or security guards may be armed. The safety of staff and compliance with local laws has to be balanced against the imperative to protect the company's other resources.

It is much easier for employees to use secure behavior in these situations if they know that their actions are conforming to a standard of behavior that has been agreed and is expected of them.

Testing Controls

Software-based security controls can be tested using penetration testing software suites and techniques. Physical security controls, plus the effectiveness of administrative controls, such as procedures to deter social engineering, can be even more challenging to test effectively. Drills could be set up to perform simulated attacks, to try to get access to a building for instance or obtain information from staff.



See [Unit 1.4](#) for more information about vulnerability assessments and pentests.

There should be a rigorous inspection regimen to ensure that barriers, locks, alarms, and monitoring systems are intact and show no signs of tampering.

Hardware Security



As well as access to the site, physical security can be used for network appliances and cabling.

Cable Locks and Locking Cabinets

The most vulnerable point of the network infrastructure will be the communications room. This should be subject to the most stringent access and surveillance controls that can be afforded.

Another layer of security can be provided by installing equipment within **lockable rack cabinets**. These can be supplied with key-operated or electronic locks.

If installing equipment within a cabinet is not an option, it is also possible to obtain **cable hardware locks** for use with portable devices such as laptops.



HP rack cabinet with key-operated lock



Kensington cable lock installed on an HP laptop docking station

Safes

Portable devices and media (backup tapes or USB media storing encryption keys for instance) may be stored in a **safe**. Safes can feature key-operated or combination locks but are more likely to come with electronic locking mechanisms.

Safes can be rated to a particular cash value for the contents against various international grading schemes. There are also fire safes that give a certain level of protection against exposure to smoke and flame and to water penetration (from fire extinguishing efforts).

Protected Distribution

As well as the switches, routers, and servers housed in equipment cabinets, thought needs to be given to cabling. A physically secure cabled network is referred to as a **Protected Distribution System (PDS)**. There are two principal risks:

- An intruder could attach eavesdropping equipment to the cable (a **tap**).
- An intruder could cut the cable (Denial of Service).

A hardened PDS is one where all cabling is routed through sealed metal conduit and subject to periodic visual inspection. Lower grade options are to use different materials for the conduit (plastic for instance). Another option is to install an alarm system within the cable conduit, so that intrusions can be detected automatically.

Environmental Controls



Oiyml



kv25t

Environmental security means maintaining a climate that is not damaging to electronic systems (or staff!) and ensuring stable supply of power.

Site Location

In terms of choosing the location of a new site, the following factors are important security considerations:

Accessibility

A geographically remote site has advantages in terms of deterring and detecting intruders. It is much easier to detect suspicious activity in a quiet, remote environment than it is in a busy, urban one.

On the other hand, a remote location carries risks. Infrastructure (electricity, heating, water, telecommunications, and transport links) may not be as reliable and require longer to repair.

Natural Disaster Hazards

In many locations, flooding is the most commonly encountered natural disaster hazard. Rising sea levels mean that previously safe areas can become subject to flood risks within just a few years.

Without spending a lot of money on a solution, common-sense measures can be taken to minimize the impact of flood. If possible, the computer equipment and cabling should be positioned above the ground floor and away from major plumbing.

Certain local areas may also be subject to specific known hazards, such as earthquakes, volcanoes, and storms.

Natural disaster risks such as this can often be mitigated by building designs that have been developed to cope with local conditions.

Dust

Dust can damage computer components with moving parts or openings, such as floppy drives, tape drives, and fans. If a layer of dust builds up on components, it can contribute to overheating.

Dust can be controlled by periodic cleaning but this will involve switching the server off. Fans and vents can be fitted with filters to remove dust, but these require periodic cleaning or replacement. A costlier solution is to provide for air filters as part of the air conditioning system.

As with any computer system, ensure that any unused adapter slots or drive bays on the server case are covered by blanking plates.

It is also best not to carpet the floor in the server room, as this generates more dust and can increase the risk of ESD damage.

Temperature and Humidity

It is highly beneficial to install servers and network equipment in a dedicated room or area. This can be isolated from the rest of the premises for security and also helps to control the environmental conditions around the server equipment. Servers and other networking equipment are often housed in a purpose-built building (a data center).

Servers generate quite a large amount of heat. To cool the inside of the server, fans draw (cool) air from vents in the front of the case and blow it out (warm) through exhausts in the back.

If installed in a smallish room, the fans will warm the air making it difficult to cool the server efficiently (the fans will be drawing in warm air).

An environment that is too warm will raise the chances of system components overheating and failing. An environment that is too cold can cause stress on components with moving parts (such as hard drives and fans) and is more susceptible to static damage (ESD).



Data center

Also, the temperature in the server room should not be allowed to vary by too much. Temperature variations could cause condensation and, if extreme enough, cause components to expand or contract. Over time, connectors can work free from their sockets (chip creep) and cause errors.

A humid environment runs the risk of condensation forming on components, which can lead to short circuits or corrosion. A low humidity environment greatly increases the chance of ESD.

Ideally, use a thermostatically controlled environment to keep the temperature to around 20-22°C (68-70°F) and relative humidity to around 50%. Temperature and humidity monitors should be used to keep the environment constant. These are usually installed as part of a **Heating, Ventilation, and Air Conditioning (HVAC)** system.



Some data centers (notably those operated by Google) are allowing higher temperatures (up to around 26°C / 80°F). This can achieve significant energy cost savings and modern electronics is proving reliable at this temperature.

HVAC (Heating, Ventilation, Air Conditioning)

Building control systems maintain an optimum working environment for different parts of the building. The acronym **HVAC (Heating, Ventilation, Air Conditioning)** is often used to describe these services. For general office areas, this basically means heating and cooling; for other areas different aspects of climate control, such as humidity may be important.

HVAC ensures adequate cooling and humidity and dust control within a room or other enclosed space. All air flow into and out of the room is run through ducts, fans, and filters and warmed or cooled to the correct temperature and humidity.

A server or equipment room should also provide decent air flow around the server equipment. Air flow is provided by ensuring enough space (at least 3 feet or 1 meter) around the server or rack. Obviously, air conditioning vents should not be blocked by racks or equipment. Where possible, the space should not be exposed to direct sunlight.



The server room should not be used as storage space. Do not leave boxes or unused equipment in it. Also, do not install unnecessary devices that generate a lot of heat, such as printers.

The heat generated by equipment per hour is measured in British Thermal Units (BTU) or Kilowatts (KW). 1 KW is 3412 BTU. To calculate the cooling requirement for an air conditioning system, multiply the wattage of all equipment in the room (including lighting) by 3.41 to get the BTU/hour. If the server room is occupied (unlikely in most cases), add 400 BTU/person. The air conditioner's BTU-rating must exceed this total value.



Low-end air conditioning systems are usually rated between 5000 and 10000 BTU. Larger units may be rated by tonnage. One ton of load is 12000 BTU/hour.

When using an air conditioning system, ensure that it is inspected and maintained periodically. Systems may be fitted with alarms to alert staff to problems. Highly mission-critical systems may require a backup air conditioning system.

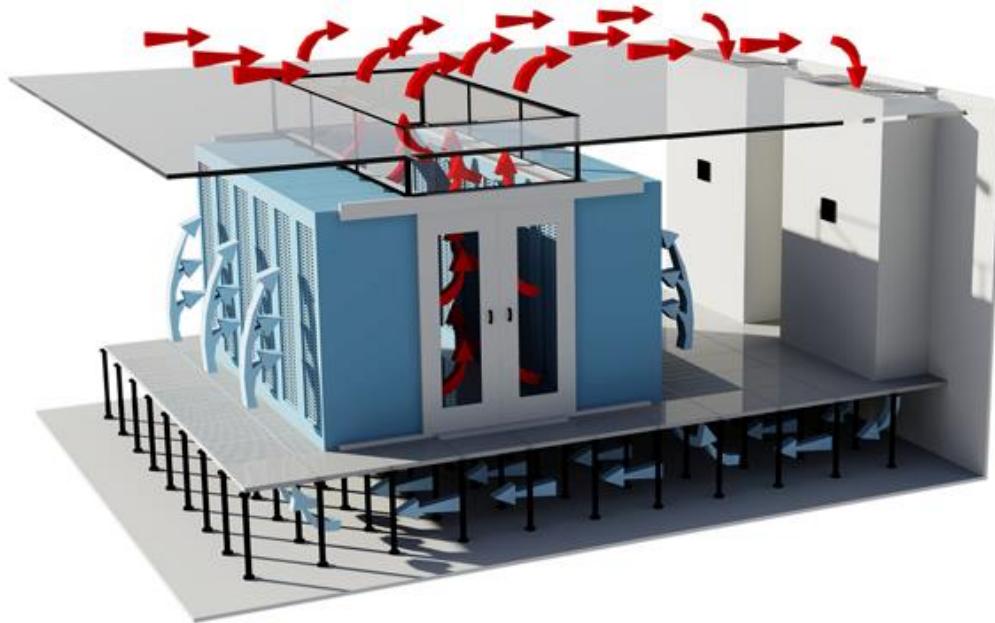


Use a portable monitor to verify that the HVAC's temperature and humidity sensors are returning the correct readings.



Hot and Cold Aisles

A data center or server room should be designed in such a way as to maximize air flow across the server or racks. If multiple racks are used, install equipment so that servers are placed back-to-back not front-to-back, so that the warm exhaust from one bank of servers is not forming the air intake for another bank. This is referred to as a **hot aisle / cold aisle** arrangement. In order to prevent **air leaks** from the hot aisle to the cold aisle, ensure that any gaps in racks are filled by blank panels and use strip curtains or excluders to cover any spaces above or between racks.



Hot aisle containment design by www.keyzone.com - cold air circulates from the air conditioner under the floor and around the rack while hot air is drawn from between the racks through the ceiling space (plenum) to a heat exchanger; in this design it is very important that hot air does not leak from the ceiling or from the floor space between the racks

Make sure that cabling is secured by cable ties or ducting and does not run across walkways. Cable is best run using a raised floor. If running cable through plenum spaces, make sure it is fire-retardant and be conscious of minimizing proximity to electrical sources, such as electrical cable and fluorescent light, which can corrupt data signals (EMI). You also need to ensure that there is sufficient space in the plenum for the air conditioning system to work properly - filling the area with cable is not the best idea.



To reduce interference, data/network cabling should not be run parallel to power cabling. If EMI is a problem, shielded cabling can be installed.

RFI / EMI



ooeja

Radio Frequency Interference (RFI) is electromagnetic "noise". Noise in this context is anything that interferes with the signal you want to transmit (or receive). Typical man-made sources of electromagnetic noise include power lines, generators, transformers, magnets, fluorescent lights, fans, air-conditioning units, cordless phones, baby monitors, and microwave ovens.

The signal from one device also counts as interference when it disrupts another device - for example, if you use a cell phone in proximity to stereo speakers you may be able to hear the interference. Similarly, the signals from two access points can interfere with one another in some circumstances.

RFI has the potential to disrupt wireless communications. Microwaves and cordless phones are a particular problem because they use the same general part of the spectrum as some wireless network standards (2.4 GHz).

When electromagnetic noise affects electronic equipment, it is often referred to specifically as **ElectroMagnetic Interference (EMI)**. To affect an electronic circuit, the source of EMI would have to be quite close to the component. Examples include a fan positioned next to a monitor or a network cable running next to a fluorescent light.

If a troublesome EMI source is identified and cannot be relocated, the only option is to install some sort of **EMI shielding**. Wired network links can be implemented using the following media:

- Twisted-pair - this carries electrical signals over copper wire cable pairs. Cabling is usually unshielded (UTP) but can be screened (ScTP / FTP [Foil Twisted Pair]) or shielded (STP) to further reduce interference and / or eavesdropping.
- Fiber optic - this carries light signals generated by a laser or LED. Fiber optic supports much higher bandwidth than copper cable over longer distances and is not susceptible to interference. It is more difficult to attach eavesdropping equipment on fiber.



As the exploits of the UK's GCHQ spy agency have shown, fiber optic is not immune to taps.

- Coaxial - another type of copper cabling. Coax is obsolete in terms of network data cabling but is still used for Audio/Video applications (such as CCTV) and for the wiring within premises for cable TV/internet providers.

Fire Prevention and Suppression



Fire can be catastrophic to a business, not to mention the danger it poses to people.

Fire Prevention

The essential point about fire prevention is that flammable materials should be kept away from sources of ignition. Office spaces should be kept clear of flammable materials, such as boxes or polystyrene, and ignition sources (no smoking!).

Most countries require businesses to commission a fire inspection annually, during which an inspector will advise of any risks and check safety procedures and equipment. It is also wise to carry out your own checks monthly, to ensure that fire detectors and alarms work.

Fire Detection

Health and safety legislation dictates what mechanisms an organization must put in place to detect and suppress fires. At the very least each building must have well-marked fire exits and an emergency evacuation procedure that is tested and practiced regularly.

Larger buildings need to be designed in such a way that fire cannot be allowed to spread quickly, by separating different areas with fire-resistant walls and doors (which must be kept shut).

Buildings also need to be fitted with automatic smoke or fire detection systems, as well as alarms that can be operated manually. There are several types of detector:

- Photoelectric smoke detector - measures the integrity of an internal beam of light. The alarm will sound if the beam degrades (for example, if it is obscured by smoke).
- Ionization smoke detector - a radioactive source creates a regular movement of ionized particles, which can be disrupted by smoke.
- Heat detector - these alarms sound if heat rises to a certain point or if the rate of temperature increase exceeds the defined limit.
- Flame detector - these use infrared sensors to detect flames, and are the most effective (and expensive) type.

More sensitive detection systems may be used for certain areas of the building, such as within computer server rooms or rooms used to store archive material.

Escape Plans, Routes, and Drills

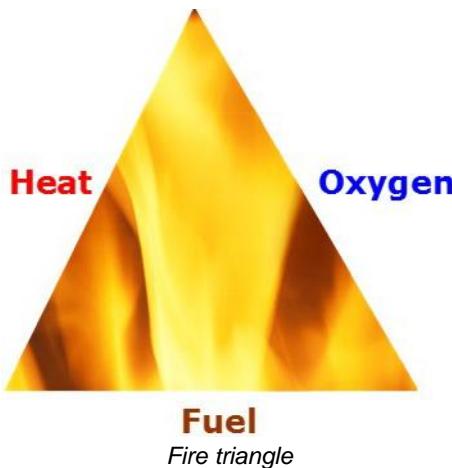
Every building requires an **escape plan** (or **evacuation plan**) for use in emergency. The plan instructs staff on how to leave the building safely and assemble at a designated marshal point outside. The plan assigns the persons responsible for ensuring that the building has been cleared and that everyone (staff and visitors) has been accounted for.

Escape routes from the building must be clearly signed and kept unobstructed. The plan should also set out the procedure to follow should an escape route be blocked; usually this will be to find an opening window and close the doors to the room.

The escape plan should be tested by performing an evacuation **drill** periodically. This ensures that all staff are familiar with the plan and with escape routes and marshal points.

Fire Suppression

Fire suppression systems work on the basis of the Fire Triangle. The Fire Triangle works on the assumption that a fire requires heat, oxygen, and fuel to ignite and burn. Removing any one of those elements provides fire suppression (and prevention).



The fire triangle has been updated in most firefighting literature to the fire tetrahedron (or pyramid). This is because some fires involving chemicals can be sustained by the chain reaction of the chemicals involved and cannot safely be extinguished by normal means.

In the US (and most other countries), fires are divided by class under the NFPA (National Fire Protection Association) system, according to the combustible material that fuels the fire.

- Class A - ordinary combustible materials such as paper, wood, cardboard, and most plastics.
- Class B - flammable or combustible liquids, solids (notably oils, paints, alcohol), and gases.

- Class C - electrical equipment.
- Class D - combustible metals, such as those found in a laboratory.
- Class K - highly flammable materials, such as cooking oils or fats.



Fire extinguisher



Under the European classification system, "electrical" fires are Class E and cooking oil fires are Class F.

Firefighting equipment requires adequate training to use properly. In an office workspace, this equipment will normally consist of a number of fire extinguishers.

Extinguishers come in several different types; each type being designed for fighting a particular class of fire. Using the wrong type of extinguisher on a fire can have catastrophic effects. A fire extinguisher should only be used to tackle a small fire. The first consideration should be to identify a clear route to an emergency exit.

Class	Color	Symbol	Pictogram
A	Silver	Green Triangle	
B	Red	Red Square	
C	Red	Blue Circle	
D	Yellow	Yellow Star	
K	Red	Black Hexagon	

Water-based extinguishers work by removing heat; most other types work by removing oxygen supply. Dry Chemical extinguishers can be used for Class D fires. Wet Chemical extinguishers can be used against Class K fires. The color code can refer either to the color of the extinguisher unit itself or to a predominant block or strip on an otherwise red unit.

A number of staff should be trained in firefighting. To use a water-based extinguisher, pull the pin then aim at the base of the fire. Squeeze the handle and sweep slowly left and right. Continue to spray the source past the point that flames are no longer visible so that any smoldering embers are extinguished.

Premises may also be fitted with an overhead **sprinkler** system. This is often a legal requirement if a building contains more than 100 people, if the building is high rise, if it contains overnight accommodation, or if it is a public building.

Most sprinklers work automatically, are triggered by heat, and discharge water. These are referred to as "wet-pipe" systems. Wet-pipe poses a problem for areas containing sensitive equipment or materials, such as network communications rooms and library or museum archives. Wet-pipe systems constantly hold water at high pressure, so there is some risk of burst pipes and accidental triggering, as well as the damage that would be caused in the event of an actual fire.

There are a number of alternatives to wet-pipe systems that can minimize damage that may be caused by water flooding the room.

- Dry-pipe - these are used in areas where freezing is possible; water only enters this part of the system if sprinklers elsewhere are triggered.
- Pre-action - a pre-action system only fills with water when an alarm is triggered; it will then spray when the heat rises. This gives protection against accidental discharges and burst pipes and gives some time to contain the fire manually before the sprinkler operates.
- Halon - gas-based systems have the advantage of not short circuiting electrical systems and leaving no residue. Up until a few years ago, most systems used Halon 1301. The use of Halon has been banned in most countries as it is ozone depleting, though existing installations have not been replaced in many instances and can continue to operate legally.
- Clean agent - alternatives to Halon are referred to as "clean agent". As well as not being environmentally damaging, these gases are considered non-toxic to humans. Examples include INERGEN (a mixture of CO₂, Argon, and Nitrogen), FM-200 / HFC-227, and FE-13. The gases both deplete the concentration of oxygen in the area (though not to levels dangerous to humans) and have a cooling effect. CO₂ can be used too but it is not safe for use in occupied areas.



Review Questions / Module 5 / Unit 1 / Site Security

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What basic principles can you follow to plan site security?
- 2) What principle should you apply regarding furniture layout in public spaces?
- 3) What use might a proximity reader be for site security?
- 4) What three types of intruder alarm can be used in a security system?
- 5) What are the main considerations to make when setting up a video surveillance system?
- 6) What three elements should be in place to reduce the risk of fire?
- 7) What security controls might be used to implement protected distribution of cabling?
- 8) Where would you expect to find "hot and cold" aisles and what is their purpose?
- 9) What physical security device could you use to ensure the safety of onsite backup tapes?
- 10) What physical site security controls act as deterrents?

Module 5 / Unit 2

Mobile and Embedded Device Security

Objectives

On completion of this unit, you will be able to:

- Identify different types of static environments and methods of mitigating risks in static and embedded systems.
- Describe mobile security concepts and technologies.
- Implement BYOD policies and Mobile Device Management (MDM).
- Identify uses and risks in short-range radio communications (Bluetooth and NFC).



Static Environments

A **static environment** in computing is one that the *user* cannot change (at least, not frequently). A PC is a dynamic environment. The user can add or remove programs and data files, install new hardware components, and upgrade the operating system. A static environment does not allow or require such frequent changes.

In terms of security this can be ideal, because unchanging (versus dynamic) environments are typically easier to protect and defend. Static computing environments pose several risks however. A static environment is often a "black box" to security administrators. Unlike an OS environment such as Windows, there may be little support for identifying and correcting security issues.

Embedded Systems

An **embedded system** is a complete computer system that is designed to perform a specific, dedicated function. These systems can be as small and simple as a microcontroller in an intravenous drip-rate meter or as large and complex as an industrial control system managing a water treatment plant.

As noted above, in computing, a "static" environment is not completely static. Updates are possible, but usually only through specific management interfaces. Embedded systems are normally based on **firmware** running on a **Programmable Logic Controller (PLC)**. This firmware can be updated and reprogrammed. The method used to do so must be extremely carefully controlled however.

SCADA (Supervisory Control and Data Acquisition System) / HVAC Control

Supervisory Control and Data Acquisition Systems (SCADA) are typically components of large-scale, multiple-site **Industrial Control Systems (ICS)** deployed to monitor and manage industrial-, infrastructure-, and facility-based processes. They typically run as software on ordinary computers gathering data from and managing plant devices and equipment with embedded PLCs, referred to as **field devices**. They are used in fabrication and manufacturing; controlling automated assembly lines for example. They are also used in refining, power generation and transmission, wind farms, large communication systems, and so on. In this latter case, field devices may be distributed over a very wide area. SCADA can also be used in building **Heating, Ventilation, and Air Conditioning (HVAC)** systems.

SCADA are often built without regard to security though there is growing awareness of the necessity of enforcing security controls to protect them, especially when they operate in a networked environment.

NIST Special Publication 800-82 covers some recommendations for implementing security controls for ICS and SCADA (gtsgo.to/79lce).



One famous example of an attack on an embedded system is the Stuxnet worm. This was designed to attack the SCADA management software running on Windows PCs to damage the centrifuges used by Iran's nuclear fuels program.

Printers, Scanners, and Fax Machines

Most modern print devices, scanners, and fax machines have hard drives and sophisticated firmware, allowing their use without attachment to a computer and over a network. Often these print/scan/fax functions are performed by single devices, referred to as **Multifunction Devices (MFD)**.

Unless they have been securely deleted, images and documents are frequently recoverable from all of these machines. Many also contain logs. Sometimes simply knowing who has sent how much information to whom and when it was sent is enough for an aggregation and inference attack.

Some of the more feature-rich, networked printers and MFD can also be used as a jump point to attack the rest of the network. These machines also have their own firmware that must be kept patched and updated.

In-vehicle Computing Systems

Modern motor vehicles use a substantial amount of electronics. As well as computer systems to control the vehicle's engine and brakes there may be embedded systems for in-vehicle entertainment and for navigation (sat-nav), using Global Positioning Systems (GPS). Some vehicles are now also fitted with a "black box", or event data recorder, that can log the car's telemetry (acceleration, braking, and position).



In 2010 researchers demonstrated a way to remotely activate the brakes of a car using Wi-Fi and a laptop hooked up to the car's diagnostic port.



Static OS Environments

The embedded systems described above are very closely tied to the hardware design. A wide range of devices fall between the concept of an embedded system and a fully functional personal computing environment. Such devices include smartphones and tablets, games consoles, smart TVs, and mainframe computers.

These types of devices are "static" in the sense that they typically support updates and installations from a single source only. For example, an Apple iPhone can only be updated with OS and application code delivered from Apple's servers (unless the device has been "jailbroken").

iOS

iOS is the operating system for Apple's iPhone smartphone and iPad tablet. There are four major versions (v4 [2010], v5 [2011], v6 [2012], and v7 [2013]) with various .x updates. Apple makes new versions freely available, though older hardware devices may not support all the features of a new version (or may not be supported at all).

While derived from UNIX (through Apple's Mac OS X), iOS is a closed source operating system.

In iOS, what would be called programs on a PC are described as **apps**. A number of apps are included with iOS but third-party developers can also create them using Apple's Software Development Kit, available only on Mac OS. Apps have to be submitted to and approved by Apple before they are released to users, via the **App Store**.

Most iOS attacks are the same as with any system; users clicking on malicious links or entering information into phishing sites for instance. As a closed and proprietary system, it should not be possible for malware to infect an iOS device as all code is updated from Apple's servers only. There remains the risk that a vulnerability in either iOS or an app could be discovered and exploited. In this event users would need to update iOS or the app to a version that mitigates the exploit.



iOS Home Screen (left) and multitasking bar (right)

Android

Android is a smartphone / tablet OS developed by the Open Handset Alliance (primarily driven by Google). Unlike iOS it is an open-source OS, based on Linux. This means that there is more scope for hardware vendors, such as Asus, HTC, LG, Samsung, and Sony, to produce vendor-specific versions. The principal versions of Android are:

- Android 2.3 "Gingerbread" (2010) - still used on a large number of devices. One of the issues with Android is that hardware vendors can be slow to update devices to the latest version.
- Android 3 "Honeycomb" (2011) - a tablet-only release.
- Android 4.0 "Ice Cream Sandwich" (2011) - this preserves compatibility with devices designed to run 2.3.
- Android 4.1/4.2/4.3 "Jelly Bean" (2012).
- Android 4.4 "KitKat" (2013) - the latest version (at the time of writing).

The app model is also more relaxed, with apps available from both Google Play (Android Market) and third-party sites, such as Amazon's app store. The SDK is available on Linux, Windows, and Mac OS X. Apps are supposed to run in a sandbox and have only the privileges granted by the user.

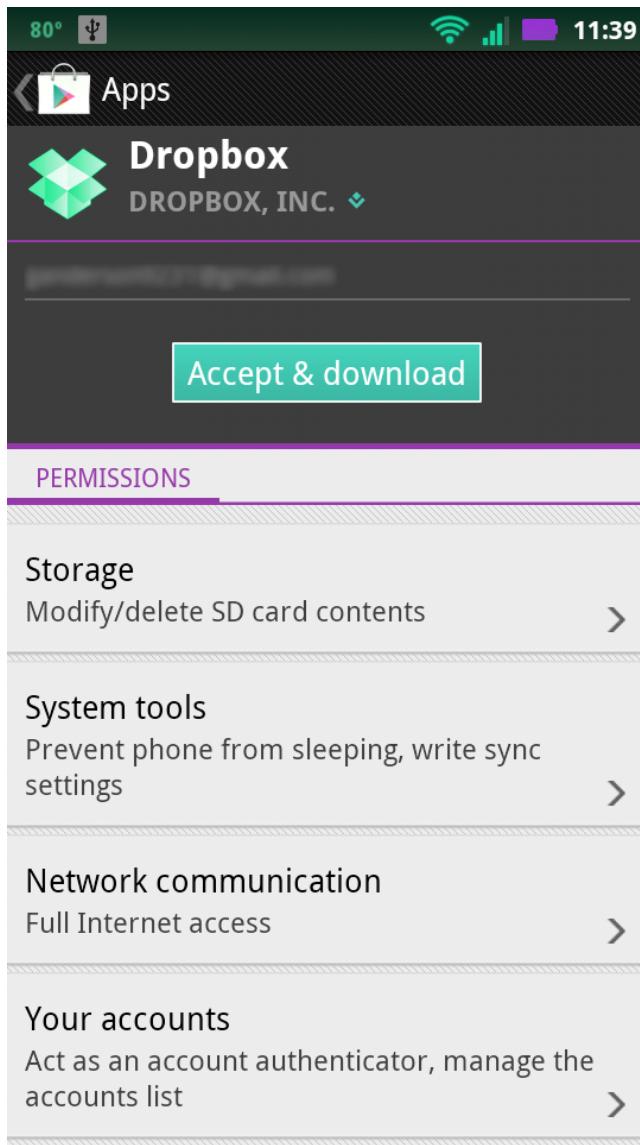
iOS devices are normally updated very quickly. With Android, the situation is far more patchy as updates often depend on the handset vendor to complete the new version or issue the patch for their "flavor" of Android.

Android OS is more open and there is Android malware, though as with Apple it is difficult for would-be hackers and spammers to get it into any of the major app repositories.



One technique used is called "Staged Payloads". The malware writers release an app that appears innocuous in the store but once installed it attempts to download additional components infected with malware (for more information, visit gtsgo.to/wpitc). At the time of writing Google are planning to release a server-side malware scanning product that will both warn users if an app is potentially damaging and scan apps that have already been purchased and warn the user if any security issues have been discovered.

Like iOS, Android apps operate within a sandbox. When the app is installed, access is granted (or not) to specific shared features, such as contact details, SMS texting, and email.



Configuring app permissions in Android OS

As well as being programmed with the code for known malware, A-V software for Android can help the user determine whether an app install is seeking more permissions than it should. However because the A-V software is also sandboxed, it is often not very effective. Mobile A-V software can also have a substantial impact on performance and battery life.

Smart TVs

Smart TV, also known as "connected or "hybrid" TV, is a technological merging of computers and television sets or set-top boxes. These boxes combine broadcast reception with home networking access, online interactive media, and on-demand streaming media. They can deliver content such as movies and music as well as provide access to internet-based services such as video-on-demand, interactive advertising, personalization, games, social networking, and even voting.

Most smart TVs use a Linux kernel. Because they're effectively running mini-computers, Smart TVs can of course be hacked. Some of the apps it might use, such as Skype or Facebook, are written in Java, JavaScript, or HTML5 and are therefore vulnerable to any of the standard attacks associated with web applications. Once the TV is compromised and the hacker has full control, she can spread her attack to the victim's contacts. Hackers taking over cameras or microphones for eavesdropping can also be an issue.

As smart TVs may be deployed within an office simply as screens, any unused smart features should be disabled.

Mainframes

Mainframe computers were the first basis for enterprise computing systems, before the development of PC servers. Mainframes are primarily used for critical applications and bulk data and transaction processing, often in long-established businesses such as banks. In hardware terms, a mainframe will have redundant internal engineering, resulting in high stability, reliability, and security, which means that they can run uninterrupted for decades. They also have the security advantage (or disadvantage) of having proprietary software written for them.

Like embedded systems, mainframes and the software they run are usually a bit of a "black box" to the mainstream IT support and security departments. This sort of concentration of knowledge about the programming and operation to a small group of individuals is a significant risk.

However, mainframes are also a black box to the wider "hacking" community so any attack against a mainframe is likely to be highly specialized and targeted and much more likely to come from an insider threat source than an external one.

Game Consoles

The major difference between a game console and a PC is that a game console has more specifically tuned hardware and a more streamlined operating system, though the kernel is still based on Windows (Xbox) or Linux (PlayStation). From a security perspective, it is important to remember that consoles often have very large hard drives, and as such, can be used for storage or even act as a server on a network. "Rooting" or "jailbreaking" the console by applying specially modified firmware gives an attacker complete control over the device and its underlying OS. Some companies provide on-site game consoles for staff or guests to use. They should be kept isolated from the corporate network.

Mitigating Risk in Static Environments



Embedded systems and the "static" environments of mobile and game console OS must not be overlooked when designing the security system. The following methods can be used to mitigate risk in static environments.

Security Layers and Control Redundancy and Diversity

Any individual security control, whether administrative, technical or physical, can be compromised. **Layered security**, also known as **defense-in-depth**, is imperative to maintaining the security of your environment. This applies particularly to static environments where conventional IT security controls (such as firewalls or malware scanning) may not be directly applicable or available. Banks, for example, do not depend on a single layer of security, but instead put a series of layers in place to safeguard their assets. These might include controls such as guards, policies, procedures, cameras, vaults, alarms, a variety of locks and other access controls. The **diversity of controls** presents a potential attacker with multiple hurdles to overcome. If one layer fails, the next layer will protect the asset; if that layer fails, there's another behind it, and so on.

Note here that none in the series of controls described can depend on another layered control. If they did, they should be considered a single point of failure, which is the antithesis of layered security. Similarly, controls should not share paths. For example, not all of your controls should depend on electricity.

Redundant controls are put into place to improve resilience in defense and should remain standing to replace controls that are rendered unavailable for whatever reason.

Network Segmentation

Network segmentation is one of the basics of IT and network security. Network access for static environments should only be required for applying firmware updates and management controls from the host software to the devices and for reporting status and diagnostic information from the devices back to the host software. This **control network** should be separated from the **corporate network** using firewalls.

With environments such as SCADA the management software may require legacy versions of operating systems, making the hosts particularly difficult to secure. Isolating these hosts from others through network segmentation and using endpoint security (preventing the attachment of USB devices) can help to ensure they do not become infected with malware.

Application Firewalls

As embedded devices make greater use of a network for diagnostic reporting and updating, they are exposed to greater risks. These risks could be mitigated by deploying application firewalls. These are firewalls designed to protect specific applications and devices, such as a SCADA. This sort of dedicated firewall software to protect the management software and embedded device's network interfaces is relatively difficult to find for embedded systems, though solutions are starting to appear. The main issue with firewalls implemented on the device firmware is the lack of processing power and memory space available to run such functions.

Wrappers

One way of increasing the security of data in transit for embedded systems is through the use of **wrappers**. A wrapper usually includes a header, which precedes the encapsulated data, and a trailer, which follows it. We find an excellent example of wrappers used for security with IPsec run in tunnel mode, wherein the entire original packet, including the data and the AH, ESP, TCP/UDP, and IP headers are all encapsulated. The only thing visible to an attacker or anyone sniffing the wire is the IPsec header, which describes only the tunnel endpoints. This is useful for protecting traffic between trusted networks when the traffic has to go through an untrusted network to go between them, or between trusted nodes on the same network.



See [Unit 3.4](#) for more information about IPsec.

Firmware Version Control and Manual Updates

Firmware version control is the process of patch management for static and embedded environments. This process is just as vital as keeping host OS software up-to-date with patches but for many embedded systems and static environments it is far more of a challenge:

- Many embedded systems use low-cost firmware chips and the vendor never produces updates to fix security problems or only produces updates for a relatively short product cycle (while the device could remain in operational use for much longer).
- Many embedded systems require **manual updates**, which are perceived as too time-consuming for a security department with other priorities to perform.



2s6xb

It is critical that the organization's mobile device security practices be specified via policies, procedures, and training. Although we always want our practices specified via policies and procedures, it is particularly important with respect to mobile devices because these devices tend to be forgotten or overlooked.

They don't reside, or "live" in the workplace in the same way as, for example, a desktop computer and they won't necessarily be there when virus databases are being updated, patches are being installed, files are backed up, and so on. Part of the practices of managing these devices involve making sure that they are kept as secure as devices that reside permanently within the physical infrastructure.

Maintaining mobile security is one of the great challenges in a "post-PC" world. There are two central challenges when it comes to mobile device security: portability and capacity:

- Portability - devices that are portable are easy to lose or to steal or to sneak into somewhere they should not be allowed.
- Capacity - while great for consumers, the capacity and ease of portability of flash media, removable hard drives, smartphones, and tablets is a big problem for information security. A typical removable hard drive or Network Attached Storage (NAS) device or even a smartphone can copy down the contents of a workstation or even a server in a few minutes. Because they use USB or network ports, it is difficult to prevent the attachment of such devices.

Our problems, therefore, surround the fact that because of their portability and capacity, mobile devices can be both targets of attack and the means by which an attack can be accomplished. We have to protect the data on our mobile devices from being compromised and we have to protect the data in any of our systems from being removed by mobile devices.

Device Access Control

The majority of smartphones and tablets are single-user devices. Access control can be implemented by configuring a password or PIN and screen lock. iOS does not support multiple user accounts at all; Android supports multiple user accounts on tablets but not on smartphones.



There is also the issue of implementing access control when a mobile device is used on an enterprise network to access corporate data. This is discussed in more detail under "BYOD Concerns" below.

Screen Locks, Lockout, and Remote Wiping

If an attacker is able to gain access to a smartphone or tablet, they can obtain a huge amount of information and the tools with which to launch further attacks. Quite apart from confidential data files that might be stored on the device, it is highly likely that the user has cached passwords for services such as email or remote access VPN and websites. In addition to this access to contacts and message history (SMS, email, and IM) greatly assists social engineering attacks.

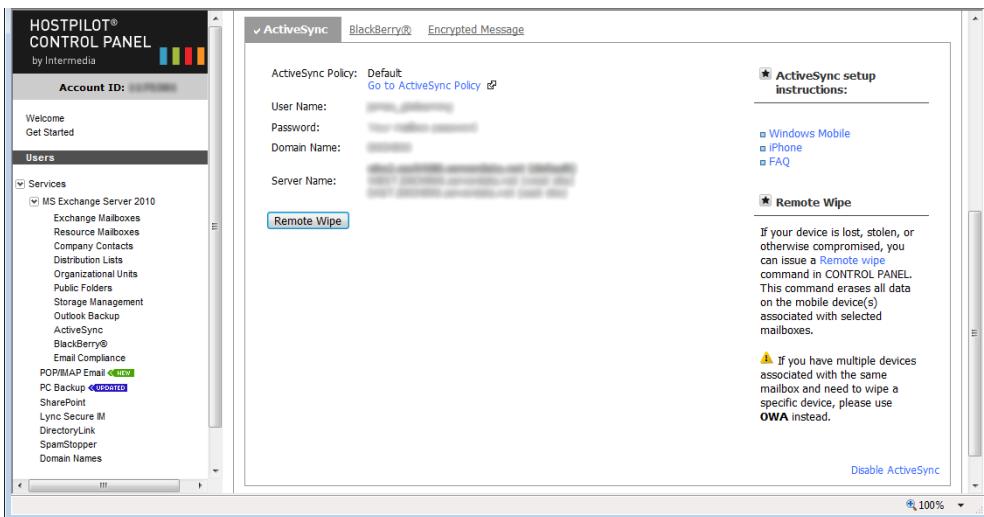
Consequently it is imperative that data stored on the device be encrypted and access to the device protected by a **screen lock**. This means that a password (or at the very least a PIN) is required to use the device. There are also "join-the-dots" pattern locks. Some smartphones with biometric fingerprint readers are also appearing on the market.



Configuring passcode lock and restrictions on iOS

The screen lock can also be configured with a **lockout** policy. This means that if an incorrect passcode is entered, the device locks for a set period. This could be configured to escalate (so the first incorrect attempt locks the device for 30 seconds while the third locks it for 10 minutes for instance). This deters attempts to guess the passcode.

Another possibility is for the phone to support a **remote wipe** or "kill switch". This means that if the handset is stolen it can be set to the factory defaults or cleared of any personal data. Some utilities may also be able to wipe any plug-in memory cards too. The remote wipe could be triggered by a number of incorrect passcode attempts or by enterprise management software. Other features include backing up data from the phone to a server first and displaying a "Lost / stolen phone - return to XX" message on the handset.



Most corporate messaging systems come with a **Remote Wipe** feature, allowing mail, calendar, and contacts information to be deleted from mobile devices

Remote wipe tends to be a feature of newer smartphones only. Clearing (or "sanitizing") older handsets ("feature phones") of personal data is often a complex, manual process.

A thief can (in theory) prevent a remote wipe by ensuring the phone cannot connect to the network then hacking the phone and disabling the security.

Full Device Encryption

All but the early versions of mobile device OS for smartphones and tablets (such as Android and iOS) provide **full device encryption**.

In iOS 5 (and up), there are various levels of encryption.

- All user data on the device is always encrypted but the key is stored on the device. This is primarily used as a means of wiping the device. The OS just needs to delete the key to make the data inaccessible rather than wiping each storage location.
- Email data and any apps using the "Data Protection" option are also encrypted using a key derived from the user's passcode (if this is configured). This provides security for data in the event that the device is stolen. Not all user data is encrypted; contacts, SMS messages, and pictures are not, for example.

In iOS, Data Protection encryption is enabled automatically when you configure a password lock on the device. In Android, you need to enable encryption via Settings > Security. Android uses full-disk encryption with a passcode-derived key. When encryption is enabled, it can take some time to encrypt the device.



The encryption key is derived from the PIN or password. In order to generate a strong key, you should use a strong password. Of course, this makes accessing the device each time the screen locks more difficult...



See [Unit 4.2](#) for more information about data encryption.

Removable Storage

A mobile device contains a solid state (flash memory) drive for persistent storage of apps and data. Typical capacities range from 8 - 256GB. This storage is not upgradeable. Some Android and Windows devices support removable storage through a plug-in SecureDigital (SD) card slot; some may support the connection of USB-based storage devices. The disk encryption software will usually allow encryption of the removable storage too.

iOS-based devices cannot use removable storage, though there are adapters for importing media via an SD card reader or camera connection kit.

Triangulation and GPS Tracking

The carrier can use the cell system to triangulate the location of a phone to within a few meters. This is useful for making emergency calls with a phone, but has privacy and security implications. In some countries, providers are willing to sell this information to third-parties, including private investigators and debt collectors, as well as making the information available to law enforcement.

Many devices are now fitted with **GPS (Global Positioning System)** chips. GPS is a means of determining a receiver's position on the Earth based on information received from GPS satellites. The receiver must have line-of-sight to the GPS satellites. GPS provides another means of locating the device. The user needs to install some tracking software and register the phone with the locator application (these are normally subscription services). Having done this, the location of the phone (so long as it is powered on) can be tracked from any web browser.



You can use the iCloud and Find My Phone apps to locate an iOS device and remotely lock or wipe it (or send the current holder a polite message to please return it ASAP)

As GPS requires line-of-sight, it does not work indoors. **Indoor Positioning Systems (IPS)** work out a device's location by triangulating its proximity to other radio sources, such as Wi-Fi access points or Bluetooth beacons.

Knowing the device's position also allows app vendors and websites to offer location-specific services (relating to search or local weather for instance) and (inevitably) advertising. You can use **Location Services** settings to determine how visible your phone is to these services.

The primary concern surrounding GPS systems is one of privacy. Although very useful when used with navigation systems, it provides a mechanism to track an individual's movements, and therefore their social habits. The problem is further compounded by the plethora of mobile apps that require access to location services and then both send the information to the application developers and store it within the device's file structure. If an attacker can gain access to this data then stalking, social engineering and even identity theft becomes a real possibility.

Mobile Device Management

Mobile Device Management (MDM) is a class of management software designed to apply security policies to the use of mobile devices in the enterprise. This software can be used to manage enterprise-owned devices as well as **Bring Your Own Device (BYOD)**.

The core functionality of these suites is rather similar to **Network Access Control (NAC)** solutions. The management software logs use of a device on the network and determines whether to allow it to connect or not, based on administrator-set parameters. When the device is enrolled with the management software it can be configured with policies to allow or restrict use of apps, corporate data, and built-in functions such as a video camera or microphone.

A key feature is the ability to support multiple operating systems (such as iOS, Android, BlackBerry, and the various iterations of Windows and Windows Mobile). A few MDM suites are OS-specific but the major ones, such as AirWatch (www.air-watch.com), Symantec (gtsgo.to/gs3rq), and ZenMobile (gtsgo.to/9blug), support multiple device vendors.

Asset Tracking and Inventory Control

Mobile assets are often taken off-site and used beyond the control of the organization that owns the devices. The enterprise will certainly add an asset tag to each device and enter the tag number and the user to which the device was issued into a database. This will usually be integrated with the MDM software.

The location services built into smartphones and tablets can be used to track a device too. Asset tracking software must be locked so that the user can't uninstall or disable it. Some organizations may choose to run such software "invisibly" for this reason, but this really only amounts to security by obscurity. Users should be told that their whereabouts may be monitored via possession of the device.

Application Control and Disabling Unused Features

MDM software can also be used for application control. When the device is joined to the corporate network through enrollment with the MDM software, it can be configured into a corporate "workspace" mode in which only a certain number whitelisted applications can run. The MDM software may also be able to lock down use of unused features (or features that the enterprise wants to remain unused!), such as Bluetooth or the on-board camera or microphone.

BYOD Concerns



Bring Your Own Device (BYOD) means allowing employees to use their private smartphone and tablet devices to access corporate data. BYOD presents an ever increasing challenge for businesses.

User Acceptance and Adherence to Corporate Policies

If given a free choice, most IT departments would rather not allow BYOD at all but it's almost impossible to successfully ban them. Users are demanding to be able to use personal devices. Given that demand, for BYOD to work, there must be **user acceptance** of some degree of corporate control and monitoring of the device while it is being used in a "work" role and also acceptance that this will impact to at least some degree on private use of the device.

This control and monitoring can be formulated in "soft" policies and guidance set out in employment contracts. These policies can be backed up with Mobile Device Management (MDM) technical security controls to ensure BYODs are used in **adherence to corporate policies**.

Architecture / Infrastructure Considerations

One of the first steps in formulating a policy for BYOD is to determine which devices and mobile operating systems qualify. The devices must be capable of integrating with the existing ICT network and security architecture and infrastructure. For example, it would be highly risky to allow BYODs that cannot be managed effectively. Most companies publish a "choose from" list of personal devices that can be supported.

Secondly the infrastructure must be present to support the chosen range of devices. Apart from appropriate network access technologies, this will usually mean selecting and deploying an MDM software suite to manage the devices plus developing support options for users who need help using their device within the enterprise.

Support Ownership and On-boarding / Off-boarding

Where BYOD has worked most successfully, users sign a policy allowing corporate IT some control over the device and **ownership of the support process**, so far as corporate data and confidentiality is impacted. For example if the device goes missing, the first call is to the organization rather than the telecoms provider to allow for a selective wipe of corporate data, settings, and applications while leaving personal data and settings intact.

There must also be a policy for **on-boarding** and **off-boarding**, ensuring that devices are brought into and out of the organization securely, including the removal of corporate settings, data, and so on. Policy can be supported by technical controls, in the form of MDM suites, which can perform the enrollment and un-enrollment of devices automatically, according to administrator-set policies.



MDM products may have their own Data Loss Prevention (DLP) software or tie in with other DLP products to prevent data files from being copied to insecure storage areas on a mobile device. See [Unit 4.2](#) for more information about DLP.

Patch and Anti-Virus Management

As with remote access solutions, one issue for BYOD is that users cannot be relied upon to perform effective patch and anti-virus management. There are several potential issues:

- The user could install a vendor patch that breaks compatibility with one or more of the corporate network's applications or device management software.
- The user might not install critical security patches or provide any sort of malware scanning.

Again, these issues can be at least partially addressed using MDM suites but there is always likely to be a substantial support cost for BYOD.

Data Ownership, Privacy, and Storage Segmentation

When a device is privately owned and stores a mix of corporate and personal data, the questions of **data ownership** and **privacy** arise.

- Data ownership - how can rights over corporate data be asserted on a device that does not belong to the corporation?
- Privacy - how can the corporation inspect and manage a BYOD without intruding on private data and device usage?

At one level, these concerns need to be addressed by policy and guidance, agreed between the employer and employees. These sorts of concerns have also been addressed by MDM vendors in the form of **storage segmentation**. This allows the employer to manage and maintain the portion of the device that connects/interfaces with the corporate network. When the device is used on the enterprise network, a corporate workspace with a defined selection of apps and a separate storage container is created. The enterprise is thereby able to maintain the security it needs but does not have access to personal data/applications.

Examples of storage segmentation include BlackBerry's "BlackBerry Balance" technology and AirWatch's "Workspace Management" features.

On-board Camera / Video

Another concern with smartphones and tablets is that the on-board camera and/or microphone could be used for snooping. **Geo-fencing** can be a useful tool with respect to controlling the use of camera or video functions. This involves disabling cameras on mobile devices when they are in areas that should not allow photographs or video according to policy.

Acceptable Use Policy

Once mobile devices are connected, they effectively become a part of the corporation. While not owned by the company, both device and user must adhere to corporate policies. **Acceptable Use Policies (AUP)** can be particularly tricky here. For example, on the one hand, you can't prevent users from going to the more "questionable" areas of the internet on their devices; on the other, the organization must avoid allowing a potentially hostile work environment to be created.



See [Unit 5.6](#) for more information about operational policies and procedures.

Forensics and Legal Concerns

It can be difficult to assess data breach exposure on personal devices and even harder to perform digital forensics. In many cases the organization might not even be made aware that anything has gone wrong. Bypassing inbound and outbound filters can be a huge problem in terms of avoiding attack on the one hand and complying with regulations, such as those pertaining to data privacy laws, on the other.

Also consider legal issues, such as whether the organization has the right to seize and examine the device. When the device was owned by the company, the answer was a straightforward "yes" but with BYOD, this is not straightforward at all. There must be a clearly articulated expectation of privacy policy with BYOD addressing such questions.



See [Unit 5.5](#) for more information about digital forensics procedures.

Multinationals face unique challenges, because they will find themselves confronted with the differing privacy laws with which they must be compliant.

Mobile Application Security



In iOS and Android, what would be called programs on a PC are described as **apps**. Third-party developers can create apps using the relevant Apple or Android Software Development Kit (SDK). Apps have to be submitted to and approved by the vendor before they are released to users. Apps are made available for free or can be bought from the iTunes App Store or Google Play (or other marketplace supported by the device).

Encryption and Key Management

The importance of encrypting any confidential data processed by an app is obvious. The issue is the means of accomplishing this when the client-side device on which the app runs cannot be trusted. Developers must always consider the possibility that the mobile OS could be jailbroken (iOS) or rooted (Android), allowing the user to compromise the way the app works.

Encrypting the app itself is of limited value, as although encryption is possible, the private encryption key has to be stored on the device itself so that the app can be decrypted for execution. This means that if the mobile OS is jailbroken or rooted, an attacker can recover the key and decrypt the application.

Attempts to bury the key amount only to "security by obscurity". This is also a significant problem for credential management and authentication (see below).



There are various methods of obfuscating secrets hidden with code. These can only ever slow down a determined attacker however.

More important is the question of whether the application offers encryption for data it stores and data it transmits so that users' confidential and private data is protected. Apps can use the Application Programming Interfaces (API) of the mobile OS to use encryption and use SSL/TLS to ensure data transmitted over a network to the app's servers is encrypted.

In terms of public keys, the list of trusted root CAs is stored in **Settings > Security > Trusted Credentials** under Android. In iOS you need to check Apple's website (gtsgo.to/q3mxg) for the version of the Trust Store listed under **Settings > General > About**. Adding a CA to a mobile device (to trust enterprise-generated certificates for instance) would normally be done through MDM software.



See [Unit 2.1](#) and [Unit 2.2](#) for more information about encryption and CAs.

Credential Management

As with private encryption keys, passwords cannot be securely included with app code. If this code can be accessed, malicious users will be able to extract any credentials that have been embedded within the application. Once accessed, the attacker may be able to impersonate the application to malicious intent. This is a big problem if the app needs to store some sort of system-wide secret, such as a developer's credentials for a web service. All such processing really has to be done on the server-side.

In terms of user authentication, they can authenticate with the app's server using a secure mechanism such as HTTPS. Subsequently, the app server can transmit authorization tokens to the app as the basis of an access control mechanism. These tokens can be encrypted with the server's private key and decrypted with the related public key stored on the device. Tokens should be time-limited to prevent replay attacks.

Authentication and Transitive Trust

Providing these sorts of server-side authentication and authorization systems is obviously difficult. Many app developers use federated authentication, whereby the user authenticates via another provider (such as Facebook or Google).



See [Unit 2.4](#) for more information about authentication technologies and federation and trust issues.

Geotagging

Geotagging is the process of adding geographical identification metadata to media such as photographs, SMS messages, video, and so on. It allows the app to place the media at specific latitude and longitude coordinates. Geotagging is highly sensitive personal information and should be processed carefully by an app. The user must be able to consent to the ways in which this information is used and published. Consider for example geotagged pictures uploaded to social media. These could be used to track a person's movements and location very easily.

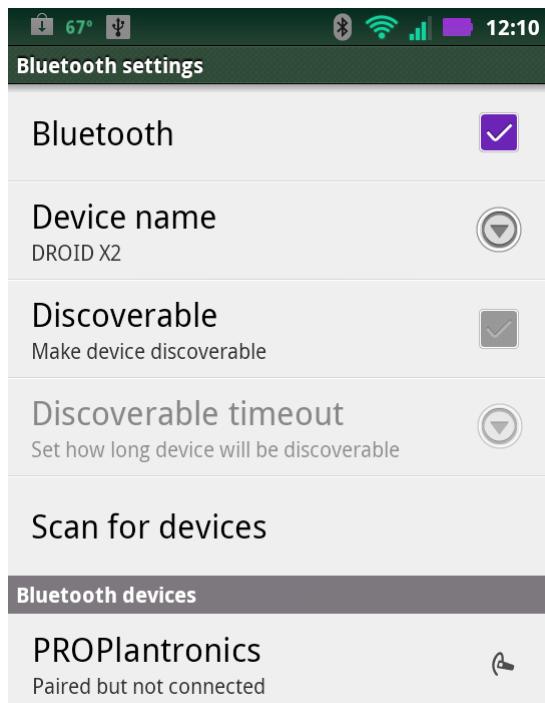
Bluetooth and NFC

As well as being able to connect to Wi-Fi and cellular networks, mobile devices also support the use of short-range radio technology.



Bluetooth

Bluetooth is a short-range (up to about 10m) radio link, working at a nominal rate of up to about 3 Mbps (for v2.0 + EDR). It is used for so-called Personal Area Networks (PAN) to share data with a PC, connect to a printer, use a wireless headset, and so on.



Configuring Bluetooth on Android OS

Bluetooth devices have their own security issues, summarized below:

- Device discovery - a device can be put into discoverable mode meaning that it will connect to any other Bluetooth devices nearby. Unfortunately, even a device in non-discoverable mode is quite easy to detect.
- Authentication and authorization - devices authenticate ("pair") using a simple passkey configured on both devices. This should always be changed to some secure phrase and never left as the default. Also, check the device's pairing list regularly to confirm that the devices listed are valid.
- Malware - there are various "proof-of-concept" Bluetooth worms and application exploits. There are also vulnerabilities in the authentication schemes of many devices. Keep devices updated with the latest firmware.

Unless some sort of authentication is configured, a discoverable device is vulnerable to **bluejacking**, a sort of spam where someone sends you an unsolicited text (or picture / video) message or vCard (contact details). While there are no known instances, this could also become a vector for malware.



Pairing a computer with a smartphone

Bluesnarfing refers to using an exploit in Bluetooth to steal information from someone else's phone. The exploit (now patched) allows attackers to circumvent the authentication mechanism. Even without an exploit, a short (4 digit) PIN code is extremely vulnerable to brute force password guessing.



Near Field Communications (NFC)

Near Field Communications (NFC) is a very short range radio link based on **Radio Frequency IDs (RFID)**. NFC works at up to 4cm at data rates of 106, 212, and 424 Kbps. NFC sensors and functionality are starting to be incorporated into smartphones. NFC is mostly used for contactless payment readers. It can also be used to configure other types of connection (pairing Bluetooth devices for instance) and for exchanging information, such as contact cards.

As well as powered sensors, an NFC function can be programmed into an unpowered chip that can be delivered as a sticker (an NFC tag). When the phone's sensor is brought close to the tag, the radio field activates it and triggers some action that has been pre-programmed into the phone.

As a relatively new technology, there are few proven attacks or exploits relating to NFC. It is possible to envisage how such attacks may develop however. NFC does not provide encryption so eavesdropping and Man-in-the-Middle is possible if the attacker can find some way of intercepting the communication and the software services are not encrypting the data. Vulnerabilities and exploits are also likely to be found in the software services that use NFC. It is also possible to jam NFC signals, creating a Denial-of-Service attack.

Some software, such as Google's Beam, allows NFC transfers to occur without user intervention. It is possible that there may be some way to exploit this by crafting tags to direct the device browser to a malicious web page where the attacker could try to exploit any vulnerabilities in the browser.



Review Questions / Module 5 / Unit 2 / Mobile Device Security

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) True or false? The short range of Bluetooth devices make them low risk from a security point-of-view.
- 2) What are SCADA devices and what are the security issues associated with them?
- 3) Why do we segment networks?
- 4) Aside from leaving sensitive documents on it, are there security concerns with respect to printers?
- 5) What are the two main security concerns when it comes to mobile devices?
- 6) What is Mobile Device Management (MDM)?
- 7) What is the first and last concern on the timeline with respect to managing security on employee owned devices?
- 8) What must be done with mobile devices and storage to best defend against the interception or extraction of sensitive data?
- 9) Why allow employees to use their own mobile devices at work?
- 10) Why not thoroughly lock employees' own devices down, as you would with corporate-owned devices?

Module 5 / Unit 3

Risk Management

Objectives

On completion of this unit, you will be able to:

- Understand the use of business continuity planning, Business Impact Analysis, and risk assessment.
- Identify risk mitigation options and metrics.
- Describe risks involved in integrating data and systems with third parties.
- Use configuration management and change management policies to reduce risk.

Business Continuity Concepts



crlk3 0q7ai

Business continuity means planning and testing systems and operations so that they are as little affected by incidents as possible and so that the resources are available to recover from them.



NIST have published a guide to IT contingency planning (SP800-34) available at gtsgo.to/eukoi. There are also BSI and ISO standards associated with business continuity planning.



Organizations other than businesses need continuity plans so sometimes the terms "Continuity of Operations (COOP)" or "Continuity of Government (COG)" are used.

Business Impact Analysis

When setting up a security system (or reviewing an existing one), one of the first steps is to set up a team responsible for **risk management**.

Risk management starts with an initial risk investigation or analysis, often called a **Business Impact Analysis (BIA)**. This has four main components:

- Identify the critical functions or processes of the business or organization.
- Identify the assets and resources on which the organization depends.
- Identify threats to the organization's functions and assets.

- Assess the risk to each function or asset, given the threats.

The results of the BIA are then used to create business continuity plans. The cornerstone of which will be selecting countermeasures (or security controls) to mitigate the risks identified in the BIA.

Assessment Types (Risks, Threats, and Vulnerabilities)



Recall the uses of the terms risk, threat, and vulnerability discussed at the start of the course:

- Risk assesses the likelihood of loss or damage and its consequence (cost).
- Threat refers to the sources or motivations of people and things that could cause loss or damage.
- Vulnerability refers to a specific flaw or weakness that could be exploited to overcome a security system. Sometimes a distinction is also drawn between a theoretical vulnerability and an exploitable one.

It is important to assess these things separately to at least some extent. You need to identify as many actual and potential threats as you can without spending too much time evaluating the probability of each. Similarly, you should try to identify as many vulnerabilities as possible. Once you have made those assessments, you can start to evaluate risk (likelihood and consequence) and from a risk assessment start to identify suitable controls and measures.

Identification of Critical Systems



In order to design a security plan, you must know what you want to make secure. It is crucial for an organization to perform the **identification of critical systems**. This means compiling an inventory of its business processes and its tangible and intangible assets and resources. These could include:

- People (employees, visitors, and suppliers).
- Tangible assets (buildings, furniture, equipment and machinery (plant), ICT equipment, electronic data files, and paper documents).
- Intangible assets (ideas, commercial reputation, brand, and so on).
- Procedures (supply chains, critical procedures, standard operating procedures).

There are many software suites and associated hardware solutions available for tracking and managing assets (or **inventory**). An asset management database can be configured to store as much or as little information as is deemed necessary, though typical data would be type, model, serial number, asset ID, location, user(s), value, and service information.

Tangible assets can be identified using a barcode label or **Radio Frequency ID (RFID)** tag attached to the device (or more simply using an identification number). An RFID tag is a chip programmed with asset data. When in range of a scanner, the chip activates and signals the scanner. The scanner alerts management software to update the device's location. As well as asset tracking, this allows the management software to track the location of the device, making theft more difficult.

Within the inventory of assets and business processes it is important to assess their relative importance. Which business functions are critical and which are only necessary? In the event of a disaster that requires recovery processes take place over an extended period, critical systems must be prioritized over merely necessary ones.

If there is a natural disaster, the item at the top of the list will always be people's personal safety. If there is a threat to life or of injury, that must be dealt with first.

Given that, the business continuity plan should classify systems and hardware according to their importance to business processes. The situation will still be complex - there are likely to be dependencies between systems that make it difficult to make the right decisions - but classifying the systems beforehand will help to reduce confusion during the stressful period after a disaster has struck.

For most businesses, the most critical systems will be those that enable customers to find them and for the business to interact with them. In practical terms, this means telecoms and web presence. Following that is probably the capability to fulfil products and services. Back-office functions such as accounting, HR, and marketing are probably necessary rather than critical.



This is all subject to circumstance. If the disaster strikes the day before the CEO is due to present to the company's most important customers, ensuring that the presentation goes ahead smoothly might be expected to take precedence. If the customers are all going to be there in that room, getting the web server back is not going to be as high a priority.

Threat Identification

Threat identification means compiling a prioritized list of probable and possible threats. Some of these can be derived from the list of assets (that is, threats that are specific to your organization); others may be non-specific to your particular organization.

- Natural disaster (flood, earthquake)
- Theft, vandalism, conflict
- Espionage
- Fire (accidental or malicious)

It's important to note that threats could be created by something that the organization is *not* doing or an asset that it does *not* own as much as they can from things that it *is* doing or *does* own. Consider (for instance) the impact on business processes of the following:

- Public infrastructure (transport, utilities, law and order).
- Supplier contracts (security of supply chain).
- Customer's security (the sudden failure of important customers due to their own security vulnerabilities can be as damaging as an attack on your own organization).
- Epidemic disease.



See [Unit 1.2](#) for more information on types of threat.

As well as understanding the range of threats, it is important to be up-to-date with best practice and standards relevant to the type of business or organization. This can help to identify procedures or standards that are not currently being implemented but should be. Make sure that the asset identification process captures systems architecture as well as individual assets (that is, understand and document the way assets are deployed and used and how they work together).



Diagrams are the most useful way to show how systems interconnect or how processes and procedures work. There are a number of tools for doing this, notably Microsoft Visio.

Risk Calculation



For each resource and each threat, you must quantify the degree of risk that exists. Calculating risk is complex. It depends on variables such as:

- **Likelihood** of the threat being realized.
- **Impact** - this may be determined by factors such as the value of the asset or the cost of disruption if the asset is compromised.

It is important to realize that the value of an asset does not refer solely to its material value. The two principal additional considerations are direct knock-on costs associated with the asset being compromised (downtime) and cost to intangible assets, such as the company's reputation.

For example, a server may have a material cost of a few hundred dollars. If the server were stolen, the costs incurred from not being able to do business until it can be recovered or replaced could run to thousands. In addition, that period of interruption where orders cannot be taken or go unfulfilled leads customers to look at alternative suppliers, resulting in perhaps more thousands of lost sales and goodwill.

There are two methods of risk assessment: quantitative and qualitative.

Quantitative Risk Assessment

Quantitative risk assessment aims to assign concrete values to each risk factor.

- Single Loss Expectancy (SLE) - the amount that would be lost in a single occurrence of the risk factor. This is determined by multiplying the value of the asset by an Exposure Factor (EF). EF is the percentage of the asset's value that would be lost.
- Annual Loss Expectancy (ALE) - the amount that would be lost over the course of a year. This is determined by multiplying the SLE by the Annual Rate of Occurrence (ARO).



Quantitative risk assessment aims to assign concrete values to each risk factor

The problem with quantitative risk assessment is that the process of determining and assigning these values is extremely complex and time consuming. The accuracy of the values assigned is also very difficult to determine without historical data (often, it has to be based on subjective guesswork). However, over time and with experience this approach can yield a detailed and sophisticated description of assets and risks and provide a sound basis for justifying and prioritizing security expenditure.

Qualitative Risk Assessment

Qualitative risk assessment avoids the complexity of the quantitative approach and is focused on identifying significant risk factors. The qualitative approach seeks out people's opinions of which risk factors are significant. Assets and risks may be placed in simple categories. For example assets could be categorized as Irreplaceable, High Value, Medium Value, and Low Value; risks could be categorized as one-off or recurring and as Critical, High, Medium, and Low probability.

Another simple approach is the "Traffic Light" impact grid. For each risk, a simple Red, Amber, or Green indicator can be put into each column to represent the severity of the risk, its likelihood, cost of controls, and so on. This approach is simplistic but does give an immediate impression of where efforts should be concentrated to improve security.

Risk Factor	Impact	ARO	Cost of Controls	Overall Risk
Legacy Windows clients				
Untrained staff				
No anti-virus software				

Traffic light impact grid

Impact and FIPS Security Categorizations

FIPS 199 (gtsgo.to/alm14) discusses how to apply **Security Categorizations (SC)** to information systems based on the impact that a breach of confidentiality, integrity, or availability would have on the organization as a whole.

Potential impacts can be classed as:

- Low - minor damage or loss to an asset or loss of performance (though essential functions remain operational).
- Moderate - significant damage or loss to assets or performance.
- High - major damage or loss or the inability to perform one or more essential functions.

Approaching Risk Assessment

Whichever methodology is applied, when initiating risk assessment you should prioritize the most important assets and threats. There is no point undertaking lengthy and detailed asset and risk analysis without first deploying common sense, practical security measures. As long as it does not lead to a sense of complacency, some security is better than no security.



Risk Mitigation

Having completed the asset and threat identification and completed a risk assessment, **vulnerabilities** can then be identified:

- High value asset, regardless of the likelihood of the threat(s).
- Threats with high likelihood (that is, high ARO).
- Procedures, equipment, or software that increase the likelihood of threats (for example, legacy applications, lack of user training, old software versions, unpatched software, running unnecessary services, not having auditing procedures in place, and so on).

At this point, security measures (controls or countermeasures) can be introduced to address each vulnerability. The difficulty here is in balancing the cost of the control with the cost associated with the risk. It is not often possible to eliminate risk; rather the aim is to mitigate risk factors to the point where the organization is exposed only to a level of risk that it can afford (residual risk).



In the quantitative approach, the Return On Security Investment (ROSI) can be determined by calculating a new ALE, based on the reduction in loss that will be created by the security controls introduced. The ROSI is $ALE(\text{before control}) - ALE(\text{after control}) - \text{Annual Cost of Control}$.

RPO and RTO

Impact analysis is generally governed by two main metrics:

- **Recovery Point Objective (RPO)** - the amount of data loss that a system can sustain, measured in time. That is, if a database is destroyed by a virus, an RPO of 24 hours means that the data can be recovered (from a backup copy) to a point not more than 24 hours before the database was infected.

For example, a customer leads database might be able to sustain the loss of a few hours' or days' worth of data (the salespeople will generally be able to remember who they have contacted and re-key the data manually). Conversely, order processing may be considered more critical, as any loss will represent lost orders. Some organizations may define RPO for mission critical systems as zero.

- **Recovery Time Objective (RTO)** - this is the period following a disaster that a system may remain offline. This represents the amount of time it takes to identify that there is a problem and then perform recovery (restore from backup or switch in an alternative system for instance).

RPO and RTO help to determine which business functions are critical and also to specify appropriate risk countermeasures. For example, if your RPO is measured in days then a simple tape backup system should suffice; if RPO is zero or measured in minutes or seconds, a more expensive server cluster backup and redundancy solution will be required.

Risk Mitigation Options

Risk **mitigation** (or **remediation**) is the overall process of reducing exposure to or the effects of risk factors. There are a number of ways of mitigating risk. If you deploy a countermeasure that reduces exposure to a threat or vulnerability that is risk **deterrence** (or reduction). Risk reduction refers to controls that can either make a risk incident less likely or less costly (or perhaps both).

For example, if fire is a threat, a policy strictly controlling the use of flammable materials on site reduces likelihood while a system of alarms and sprinklers reduces impact by (hopefully) containing any incident to a small area. Another example is offsite data backup, which provides a remediation option in the event of servers being destroyed by fire.

Other risk mitigation strategies are as follows:

- **Avoidance** means that you stop doing the activity that is risk-bearing.

For example, a company may develop an in-house application for managing inventory and then try to sell it. If while selling it the application is discovered to have numerous security vulnerabilities that generate complaints and threats of legal action the company may take the decision that the cost of maintaining the security of the software is not worth the revenue and withdraw it from sale.

Obviously this would generate considerable bad feeling amongst existing customers. Avoidance is not often a credible option.

- **Transference** (or sharing) means assigning risk to a third-party (such as an insurance company or a contract with a supplier that defines liabilities). For example, a company could stop in-house maintenance of an ecommerce site and contract the services to a third-party, who would be liable for any fraud or data theft.



Note that in this sort of case it is relatively simple to transfer the obvious risks but risks to the company's reputation remain. If a customer's credit card details are stolen because they used your insecure ecommerce application, the customer won't care if you or a third-party were nominally responsible for security. It is also unlikely that legal liabilities could be completely transferred in this way.

- **Acceptance** (or retention) means that no countermeasures are put in place either because the level of risk does not justify the cost or because there will be unavoidable delay before the countermeasures are deployed. In this case you should continue to monitor the risk (as opposed to ignoring it).

Security Posture and Continuous Security Monitoring



5shhh



rr21t

Typically, security is only seriously investigated after some sort of incident. In contrast to this reactive approach, adopting a **security posture** means that a company has thought carefully about security and puts it on a level priority with other critical business functions. A security posture refers to the whole range of security controls and risk mitigation techniques that the company has put in place. **Continuous Security Monitoring** (also referred to as **Security Continuous Monitoring**) refers to a process of continual risk re-assessment. This means maintaining a high level of awareness of emerging threats and vulnerabilities. It also refers to **performing routine audits** of rights and privileges plus other key security metrics in "real time" (that is, every day rather than every week or every month for example). These are compared against the **initial baseline configuration** to identify variations that could represent a security incident that must be investigated.

Even by partially automating the process using Intrusion Detection Systems (IDS) this is obviously extremely labor-intensive. Care needs to be taken to identify the metrics that best represent the risks to which an organization is most exposed.



NIST have published a guide to continuous security monitoring (SP800-137), available at gtsgo.to/14417.



See [Unit 3.2](#) for more information about log analysis and IDS.

Integration with Third Parties



9f8rg

Organizations will frequently find themselves needing to integrate their activities with those of third parties, whether these third parties are individual private contractors, providers of services, vendor reps, "cloud" service providers or whether as a result of mergers or acquisitions. Irrespective of the specifics of the individual situation, the critical thing to remember is to go into these relationships having done due care and due diligence and having made sure that this due care and due diligence is written into carefully vetted and legally binding contracts and agreements.



z88xc



n1z1z

Risk Awareness and Security Policy

When two different systems are brought together, the intention and likely focus will be seamless technological integration. Remember that the overall goals of security and compliance must be addressed as well. Before implementing technological solutions and making physical changes, sit down with the information security policies of both organizations, review them, and as appropriate, combine them.

This approach ensures that security is "designed into" the integration project and that the two organizations adopt shared goals for security. It may be problematic to achieve, particularly if one organization has a more developed policy than the other one, but not adopting a similar "security posture" is likely to increase the risk of serious threats emerging as the project progresses.



Interoperability Agreements

It is important to remember that although one can outsource virtually any service or activity to a third party, one cannot outsource legal accountability for these services or actions. You are ultimately responsible for the services and actions that these third parties take. This is why it is so important that you vet them thoroughly. Do you trust their hiring practices? Their training practices? Their access controls? If they have any access to your data or systems, any security breach in their organization (for example unauthorized data sharing) is effectively a breach in yours.

Issues of security risk awareness, shared duties, and contractual responsibilities can be set out in a formal legal agreement. The following types of agreement are common:

- Memorandum of Understanding (MOU) - usually a preliminary or exploratory agreement to express an intent to work together. MOUs are usually intended to be relatively informal and not to act as binding contracts. MOUs almost always have clauses stating that the parties shall respect confidentiality however.
- Service Level Agreement (SLA) - a contractual agreement setting out the detailed terms under which a service is provided. SLAs are discussed in more detail below.
- Business Partners Agreement (BPA) - while there are many ways of establishing business partnerships, the most common model in IT is the partner agreements that large IT companies (such as Microsoft and Cisco) set up with resellers and solution providers.
- Interconnection Security Agreement (ISA) - ISAs are defined by NIST's SP800-47 "Security Guide for Interconnecting Information Technology Systems" (gtsgo.to/rugpy). Any federal agency interconnecting its IT system to a third-party must create an ISA to govern the relationship. An ISA sets out a security risk awareness process and commit the agency and supplier to implementing security controls.

A legal agreement is all very well, but it is still up to you to make sure that your suppliers, vendors, and contractors can live up to them. If they can't, you may successfully sue them, but if they go out of business, you are still accountable for their actions or failure to act.



Conversely, you need to ensure that you can comply with the requirements and performance standards of any agreements that you enter into as a service provider.

Data Backups with Third Parties



lvtco

Having agreed shared goals for security policy and identified a contractual basis on which the integration project will proceed, close attention must then be paid to the actual physical, logical and administrative security controls that will ensure confidentiality, integrity, and availability of data and systems shared between the two organizations. Think through the technological, procedural, and structural changes that will need to be put into place to ensure the security of the newly combined organization.

As an example, responsibility for data backup is of critical importance. If the other party is responsible for backup, do you have access to it for instance? Are the backups stored securely?

There must be no doubt between the two organizations who is responsible for which security procedures. It is also important to audit and review the procedures put in place to ensure they are being performed properly.



efrum



quiba

Privacy and Data Ownership

Many countries, notably in Europe, have legislation protecting the privacy of individuals. This legislation constrains organizations that process personal data. If you enter an interoperability agreement, you must carefully assess the impact of data protection legislation, especially if data will be moved or copied to servers in a different country. You need to review the terms under which personal data was collected and verify that you are authorized to transfer it to a third-party. Systems integrations that span different countries face particular difficulties, particularly when it comes to differing global laws with respect to privacy. The companies involved must have the technical/logical, administrative and physical controls in place to make sure that all such requirements are met and in many cases, must be able to demonstrate this to third parties unrelated to those in the transaction or arrangement.



See [Unit 5.6](#) for more information about data protection legislation.



s48dw

On-boarding and Off-boarding Business Partners

On-boarding is the process by which a new partner is brought into the organization. This process is quite similar to the recruitment of new staff, with the exception that a partner business is likely to bring much more of its own "baggage" along with it.

Having hopefully established agreements to set out the security policies and procedures that both parties will follow, onboarding should be a smooth process. The broad scope of activities is likely to be as follows:

- Establish secure network connections between the two IT systems, including applications and data storage areas.
- Establish a means of authenticating users from either organization and set up access controls and privileges.
- Review the security controls that apply to any shared data (such as access controls, encryption, and DLP) and systems (firewalls, IDS, and NAC for instance).

Off-boarding is the process of terminating the agreement. Again, it is imperative that this process be pre-planned. If it takes place in an ad-hoc way there is huge potential for difficulties and significant security risks. The off-boarding plan should show the IT systems integration will be dissolved and the procedures for securely destroying any data that belongs exclusively to either party.



Regardless of whether the process has been planned, off-boarding is likely to increase risks to your organization. You should consider activities such as changing passwords, re-auditing user privileges and access controls, and increasing the level of security logging and analysis.

Mergers and Acquisitions

Mergers and acquisitions pose many challenges to security. It is imperative that the security manager thoroughly understand the computing environment and all new internal and external threats that might appear as a result of bringing two different computing environments together. Because this period is known to be difficult to manage, there may be attackers who will take advantage to launch an attack. An acute security manager will be aware of this and fully prepared for it. He or she will also remember that not only are attacks more likely to be from the inside of one of the organizations than from the outside, but that mergers and acquisitions invariably result in redundancies and as such, there may be many extremely anxious, angry, or disgruntled employees in either or both companies. Keep an eye out for unexpected high-level connections, for example, and keep a careful watch on employees whose access or access levels are changing. Certainly increase logging and analysis throughout this period.



yfoeu

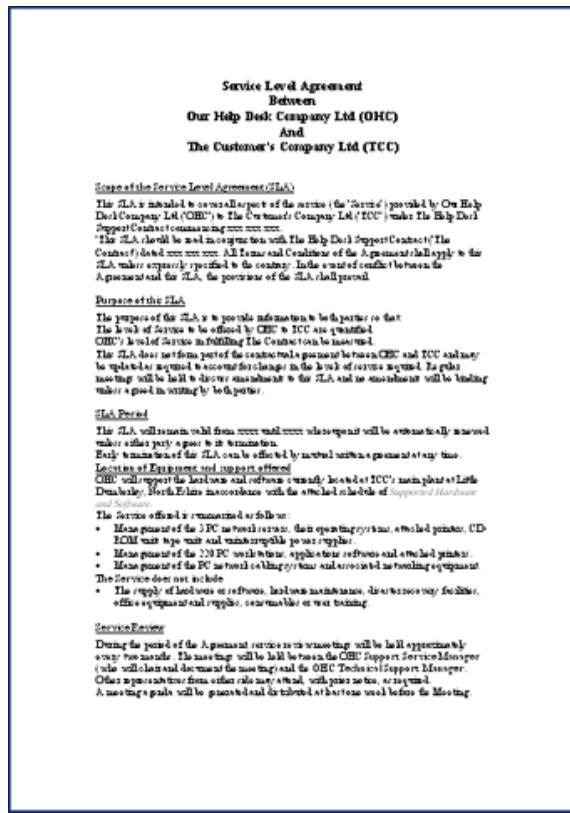
Social Media Networks

One of the ways that companies find themselves integrating with third parties, possibly inadvertently, is through social media. Most companies make active use of social media for marketing and are likely to encourage their employees to contribute enthusiastically. Of course, employees have to be careful not to post confidential information. Social media can also reveal a huge amount about personal lives, all of which is useful to social engineering attacks. With social media blurring the lines between people's professional and private identities it is useful for companies to train their employees about some of the risks of "over-sharing" via social networks.

Service Level Agreements

A **Service Level Agreement (SLA)** is a promise to provide a specific service to a specific standard which has been agreed between two organizations. The SLA is beneficial to both parties as it establishes the scope of the support to be offered and the scope of the support that can be expected by the customer. The SLA helps to ensure that no dispute arises about what incidents are covered and what level of response can be expected.

- Sets customer expectations.
- Provider can manage allocation of resources to meet known targets.
- Acts as a performance benchmark for monitoring and evaluation.



Service Level Agreement

From a security point-of-view, SLAs must be viewed in terms of services that your organization provides and receives. When outsourcing services, it is imperative to obtain an SLA with the contractor. An SLA is a means of transferring risk.

In terms of providing services, your organization is bound to fulfill the terms of the SLA. This means that disaster or incident response policies must be sufficient to provide the service levels defined in the SLA. The input of security managers is essential in drafting an SLA to ensure that its terms are realistic.



10ade

Key Performance Indicators

Key Performance Indicators (KPI) are metrics used in quality and performance management and are also likely to be quoted in an SLA. Some of the main KPIs relating to service availability are as follows.

High Availability / Uptime

Availability is the percentage of time that the system is available and working, measured over the defined period (typically one year). The corollary of availability is downtime (that is, the percentage or amount of time during which the system is unavailable).

High availability is usually loosely described as 24x7 (24 hours per day, 7 days per week) or 24x365 (24 hours per day, 365 days per year). For a critical system, availability will be described as "two-nines" (99%) up to five- or six-nines (99.9999%):

Availability	Annual Downtime
99.9999%	00:00:32
99.999%	00:05:15
99.99%	00:52:34
99.9%	08:45:36
99.0%	87:36:00

Downtime is calculated from the sum of scheduled service intervals (Agreed Service Time) plus unplanned outages over the period.

Response Time

This is a measure of the mean time taken to acknowledge a support request (but not necessarily to fix the problem).

Mean Time to Failure (MTTF) and Mean Time Between Failure (MTBF)

Mean Time to Failure (MTTF) and **Mean Time Between Failures (MTBF)** represent the expected lifetime of a product or system. MTTF should be used for non-repairable systems. For example, a hard drive may be described with an MTTF while a server (which could be repaired by replacing the hard drive) would be described with an MTBF. You will often see MTBF used indiscriminately however. For most devices, failure is more likely early and late in life, producing the so-called "bathtub curve".

Mean Time to Repair (MTTR)

Mean Time to Repair (MTTR) is a measure of the time taken to correct a fault so that the system is restored to full operation. This can also be described as mean time to "replace" or "recover".

Mean Time Between Service Incidents (MTBSI)

Mean Time Between Service Incidents (MTBSI) represents the time between the point of failure of a system and its next point of failure (that is, MTBF + MTTR).

Change and Configuration Management

Configuration Management means identifying all components of ICT infrastructure (hardware, software, and procedures) and their properties.

Change management means putting policies in place to reduce the risk that changes to these components could mean service disruption (network downtime). Both are important parts of an effective risk mitigation strategy.

ITIL Configuration Management Model

ITIL® (IT Infrastructure Library) is a popular documentation of *good and best practice* activities and processes for delivering IT services. Under ITIL, configuration management is implemented using the following elements:

- **Service asset** - things, processes, or people that contribute to the delivery of an IT service.
- **Configuration Item (CI)** - an asset that requires specific management procedures for it to be used to deliver the service. Each CI must be identified by some sort of label. CIs are defined by their **attributes**, which are stored in a **Configuration Management Database (CMDB)**.
- **Baseline** - the baseline represents "the way it was". A baseline can be a **configuration baseline** (the ACL applied to a firewall for instance) or a **performance baseline** (the throughput achieved by a particular server for example).
- **Configuration Management System (CMS)** - the CMS is tools and databases that collect, store, manage, update, and present information about CIs. One of the goals of the CMS is to understand the *relationships* between CIs. Another is to track *changes* to CI attributes (and therefore variance from the baseline) over time.

Implementing Configuration Management

The main difficulty in implementing a workable configuration management system is in determining the level of *detail* that must be preserved. This is not only evident in capturing the asset database and configuration baseline in the first place but also in managing **Moves, Adds, and Changes (MACs)** within the network infrastructure.

In terms of network tasks, a CMS will require that configuration changes be made *only* when there is a valid job ticket authorizing the change. This means that the activity of all network personnel, whether it be installing new devices or troubleshooting, is recorded in **job logs**. Consequently, configuration management involves drafting and enforcing **policies** and **procedures** (Standard Operating Procedures or SOPs) to govern all levels of network configuration and troubleshooting activity.



Implementing Change Management

In order to reduce the risk that changes to configuration items will cause service disruption, a documented change management process can be used to implement changes in a planned and controlled way.

The need to change is often described either as **reactive**, where the change is forced on the organization, or as **proactive**, where the need for change is initiated internally. Changes can also be categorized according to their impact and level or risk (major, significant, minor, or normal for instance).

In a formal change management process, the need for change and the procedure for implementing the change is captured in a **Request for Change (RFC)** document and submitted for approval. The RFC will then be considered at the appropriate level. This might be a supervisor or department manager if the change is normal or minor. Major or significant changes might be managed as a separate project and require approval through a **Change Advisory Board (CAB)**.

Regardless of whether an organization is large enough to require formal change management procedures and staff, the implementation of changes should be carefully planned, with consideration for how the change will affect dependent components. For most significant or major changes, organizations should attempt to trial the change first. Every change should be accompanied by a rollback (or remediation) plan, so that the change can be reversed if it has harmful or unforeseen consequences. Changes should also be scheduled sensitively if they are likely to cause system downtime or other negative impact on the workflow of the business units that depend on the IT system being modified.

When the change has been implemented, its impact should be assessed and the process reviewed and documented to identify any outcomes that could help future change management projects.



Review Questions / Module 5 / Unit 3 / Risk Management

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What are the main components of BIA?
- 2) What is a Continuity of Operations plan?
- 3) What metric(s) could be used to make a quantitative calculation of risk due to a specific threat to a specific function or asset?
- 4) What factors determine the selection of security controls in terms of an overall budget?
- 5) What metric would be put in-place to minimize acceptable downtime following a security incident?
- 6) What type of risk mitigation option is offered by purchasing insurance?
- 7) What type of interoperability agreement would be appropriate at the outset of two companies agreeing to work with one another?
- 8) What type of interoperability agreement is designed to ensure specific performance standards?
- 9) What metric is used to identify the expected service lifetime of a non-repairable appliance?
- 10) What is the first step in initiating a change if an organization is following a formal change management process?

Module 5 / Unit 4

Disaster Recovery

Objectives

On completion of this unit, you will be able to:

- Develop effective disaster recovery plans.
- Use IT contingency planning to eliminate single points of failure and provide fault tolerance and redundancy.



Disaster Recovery Planning

Business continuity means planning systems and operations so that they are as little affected by incidents as possible and so that the resources are available to recover from them. **Disaster recovery** plans describe the procedures to follow in the event of severe incidents. When planning a network, the administrator must consider the impact of data loss and service unavailability on the organization. If a local plumber loses his email connection for a day, then the chances are he or she will lose little business because of it and he will still be able to function in his primary role of plumber (conversely, losing a cell phone could be catastrophic!). Therefore little consideration would be needed to plan for disasters. Conversely, if a major bank lost its trading floor link to its partners, even for an hour, since the organization's primary function (trading) would be impossible, huge losses may result. Significant thought is required to ensure that a disaster does not cause this kind of loss to what are termed **mission critical systems**.

A disaster could be anything from a fairly trivial loss of power, or failure of a minor component, through to man-made or natural disasters, such as fires, earthquakes, or acts of terrorism.

Creating Disaster Recovery Plans

An organization sensitive to these risks will develop an effective, documented **Disaster Recovery Plan (DRP)**. This should accomplish the following:

- Identify scenarios for natural and non-natural disaster and options for protecting systems. Plans need to take account of **risk** (a combination of the likelihood the disaster will occur and the possible impact on the organization) and **cost**.

There is no point implementing disaster recovery plans that financially cripple the organization. The business case is made by comparing the cost of recovery measures against the cost of downtime. Downtime cost is calculated from lost revenues and ongoing costs (principally salary). The recovery plan should not generally exceed the downtime cost. Of course, downtime will include indefinable costs, such as loss of customer goodwill, restitution for not meeting service contracts, and so on.

For each disaster scenario, a **Business Impact Analysis (BIA)** is made, identifying risks and vulnerabilities and advising on appropriate countermeasures.

- Identify tasks, resources, and responsibilities for responding to a disaster.
 - Who is responsible for doing what? How can they be contacted? What happens if they are not available?
 - Which functions are most critical? Where should effort be concentrated first?
 - What resources are available? Should they be pre-purchased and held as stock? Will the disaster affect availability of supplies? (see the topic on redundancy below).
 - What are the timescales for resumption of normal operations?
- Train staff in the disaster planning procedures and how to react well to change.



x5r8h

Succession Planning

As well as risks to systems, a BIA has to take on the macabre issue of human capital resilience. Put bluntly, this means "Is someone else available to fulfil the same role if an employee is incapacitated?"

Succession planning targets the specific issue of leadership and senior management. Most disaster recovery plans are heavily dependent on a few key people to take charge during the disaster and ensure that the plan is put into effect. Succession planning ensures that these sorts of competencies are widely available to an organization.



o63z6

Testing Disaster Recovery Plans

It is necessary to test disaster recovery procedures. There are two means of doing this:

- Tabletop exercise – staff "ghost" the same procedures as they would in a disaster, without actually creating disaster conditions or applying or changing anything. These are simple to set up but do not provide any sort of practical evidence of things that could go wrong, time to complete, and so on.
- Disaster recovery exercises designed to simulate different scenarios. These are extremely complex to set up, especially if run in the production environment rather than a test environment.

Also identify timescales for disaster plans to be reviewed, to take account of changing circumstances and business needs. Following an incident, it is vital to hold a review meeting to analyze why the incident occurred, what could have been done to prevent it, and how effective was the response?



Disaster recovery is closely related to incident response. Refer to [Unit 5.5](#) for more information about incident response policies and personnel.

As well as restoring systems, the disaster recovery plan should identify stakeholders who need to be informed about any security incidents. There may be a legal requirement to inform the police or fire service or buildings inspectors about any safety-related or criminal incidents. If third-party or personal data is lost or stolen, the data subjects may need to be informed. If the disaster affects services, customers need to be informed about the time-to-fix and any alternative arrangements that can be made.

Secure Recovery

When a disaster has occurred, then the recovery plan will swing into action to get the failed part of the network operational as soon as possible. If a disk has failed, swap it out. If a node in a cluster has failed, remove and replace or repair the node to provide for high reliability as soon as possible. If data becomes corrupted or lost, utilize your restore plan to recover the data.

With the pressure to get systems running again though, it is important not to overlook the process of re-securing the system against intrusion. The system needs to be restored to its baseline **secure** configuration.

Another issue is that creating a duplicate of anything doubles the complexity of securing that resource properly. The same security procedures must apply to redundant sites, spare systems, and backup data as applies to the main copy.

IT Contingency Planning



Computer systems require protection from hardware failure, software failure, and system failure (failure of network connectivity devices for instance).

When implementing a network, the goal will always be to minimize the **single points of failure** and to allow ongoing service provision despite a disaster. To perform **IT Contingency Planning (ITCP)**, think of all the things that could fail, determine whether the result would be critical loss of service, and whether this is unacceptable. Then work out how to make the service fault tolerant.

Fault Tolerance

A system that can experience failures and continue to provide the same (or nearly the same) level of service is said to be **fault tolerant**. Fault tolerance is often achieved by provisioning **redundant** components. A redundant component is one that is not essential to the normal function of a system but that allows the system to recover from the failure of another component.

Examples of devices and solutions that provide fault tolerance and high availability include the following:

- Redundant components (power supplies, network cards, drives (RAID), and cooling fans) provide protection against hardware failures. Hot swappable components allow for easy replacement (without having to shut down the server).
- Uninterruptible Power Supplies (UPS) and Standby Power Supplies.
- Backup strategies - provide protection for data.
- Cluster services are an (expensive) way of ensuring that the total failure of a server does not disrupt services generally.

While these computer systems are important, thought also needs to be given about how to make a business "fault tolerant" in terms of staffing, utilities (heat, power, communications, transport), customers, and suppliers.

The following components are often provided with redundancy on server systems.

Load Balancing Network Links

Without a network connection, a server is not of much use! As network cards are cheap, it is commonplace for a server to have multiple cards (adapter fault tolerance).

Multiple adapters can be configured to work together (adapter teaming). This provides fault tolerance (if one adapter fails, the network connection will not be lost) and can also provide **load balancing** (connections can be spread between the cards).



Note that adapter teaming does have a functional benefit (higher bandwidth). If one of the adapters fails, that benefit would be lost. For the system to be fault tolerant, the higher bandwidth must not be critical to the function.

Network cabling should be designed to allow for **multiple paths** between the various servers, so that during a failure of one part of the network, the rest remains operational (**redundant connections**). Routers are great fault tolerant devices, because they can communicate system failures and IP packets can be routed via an alternate device.



Multiple switching paths require use of Spanning Tree Protocol (STP) to prevent loops. Also note that routers can only be fault tolerant if there are multiple routes to choose from!

Power Supply

Power supplies are one of the components more likely to break down than others. They are cheap, but they do take up a lot of space. A second power supply can be configured to take over from the first if it fails.

A redundant power supply unit does not protect against problems with the supply of power itself. For this you need a Universal Power Supply (UPS) and/or backup generator.

A **UPS** is always required to provide against any interruption to computer services. A backup generator cannot be brought online fast enough to respond to a power failure. The drawback of a UPS is that it is battery-based and therefore only able to provide power for a limited time; this could range from a few minutes to a few hours depending on the size of the battery bank and the server load. The UPS also obviously only provides power to critical server components, not lighting, HVAC, mains distribution, or other features of buildings power.

A **backup generator** can provide power to the whole building, often for several days. Most generators use diesel, propane, or natural gas as a fuel source. With diesel and propane, the main drawback is safe storage (diesel also has a shelf-life of between 18 months and 2 years); with natural gas, the issue is the reliability of the gas supply in the event of a natural disaster.

Cooling Fans

Because servers contain many heat generating components (notably processors, hard drives, and power supplies), efficient cooling systems are particularly important. As a mechanical component, fans are more likely to fail than many other computer components. Each component that "runs hot" will have its own cooling fan. Obviously it is not practical to provide redundant versions of these, but the system may have "general" fans to cool the interior of the case and monitoring in-place to warn of failures.

Hardware and Spare Parts

Subject to budget and storage facilities, companies may keep an inventory of spare parts.

The simplest (but most expensive) approach is to keep fully functioning hardware such as spare servers and workstations so that faulty units can simply be swapped out and the fault investigated offline. This provides the least downtime.

Alternatively, spares of CPUs, memory, network cards, hard disks, and so on can be kept. The main issue here is maintaining an inventory that is compatible with the various technologies deployed on the network.

Given the swift turnover of technology, obsolescence makes spare part storage an expensive business. One solution is to use older equipment for emergency failovers, but there will be a substantial decrease in performance.

Hard Disks

The hard disks store the most valuable component of any computer system: data. Data can be protected by making backups, but only very expensive backup solutions can make up-to-the minute copies of data. Multiple disks on a server are typically configured as RAID arrays.

Drive Arrays (RAID)

With **RAID (Redundant Array of Independent Disks)**, many disks can act as backups for each other to increase reliability and fault tolerance. If one disk fails, the data is not lost and the server can keep functioning. The RAID advisory board defines RAID levels, numbered from 0 to 6, where each level corresponds to a specific type of fault tolerance. There are also proprietary and nested RAID solutions. Some of the most commonly implemented types of RAID are listed below:

RAID Level	Fault Tolerance
Level 0	Striping without parity (no fault tolerance). This means that data is written in blocks across several disks simultaneously. This can improve performance, but if one disk fails, so does the whole volume and data on it will be corrupted.
Level 1	Mirroring - data is written to two disks simultaneously, providing redundancy (if one disk fails, there is a copy of data on the other). The main drawback is that storage efficiency is only 50%.
Level 5	Striping with parity - data is written across three or more disks but additional information (parity) is calculated. This allows the volume to continue if one disk is lost. This solution has better storage efficiency than RAID 1.
Nested (0+1, 1+0, or 5+0)	Nesting RAID sets generally improves performance or redundancy (for example, some nested RAID solutions can support the failure of more than one disk).

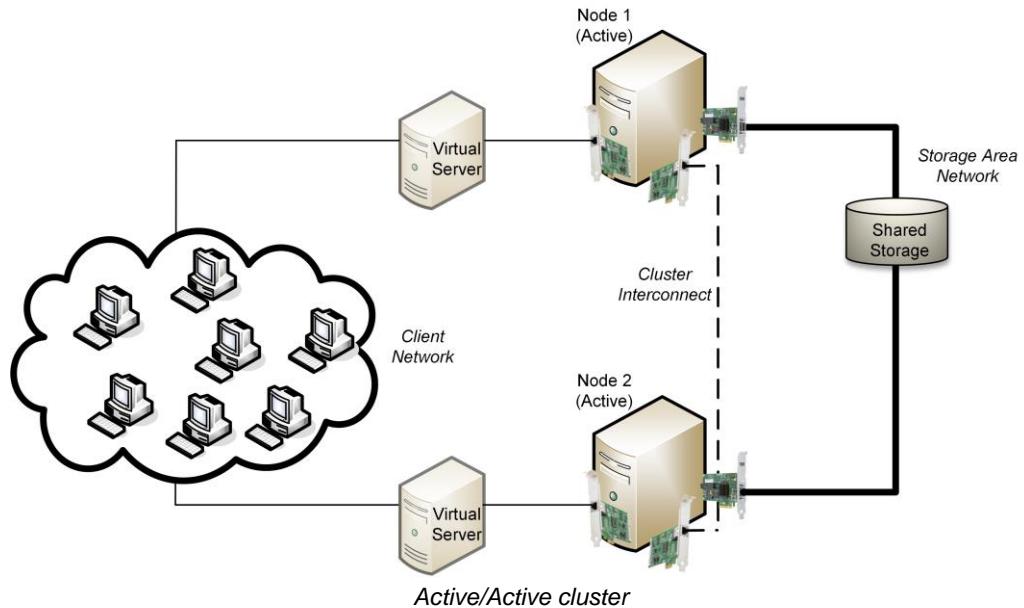
Clusters and Sites

As well as providing redundancy at a device level, whole servers or even sites can be provisioned.

Clusters

A **cluster** is a group of servers, each of which is referred to as a node. A cluster provides fault tolerance for critical applications. They do this by being in a position to take over the processing of a failed node in the cluster should a problem occur. There are essentially two types of clustering: Active/Active and Active/Passive.

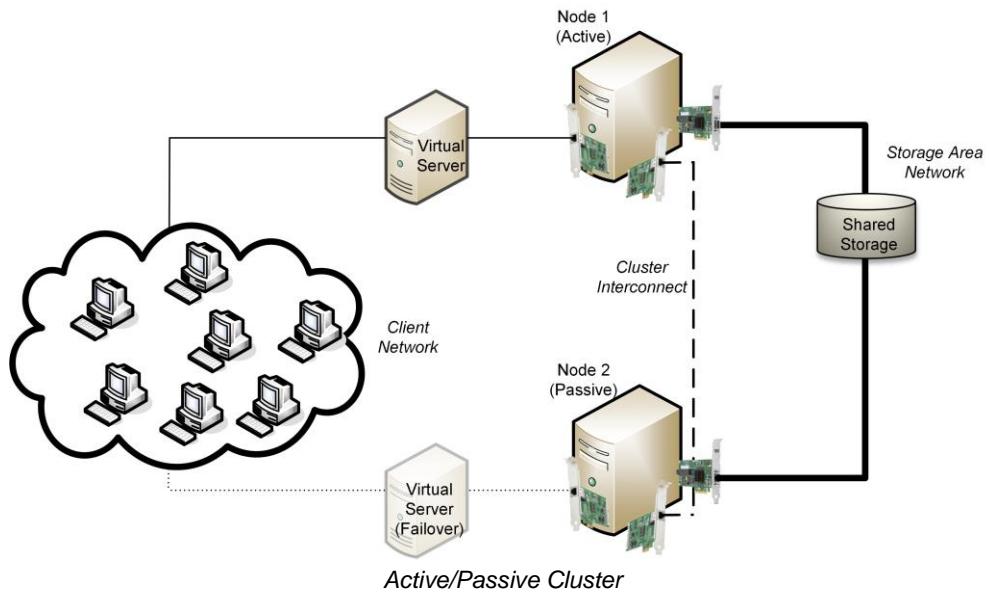
Active/Active (A/A) Clustering



Active/Active configurations consist of n nodes, all of which are processing concurrently. This allows the administrator to use the maximum capacity from the available hardware while all nodes are functional. In the event of a failover (the term used to describe the situation where a node has failed) the workload of the failed node is immediately (and transparently) shifted onto the remaining node(s). At this time, the workload on the remaining nodes is higher and performance is degraded during failover - a significant disadvantage.

Active/Passive (A/P) Clustering

Active/Passive configurations use a redundant node to failover. In other words, in an 8-node Active/Passive cluster, the eighth node doesn't do anything and supports no services (other than those needed to support the cluster itself) until a failover occurs. It then assumes responsibility for the failed node's services. The major advantage of Active/Passive configurations is that performance is not adversely affected during failover. However, the hardware and operating system costs are higher because of the unused capacity.



Some applications and services will not function in a clustered environment and some sub-components of cluster aware applications cannot run on a cluster. You will need to be aware of these restrictions when planning the cluster implementation.

Uses for Clustering

Clustering is generally used to provide a high level of fault tolerance for **back-end** applications. For example, if you wanted to provide a resilient online purchasing system based around SQL Server, you might install a clustering solution to support the actual SQL databases.

At the **front-end**, a network load balancing solution for the web servers might be more suitable than a cluster. This is because the web servers don't contain data that changes; they merely handle client requests to such data. The SQL Servers do contain data which will change (stateful data).

Most implementations of clustering work on the principle of linking the nodes together using a private network, which does not support client connections (another network is provided for this). A message is sent periodically between the nodes to demonstrate that a node is healthy and available. Absence of this message from a node would cause a failover.

To allow for the quick shift of services from one node to another, most vendors support a shared disk technology. As well as their own private storage, nodes share access to a disk array (usually a Storage Area Network), which contains the data that will be switched in during failover.

Hot, Warm, and Cold Spares

In the absence of configuring clusters, many administrators have standby servers set aside (spares), which are not on the live network, in readiness for recovery situations. Standby servers can be classified as cold, warm, or hot:

- **Cold server** - the server is configured with the OS and then left turned off.
- **Warm server** - the server is updated periodically with backup data.
- **Hot server** - the server is updated regularly and is ready to take over in the event of a failure.



Hot, Warm, and Cold Sites

Providing redundant devices and spares allows the spare devices to be swapped in if existing systems fail. Enterprise-level networks often also provide for spare **sites**. A site is another location that can provide the same (or similar) level of service. Operations are swapped over to the new site until the previous site can be brought back online.

Sites are also referred to as being **hot**, **warm**, or **cold**. A hot site can be brought into operation almost immediately (within 24 hours for example). It generally means that the spare or site is already within the organization's ownership and is ready to deploy. A cold site takes longer to set up (up to a week).

For example, a hot site could consist of a building with operational computer equipment that is kept updated with a live data set. A warm site could be similar, but with the requirement that the latest data set will need to be loaded. A cold site may be an empty building with a lease agreement in place to install whatever equipment is required when necessary.

Clearly, providing redundancy on this scale can be very expensive. Sites are often leased from service providers, such as Comdisco or IBM (a **subscription service**). However, in the event of a nationwide emergency, demand for the services is likely to outstrip supply!

Another option is for businesses to enter into **reciprocal arrangements** to provide mutual support. This is cost effective but complex to plan and set up.

Replication

Replication is the process of duplicating data between different servers or sites. RAID mirroring and server clustering are examples of disk-to-disk and server-to-server replication.

Replication can either be **synchronous** or **asynchronous**. Synchronous replication means that the data must be written at both sites before it can be considered committed. Asynchronous replication means that data is mirrored from a primary site to a secondary site.

Disk-to-disk and server-to-server replication are relatively simple to accomplish as they can use direct access RAID or local network technologies. Site-to-site replication is considerably harder and more expensive as it relies on Wide Area Network technologies. Determining the optimum distance between two replicating sites depends on evaluating two competing factors:

- If the sites are too close together (within about 500km), they could *both* be affected by the same disaster.
- The farther apart the sites are, the more costly replication will be. Synchronous replication is particularly sensitive to distance as the longer the communications pathway, the greater the latency of the link. Latency can be mitigated by provisioning fiber optic links.



Review Questions / Module 5 / Unit 4 / Disaster Recovery

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What is the difference between disaster recovery and business continuity planning?
- 2) Why are disaster recovery exercises an important part of creating a disaster recovery plan?
- 3) In which types of disaster recovery site(s) would you expect to have to install computer equipment?
- 4) Is RAID mirroring a backup technology?
- 5) True or false? UPS can provide emergency power for days at a time.
- 6) What factor is most likely to reduce a system's fault tolerance?
- 7) What phrase describes ensuring that critical functions remain properly staffed?
- 8) What is a tabletop exercise?
- 9) What security considerations affect an alternate hot site that do not generally apply to warm or cold sites?
- 10) What risk is there in leasing alternate sites (as opposed to owning them)?



If you have access to the Hands On Live Labs, complete the "Compliance / RAID" and "Compliance / Clustering" labs now.

Module 5 / Unit 5

Incident Response and Forensics

Objectives

On completion of this unit, you will be able to:

- Describe the stages and responsibilities of a formal incident response policy.
- Describe the characteristics of the forensic investigation of computer systems.

Incident Response Procedures



jj2y1

Incident management or **incident response procedures** are the actions and guidelines for dealing with security incidents. An incident is where security is breached or there is an attempted breach; NIST describe an incident as "the act of violating an explicit or implied security policy". Incident management is vital to mitigating risk. As well as controlling the immediate or specific threat to security, effective incident management preserves an organization's reputation.

However, incident response is also one of the most difficult areas of security to plan for and implement because its aims are often incompatible:

- Re-establish a secure working system.
- Preserve evidence of the incident with the aim of prosecuting the perpetrators.
- Prevent reoccurrence of the incident.

The actions of staff immediately following detection of an incident can have a critical impact on these aims, so an effective policy and well-trained employees are crucial. They help to calm nerves in the aftermath of an incident. Incident response is also likely to require coordinated action and authorization from several different departments or managers, which adds further levels of complexity.

The **NIST Computer Security Incident Handling Guide** special publication ([SP800-61](#)) identifies the following stages in an incident response lifecycle:

- **Preparation** - making the system resilient to attack in the first place. This includes hardening systems, writing policies and procedures, and establishing confidential lines of communication. It also implies creating incident response resources and procedures.

- **Detection and Analysis** - determining whether an incident has taken place and assessing how severe it might be, followed by notification of the incident to stakeholders.
- **Containment, Eradication, and Recovery** - limiting the scope and magnitude of the incident. The typical response is to "pull the plug" on the affected system, but this is not always appropriate. Once the incident is contained, the cause can then be removed and the system brought back to a secure state.
- **Post-incident Activity** - analyzing the incident and responses to identify whether procedures or systems could be improved. It is imperative to document the incident.

Preparation



c49n5

As defined above, an incident is any event that breaches security policy. Of course, this covers a huge number and variety of different scenarios. Preparing for incident response means establishing the **policies and procedures** for dealing with security breaches and the **personnel and resources** to implement those policies. In order to identify and manage incidents, an organization should develop some method of reporting, categorizing, and prioritizing them (**triage**), in the same way that troubleshooting support incidents can be logged and managed.

Incident response policies should also establish clear lines of communication, both for reporting incidents and for notifying affected parties as the management of an incident progresses. It is vital to have essential contact information readily available. Also consider that the incident response personnel might require secure, out-of-band communication methods, in case standard network communication channels have been compromised.

From the policies, incident response procedures can be developed and resources put in place to implement them. As well as investment in appropriate detection and analysis software, incident response requires expert staffing.

Computer Security Incident Response Team (CSIRT)

Larger organizations will provide a dedicated **Computer Security Incident Response Team (CSIRT)** as a single point-of-contact for the **notification** of security incidents. The members of this team should be able to provide the range of decision making and technical skills required to deal with different types of incident. The team needs a mixture of senior decision makers (up to director level), who can authorize actions following the most serious incidents, managers, and technicians (who can deal with minor incidents on their own initiative).

It is also important to have legal expertise, so that the team can evaluate incident response from the perspective of compliance with laws and industry regulations. Finally, the team is likely to require marketing or public relations input, so that any negative publicity from a serious incident can be managed.

Another important consideration is availability. Incident response will typically require 24/7 availability, which will be expensive to provide.

Some organizations may prefer to outsource some of the CSIRT functions to third-party agencies. External agents may also be able to deal more effectively with insider threats.

As well as incident management and forensic software (see later in this unit) the team will need communication resources and contact information. It is often appropriate to provide separate and secure work areas and networking and storage facilities so that incidents can be investigated with some degree of independence from the setting under scrutiny.

Prevention

Of course, the best outcome is to minimize the number of incidents that occur. The company's overall risk mitigation, business continuity, disaster recovery, intrusion prevention, and training and education programs should all be in place.

Detection and Analysis



Detection is the process of collating events and determining whether any of them should be managed as incidents or as possible **precursors** to an incident; that is, an event that makes an incident more likely to happen. There are multiple channels by which events or precursors may be recorded:

- Automated malware and intrusion detection and log analysis software.
- Manual or physical inspections of site, premises, networks, and hosts.
- Notification by an employee, customer, or supplier.
- Public reporting of new vulnerabilities or threats by a system vendor, regulator, the media, or other outside party.

It is wise to provide for confidential reporting so that employees are not afraid to report insider threats, such as fraud or misconduct. It may also be necessary to use an "out-of-band" method of communication so as not to alert the intruder that his or her attack has been detected.



An employee (or ex-employee) who reports misconduct is referred to as a whistleblower.

First Responder



6bh7m

When a suspicious event is detected, it is critical that the appropriate person on the CSIRT be notified so that they can take charge of the situation and formulate the appropriate response. This person is referred to as the **first responder**. This means that employees at all levels of the organization must be trained to recognize and respond appropriately to actual or suspected security incidents. A good level of security awareness across the whole organization will reduce the incidence of false positives and negatives. For the most serious incidents, the entire CSIRT may be involved in formulating an effective response.



It is important to provide redundancy in terms of personnel that can respond to an incident (succession planning). Consider a scenario in which a key staff member cannot be contacted; is there a backup option? This scenario also illustrates the importance of maintaining documented procedures.

Analysis and Incident Identification



strkx

When notification has taken place, the CSIRT or other responsible person(s) must analyze the event to determine whether a genuine incident has been identified and what level of priority it should be assigned. Analysis will depend on identifying the type of incident and the data or resources affected (its scope and impact).

At this point, the incident management database should have a record of the event indicators, the nature of the incident, its impact, and the incident investigator responsible. The next phase of incident management is to determine an appropriate response.

Containment



6nmgq



xzxpv

As incidents cover such a wide range of different scenarios, technologies, motivations, and degrees of seriousness, there is no standard approach to **containment** or **incident isolation**. Some of the many complex issues facing the CSIRT are:

- What damage or theft has occurred already? How much more could be inflicted and in what sort of time frame (loss control)?
- What countermeasures are available? What are their costs and implications?
- What actions could alert the attacker to the fact that the attack has been detected? What evidence of the attack must be gathered and preserved?

Quarantine and Device Removal

If further evidence needs to be gathered, the best approach may be to **quarantine** or **sandbox** the affected system or network. This allows for analysis of the attack and collection of evidence using digital forensic techniques (see below). This can only be done if there is no scope for the attacker to cause additional damage or loss however.

There are great practical problems in establishing an effective quarantine however. It may be possible to redirect the attacker into some kind of honeypot or honeynet or to use a firewall or intrusion detection to limit wider access. It may also be possible to restrict the attack by changing account passwords or privileges or to apply patches to hosts not yet affected by the attack.

Another option is to remove an affected device from the system it is attached to ("pull the plug"). This will prevent the attacker from widening the attack but may alert him or her to the fact that the attack has been detected. A sophisticated attacker may have retaliatory attacks prepared to meet this sort of contingency.



Escalation

An incident may be judged too critical to continue to be managed by the first responder. The process by which more senior staff become involved in the management of an incident is called **escalation**. Escalation may also be necessary if no response is made to an incident within a certain time frame.



Data Breach and Notification

A **data breach** is where an attack succeeds in obtaining information that should have been kept secret or confidential. Once data has been stolen in this way, it is virtually impossible to prevent further copies of it being made, though it may be possible to act against those that try to publish it.

It has to be assumed however that the data stolen is no longer confidential. It is critical to identify precisely what has been stolen, though often this is a difficult enough task in itself. Security systems must be reanalyzed and re-secured, so that things like passwords are changed, even if there is no direct evidence that they have been compromised. Note that in this context the suspicion of data theft may be enough to have to trigger reporting procedures. Even if it is only suspected that customer passwords or credit card numbers have been stolen (for instance), customers must be notified so that they can take steps to re-secure other online accounts or financial accounts.

As well as attempting to identify the attacker, a data breach will normally require that affected parties be notified, especially if Personally Identifiable Information (PII) or account security information is involved. As well as data protection legislation, many industries have strict regulations regarding the safe processing of data and will set out requirements for notifying affected customers as well as the regulator. The regulator will also require evidence that the systems that allowed the breach have been improved.

Eradication and Recovery



There are often no right answers to the question of what **mitigation steps** are appropriate to contain, eradicate, and recover from an incident. The response team may have to choose the "least bad" option. While prosecution of the offenders may be important, business continuity is likely to be the team's overriding goal. Again though, every situation is different and if there is sufficient time, a full evaluation of the different issues should be made so that the best response can be selected. Some sample responses to incidents include the following:

- Investigation and escalation - the causes or nature of the incident might not be clear, in which case further (careful) investigation is warranted.
- Containment - allow the attack to proceed but ensure that valuable systems or data are not at risk. This allows collection of more evidence, making a prosecution more likely and also gathering information about the way the attack was perpetrated.
- Hot swap - a backup system is brought into operation and the live system frozen to preserve evidence of the attack.
- Prevention - countermeasures to end the incident are taken on the live system (even though this may destroy valuable evidence).

Recovery from the attack will involve a number of steps:

- Reconstitution of affected systems - either remove the malicious files or tools from affected systems or restore the systems from secure backups.



If reinstalling from baseline template configurations, make sure that there is nothing in the baseline that allowed the incident to occur! If so, update the template before rolling it out again.

- Re-audit security controls - ensure they are not vulnerable to another attack. This could be the same attack or from some new attack that the attacker could launch through information they have gained about your network.



If your organization is subjected to a targeted attack, be aware that one incident may be very quickly followed by another.

- Ensure that affected parties are notified and provided with the means to remediate their own systems. For example, if customers' passwords are stolen, they should be advised to change the credentials for any other accounts where that password might have been used (not good practice, but most people do it).

Post-incident Activity



ak606

Once the attack or immediate threat has been neutralized and the system restored to secure operation, some follow-up actions are appropriate. The most important is to review security incidents to determine their cause and whether they were avoidable. This can be referred to as "**lessons learned**". It is also necessary to review the response to the incident, to determine whether it was appropriate and well implemented.

You also need to consider obligations to **report** the attack. As mentioned above, it may be necessary to inform affected parties during or immediately after the incident so that they can perform their own remediation. It may also be necessary to report to regulators or law enforcement. You also need to consider the marketing and PR impact of an incident. This can be highly damaging and you will need to demonstrate to customers that security systems have been improved.

Forensic Procedures

Computer **forensics** is the science of collecting evidence from computer systems to a standard that will be accepted in a court of law. It is highly unlikely that a computer forensic professional will be retained by an organization, so such investigations are normally handled by law enforcement agencies.



Law enforcement agencies will prioritize the investigation of the crime over business continuity. This can greatly compromise the recovery process, especially in smaller businesses, as an organization's key assets may be taken as evidence.

Like DNA or fingerprints, digital evidence is mostly **latent**. Latent means that the evidence cannot be seen with the naked eye; rather it must be interpreted using a machine or process. Forensic investigations are most likely to be launched against crimes arising from insider threats, notably fraud or misuse of equipment (to download or store obscene material for instance). Prosecuting external threat sources is often extremely difficult, as the attacker may well be located in a different country or have taken effective steps to disguise his or her location and identity. Such prosecutions are normally initiated by law enforcement agencies, where the threat is directed against military or governmental agencies or is linked to organized crime. Cases can take years to come to trial.

Due Process

Due process is a term used in US and UK common law to require that people only be convicted of crimes following the fair application of the laws of the land. More generally, due process can be understood to mean having a set of procedural safeguards to ensure fairness. This principle is central to forensic investigation.

If a forensic investigation is launched (or if one is a possibility) it is important that technicians and managers are aware of the processes that the investigation will use. It is vital that they are able to assist the investigator and that they not do anything to compromise the investigation. In a trial, defense counsel will try to exploit any uncertainty or mistake regarding the integrity of evidence or the process of collecting it.



As mentioned above, the "first response" period following detection and notification is often critical. To gather evidence successfully, it is vital that staff do not panic and act without thinking.

Computer Misuse Legislation

Computer misuse is often, but not always, criminalized by national legislation. In the UK, the principal pieces of legislation are the **Computer Misuse Act (1990)** and the **Police and Justice Act (2006)**; in the US, the principal piece of legislation is the **Computer Fraud and Abuse Act (1996)**.

Legislation against fraud and espionage and protecting consumer rights can also apply.

Collection of Evidence



vvjp1

The first phase of a forensic investigation is collection of evidence. The two principal questions here are:

- What evidence must be collected?
- How should the evidence be collected?

Neither question is trivial. A computer system may contain multiple gigabytes (or even terabytes) of data, most of which will not be relevant to the incident. Additionally, evidence may only exist in volatile storage (system or cache RAM). Additionally, if the computer system or device is not owned by the organization, there is the question of whether search or seizure is legally valid. This impacts on Bring Your Own Device (BYOD) policies for instance. This may also make it difficult for law enforcement agents to begin an investigation. For example, if an employee is accused of fraud you must verify that the employee's equipment and data can be legally seized and searched. Any mistake may make evidence gained from the search inadmissible.



There is an ISOC best practice guide to evidence collection and archiving published as [RFC 3227](#).

The question of "how" is complicated because it is much more difficult to capture evidence from a digital "crime scene" than it is from a physical one. As mentioned above, some evidence will be lost if the computer system is powered off; on the other hand some evidence may be unobtainable *until* the system is powered off. Additionally, evidence may be lost depending on whether the system is shut down or "frozen" by suddenly disconnecting the power.

The general principle is to capture evidence in the **order of volatility**, from more volatile to less volatile. [RFC 3227](#) sets out the general order as follows:

- CPU registers and cache memory (including cache on disk controllers, GPUs, and so on).
- Routing table, arp cache, process table, kernel statistics.
- Memory (RAM).
- Temporary file systems.
- Disk.
- Remote logging and monitoring data.
- Physical configuration and network topology.
- Archival media.



Capture Video and Screenshots

The crime scene must be thoroughly documented using photographs and ideally video and audio. Investigators must record every action they take in identifying, collecting, and handling evidence.



Remember that if the matter comes to trial, the trial could take place months or years after the event. It is vital to record impressions and actions in notes.

If possible, evidence is gathered from the live system (including screenshots of display screens and the contents of cache and system memory) using forensic software tools. It is vital that these tools do nothing to modify the digital data that they capture.



Also consider that in-place CCTV systems or webcams might have captured valuable evidence.

Capture System Image



vp8fr



8wykx

Forensic tools are used to make a copy of data on the hard drive(s). This is performed using drive imaging rather than file copy methods, so that the copy is made at sector level. A cryptographic hash is made of the collected data. This can be used to prove that the digital evidence collected has not been modified subsequently to its collection.



Forensic procedures are assisted by having an appropriate software toolkit. These are programs that provide secure drive imaging, encryption, and data analysis. There are commercial toolkits (such as EnCase, Vogon, and SafeBack) plus free software, though these tend to be oriented to Linux (such as data dumper [dd], md5sum, grep, and The Coroner's Toolkit).



4429t

Record Time Offset

Different OS and different file systems use different methods to identify the time at which something occurred.

The benchmark time is **Coordinated Universal Time (UTC)**, which is essentially the time at the Greenwich meridian. Local time is the time within a particular time zone, which will be offset from UTC by a number of hours (or in some cases half hours). The local time offset may also vary if a seasonal daylight saving time is in place (as this is the case in the UK, you can be standing on the Greenwich meridian and still be offset from UTC).

NTFS uses UTC "internally" but many OS and file systems record time stamps as the local system time. When collecting evidence it is vital to establish this fact and note the offset between the local system time and UTC.

Forensics also needs to consider that a computer's system clock may not be properly synchronized to a valid time source or may have been tampered with. Most computers are configured to synchronize the clock to a **Network Time Protocol (NTP)** server. Closely synchronized time is important for authentication and audit systems to work properly. The right to modify a computer's time would normally be restricted to administrator-level accounts (on enterprise networks) and time change events should be logged.



twllu

Network Traffic and Logs

Most machines are not configured to record all network traffic, as this would generate a very considerable amount of data. There are certainly protocol analyzers that can do this job but few organizations would deploy them continually.

Most network appliances, such as firewalls and IDS, do log events and these are likely to be valuable evidence of an intrusion or security breach.



Interview Witnesses

As well as digital evidence, an investigator should also interview witnesses to establish what they were doing at the scene, whether they observed any suspicious behavior or activity, and also to gather information about the computer system.

An investigator might ask questions informally and record the answers as notes to gain an initial understanding of the circumstances surrounding an incident. An investigator must ask questions carefully, to ensure that the witness is giving reliable information and to avoid leading the witness to a particular conclusion.

Making a video or audio recording of witness statements produces a more reliable record but may make witnesses less willing to make a statement. If a witness needs to be compelled to make a statement, there will be legal issues around employment contracts (if the witness is an employee) and right to legal representation.

Handling and Analyzing Evidence

It is vital that the evidence collected at the crime scene conform to a valid **timeline**. Digital information is susceptible to tampering, so access to the evidence must be tightly controlled.



Preservation of Evidence

Depending on the strength of evidence required, physical drives taken from the crime scene can be identified, bagged, sealed, and labeled (using tamper-proof bags). It is also appropriate to ensure that the bags have anti-static shielding to reduce the possibility that data will be damaged or corrupted on the electronic media by ElectroStatic Discharge (ESD). Any other physical evidence deemed necessary is also "Bagged and Tagged".

A crucial element of the investigation is that each step is documented and (ideally) recorded. This proves that the evidence has been handled correctly and has not been tampered with. Once evidence has been bagged, it must not subsequently be handled or inspected, except in controlled circumstances. A **Chain Of Custody** form records where, when, and who collected the evidence, who has handled it subsequently, and where it was stored. The chain of custody must show access to, plus storage and transportation of, the evidence at every point from the crime scene to the court room. Anyone handling the evidence must sign the chain of custody and indicate what they were doing with it.

The evidence should be stored in a secure facility; this not only means access control but also environmental control, so that the electronic systems are not damaged by condensation, ESD, fire, and other hazards. Similarly, if the evidence is transported, the transport must also be secure.

Analysis of Evidence



9t09h

All analysis should be performed on a **copy** of the evidence rather than on the original devices or the secure image created at the crime scene.

When analyzing information from hard drives taken as evidence, one of the most significant challenges is dealing with the sheer volume of information captured. Within the thousands of files and hundreds of gigabytes there may only be a few items that provide incriminating evidence. Forensic analysis tools help to identify what could be of interest to the forensic examiner.

"Big Data" analysis techniques can assist in this process. Big data refers to large stores of unstructured information. Big data analysis tools use search query like functions to identify patterns and information of interest within unstructured files such as documents and spreadsheets.



See [Unit 4.4](#) for a comparison of big data stores and traditional databases.

As well as the contents of the file, analysis of the file metadata, including time stamps, can reveal useful information. As well as examining the information on hard drives, big data analysis techniques can also be used to analyze network traffic. Big data analysis tools oriented towards security and computer intrusion detection and forensics will certainly become more widely available over the next few years.

Big data analysis software often includes **data visualization** tools. Visualization is a very powerful analysis technique for identifying trends or unusual activity. For example, a graph of network activity will reveal unusually high activity from a particular host much more easily than analysis of the raw data packets. A "tag cloud" (a visual representation of how frequently words or phrases appear in a data store) of the information on a hard drive might reveal clues about malicious behavior that could not be found by examining each file individually.



ujwhm

Tracking Man Hours and Expense

Third-party investigators need to keep track of the man hours spent on the investigation and note incidental expenses as part of the billing process. The overall cost of an incident and its investigation is important to establish to feed back into risk assessment. It provides quantitative information about the impact of security incidents and the value of security controls. Establishing the true cost of an incident may also be required in a subsequent claim for compensation against the attacker.



Review Questions / Module 5 / Unit 5 / Incident Response and Forensics

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What are the 4 phases of the incident response lifecycle defined by NIST?
- 2) What is a CSIRT?
- 3) What type of threat source does supporting and protecting whistleblowers help to negate?
- 4) What is the significance of the fact that digital evidence is latent?
- 5) What should be the first action at a crime scene during a forensic investigation?
- 6) What software tools may be of use to a forensic investigator seeking to prepare a hard drive for analysis of its contents?
- 7) Why might a file time stamp not show the time at which a crime was committed?
- 8) What is a Chain of Custody form?
- 9) What is meant by a "first responder" and what initial actions should they perform?
- 10) Why might simply removing a device not be an appropriate response to an incident?
- 11) How might "big data" assist with a forensic examination of a computer hard drive?

Module 5 / Unit 6

Security Policies and Training

Objectives

On completion of this unit, you will be able to:

- Describe the use of security policy and standards and guidelines.
- Understand the importance of operational policies in reducing risk.
- Understand the use of privacy and acceptable usage policies.
- Understand the importance of security awareness training.

Corporate Security Policy



xgsd4

As a vital component of a company's IT infrastructure, employees must understand how to use ICT securely and safely and be aware of their *responsibilities*. To support this, the organization needs to create proper documentation, to help staff to understand and fulfill their responsibilities and follow proper procedures.

Adopting an effective **security posture** is a difficult and costly change for an organization to make, as it involves disruption to "normal" practice at almost every level without any tangible reward or benefit. Security compliance requires the cooperation and support of *all* the organization's employees.

The value of a comprehensive policy is that it removes any *uncertainty* that employees may have about what to do in a given situation. For example, if you work for a large company and meet someone you do not recognize in your work area, should you smile and say hello or smile, say hello, ask them where they want to be, and then escort them to that place? If there is a company policy saying that visitors to the workplace **must** be escorted at all times, it will be much easier for employees to take it upon themselves to "act the policeman" in this sort of circumstance.

The aim of a **corporate security policy** should be to obtain *support* for security awareness in the organization and outline in general terms risks, guidelines, and responsibilities. The creation and *enforcement* of a security policy also demonstrates that **due care** (and due diligence) has been applied.

Drafting a Security Policy

Some relevant topic areas for a security policy are:

- Security mission statement - explaining the importance of security to the organization and the goal of the security policy (for example, "Secure our business data against all intrusions and maintain full business operations for 98% of working time throughout the year").



Deciding security policy

- Legal obligations.
- Areas of responsibility and lines of reporting (for example, reporting an intruder, computer virus infection, or health and safety hazard).
- Types of data used by the organization (with examples, such as: sales database, accounting system, correspondence [post, email, telephone, fax], diary, product design/specification documents, marketing literature, computer network design documents, passwords, and so on).
- Outline of locations used by the company to store data and materials (servers, portable equipment, paper archives).
- Overview of access control systems (computer network and building security, controlled areas, and so on).
- Overview of methods used to transfer data and security measures in place (use of email, teleworking, telephone use, and so on).
- Guidelines for general users (basic safety and security procedures, document authoring, confidentiality, and distribution, acceptable use of internet/email privileges).
- Use of systems for employees' private communications.
- Disciplinary measures for security breaches and procedures for ensuring data security when hiring and firing staff.
- Statement of policy for system acquisition and asset maintenance (to ensure that new systems conform to the best security standards).
- Disaster recovery procedures and lines of responsibility.

- Source(s) of further information (area of organization's website, designated security management office, or training courses).

It is important for the policy to stress aims and responsibilities. While some parts may require technical detail, others need to be accessible to a wide, non-technical audience at all levels of the organization. Guidelines in the policy can then be backed up by detailed technical implementation policies at departmental / managerial level. For example, the Network Manager can implement a policy to protect data passing through the organization's computer network; the Human Resources department can undertake security training and awareness programs and ensure compliance when staff are hired or dismissed.



Some parts of the security policy and associated standards, procedures, and guidelines should be kept confidential. For example, it is unwise to make the details of security systems or disaster recovery plans general knowledge, as this sort of information could greatly assist malicious attacks. As with any documentation, ensure that the parts of the security policy are classified and secured on a "Need To Know" basis.



The Site Security Handbook, published as [RFC 2196](#), is a valuable source of information and advice on computer security policies. Guidance can also be found on SANS' Security Policy Project ([gtsgo.to/svmb4](#)).

HR Policies

Human Resources (HR) is the department tasked with recruiting and managing the organization's most valuable and critical resource: people. HR policy can be conceived as applying in three phases:

- Recruitment (hiring) - locating and selecting people to work in particular job roles. Security issues here include screening candidates and performing background checks.
- Operation (working) - it is often the HR department that manages the communication of policy and training to employees (though there may be a separate training and personal development department within larger organizations). As such, it is critical that HR managers devise training programs that communicate the importance of security to employees.
- Termination or separation (firing or retiring) - whether an employee leaves voluntarily or involuntarily, termination is a difficult process, with numerous security implications.

Operational Policies

Operational policies include privilege management, data handling, and incident response, as discussed elsewhere. One function of HR is to communicate these policies to employees, including any updates to the policies. Another function is to enforce disciplinary measures (perhaps in conjunction with departmental managers).

Separation of Duties, Job Rotation, and Mandatory Vacations

Organizations must be alert to the possibility that their employees may attempt fraud or vandalism. **Separation of duties** is a means of establishing checks and balances against the possibility that critical systems or procedures can be compromised by insider threats.

Several different policies can be applied to enforce separation of duties:

- Standard Operating Procedures (SOP) mean that an employee has no excuse for not following protocol in terms of performing this type of critical operation.
- Shared authority means that no one user is able to action or enable changes on his or her own authority. At least two people must authorize the change.
- The principle of least privilege means that a user is granted sufficient rights to perform their job and no more. For critical tasks, duties should be divided between a number of people.
- Effective auditing means that decisions and changes are recorded and can be scrutinized independently of the person that made the decision.
- Mandatory vacations means that employees are forced to take their vacation time, during which someone else fulfils their duties.
- Job rotation (or rotation of duties) means that no one person is permitted to remain in the same job for an extended period. For example, managers may be moved to different departments periodically or employees may perform more than one job role, switching between them throughout the year. Job rotation is also seen as beneficial in terms of developing skills and experience.

Separation of duties is most evident in accounts and financial departments. One example is requiring all checks to be co-signed (that is, signed by two people); another is separating responsibility for purchasing (ordering) and payment. M-of-N control, discussed in the section on cryptography, is another example of separation of duties.



Separation of duties aims to avoid putting employees in a position where there is a conflict of interest. An employee is supposed to work for the interests of their organization exclusively. A situation where someone is able to act in their own interest personally or in the interests of a third-party is said to be a conflict of interest. The most common example is abuse of business expense accounts.



Separation of duties does not completely eliminate risk because there is still the chance of collusion between two or more people. This is a much less likely occurrence than a single rogue employee however.

Whistleblowing

The HR department is also likely to be the internal point-of-contact for whistleblowers. An organization's best defense against internal fraud, collusion (where two or more people conspire to commit fraud), vandalism, or poor practice is the alertness of other employees. However, to maximize this resource, employees must be confident that they can report incidents in confidence without seriously impacting their own career prospects.

Prevent Tailgating

If a security measure is unpopular, you need to be able to explain why it has been introduced and what the implications of persisting with the old system would be.

A good example is tailgating (the social engineering trick of following someone through a secure entrance without being directly authenticated). It is very hard for someone to shut a door in someone else's face rather than hold it open for them or to take hold of someone who has slipped through a door behind them and tell them to step out and swipe their card to gain entry. Ordinary employees can only really be expected to do this with training.

Password Behaviors

There should be a formal policy enforcing good password and credential management.



See [Unit 2.3](#) for notes on selecting strong passwords and keeping passwords secure.

Clean Desk Policy

A **clean desk** policy means that each employee's work area should be free from any documents if left unattended (or at the end of the day, depending on how strict the policy is). The aim of the policy is to prevent sensitive information from being obtained by unauthorized staff or guests to the workplace.

There can be some problematic areas in enforcing a clean desk policy. For example, employees may use visual aids for things such as process flowcharts that would have to be tidied and taken out again each day.

Privacy and Employee Conduct Policies



Other important security policies include those governing employee conduct and respect for privacy.

Acceptable Use Policy

An **Acceptable Use Policy** (or **Fair Use Policy**) sets out what someone is allowed to use a particular service or resource for. Such a policy might be used in different contexts. For example, an acceptable use policy could be enforced by a business to govern how employees use equipment and services (such as telephone or internet access) provided to them at work. Another example might be an ISP enforcing a fair use policy governing usage of its internet access services.

Enforcing an acceptable use policy is important to protect the organization from the security and legal implications of employees (or customers) misusing its equipment. Typically, the policy will forbid the use of equipment to defraud, defame, or to obtain illegal material. It is also likely to prohibit the installation of unauthorized hardware or software and to explicitly forbid actual or attempted intrusion (snooping). An organization's acceptable use policy may forbid use of internet tools outside of work-related duties or restrict such use to break times.

Use of the Internet in the Workplace

The equipment used to access the internet in the workplace is owned by the employer. Many employees expect relatively unrestricted access to internet facilities for personal use. In fact, employees' use of the social networking and file sharing poses substantial risks to the organization, including threat of virus infection or systems intrusion, lost work time, copyright infringement, and defamation. If an employee breaks copyright laws or libels someone using an organization's equipment, the organization itself *could* be held liable.

To avoid confusion, an employee's handbook should set out the terms under which use of web browser/email/social networking/P2P software is permitted for personal use, and what penalties infringements could incur. Employers are within their rights to prohibit all private use of internet tools.

Users should be aware that any data communications, such as email, made through an organization's computer system are liable to be stored within the system, on servers, backup devices, and so on. Consequently, users should not use computers at work to send personal information (for their own security if nothing else).

Use of Personally Owned Devices in the Workplace

As discussed earlier, portable devices such as smartphones, USB sticks, media players, and so on pose a considerable threat to data security as they make file copy so easy. Camera and voice recording functions are other obvious security issues.

Network access control / endpoint security and data loss prevention solutions can be of some use in preventing the attachment of such devices to corporate networks. Some companies may try to prevent staff from bringing such devices on site. This is quite difficult to enforce though.

Privacy Policy

The right to privacy is one expected by citizens of most countries. However the right to privacy has to be balanced against the need for the companies we work for and shop with to receive and process (and in some cases keep) information about us.

For example, a mail order company needs to know your address in order to deliver goods to you. When you tell them your address, you might expect them to use it only for delivering goods that you have ordered and not to use it to contact you about other products or to pass it to another company without your permission.

In order to protect their business, employers claim a responsibility to monitor the way employees put the IT equipment provided to them to use. Employees claim rights deriving from human rights legislation that they should not be treated cruelly or unusually. The balance between these rights and responsibilities is not always clearly defined in law, though as workplace privacy becomes more of an issue, laws and company guidelines are being instituted to account for it. A **contract of employment** may set out what an employee must agree to as a condition of employment.

Workplace surveillance can be divided into several categories:

- **Security assurance** - monitoring data communications and employee's behavior to ensure that they do not divulge confidential information or compromise the security of the organization. Employers may also use security systems such as CCTV to prevent theft.
- **Monitoring data** - analyzing data communications to measure an employee's productivity. For example, a contact management system may record the frequency and duration of telephone contacts.
- **Physical monitoring** - recording employee's movement, location, and behavior within the workplace, often using CCTV and drugs/alcohol testing.

A good employer will make the procedures for workplace surveillance clear and unambiguous. To this end, a contract of employment or staff handbook should make clear the rules for employee conduct (as regards security, refreshment breaks, and use of equipment) and define prohibited actions and appropriate disciplinary procedures and punishments. Each employee should be given the opportunity to read these guidelines and the employer should check that the employee understands them.

Additionally, some thought needs to be given to guests and callers, where the issue of consent is even more ambiguous.

Standards and Best Practice



yo061

Policy is an overall statement of intent. In order to establish the correct working practices, three different mechanisms can be put in place:

- Standard - a standard is a measure by which to evaluate compliance with the policy.
- Procedure - a procedure (often referred to as a SOP [Standard Operating Procedure]) is an inflexible, step-by-step listing of the actions that must be completed for any given task. Most critical tasks should be governed by SOPs.
- Guidance - guidelines exist for areas of policy where there are no procedures, either because the situation has not been fully assessed or because the decision-making process is too complex and subject to variables to be able to capture it in a procedure. Guidance may also describe circumstances where it is appropriate to deviate from a specified procedure.



In legislation, there is a distinction between regulations, which carry the full force of law, and guidance. Guidance is often issued by the regulatory body responsible for drafting and enforcing regulations to assist with compliance with the regulations. Guidance often sets out "best practice" that in normal circumstances will result in compliance. Guidance is not mandatory however.

Compliance and Laws

A formal security policy is also of use in demonstrating compliance with laws, standards, and best practice.



Compliance

Due diligence is a legal term meaning that responsible persons have not been negligent in discharging their duties. Negligence may create criminal and civil liabilities. Many countries have enacted legislation that **criminalizes** negligence in information management.

In the US for example, the passage of the **Sarbanes-Oxley Act (SOX)** has mandated the implementation of risk assessments, internal controls, and audit procedures. The act was introduced following a number of high-profile accounting scandals, including the collapse of Enron. The **Computer Security Act (1987)** requires federal agencies to develop security policies for computer systems that process confidential information. There are also acts that require security standard and controls to ensure customer privacy in particular industries, notably financial services (the **Gramm-Leach-Bliley Act [GLBA]**) and healthcare (the **Health Insurance Portability and Accountability Act [HIPAA]**).

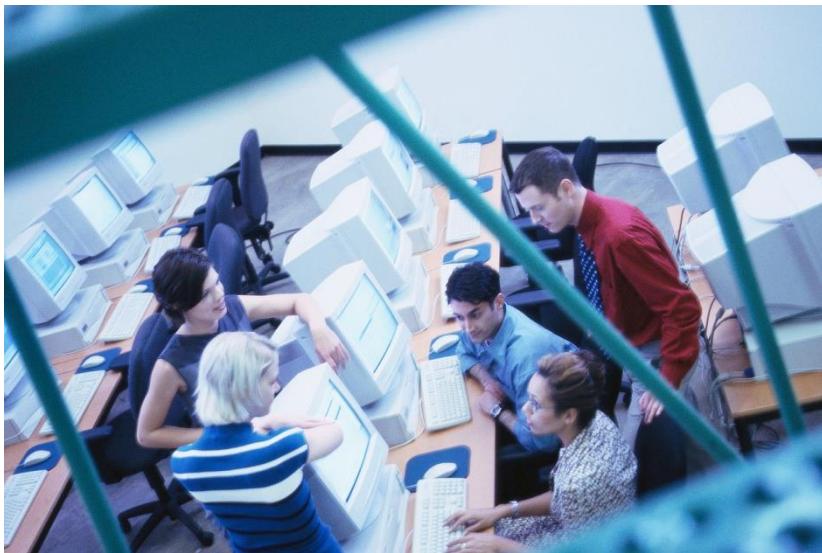
A **civil** liability means that in the case of a security incident where liability cannot be assigned to the perpetrator or damages cannot be recovered, those responsible for security (such as directors and senior managers) may be forced to pay damages to third parties (such as customers or suppliers affected by the incident).

There are also industry-enforced regulations mandating data security. A good example is the **Payment Card Industry Data Security Standard (PCI DSS)** governing processing of credit card payments.

The organization needs to **test** security policies regularly during development and implementation. It is equally important to test continually for compliance with the policy and to institute periodic reviews to ensure that new risks are identified and that changes within the organization do not compromise security.

Security Policy Training and User Habits

Another essential component of a secure system is effective user training.



Train users in secure behavior

A security system cannot be too inflexible or users will complain or adopt insecure behavior. For example, when users have too many passwords to remember, they often start recycling them; also, when users are presented with numerous security warnings, they start to click through without really thinking about what they are doing. It is much better to educate users about security risks and to monitor behavior, to ensure that users are following best practice. This needs to be backed up by a strong disciplinary procedure to sanction users who continue to act carelessly. As mentioned above, training might be the responsibility of HR or of a dedicated training department. Training methods include facilitated workshops, one-to-one instruction and mentoring, plus resources such as online training, books, and newsletters.



fb5gf

Security Awareness Training

Appropriate security awareness training needs to be delivered to employees at all levels; including end users, technical staff, and executives. NIST have created a guide to designing security awareness programs, published as SP800-50 (gtsgo.to/5ii1f). Some of the general topics that need to be covered include the following:

- Overview of the organization's security policies and the penalties for non-compliance.
- Incident response identification and reporting procedures.
- Site security procedures, restrictions, and advice, including safety drills, escorting guests, use of secure areas, and use of personal devices.
- Data handling, including document confidentiality, PII, backup, encryption, and so on.

- Password and account management plus security features of PCs and mobile devices.
- Awareness of social engineering and malware threats, including phishing, websites exploits, and spam plus alerting methods for new threats.
- Secure use of software such as browsers and email clients plus appropriate use of internet access, including social networking sites.

It is necessary to frame security training in language that end users will respond to. Education should focus on responsibilities and threats that are relevant to users. It is necessary to educate users about new or emerging threats (such as viruses and Trojans, phishing scams, or "zero-day" exploits in software such as browser plug-ins) but this needs to be framed in language that users understand.

For example, if you try to inform users about "The threat of Trojan Horse software being used to install rootkits that can launch DoS attacks", their response will typically be either to fall asleep, laugh, or stare at you blankly. Instead, user education should be phrased in terms that are relevant to what they do from day-to-day at work and avoid technical language and jargon. For example, "Don't try to disable anti-virus software and don't open email file attachments if you are not sure what they contain."

Similarly, when security alerts are issued, these must be drafted carefully so as not to cause confusion or alarm. It is important to only issue alerts for critical incidents or risks. If users are faced with a continual series of alerts they will start to ignore them.



Role-based Training

There should also be a system for identifying staff performing security-sensitive roles and grading the level of training and education required (between beginner, intermediate, and advanced for instance). Note that in defining such training programs you need to focus on job roles, rather than job titles, as employees may perform different roles and have different security training, education, or awareness requirements in each role.

Advanced security training will be required by job roles such as IT and networking, management, software development, and accounts.



The NIST publication SP800-16 "IT Security Training Requirements" (gtsgo.to/xf5gh) sets out a role-specific training program in detail.



Follow Up and Gather Training Metrics

Simply delivering security awareness training and alerting programs is not sufficient. If you send an alert, how do you know whether people have read and acted on it? If you have delivered a training session, are you confident that the participants have understood and can apply the training to their jobs?

Most training includes various types of assessment. **Formative** assessment helps students to understand the material, tests basic recall of facts, and identifies areas of weakness and strength. **Summative** assessment ensures that the training they have received has delivered the skills and knowledge they need to perform the tasks that they have to do. Summative assessment may be devised in-house or may be linked to a third-party certification program, as this course is.

To track progress through various training and awareness programs, you can use a **Learning Management System (LMS)**. This is software capable of recording use of training and performance in assessments. Many LMS can also deliver online training, using a framework such as SCORM (Sharable Content Object Reference Model) or TinCan. An LMS is also likely to provide tools to facilitate other types of training or education, such as workshops, blogs, tutor support, and learner forums. The LMS may also provide features for delivering different training paths; series of courses tailored to particular job roles. An LMS provides many metrics to use for compliance reasons to validate the success of training programs and prove that the organization has adopted an effective security posture. As well as assessment scores, an LMS might be able to track time spent or pages/screens viewed and the percentage of users that have completed training successfully. It may be used to obtain learner feedback about the courses and analyze the performance of assessment items.



Review Questions / Module 5 / Unit 6 / Security Policies and Training

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) In what situations would it be appropriate to apply separation of duties to privilege management?
- 2) What type of organizational policy ensures that at least two people have oversight of a critical business process?
- 3) What sort of workplace security issues should be covered by HR policies?
- 4) What type of software assists with collection of training metrics?
- 5) True or false? It is important to publish all security alerts to all members of staff.
- 6) What risk, apart from time-wasting, might employee use of social networking pose to an organization?
- 7) Why should an organization design role-based training programs?

Module 5 / Summary

Operational Security

In this module, you learned the importance of operational security procedures, such as site access control, business continuity / risk assessment plans, disaster recovery procedures, incident response, and employee training and policies.

Module 5 / Unit 1 / Site Security

- Physical security means controlling access to premises and ensuring a safe and stable operating environment for computer and network systems.
- Sites can be protected through gateways, locks, and alarms and through surveillance methods, such as CCTV, guards, and lighting.
- Environmental controls reduce the risk of damage or interference due to climate, fire, and EMI/RFI.

Module 5 / Unit 2 / Mobile and Embedded Device Security

- Static environments and embedded systems pose special security challenges as they may be unfamiliar and not as well supported as ordinary OS and network systems.
- Encryption, passcode authentication, and geotracking help to secure data on mobile devices.
- Bring Your Own Device (BYOD) policies and Mobile Device Management (MDM) software allow companies to assert corporate control over data processed on personally-owned devices.
- Short-range radio technologies such as Bluetooth and NFC may be vulnerable to attacks as use of these technologies increases.

Module 5 / Unit 3 / Risk Management

- Business continuity means planning and testing systems and operations so that they are as little affected by incidents as possible and so that the resources are available to recover from them.
- Organizations should perform Business Impact Analysis (BIA) asset identification and risk assessment and then put security controls in place to mitigate risk and reduce vulnerabilities.
- Risk can be calculated using quantitative measures (such as SLE, ARE, and ARO) or qualitative assessments.
- Risk mitigation options include deterrence, avoidance, transference, and acceptance.

- Integrating systems with third parties should first be considered from the point-of-view of security policies and legal agreements before tackling the technical issues. Agreements can identify key performance metrics to agree quality of service.
- A proactive configuration and change management policy reduces risk.

Module 5 / Unit 4 / Disaster Recovery

- Disaster recovery plans identify threats and outline resources and responsibilities to put into practice in the event of an incident.
- Business continuity depends on systems that are fault tolerant and high availability. This is often accomplished using components and technologies that provide redundancy:
 - RAID provides fault tolerant disk storage
 - Clusters provide fault tolerant network services
 - UPS provides fault tolerant power supply
- Alternate sites can be used to recover from catastrophic events. Sites are categorized as cold, warm, or hot, according to their state of readiness.
- Disaster recovery and business continuity plans may involve duplicating data to other sites. The security of data away from the primary site should not be overlooked.

Module 5 / Unit 5 / Incident Response and Forensics

- Organizations should set up incident response policies and procedures plus an individual or team trained to deal with incidents.
- A typical incident response lifecycle includes the steps preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.
- Computer forensics refers to procedures for collecting and preserving evidence so that it can be presented at trial.

Module 5 / Unit 6 / Security Policies and Training

- Every organization should institute a security policy backed up by resources, standards, guidelines, and procedures.
- Operational policies should govern issues such as use of portable devices and the internet in the workplace and privacy.
- User awareness, education, and training is important to prevent security vulnerabilities being created through poor data handling practice or social engineering.

Taking the Exams

When you think you have learned and practiced the material sufficiently, you can book a time to take the test.

Preparing for the Exam

We've tried to balance this course to reflect the percentages in the exam so that you have learned the correct level of detail about each topic to comfortably answer the exam questions. Read the following notes to find out what you need to do to register for the exam and get some tips on what to expect during the exam and how to prepare for it.

Questions in the exam are weighted by domain area as follows:

CompTIA Security+ Certification Domain Areas	Weighting
1.0 Network Security	20%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	20%
4.0 Application, Data and Host Security	15%
5.0 Access Control and Identity Management	15%
6.0 Cryptography	12%

The objectives and content examples are covered in units in the course as listed in the table below. You can also use the index at the back of the book to look up specific content examples:

Domain Objectives/Examples	Refer To
1.1 Implement security configuration parameters on network devices and other technologies Protocol analyzers • Sniffers Routers • Switches	Unit 1.3 Network Attacks Unit 3.1 Secure Network Design
Firewalls • Proxies • Web security gateways • NIDS and NIPS (Behavior based, Signature based, Anomaly based, Heuristic) • Spam filter • UTM security appliances (URL filter, Content inspection, Malware inspection) • Web application firewall vs. network firewall • Application aware devices (Firewalls, IPS, IDS, Proxies)	Unit 3.2 Security Appliances and Applications
VPN concentrators	Unit 3.4 VPN and Remote Access Security
Load Balancers	Unit 4.3 Web Services Security
1.2 Given a scenario, use secure network administration principles VLAN management • Secure router configuration • Loop protection • Network separation Rule-based management • Firewall rules • Access control lists • Flood guards • Implicit deny • Log analysis • Unified Threat Management	Unit 3.1 Secure Network Design Unit 3.2 Security Appliances and Applications
Port security • 802.1X	Unit 4.1 Host Security

Domain Objectives/Examples	Refer To
1.3 Explain network design elements and components DMZ • Subnetting • VLAN • NAT • Layered security / Defense in depth	Unit 3.1 Secure Network Design
Remote Access	Unit 3.4 VPN and Security
Telephony	Unit 3.5 Network Applications
NAC	Unit 4.1 Host Security
Virtualization • Cloud Computing (Platform as a Service, Software as a Service, Infrastructure as a Service, Private, Public, Hybrid, Community)	Unit 4.5 Virtualization and Cloud Security
1.4 Given a scenario, implement common protocols and services Protocols (TCP/IP, ICMP) • OSI relevance Ports (25, 110, 143)	Unit 1.3 Network Attacks
Protocols (IPSec, SSH, SCP, TELNET) • Ports (22, 3389)	Unit 3.2 Security Appliances
Protocols (SNMP, DNS, IPv4 vs. IPv6, iSCSI, Fibre Channel, FCoE, NetBIOS) • Ports (53, 139)	Unit 3.4 VPN Security
Protocols (TLS, SSL, FTPS, HTTPS, FTP, SFTP, TFTP, HTTP) • Ports (21, 80, 443)	Unit 4.3 Web Services Security
1.5 Given a scenario, troubleshoot security issues related to wireless networking EAP • PEAP • LEAP	Unit 2.4 Strong Authentication
WPA • WPA2 • WEP • MAC filter • Disable SSID broadcast • TKIP • CCMP • Antenna Placement • Power level controls • Captive portals • Antenna types • Site surveys • VPN (over open wireless)	Unit 3.3 Wireless Network Security
2.1 Explain the importance of risk related concepts Control types (Technical, Management, Operational) • Importance of policies in reducing risk (Least privilege)	Unit 1.1 Security Controls
Vulnerabilities • Threat vectors	Unit 1.2 Threats and Attacks
False positives • False negatives	Unit 3.2 Security Appliances and Applications
Risks associated with Cloud Computing and Virtualization	Unit 4.5 Virtualization and Cloud Security
Risk calculation (Likelihood, ALE, Impact, SLE, ARO, MTTR, MTTF, MTBF) • Quantitative vs. qualitative • Probability / threat likelihood • Risk-avoidance, transference, acceptance, mitigation, deterrence • Recovery time objective and recovery point objective	Unit 5.3 Risk Management
Importance of policies in reducing risk (Privacy policy, Acceptable use, Security policy, Mandatory vacations, Job rotation, Separation of duties)	Unit 5.6 Security Policies and Training
2.2 Summarize the security implications of integrating systems and data with third parties On-boarding/off-boarding business partners • Social media networks and/or applications • Interoperability agreements (SLA, BPA, MOU, ISA) • Privacy considerations • Risk awareness • Unauthorized data sharing • Data ownership • Data backups • Follow security policy and procedures • Review agreement requirements to verify compliance and performance standards	Unit 5.3 Risk Management
2.3 Given a scenario, implement appropriate risk mitigation strategies User rights and permissions reviews	Unit 2.5 Authorization and Account Management
Enforce policies and procedures to prevent data loss or theft • Enforce technology controls (Data Loss Prevention [DLP])	Unit 4.2 Data Security
Change management • Perform routine audits	Unit 5.3 Risk Management
Incident management	Unit 5.5 Incident Response and Forensics

Domain Objectives/Examples	Refer To
2.4 Given a scenario, implement basic forensic procedures Order of volatility • Capture system image • Network traffic and logs • Capture video • Record time offset • Take hashes • Screenshots • Witnesses • Track man hours and expense • Chain of custody • Big Data analysis	Unit 5.5 Incident Response and Forensics
2.5 Summarize common incident response procedures Preparation • Incident identification • Escalation and notification • Mitigation steps • Lessons learned • Reporting • Recovery/reconstitution procedures • First responder • Incident isolation (Quarantine, Device removal) • Data breach • Damage and loss control	Unit 5.5 Incident Response and Forensics
2.6 Explain the importance of security related awareness and training Personally identifiable information • Information classification (High, Medium, Low, Confidential, Private, Public) • Data labeling, handling and disposal • User habits (Data handling)	Unit 4.2 Data Security
Security policy training and procedures • Role-based training • Compliance with laws, best practices and standards • User habits (Password behaviors, Clean desk policies, Prevent tailgating, Personally owned devices) • New threats and new security trends/alerts (New viruses, Phishing attacks, Zero-day exploits) • Use of social networking and P2P • Follow up and gather training metrics to validate compliance and security posture	Unit 5.6 Security Policies and Training
2.7 Compare and contrast physical security and environmental controls Control types (Deterrent, Preventive, Detective, Compensating, Technical, Administrative)	Unit 1.1 Security Controls
Environmental controls (HVAC, Fire suppression, EMI shielding, Hot and cold aisles, Environmental monitoring, Temperature and humidity controls) • Physical security (Hardware locks, Mantraps, Video Surveillance, Fencing, Proximity readers, Access list, Proper lighting, Signs, Guards, Barricades, Biometrics, Protected distribution [cabling], Alarms, Motion detection)	Unit 5.1 Site Security
2.8 Summarize risk management best practices Disaster recovery concepts (Backup plans/policies, Backup execution/frequency)	Unit 4.2 Data Security
Business continuity concepts (Business Impact Analysis, Identification of critical systems and components, Business continuity planning and testing, Risk assessment, Continuity of operations, High availability)	Unit 5.3 Risk Management
Business continuity concepts (Removing single points of failure, Disaster recovery, IT contingency planning, Succession planning, Redundancy, Tabletop exercises) • Fault tolerance (Hardware, RAID, Clustering, Load balancing, Servers) • Disaster recovery concepts (Cold site, Hot site, Warm site)	Unit 5.4 Disaster Recovery
2.9 Given a scenario, select the appropriate control to meet the goals of security Confidentiality (Encryption, Access controls, Steganography) • Integrity (Hashing, Digital signatures, Non-repudiation)	Unit 2.1 Cryptography
Integrity (Certificates)	Unit 2.2 PKI
Availability (Patching)	Unit 4.1 Host Security
Safety (Fencing, Lighting, Locks, CCTV, Escape plans, Drills, Escape routes, Testing controls)	Unit 5.1 Site Security
Availability (Redundancy, Fault tolerance)	Unit 5.4 Disaster Recovery
3.1 Explain types of malware Adware • Virus • Spyware • Trojan • Rootkits • Backdoors • Logic bomb • Botnets • Ransomware • Polymorphic malware • Armored virus	Unit 1.2 Threats and Attacks
3.2 Summarize various types of attacks Spam • Phishing • Spim • Vishing • Spear phishing • Pharming • Malicious insider threat • Watering hole attack	Unit 1.2 Threats and Attacks
Man-in-the-middle • DDoS • DoS • Replay • Smurf attack • Spoofing • Xmas attack • ARP poisoning	Unit 1.3 Network Attacks
Password attacks (Brute force, Dictionary attacks, Hybrid, Birthday attacks, Rainbow tables)	Unit 2.3 Password Authentication
DNS poisoning • Typo squatting/URL hijacking	Unit 3.5 Network Applications
Privilege escalation • Transitive access • Client-side attacks	Unit 4.4 Web Applications

Domain Objectives/Examples	Refer To
<p>3.3 Summarize social engineering attacks and the associated effectiveness with each attack</p> <p>Shoulder surfing • Dumpster diving • Tailgating • Impersonation • Hoaxes • Whaling • Vishing • Principles / reasons for effectiveness (Authority, Intimidation, Consensus/Social proof, Scarcity, Urgency, Familiarity/liking, Trust)</p>	Unit 1.2 Threats and Attacks
<p>3.4 Explain types of wireless attacks</p> <p>Rogue access points • Jamming/Interference • Evil twin • War driving • War chalking • IV attack • Packet sniffing • Replay attacks • WEP/WPA attacks • WPS attacks</p>	Unit 3.3 Wireless Network Security
<p>Bluejacking • Bluesnarfing • Near Field Communication</p>	Unit 5.2 Mobile / Embedded Device Security
<p>3.5 Explain types of application attacks</p> <p>LDAP injection</p>	Unit 2.5 Authorization and Account Management
<p>Cross-site scripting • SQL injection • XML injection • Directory traversal/command injection • Buffer overflow • Integer overflow • Zero-day • Cookies and attachments • Malicious add-ons • Session hijacking • Header manipulation • Arbitrary code execution / remote code execution</p>	Unit 4.4 Web Application Security
<p>3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques</p> <p>Hardening (Password protection • Disabling unnecessary accounts)</p>	Unit 2.5 Authorization and Account Management
<p>Monitoring system logs (Event logs, Audit logs, Security logs, Access logs) • Reporting (Alarms • Alerts • Trends) • Detection controls vs. prevention controls (IDS vs. IPS)</p>	Unit 3.2 Security Appliances and Applications
<p>Hardening (Disabling unnecessary services • Protecting management interfaces and applications) • Network security (MAC limiting and filtering, 802.1X, Disabling unused interfaces and unused application service ports, Rogue machine detection)</p>	Unit 4.1 Host Security
<p>Detection controls vs. prevention controls (Camera vs. guard)</p>	Unit 5.1 Site Security
<p>Security posture (Initial baseline configuration, Continuous security monitoring, Remediation)</p>	Unit 5.3 Risk Management
<p>3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities</p> <p>Tools (Protocol analyzer, Port scanner, Banner grabbing)</p>	Unit 1.3 Network Attacks
<p>Interpret results of security assessment tools • Tools (Vulnerability scanner, Honeypots, Honeynets, Passive vs. active tools)</p>	Unit 1.4 Assessment Tools and Techniques
<p>Assessment technique (Baseline reporting)</p>	Unit 4.1 Host Security
<p>Assessment technique (Code review • Determine attack surface • Review architecture, Review designs)</p>	Unit 4.4 Web Application Security
<p>Risk calculations (Threat vs. Likelihood) • Assessment types (Risk • Threat • Vulnerability)</p>	Unit 5.3 Risk Management
<p>3.8 Explain the proper use of penetration testing versus vulnerability scanning</p> <p>Penetration testing (Verify a threat exists, Bypass security controls, Actively test security controls, Exploiting vulnerabilities) • Vulnerability scanning (Passively testing security controls, Identify vulnerability, Identify lack of security controls, Identify common misconfigurations, Intrusive vs. non-intrusive, Credentialled vs. non-credentialled, False positive) • Black box • White box • Gray box</p>	Unit 1.4 Assessment Tools and Techniques
<p>4.1 Explain the importance of application security controls and techniques</p> <p>Application configuration baseline (proper settings) • Application hardening • Application patch management</p>	Unit 4.1 Host Security
<p>Fuzzing • Secure coding concepts (Error and exception handling, Input validation) • Cross-site scripting prevention • Cross-site Request Forgery (XSRF) prevention • NoSQL databases vs. SQL databases • Server-side vs. Client-side validation</p>	Unit 4.4 Web Application Security

Domain Objectives/Examples	Refer To
4.2 Summarize mobile security concepts and technologies Device security (Full device encryption, Remote wiping, Lockout, Screen-locks, GPS, Application control, Storage segmentation, Asset tracking, Inventory control, Mobile device management, Device access control, Removable storage, Disabling unused features) • Application security (Key management, Credential management, Authentication, Geotagging, Encryption, Application whitelisting, Transitive trust/authentication) • BYOD concerns (Data ownership, Support ownership, Patch management, Antivirus management, Forensics, Privacy, On-boarding/off-boarding, Adherence to corporate policies, User acceptance, Architecture/infrastructure considerations, Legal concerns, Acceptable use policy, On-board camera/video)	Unit 5.2 Mobile / Embedded Device Security
4.3 Given a scenario, select the appropriate solution to establish host security	Unit 1.2 Threats and Attacks
Anti-malware (Antivirus, Anti-spam, Anti-spyware, Pop-up blockers) Host-based firewalls • Host-based intrusion detection	Unit 3.2 Security Appliances and Applications
Operating system security and settings • OS hardening • Patch management • Whitelisting vs. blacklisting applications • Trusted OS • Host software baselining	Unit 4.1 Host Security
Virtualization (Snapshots, Patch compatibility, Host availability/elasticity, Security control testing, Sandboxing)	Unit 4.5 Virtualization and Cloud Security
Hardware security (Cable locks, Safe, Locking cabinets)	Unit 5.1 Site Security
4.4 Implement the appropriate controls to ensure data security	Unit 2.2 Public Key Infrastructure
Hardware based encryption devices (HSM) SAN	Unit 3.5 Network Application Security
Handling Big Data • Data encryption (Full disk, Database, Individual files, Removable media, Mobile devices) • Hardware based encryption devices (TPM, USB encryption, Hard drive) • Data in-transit, Data at-rest, Data in-use • Permissions/ACL • Data policies (Wiping, Disposing, Retention, Storage)	Unit 4.2 Data Security
Cloud storage	Unit 4.5 Virtualization and Cloud Security
4.5 Compare and contrast alternative methods to mitigate security risks in static environments	Unit 5.2 Mobile / Embedded Device Security
Environments (SCADA, Embedded (Printer, Smart TV, HVAC control), Android, iOS, Mainframe, Game consoles, In-vehicle computing systems) • Methods (Network segmentation, Security layers, Application firewalls, Manual updates, Firmware version control, Wrappers, Control redundancy and diversity)	
5.1 Compare and contrast the function and purpose of authentication services	Unit 2.3 Password Authentication
Kerberos RADIUS • TACACS • TACACS+ • XTACACS • SAML	Unit 2.4 Strong Authentication
LDAP • Secure LDAP	Unit 2.5 Authorization and Account Management

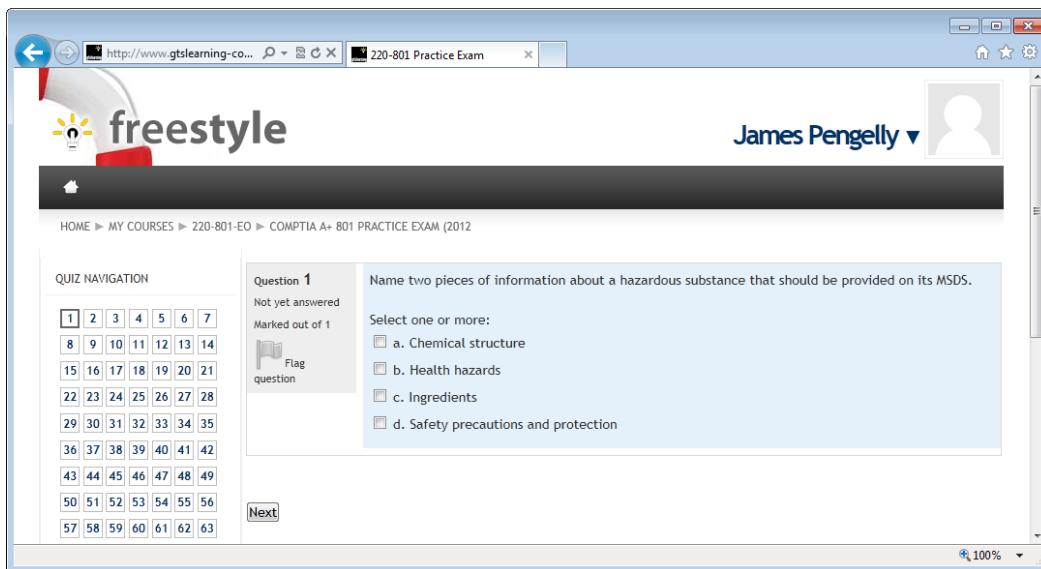
Domain Objectives/Examples	Refer To
<p>5.2 Given a scenario, select the appropriate authentication, authorization or access control</p> <p><i>Identification vs. authentication vs. authorization • Authorization (Least privilege, ACLs, Mandatory access, Discretionary access, Rule-based access control, Role-based access control) • Authentication (Multifactor authentication, Single sign-on, Access control, Implicit deny)</i></p>	Unit 1.1 Security Controls
<p><i>Authentication (CHAP, PAP) • Authentication factors (Something you know) • Identification (Username)</i></p>	Unit 2.3 Password Authentication
<p><i>Authentication (Tokens, Common access card, Smart card, TOTP, HOTP) • Authentication factors (Something you are, Something you have, Something you do) • Identification (Biometrics, Personal identification verification card) • Federation • Transitive trust/authentication</i></p>	Unit 2.4 Strong Authentication
<p><i>Authorization (Time of day restrictions)</i></p>	Unit 2.5 Authorization and Account Management
<p><i>Authentication (Trusted OS)</i></p>	Unit 4.1 Host Security
<p><i>Authorization (Separation of duties)</i></p>	Unit 5.6 Security Policies and Training
<p>5.3 Install and configure security controls when performing account management, based on best practices</p> <p><i>Mitigate issues associated with users with multiple account/roles and/or shared accounts • Account policy enforcement (Credential management, Group policy, Password complexity, Expiration, Recovery, Disablement, Lockout, Password history, Password reuse, Password length, Generic account prohibition) • Group based privileges • User assigned privileges • User access reviews • Continuous monitoring</i></p>	Unit 2.5 Authorization and Account Management
<p>6.1 Given a scenario, utilize general cryptography concepts</p> <p><i>Symmetric vs. asymmetric • Session keys • In-band vs. out-of-band key exchange • Fundamental differences and encryption methods (Block vs. stream) • Transport encryption • Non-repudiation • Hashing • Steganography • Digital signatures • Elliptic curve and quantum cryptography • Ephemeral key • Perfect forward secrecy</i></p>	Unit 2.1 Cryptography
<p><i>Key escrow • Use of proven technologies</i></p>	Unit 2.2 Public Key Infrastructure
<p>6.2 Given a scenario, use appropriate cryptographic methods</p> <p><i>MD5 • SHA • RIPEMD • AES • DES • 3DES • HMAC • RSA • Diffie-Hellman • RC4 • One-time pads • Blowfish • TwoFish • DHE • ECDHE • Comparative strengths and performance of algorithms • Cipher suites (Strong vs. weak ciphers)</i></p>	Unit 2.1 Cryptography
<p><i>PGP/GPG</i></p>	Unit 2.2 Public Key Infrastructure
<p><i>NTLM • NTLMv2 • CHAP • PAP • Key stretching (PBKDF2, Bcrypt)</i></p>	Unit 2.3 Password Authentication
<p><i>WEP vs. WPA/WPA2 and pre-shared key</i></p>	Unit 3.3 Wireless Network Security
<p><i>Use of algorithms/protocols with transport encryption (IPSec, SSH)</i></p>	Unit 3.4 VPN and Remote Access Security
<p><i>Use of algorithms/protocols with transport encryption (SSL, TLS, HTTPS)</i></p>	Unit 4.3 Web Services Security
<p>6.3 Given a scenario, use appropriate PKI, certificate management and associated components</p> <p><i>Certificate authorities and digital certificates (CA, CRLs, OCSP, CSR) • PKI • Recovery agent • Public key • Private key • Registration • Key escrow • Trust models</i></p>	Unit 2.2 Public Key Infrastructure

Scenarios

To ensure good practical understanding of the syllabus objectives and content examples, CompTIA multiple-choice and performance-based test items will ask you to choose between appropriate technologies and solutions in "real-world" scenarios. On the course support site (gtsgo.to/0l4i2) you can find written exercises designed to help to build your confidence and experience in completing scenario-based questions. You should attempt these scenarios from the perspective of having completed the whole course. You can use the support website to record your answers and then compare them to the model answers supplied.

Taking a Practice Test

There is a practice test for the exam available on the support website. The timed 100-item test delivers randomized questions weighted to the domain objectives in the same way as the actual exam.



The screenshot shows a web browser window with the URL <http://www.gtslearning.co...> in the address bar. The page title is "220-801 Practice Exam". On the left, there's a "freestyle" logo with a lightbulb icon. On the right, there's a user profile picture for "James Pengelly". Below the header, a navigation bar includes links for "HOME", "MY COURSES", "220-801-EO", and "COMPTIA A+ 801 PRACTICE EXAM (2012)". The main content area displays a question from a practice exam:

Question 1
Not yet answered
Marked out of 1
[Flag question](#)

Name two pieces of information about a hazardous substance that should be provided on its MSDS.
Select one or more:

- a. Chemical structure
- b. Health hazards
- c. Ingredients
- d. Safety precautions and protection

At the bottom of the question box, there are "Next" and "Previous" buttons. To the left of the question, there's a "QUIZ NAVIGATION" sidebar with a grid of numbered buttons from 1 to 63, where buttons 1 through 7 are highlighted in blue.

Taking a practice exam via gtslearning's Freestyle support site



The practice exams are authored by gtslearning and are designed to replicate the style of CompTIA's questions without directly copying any specific test items. You may wish to purchase other practice tests but be careful not to use "brain dump" products where the contents of an actual exam have been replicated. Candidates using materials listed at gtsgo.to/ik8cr (or any similar "product") may have their certifications revoked.

When you think you have studied enough and know the material well, attempt the practice test. Allow yourself 90 minutes to complete the test and approach it as you would the actual exam. If you score less than 95%, you probably need to do more study. When you get a question wrong in the practice test, you are directed back to the relevant unit. You need about 85% to pass the actual exam so you should make sure you can exceed that target comfortably before booking the test.

Registering for the Exam

CompTIA Certification exams are delivered exclusively by Pearson VUE.

- Log on to VUE (www.pearsonvue.com/comptia) and register your details to create an account.
- To book a test, log in using your account credentials then click the link to schedule an appointment.
- The testing program is CompTIA and the exam code is SY0-401.
- Use the search tool to locate the test center nearest you then book an appointment.
- If you have purchased a voucher or been supplied with one already, enter the voucher number to pay for the exam. Otherwise, you can pay with a credit card.



When it comes to booking your test, you might be able to save money by using a voucher code from gtslearning. Check gtslearning's website (gtsgo.to/ljob) for any available offers.

- When you have confirmed payment, an email will be sent to the account used to register confirming the appointment and directions to the venue. Print a copy and bring it with you when you go to take your test.

Arriving for the Exam

- Arrive at the test center at least 15 minutes before the test is scheduled.
- You must have two forms of ID - one with picture, both with signature, and one preferably with your private address (driving license, passport, and so on).
- Books, calculators, laptops, cellphones, smartphones, tablets, or other reference materials are not allowed.
- You will be given a pad and marker to make notes but you must not attempt to write down questions or remove anything from the exam room.
- It is CompTIA's policy to make reasonable accommodations for individuals with disabilities.
- The test center administrator will demonstrate how to use the computer-based test system and wish you good luck. Check that your name is displayed, read the introductory note, and then click the button to start the exam.



Taking the Exam

CompTIA have prepared a Candidate Experience video. Watch this to help to familiarize yourself with the exam format and types of questions.

- There are up to 100 multiple-choice questions and performance-based items, which must be answered in 90 minutes. The passing score is 750 on a scale of 100-900.
- Read each question and its option answers carefully. Don't rush through the exam as you'll probably have more time at the end than you expect.
- At the other end of the scale, don't get "stuck" on a question and start to panic. You can mark questions for review and come back to them.
- As the exam tests your ability to recall facts and to apply them sensibly in a troubleshooting scenario, there will be questions where you cannot recall the correct answer from memory. Adopt the following strategy for dealing with these questions:
 - Narrow your choices down by eliminating obviously wrong answers.
 - Don't guess too soon! You must select not only a *correct* answer, but the *best* answer. It is therefore important that you read all of the options and not stop when you find an option that is correct. It may be impractical compared to another answer.
 - Utilize information and insights that you've acquired in working through the entire test to go back and answer earlier items that you weren't sure of.
 - Think your answer is wrong - should change it? Studies indicate that when students change their answers they usually change them to the wrong answer. If you were fairly certain you were correct the first time, leave the answer as it is.
- As well as multiple-choice questions, there will be a number of performance-based items. Performance-based items require you to complete a task or solve a problem in simulated IT environments. Make sure you read the item scenario carefully and check your submission.
- Don't leave any questions unanswered! If you really don't know the answer, just guess.
- The exam may contain "unscored" questions, which may even be outside the exam objectives. These questions do not count towards your score. Do not allow them to distract or worry you.
- The exam questions come from a regularly updated pool to deter cheating. Do not be surprised if the questions you get are quite different to someone else's experience.



Do not discuss the contents of the exam or attempt to reveal specific exam questions to anyone else. By taking the exam, you are bound by CompTIA's confidentiality agreement.

After the Exam

- A score report will be generated and a copy printed for you by the test administrator. The score report will show whether you have passed or failed and your score in each section. Make sure you retain the report!
- 5 days after passing the exam, go to www.comptia.org/careerid and create an account (or log on to an existing account) using the information in your score report. You can use this site to order your certificate and ID card.
- If 6 weeks have passed after taking your exam and you haven't received a copy of your certificate, contact questions@comptia.org.
- You can use your Career ID to track your certification progress on CompTIA's website order duplicate certificates, and download certification logos in various image file formats.



CompTIA A+ Essentials Exam Score Report 000-000

CANDIDATE: Carl Bowman
CANDIDATE ID: 5787675

REGISTRATION NUMBER: 5787675

EXAM: CompTIA A+ Essentials Exam

DATE: 01-Mar-2007
SITE NUMBER: 1

PASSING SCORE: 675
CANDIDATE SCORE: 100
PASS/FAIL: Fail

The CompTIA A+ Essentials Exam has a scaled score between 100 and 900.

You missed one or more questions in the following objective areas:

- 5.3 Identify tools, diagnostic procedures and troubleshooting techniques for networks.
- 5.2 Install, configure, optimize and upgrade networks.
- 5.1 Identify the fundamental principles of networks.
- 6.2 Install, configure, upgrade and optimize security.

CompTIA exam score report

Retaking the Test

If you do fail the certification test at the first attempt, then you can retake it at your convenience. However, should you fail the test at the second, third, or subsequent try, you will not be able to resit the exam for at least 30 days after your last attempt. Study your score report to see which areas of the exam you were weak on.

CompTIA Continuing Education Program

When you achieve your certification, it will remain valid for 3 years. The certification can either be renewed by taking the next exam iteration or by joining the **CompTIA Continuing Education Program** and earning the relevant credits. For more information, visit gtsgo.to/5zmss.

Glossary

802.11x

A suite of standards for wireless radio communications developed by IEEE. The best known and utilized are the 802.11a/b/g/n "Wi-Fi" network standards. Another important standard is 802.11i, which defines an improved security model for wireless authentication and communications.

802.1X

Port-based network access control framework. 802.1X defines how devices should provide support for Extensible Authentication Protocol (EAP) to authenticate against an authentication server, such as RADIUS. EAP allows authentication by a number of methods, including smart card/certificate.

Access Control

Barriers that restrict access to a resource to defined users and functions only. On a computer system, each resource is often tagged with an Access Control List, defining permissions for users attempting to access the resource.

Account Expiration

Some user accounts may be created to allow only temporary access (for guest users, contractors, temporary staff, and so on). These accounts may be set to expire after a certain amount of time, eliminating the possibility that they will be forgotten about and act as possible system backdoors.

ActiveX

Binary browser plug-in files that can be installed to provide extra functionality on websites. Plug-ins can act as malware. The user must choose whether to install a plug-in, but they can also be blocked completely using browser security settings. Vendors can sign plug-ins using certificates to validate their authenticity.

Adware

Software that monitors a user's internet activity and displays correspondingly targeted ads (or collects data for other marketing purposes). Adware may be installed alongside another application but is distinguished from Trojans and spyware by transparently seeking the user's consent.

ALE (Annual Loss Expectancy)

The amount that would be lost over the course of a year. This is determined by multiplying the SLE by the Annual Rate of Occurrence (ARO).

All-in-one Security Appliance

Network appliance combining multiple security functions, such as firewall, IDS, anti-malware, and content/URL filter.

Anomaly-based Monitoring

See: *Behavior-based Monitoring*.

Antenna

Different types of antenna can be used to focus a signal to a particular point or more widely (omnidirectional). Many wireless devices use a simple rod-type antenna.

Antiquated Protocols

Many of the protocols used for network transport and services were designed without regard for security (Confidentiality, Integrity, Availability). Consequently, these protocols need to be deployed with extra safeguards, either by using another protocol for security (IPsec or SSL for instance) or by filtering traffic (using a firewall for example).

Anti-spam

Techniques to prevent a user being overwhelmed with spam (junk email). Spam can be blocked from reaching an organization using a mail gateway to filter messages. At the user level, software can redirect spam to a junk folder (or similar). Anti-spam filtering needs to balance blocking illegitimate traffic with permitting legitimate messages. Anti-spam techniques can also use lists of known spam servers (blacklists).

Anti-virus

Software capable of detecting and removing virus infections and (in most cases) other types of malware, such as worms, Trojans, rootkits, adware, spyware, password crackers, network mappers, DoS tools, and so on. Anti-virus software works on the basis of both identifying malware code (signatures) and detecting suspicious behavior (heuristics). Anti-virus software must be kept up-to-date with the latest malware definitions and protect itself against tampering.

API (Application Programming Interface)

A library of programming utilities used, for example, to enable software developers to access functions of the TCP/IP network stack under a particular operating system.

Application Hardening

The basic steps in making an application secure (hardening) are to configure access control and permissions on the application data and functions and to set up a monitoring and maintenance program, so that events are logged and the application is patched against software exploits.

Archival

See: *Storage and Retention Policies*.

ARP Poisoning

The Address Resolution Protocol (ARP) maps IP addresses to network interfaces (MAC addresses). ARP poisoning means injecting a false IP:MAC lookup into the victim's ARP cache. This can be used to perform a variety of attacks, including DoS, spoofing, and Man-in-the-Middle.

Asset

A thing of economic value. For accounting purposes, assets are classified in different ways, such as tangible and intangible or short term and long term. Asset management means identifying each asset and recording its location, attributes, and value in a database.

Asymmetric Algorithm

An asymmetric cryptographic algorithm uses different keys (public and private; the keys are linked but the private key is not derivable from the public one). The most popular type of asymmetric cryptography (RSA) is based on the fact that factoring large numbers to discover whether they are prime (a number that is only divisible by itself and 1) is difficult. If there were a breakthrough in mathematics that made factoring large numbers less computationally intensive, the security of these cryptographic products would be broken. Elliptic Curve Cryptography (ECC) is a different means of creating key pairs such that it is easy to determine that the keys are linked but very difficult to determine one key from the other. The other advantage of ECC is that the algorithm is more efficient, allowing smaller keys to give the same level of security as larger RSA keys.

Attack Surface

Attack surface is the degree of exposure a network or piece of software has to attack. For example, the more ports a server has open or the more features installed under an OS, the greater the likelihood of an attacker finding a vulnerability.

Auditing

Recording and reviewing system activity to detect suspicious or unauthorized behavior.

AUP (Acceptable Use Policy)

An acceptable use policy usually governs employees' use of company equipment.

Authentication

Method of proving that a user is who he or she says s/he is. Authentication is typically based on something you know, something you have, or something you are.

Availability

Availability is the principle that something should not be so secure that it is completely inaccessible. A practical example is a password policy that forces users to adopt insecure practices (such as writing their password on a post-it attached to their monitor). Another example is providing key recovery or escrow so that encrypted data can be recovered if the encryption key is lost or damaged. Availability also involves protecting a resource against loss or damage or DoS attacks.

Backdoor

A remote administration utility providing a means of configuring a computer. Remote admin software may be installed intentionally, in which case it must be properly secured. Backdoors may also be installed by malware.

Backup

Making security data backups according to a regular schedule is a cornerstone of network security. Modern backup systems need to cope with databases and messaging systems that operate 24x7. Backup schemes balance time to backup, time to restore, availability and cost of media, and reliability. Backup schemes also need to cater for onsite (to facilitate restore operations) and offsite storage (to protect against threat or damage to the primary site). Another consideration is the security of data as the backup is made and on the backup media.

Backup Generator

A Standby Power Supply fuelled by diesel or propane. In the event of a power outage, a UPS must provide transitional power, as a backup generator cannot be cut-in fast enough.

Behavior-based Monitoring

Software that monitors a system for malware infection, intrusion detection, or performance may be configured to recognize baseline behavior and (conversely) alert the administrator to anomalous behavior. This usually works by compiling a statistical profile of expected behavior then configuring thresholds beyond which the system generates an alert (an anomaly). This sort of system requires expert tuning to minimize false negative and false positives.

BIA (Business Impact Analysis)

A risk assessment will identify a range of threats and for each significant threat perform a Business Impact Analysis (BIA) to determine the likelihood of the threat exploiting a vulnerability and the cost to the business should a vulnerability be exposed.

Big Data

Large stores of unstructured information. As well as volume, big data is often described as having velocity, as it may involve the capture and analysis of high bandwidth network links.

Biometrics

Authenticating a user based on a record (template) of some information about their physical attributes (such as fingerprint or iris pattern) obtained (and subsequently confirmed at each access attempt) via a biometric reader. One of the problems of biometric authentication is the susceptibility to errors. These are classed as false positive (when a false user is recognized as a valid one) and false negative (when a valid user is refused access).

BIOS

A computer's Basic Input Output System (BIOS) controls its startup parameters. The most important of these from a security point-of-view is the boot order. Changing the boot order allows an attacker to inject any sort of malicious software onto the network. BIOS settings can be protected using a supervisor password.

Birthday Attack

A cryptographic function may produce collisions (where the function produces the same output for two different inputs). These may be connected to weak keys. The birthday paradox means that these collisions are less computationally intensive to attack than pure brute force (that is, you do not need to try every possible permutation to discover a weakness).

Blind FTP

Configuring an FTP server so that it does not provide a file/directory listing to the client.

Bluetooth / Bluejacking / Bluesnarfing

Bluetooth is a short-range radio-based connectivity protocol used by many peripherals, cell phones, and smartphones. Bluejacking refers to sending someone an unsolicited message or picture message using a Bluetooth connection; bluesnarfing refers to hijacking a Bluetooth device using some software exploit.

Botnet

A network of computers that have been compromised by Trojan / rootkit / worm malware. Providing the botnet can also subvert any firewalls between the controller (or "herder") and the compromised computers ("zombies"), they can be remotely controlled and monitored using covert channels. The internet contains botnets of many millions of computers and their exploitation (mostly to send spam or for identity theft) is a robust part of the "shadow" economy.

BPA (Business Partners Agreement)

While there are many ways of establishing business partnerships, the most common model in IT is the partner agreements that large IT companies (such as Microsoft and Cisco) set up with resellers and solution providers.

Browser

The application used to browse websites and consequently the target of many of the exploits used to launch attacks over the web. As well as the browser itself, plug-in applications that enable use of particular file formats, such as Flash or PDF, may also be vulnerable.

Buffer Overflow

Where a software program accepts input from the user, if the programmer has not created a routine to validate the input, it may be possible for an attacker to exploit this and overfill the program's buffer (memory used by the program). This can allow the attacker to crash the system or execute arbitrary code (such as a virus).

Business Continuity

A business continuity plan is designed to ensure that critical business functions demonstrate high availability and fault tolerance. Typically, this is achieved by allowing for redundancy in specifying resources. Examples include cluster services, RAID disk arrays, UPS. Business continuity plans should not be limited to technical elements however; they should also consider employees, utilities, suppliers, and customers. Associated with business continuity is the disaster recovery plan, which sets out actions and responsibilities for foreseen and unforeseen critical incidents.

BYOD (Bring Your Own Device)

Security framework and tools to facilitate use of personally-owned devices to access corporate networks and data.

CA (Certificate Authority)

See: PKI (*Public Key Infrastructure*).

CAN (Controller Area Network)

A serial network designed to allow communications between embedded programmable logic controllers.

Captive Portal

Secondary authentication mechanism for open access points. On connecting, the user's browser is redirected to a server to enter credentials (and possibly payment for access).

CAR (Corrective Action Report / Request)

A formal response setting out the plan to correct a defect in a system, such as a security vulnerability. This type of report or request may be implemented as part of a wider Failure Reporting, Analysis and Corrective Action System (FRACAS).

CD-R Media

Recordable and re-writable CDs (and DVDs) are a popular backup solution for home users. They are also useful for archiving material. Unlike magnetic media, the data on the disc cannot be changed (assuming that the disc is closed to prevent further rewriting in the case of RW media). This makes them useful for preserving tamper-proof records.

Certificate

A public key that has been certified by some agency, validating that the owner of the key is really who he or she says s/he is. This allows a sender to encrypt a message using the public key in the knowledge that only the recipient will be able to read it (using their linked private key). Certificates can also be used as proof of identity (for authentication or signing documents). Most certificates are based on the X.509 standard though PGP web of trust certificates are also popular.

CGI (Common Gateway Interface)

Means of working with HTTP's form mechanism (POST or GET) to process user input on a web server. Poorly written CGI applications can make a web server vulnerable to exploits.

Chain of Custody

See: *Forensics*.

Change Management

A change management process ensures that planned changes are introduced effectively. A large part of this is documenting changes and informing users. Changes will generally spark a new risk assessment process as the impact of the changes on the current security configuration needs to be assessed. Two key concepts are the submission of a Request for Change (RFC) and the Change Advisory Board (CAB), responsible for authorizing change. When a system or procedure is changed, it is vital to document the change, explaining who authorized and actioned it, why it was made, details of what was changed, and the date that the change was made.

CHAP (Challenge Handshake Authentication Protocol)

Authentication scheme developed for dial-up networks that uses an encrypted three-way handshake to authenticate the client to the server. The challenge-response is repeated throughout the connection (though transparently to the user) to guard against replay attacks.

Classification

Any significant data resource or documentation should be classified. In a mandatory access control system, information is formally classified with labels such as "Top Secret", "Secret", and "Confidential". In a discretionary or role-based access control system, resources are classified using Access Control Lists. These show what permissions (or rights) given users or groups have on the resource. One of the critical points distinguishing access control models is how a resource's classification can be changed. This will generally require some process of notification (at the very least, the change should be logged).

Cloud Computing

Any environment where software (Software as a Service and Platform as a Service) or computer / network resources (Infrastructure as a Service) are provided to an end user who has no knowledge of or responsibility for how the service is provided.

Coaxial Cable

Coax cable was once used for Ethernet installations but has largely been replaced by twisted-pair cabling. Coax cable is now mostly used for cable internet and TV installations. Coax cable can be tapped fairly easily for eavesdropping.

Code of Ethics

Professional behavior depends on basic ethical standards, such as honesty and fairness. Some professions may have developed codes of ethics to cover difficult situations; some businesses may also have a code of ethics to communicate the values it expects its employees to practice.

Collection of Evidence

See: *Forensics*.

Common Access Card

An identity and authentication smart card produced for Department of Defense employees and contractors in response to a Homeland Security Directive.

Communication

Clear channels of communication and procedures for notification are essential to effective security.

Comparative Strength of Algorithms

The choice of encryption algorithm is mostly driven by application (for example, symmetric encryption is the best choice for file or folder encryption for performance reasons). The basic measure of strength within an algorithm is the key size. Most current algorithms support key sizes of 128-bit or better. Most cryptography suites are open to independent analysis but this is no guarantee that they will remain secure indefinitely. It is also important to note that while an algorithm may be secure, its implementation in a particular product may not.

Confidentiality

See: *Cryptographic Confidentiality*.

Configuration Baseline

Settings for services and policy configuration for a server operating in a particular application role (web server, mail server, file/print server, and so on). In Windows, the current configuration can be compared to the baseline defined in a security template using the Security Configuration and Analysis tool.

Continuous Security Monitoring

Typically, security is only seriously investigated after some sort of incident. Continuous security monitoring refers to a proactive approach to performing risk assessments, checking audit logs, and reviewing threat sources. This reduces risk but requires either a particularly sophisticated intrusion detection system or the manpower to review logs and other security metrics.

Control Types

See: *Security Control*.

Cookies

Text file used to store information about a user when they visit a website. Some sites still use cookies to support user sessions. This type of site can be vulnerable to replay attacks, where an attacker obtains a user's cookies and resends the session information.

CRL (Certificate Revocation List)

See: *Key Management*.

Cryptographic Access Control

Cryptography is the basis of most "Something You Have" authentication systems. The user is given a smart card that stores a digital certificate issued to the user by a certificate authority. To authenticate, the user presents the card to the reader and inputs a PIN (which protects against use of a stolen card).

Cryptographic Algorithm

A cryptographic algorithm is a mathematical function that transforms plaintext into ciphertext in such a way that the plaintext cannot be recovered without knowledge of the appropriate key. A symmetric algorithm uses the same key for encrypting and decrypting; an asymmetric algorithm uses different keys (public and private; the keys are linked but one is not derivable from the other). A hashing algorithm is one-way only; once encrypted, the ciphertext cannot be decrypted.

Cryptographic Confidentiality

Cryptography can provide message confidentiality because the message can only be read by someone in possession of the correct key. The main problem with this is secure distribution of the key. Typically asymmetric encryption is used to distribute keys. As asymmetric algorithms are processor and memory intensive, they are not suitable for encrypting long messages.

Cryptographic Integrity and Authentication

It is often important to prove that a message has not been modified in transit and to confirm the identity of the sender. This can be done using a cryptographic digital signature. This is typically achieved using a hash function. If both sender and receiver use the same hash function on the same message, they should derive the same value (a message digest). The message digest is also encrypted using an asymmetric algorithm and the sender's private key. The recipient uses the sender's linked public key to decrypt the hash. This provides authentication, as only the sender (the possessor of the private key) could have encrypted the message in this way. This also provides non-repudiation (that is, the sender cannot deny creating and sending the message).

Cryptographic Standards

The most important set of standards governing cryptography are the PKIX RFCs for digital certificates and PKI. Many cryptographic applications have been developed from RSA's PKCS. Cryptographic products may be certified by Common Criteria and FIPS.

CVE (Common Vulnerabilities and Exposures)

Scheme for identifying vulnerabilities developed by MITRE and adopted by NIST.

DAC (Discretionary Access Control)

Access control model where each resource is protected by an Access Control List (ACL) managed by the resource's owner (or owners).

Data Emanation

Unless shielded, all electrical cabling "leaks" signals to some extent. However data emanation is more of a concern for wireless media, as the signals can be received for a considerable distance and shielding / containment is not a realistic option in most environments. Consequently, it is imperative that wireless communications use a strong encryption system.

Databases

Most network applications utilize databases. Major database server products include Oracle, Microsoft SQL Server, IBM's DB2 and Informix, and Sybase. Many databases are operated using Structured Query Language (SQL, pronounced "sequel"). The freeware MySQL database is a popular choice to provide database functionality on websites. Database engines are often subject to software exploits, and so should be kept patched. Database design, programming, and administration is complex and security should be considered as a critical requirement.

DBA (Database Administrator)

The IT role responsible for the configuration, management, and support of database applications.

Default Account

Default administrative and guest accounts configured on servers and network devices are possible points of unauthorized access. It is good practice to rename the Windows administrative account and on UNIX / Linux to leave the "root" system owner account unused.

DES (Data Encryption Standard)

Symmetric encryption protocol. DES and its replacement 3DES are considered weak in comparison with modern standards, such as AES.

DHCP Servers

Dynamic Host Configuration Protocol servers provide IP addressing information to clients. DHCP is vulnerable to DoS attacks. It is important to monitor the network to ensure that only valid DHCP servers are running on the network.

Digital Signature

See: *Cryptographic Integrity and Authentication*.

Directory Services

Directory services provide general and security information (permissions) for network users and objects. Most directory services are based on the LDAP standard. The directory server is a critical point of failure for most networks; without it clients cannot log on. Most networks are configured with backup servers. It is also important to configure access control on the server to ensure that directory information can only be modified by authorized personnel.

Disaster Recovery Plan

A documented and resourced plan showing actions and responsibilities to be used in response to critical incidents. The recovery plan may also provide for practice exercises or drills for testing and to familiarize staff with procedures. As well as facilitating a smooth transition in the event of disaster, plans must stress the importance of maintaining secure systems.

Disposal / Destruction Policy

When information is no longer required, it can either be archived or destroyed. In either case, care must be taken that this is done securely. Careless disposal of paper or electronic records can lead to serious security breaches.

DLP (Data Loss Prevention)

Data Loss (or Leakage) Prevention (DLP) is software that can identify data that has been classified and apply "fine-grained" user privileges to it (preventing copying it or forwarding by email for instance).

DMZ (Demilitarized Zone)

A private network connected to the internet must be protected against intrusion from the internet. However, certain services may need to be made publicly accessible from the internet (web and email for instance). One solution is to put such servers in a DMZ. The idea of a DMZ is that traffic cannot pass through it. If communication is required between hosts on either side of a DMZ, a host within the DMZ acts as a proxy. It takes the request and checks it. If the request is valid, it re-transmits it to the destination. External hosts have no idea about what (if anything) is behind the DMZ. A DMZ is implemented using either two firewalls (screened subnet) or a single three-legged firewall (one with three network ports).

DNS Servers

DNS allows for mapping of human-readable resource names to numerical IP addresses. DNS is a hierarchical, distributed database. DNS name servers host the database for domains for which they are authoritative. Root servers hold details of the top-level domains. DNS servers also perform queries or lookups to service client requests. The DNS protocol defines the mechanisms by which DNS servers and clients interact. The DNS protocol utilizes TCP/UDP port 53. It is essential to ensure that clients utilize a reliable DNS server, to prevent spoofing attacks. A DNS server also needs to be protected against footprinting, DoS, and cache pollution (poisoning) attacks.

Documentation

Accurate and up-to-date documentation is essential for maintaining effective and secure business procedures. The sorts of things that need documenting include policies, procedures, systems architecture, and assets.

Domain Name Kiting

There are various ways of exploiting the domain name registration process. Kiting refers to continually registering a name without having to pay for it. Tasting involves registering a domain temporarily to see how many "hits" it generates while hijacking and cybersquatting are means of occupying a domain of some trusted brand or company.

DoS (Denial of Service)

A network attack that aims to disrupt a service, usually by overloading it. A Distributed DoS (DDoS) attack uses multiple compromised computers (zombies) to launch the attack.

Due Care / Diligence

See: Legislation.

Due Process

Due process is a term used in US and UK common law to require that people only be convicted of crimes following the fair application of the laws of the land. More generally, due process can be understood to mean having a set of procedural safeguards to ensure fairness. This principle is central to forensic investigation.

Dumpster Diving

A "social engineering" technique of discovering things about an organization (or person) based on what it throws away.

EAP (Extensible Authentication Protocol)

Framework for negotiating authentication methods, supporting a range of authentication devices. EAP-TLS uses PKI certificates, Protected EAP (PEAP) creates a TLS-protected tunnel between the supplicant and authenticator to secure the user authentication method, and Lightweight EAP (LEAP) is a password-based mechanism used by Cisco.

Education

See: HR Policy.

Elliptic Curve Cryptography

See Asymmetric Cryptography.

Email Servers

Internet email message transfer is performed by SMTP servers. Most clients retrieve email using POP or IMAP however. On an intranet, internet messaging is likely to be integrated with groupware messaging, in a product such as Microsoft Exchange or Lotus Notes. Servers should be kept patched and configured against abuse from spammers.

Environment

Environmental security means ensuring stable supply of essential utilities (communications links, power, heating, water, transportation), protection against disaster (such as fire or flood), and shielding for communications systems (wired and wireless) to prevent eavesdropping.

Escalation

In terms of privilege management, escalation (or elevation) is where a user gains additional privileges without authorization. This may happen because the user is able to exploit the privilege management system design to change his or her privileges. It can also be a result of software exploits, which can crash the system and give the user administrative or root privileges.

ESN (Electronic Serial Number)

A number that uniquely identifies a mobile device, similar to a network adapter MAC address. ESNs have been replaced for cdma-based devices by MEID (Mobile Equipment ID). GSM/UMTS/LTE devices are identified by an IMEI (International Mobile Station Equipment Identity).

Evil Twin

In an evil twin attack, the attacker creates a malicious wireless access point masquerading as a genuine one, enabling the attacker to harvest confidential information as users connect via the AP.

Extranet

A network of semi-trusted hosts, typically representing business partners, suppliers, or customers. Hosts must authenticate to join the extranet.

Failsafe / Failopen

An electronic lock requires a power source. If the power source fails, a lock can fail in one of two ways. Failsafe (or fail-secure) means that the door will be locked (and unlockable) while failopen means the door will be open.

False Positive / False Negative

Error in monitoring or identification technology that either reports an event as an incident when it is not (false positive) or does not report an event as an incident (false negative).

Fault Tolerance

See: Business Continuity.

FC (Fibre Channel)

High speed network communications protocol used to implement SANs.

FCoE (Fibre Channel over Ethernet)

Standard allowing for a mixed use Ethernet network with both ordinary data and storage network traffic.

Fiber Optic Cable

Fiber optic is used for WAN links and some LANs. It is immune to eavesdropping and interference. The cable is very difficult to tap.

File / Print Servers

File and print is one of the basic functions of an NOS. Setting the server up securely is a case of configuring appropriate permissions using Access Control Lists for each resource.

Fire Suppression

Fire detection and suppression systems are mandatory in most public and private commercial premises. Water-based fire suppression is a risk to computer systems, both in the event of fire and through the risk of flood. Alternatives include dry pipe and gas-based systems.

Firewall

A range of devices and software products designed to restrict access from one network zone to another to defined IP address ranges or TCP/UDP application ports. The simplest type of firewall is packet filtering. More advanced products can maintain session information (circuit level) or perform stateful inspection of packets.

First Responders

See: Incident Response Policy.

Flash Card Media

Flash memory media, including proprietary memory card formats (such as Secure Digital and Memory Stick) and USB thumb drives, has become very cheap and high capacity (up to about 64 GB).

Flood Guard

A firewall or IPS that prevents DDoD attacks where multiple compromised "bots" attempt to deny network connectivity by flooding it with malicious packets. Another type of flood guard might be deployed to protect against broadcast loops in layer 2 (MAC) and layer 3 (IP) segments.

Forensics

The process of gathering and submitting computer evidence to trial. Digital evidence is latent, meaning that it must be interpreted. This means that great care must be taken to prove that the evidence has not been tampered with or falsified. The key points in collecting evidence are to record every step and action, to gather appropriate evidence, and to bag evidence. To preserve evidence correctly, it should be stored securely. Any investigation should be done on a copy of the digital files, not the originals. Each piece of evidence must be accompanied by a chain of custody form, detailing when, where, and how it was collected, where it has been stored, and who has handled it subsequently to collection.

FTP (File Transfer Protocol)

An application-layer TCP/IP protocol used for file management across two hosts. FTP communications are unencrypted but can be secured using SSL. FTP utilizes TCP ports 20 and 21.

FTP Servers

An FTP server provides file transfer across the internet, though in most cases the file transfer is not secure. FTP servers are often integrated with web servers. Securing the server is a case of keeping it up-to-date with patches, setting up access controls and permissions on directories appropriately, and configuring logging to track usage.

FTPS

A type of FTP using SSL for confidentiality.

Fuzzing

Fuzzing is a means of testing software input validation routines by inputting random or known malicious code. Fuzzing is also used in packet crafting to generate fake IP and MAC addresses.

GPS Tracking

Many mobile phones and smartphones are fitted with Global Positioning System (GPS) chips. This records the position of the phone to within a few meters. This has some privacy implications but can also assist with recovering stolen devices.

Group Management

See: User Management.

Group Policy

On a Windows domain, per-user and per-computer settings can be deployed through Group Policy Objects, attached to Active Directory containers such as domains and Organization Units. Group policy can be used to configure security settings such as password policy, account restrictions, firewall status, and so on.

Hard Drive Media

Disk storage is increasingly popular as a long-term storage solution. Also, high capacity removable hard drives have become very cheap (making theft of data via a USB port very simple if there is no access control on the files). Hard drives are subject to mechanical failure, so mission critical data is protected by configuring an array of drives (RAID); if a drive fails, it can be swapped out with a working one without losing data.

Hardware Locks

Devices can be physically secured against theft using cable ties and padlocks. Some systems also feature lockable faceplates, preventing access to the power switch and removable drives.

Hardware Security Module

A Hardware Security Module (HSM) is an appliance for generating and storing cryptographic keys. This sort of solution may be less susceptible to tampering and insider threats than software-based storage.

Hash Algorithm

See: Cryptographic Algorithm.

Heuristic

Monitoring technique that allows dynamic pattern matching based on past experience rather than relying on pre-loaded signatures.

HIDS

See: IDS (Intrusion Detection System).

High Availability

See: Business Continuity.

Hoaxes

Email, instant messaging, and website pop-ups are commonly used to spread hoax information, such as false virus or spyware alerts. Users should be trained to identify genuine sources of information.

Honeypot

A computer set up to entice attackers with the purpose of discovering attack strategies and weaknesses in the security configuration. A related term is honeynet, meaning a whole network set up to entice attackers.

Hotfix

An update designed for and released to particular customers only, though they may be included in later Service Packs.

HR Policy

Users are usually seen as the weak point of any security system. However, effective training and HR policies can use employees to strengthen security. Other security considerations for the HR department are coordinating secure recruitment and termination procedures. This means screening new employees through background checks, ensuring employees are set up with the correct privileges when they join or change job roles, and ensuring that privileges are revoked if the employee is fired or retires.

HTTP (HyperText Transfer Protocol)

TCP/IP application protocol defining a mechanism for clients such as browsers to request content from web servers. HTTP uses TCP port 80. HTTPS(ecure) provides for encrypted transfers, utilizing SSL and port 443.

HVAC (Heating, Ventilation, Air Conditioning)

Building control systems maintain an optimum working environment for different parts of the building. The acronym HVAC (Heating, Ventilation, Air Conditioning) is often used to describe these services. For general office areas, this basically means heating and cooling; for other areas different aspects of climate control, such as humidity may be important.

ICMP (Internet Control Message Protocol)

IP-level protocol for reporting errors and status information supporting the function of troubleshooting utilities such as ping and traceroute.

Identification

Authentication identifies a particular user account to a computer system; identification (or enrollment) is the process by which a user account (and its credentials) is issued to the correct person.

IDS (Intrusion Detection System)

Software designed to monitor network traffic (NIDS) or configuration files and logs on a host (HIDS) to record and detect unusual activity. Many systems can automatically take preventive action (Intrusion Prevention System). Detection is either signature-based or anomaly-based (or both). IDS software typically requires a lengthy period of configuration and "training" to recognize baseline "normal" activity.

IM (Instant Messaging)

Real-time text communications products. IM also supports file exchange and remote desktop. Like email, communications are generally unencrypted and unauthenticated. IM can be difficult to block on private networks as most applications can work over HTTP.

IMAP4 (Internet Message Access Protocol)

TCP/IP application protocol providing a means for a client to access email messages stored in a mailbox on a remote server. Unlike POP3, messages persist on the server after the client has downloaded them. IMAP also supports mailbox management functions, such as creating subfolders and access to the same mailbox by more than one client at the same time. IMAP4 utilizes TCP port number 143.

Implicit Deny

Implicit deny is a basic principle of security stating that unless something has explicitly been granted access it should be denied access. An example of this is firewall rule processing, where the last (default) rule is to deny all connections not allowed by a previous rule.

Incident Response

An intrusion detection system may have several options for what to do when an incident is detected. Passive systems simply log the incident or display an alert. An active system can initiate a response automatically, such as closing a TCP connection.

Incident Response Policy

Procedures and guidelines covering appropriate priorities, actions, and responsibilities in the event of security incidents. The stages will generally be notification, investigation, remediation, and follow-up. Incident response is often handled by a special group - the Computer Security Incident Response Team - made up of staff with both technical skills and decision making authority.

Input Validation

Where a program expects input from a user, good programming practice dictates that the user input should be validated before the program attempts any further processing of it. Failing to do this can leave the application vulnerable to buffer overflow and similar attacks.

Integrity

See: *Cryptographic Integrity and Authentication*.

Internet Content Filter

A software application or gateway that filters client requests for various types of internet content (web, FTP, IM, and so on). The filtering software can work on the basis of keywords, URLs, time of day / total browsing time, and so on.

Internet Zone

A zone permitting anonymous access (or perhaps a mix of anonymous and authenticated access) by untrusted hosts over the internet.

Intranet

A network of trusted hosts owned and controlled by the organization.

Inventories

An inventory is a list of things, usually stored in a database. Inventories are usually compiled for assets.

IPsec

Layer 3 protocol suite providing security for TCP/IP. It can be used in two modes (transport, where only the data payload is encrypted, and tunnel, where the entire IP packet is encrypted and a new IP header added). IPsec can provide confidentiality and/or integrity. Encryption can be applied using a number of hash (MD5 or SHA) and symmetric (DES or AES) algorithms. Key exchange and security associations are handled by the Internet Key Exchange Protocol. Hosts can be authenticated by a shared secret, PKI, or Kerberos.

ISA (Interconnection Security Agreement)

Any federal agency interconnecting its IT system to a third-party must create an ISA to govern the relationship. An ISA sets out a security risk awareness process and commit the agency and supplier to implementing security controls.

iSCSI

IP tunneling protocol that enables the transfer of SCSI data over an IP-based network to create a SAN.

IV (Initialization Vector) Attack

Faults in the way that WEP implements the stream cipher used to encrypt traffic mean that the key can be recovered using cryptanalysis tools such as Aircrack given sufficient packets to analyze. Such tools can typically crack both 64-bit and 128-bit WEP encryption in a matter of minutes. WPA is not vulnerable to this attack (though weak passwords are still vulnerable to dictionary cracking).

Java

Programming language used to create web server applications (J2EE) and client-side applications (running in the Java VM).

JavaScript

Scripting language used to add interactivity to web pages and HTML-format email. JavaScript can also be used maliciously to exploit software vulnerabilities. It is possible to block scripts from running using browser security settings.

Job Rotation

Job rotation is the policy of preventing any one individual performing the same role or tasks for too long. This deters fraud and provides better oversight of the person's duties.

Kerberos

Single sign-on authentication scheme where clients authenticate once to a Key Distribution Center and are granted service tickets to use particular applications without having to log on to each application separately.

Key Management

Apart from validating a user's identity, one of the main functions of a CA is management of cryptographic keys over their lifecycle. Some of the main issues are as follows. Usage - keys should be issued for the stated purpose only; for example, a key used for signing should not be used for encryption. Storage - hardware based is generally more secure than software; it is imperative that private keys are not compromised. Lifetime - a key pair is set to expire after a number of years; it may also be revoked or suspended before that time if the key is compromised; a status checking mechanism (Certificate Revocation List) must be in place so that clients can discover whether a key is still valid. Renewal - a certificate needs to be renewed before the old one expires; however, keys should not be reused. Recovery and escrow - if a key is lost, some mechanism may be required to recover data encrypted with the key; this mechanism is typically protected by M of N control, to ensure that no one user can abuse the recovery process.

L2TP (Layer 2 Tunneling Protocol)

VPN protocol developed by Cisco. Its main advantage over PPTP is support for frame types and protocols other than PPP and TCP/IP. L2TP uses UDP port 1701. Encryption can be provided by IPsec.

Layered Security / Defense in Depth

Configuring security controls on hosts (endpoints) as well as providing network (perimeter) security, physical security, and administrative controls.

LDAP (Lightweight Directory Access Protocol)

Standard for accessing and updating information in an X.500-style network resource directory. LDAP uses port 389. Unless secure communications are used, LDAP is vulnerable to packet sniffing and Man-in-the-Middle attacks. It is also usually necessary to configure user permissions on the directory. LDAP version 3 supports simple authentication or Simple Authentication and Security Layer, which integrates it with Kerberos or TLS.

Least Privilege

Least privilege is a basic principle of security stating that something should be allocated the minimum necessary rights, privileges, or information to perform its role.

Legislation

Organizational security policies are (to some extent) driven by legislation introduced as a response to the growing appreciation of the threat posed by computer crime. Legislation can cover many aspects of security policy but the key concepts are due diligence (demonstrating awareness of security issues) and due care (demonstrating responses to identified threats). Security policy is also driven by adherence to industry codes of practice and standards.

Load Balancer

A type of switch or router that distributes client requests between different resources, such as communications links or similarly-configured servers. This provides fault tolerance and improves throughput.

Location

Site location is an important security consideration, especially as regards reliable utility supply. Conversely, remote sites may suit some organizations, as this makes surveillance easier.

Logic Bomb

A malicious program or script that is set to run under particular circumstances or in response to a defined event.

Logical Token

A single sign-on system such as Kerberos issues users with a software token to present as confirmation that they have been previously authenticated.

Logs

OS and applications software can be configured to log events automatically. This provides an audit trail of actions performed on the system as well as warning of suspicious activity. It is important that log configuration and files be made tamper-proof.

Loop Protection

If broadcast traffic is allowed to continually loop around a network, the number of broadcast packets increases exponentially, crashing the network. Loop protection in switches (such as Spanning Tree Protocol), and in routers (Time To Live for instance) is designed to prevent this.

MAC Filter

Applying an access control list to a switch or access point so that only clients with approved MAC addresses can connect to it.

Mandatory Access Control

Access control model where resources are protected by inflexible, system defined rules. Resources (objects) and users (subjects) are allocated a clearance level (or label). There are a number of privilege models, such as Bell-LaPadula, Biba, and Clark-Wilson providing either confidentiality or integrity.

Mandatory Vacations

Mandatory vacations means that employees are forced to take their vacation time, during which someone else fulfils their duties.

Man-in-the-Middle

Where the attacker intercepts communications between two hosts.

Mantrap

A secure entry system with two gateways, only one of which is open at any one time.

Mathematical Attack

If a cryptographic function (algorithm) has known weaknesses, an attack can be formulated to exploit this (for example, to decrypt a document or to fake a digital signature).

MDM (Mobile Device Management)

Software suites designed to manage use of smartphones and tablets within an enterprise.

Mobile Devices

Portable phones and smart phones can be used to interface with workstations using technologies such as Bluetooth or USB. As such, they are increasingly the focus of viruses and other malware. Portable devices storing valuable information are a considerable security risk when taken offsite.

Modems

A modem is used to interface a computer with the telephone network for data and fax communications. The "local loop" between the telecoms office and a user's premises uses analog signaling. A modem converts between the digital signaling used by the computer and the analog signaling used by the telephone line. Many computers ship with modems that might not be used; these should be disabled to prevent backdoor access to the computer.

MOU (Memorandum of Understanding)

Usually a preliminary or exploratory agreement to express an intent to work together.

MTTR / MTTF / MTBF

Mean Time to Failure (MTTF) and Mean Time Between Failures (MTBF) represent the expected lifetime of a product or system. Mean Time to Repair (MTTR) is a measure of the time taken to correct a fault so that the system is restored to full operation.

Multi-factor Authentication

Strong authentication is multi-factor. Authentication schemes work on the basis of something you know, something you have, or something you are. These schemes can be made stronger by combining them (for example, protecting use of a smart card certification [something you have] with a PIN [something you know]).

Mutual Authentication

Typically a client authenticates to a server. In many circumstances, it may be necessary for the server to authenticate to the client also (to prevent Man-in-the-Middle attacks for instance). This is referred to as mutual authentication.

NAC (Network Access Control)

NAC is a means of ensuring endpoint security; that is, ensuring that all devices connecting to the network conform to a "health" policy (patch level, anti-virus / firewall configuration, and so on). NAC can work on the basis of pre- or post-admission control. The core components are an agent running on the client, policy enforcers (network connection devices such as switches and access points), and policy decision points (NAC policy server and AAA / RADIUS server).

NAPT (Network Address Port Translation)

Similar to NAT, NAPT (or PAT or NAT overloading) maps private host IP addresses onto a single public IP address. Each host is tracked by assigning it a random high TCP port for communications.

NAS (Network Attached Storage)

NAS is a storage device with an embedded OS that supports typical network file access protocols (TCP/IP and SMB for instance). These may be subject to exploit attacks (though using an embedded OS is often thought of as more secure as it exposes a smaller attack "footprint"). The unauthorized connection of such devices to the network is also a concern.

NAT (Network Address Translation)

Where hosts on a private network need internet access, it is no longer practical or secure to allocate each host a unique IP address. Instead, hosts on the private network use private addressing. A router or proxy server provides Network Address Translation to map the private address to one or more publicly accessible IP addresses. As well as being easier to configure, this hides the private network addressing scheme from internet users.

Need to Know

A basic principle of confidentiality is that employees should know what they need to do their job and no more. Restricting the distribution of information makes it more secure.

NetBIOS

A session management protocol used to provide name registration and resolution services on older Microsoft networks. WINS provides NetBIOS name resolution.

Network Interconnections / Hardening

The basic steps in network hardening are to ensure the physical security of infrastructure (cabling, servers, switches, routers), configure services and protocols (disabling anything that is not required), configure access control (on firewalls and key devices), and set up a monitoring and maintenance program to detect unauthorized equipment or applications connected to the network and apply critical firmware or patch updates to network hardware.

Network Mapper

Software that can scan a network and identify hosts, addresses, protocols, network interconnections, and so on.

Network Monitoring

Auditing software that collects status and configuration information from network devices. Many products are based on the Simple Network Management Protocol (SNMP).

Network Separation

Enforcing a security zone by separating a segment of the network from access by the rest of the network. This could be accomplished using firewalls or VPNs or VLANs. A physically separate network or host (with no cabling or wireless links to other networks) is referred to as air-gapped.

NIDS / NIPS

See: *IDS (Intrusion Detection System)*.

Non-essential Services

A principle of computer security is that only necessary services and protocols should be run. On many OS, this means disabling or uninstalling services following a default installation. Also, services should be secured so that they can be used only by authorized accounts.

Non-repudiation

See: *Cryptographic Integrity and Authentication*.

NTP (Network Time Protocol)

TCP/IP application protocol allowing machines to synchronize to the same time clock. NTP runs over UDP port 123.

Null Session

Windows NT and 2000 allow unauthenticated access to the IPC\$ share by default. This allows an attacker to gain valuable information about the host (fingerprinting). Null sessions are disabled by default in Windows XP, Server 2003 and above.

Offsite Storage

See: *Backup*.

OS Hardening

Hardening is the process of making the OS (or Network OS) configuration secure. The exact steps vary greatly depending on the OS. However, the basic steps are to enable only necessary services (and configure access to them), set up access control on the file system and data directories, install monitoring software to protect against malware and intrusions, and establish a maintenance schedule to ensure the OS is patched to be secure against software exploits.

OVAL (Online Vulnerability and Assessment Language)

An XML schema for describing system security state and querying vulnerability reports and information.

P2P (Peer-to-Peer)

File sharing networks where data is distributed around the clients that use the network. Apart from consuming bandwidth and disk space, P2P sites are associated with hosting malware and illegal material.

PAC (Proxy Auto-Config)

A type of script that allows a browser to select and configure an appropriate proxy server address and port number without requiring user intervention. PACs can also be used maliciously to try to redirect browsers to phishing sites.

Packet Sniffing

Most original TCP/IP application protocols transmit data in plaintext. Ethernet-based networks can run in promiscuous mode, meaning that a host can receive all data packets, even if they are not intended for it. Packet sniffing software exploits these two facts and means that it is simple to capture information about the network and data that is being transmitted (including passwords) unless encryption is used.

PAP (Password Authentication Protocol)

Obsolete authentication mechanism used with PPP. PAP transfers the password in plaintext and so is vulnerable to eavesdropping.

Password Crackers

Password guessing software can attempt to crack user passwords by running through all possible combinations (brute force). This can be made less computationally intensive by using a dictionary of standard words or phrases. If a password is extremely simple or left to a default value, it may also be possible for the attacker to guess it without needing special software.

Password Policy

A weakness of password-based authentication systems is when users demonstrate poor password practice. Examples include choosing a password that is too simple, reusing passwords for different tasks, writing a password down, and not changing a password regularly. Some of these poor practices can be addressed by system policies; others are better approached by education.

Patch Management

Identifying, testing, and deploying OS and application updates. Patches are often classified as critical, security-critical, recommended, and optional.

PBX (Private Branch Exchange)

An automated switchboard providing a single connection point for the organization's voice and data lines. Access to a PBX must be carefully restricted to authorized personnel only, with special consideration for any remote admin features built into it.

Penetration Testing

White hat hacking to try to discover and exploit any weaknesses in network security.

Performance Monitor

Software that tracks the performance of system and application variables (counters). The results can be viewed in real time or logged. Actual performance needs to be measured against a baseline, usually taken when the system is first installed. Most software can also generate alerts if performance breaches defined thresholds.

Personal Software Firewall

A firewall implemented as applications software running on the host. Personal software firewalls can provide sophisticated filtering of network traffic and also block processes at the application level. However, as a user-mode application they are more vulnerable to attack and evasion than kernel mode firewalls or network firewall appliances.

PGP (Pretty Good Privacy)

Email encryption product providing message confidentiality and integrity using web of trust PGP certificates.

Phishing

Obtaining user authentication or financial information through a fraudulent request for information. Phishing is specifically associated with emailing users with a link to a faked site (or some other malware that steals the information they use to try to authenticate). Pharming is a related technique where the attacker uses DNS spoofing to redirect the user to the fake site. Vishing refers to phishing attacks conducted over voice channels (VoIP) while spear phishing or whaling refers to attacks specifically directed at managers or senior executives.

Physical Security

Physical access to premises and equipment should not be overlooked in designing security. Barriers can be physical and/or psychological. Entry control mechanisms range from ID badges and simple key locks to certificate-based (physical tokens) or biometric access control.

PII (Personally Identifiable Information)

PII is data that can be used to identify or contact an individual (or in the case of identity theft, to impersonate them). A social security number is a good example of PII. Others include names, Date of Birth, email address, telephone number, street address, biometric data, and so on.

PKI (Public Key Infrastructure)

Asymmetric encryption provides a solution to the problem of secure key distribution for symmetric encryption. The main problem is making a link between a particular public-private key pair and a specific user. One way of solving this problem is through PKI. Under this system, keys are issued as digital certificates by a Certificate Authority (CA). The CA acts as a guarantor that the user is who s/he says s/he is. Under this model, it is necessary to establish trust relationships between users and CAs. In order to build trust, CAs must publish and comply with Certificate Policies and Certificate Practice Statements.

POP3 (Post Office Protocol)

TCP/IP application protocol providing a means for a client to access email messages stored in a mailbox on a remote server. The server usually deletes messages once the client has downloaded them. POP3 utilizes TCP port 110.

Popup Blocker

Pop-ups are browser windows that open automatically using a script in the host page or some sort of adware or spyware installed on the PC. A popup blocker can prevent these windows from being opened. Some pop-ups are now implemented using Flash or Shockwave plug-ins, though blocking software can often deal with these too.

Port Scanner

Software that enumerates the status of TCP and UDP ports on a target system. Port scanning can be blocked by some firewalls and IDS.

Port Security

Preventing a device attached to a switch port from communicating on the network unless it matches a given MAC address or other protection profile.

Power Level Controls

Enterprise-class wireless access points and adapters support configurable power level controls. In some circumstances, increasing power can increase range and overcome local interference.

PPTP (Point-to-Point Tunneling Protocol)

Protocol developed by Cisco and Microsoft to support VPNs over PPP and TCP/IP. PPTP uses TCP port 1723. Encryption can be provided by Microsoft Point-to-Point Encryption.

Preservation of Evidence

See: Forensics.

Privacy Policy

Privacy policy generally covers what monitoring and data collection will be made of an organization's employees. A privacy policy is also important when collecting data from third parties, such as customers and suppliers. Privacy policy may have to be formulated within the bounds of civil rights and data protection legislation, though this is not true of all countries.

Private Key

In asymmetric encryption, the private key is known only to the holder and is linked to, but not derivable from, a public key distributed to those with which the holder wants to communicate securely. A private key can be used for encryption or decryption, but the same key should not be used for both.

Privilege Escalation

Exploiting a bug in software (such as buffer overflow) to gain elevated privileges, either within the application or OS, for a malicious process. For example an exploitable buffer overflow on web browser software might allow a virus, rootkit, or Trojan to run with system privileges rather than the privileges of the logged on user.

Privilege Management

This is the practical application of access control measures. The basic task is to set up and monitor (audit) resources and users to ensure that user privileges (or rights) on each resource are correct. The way privilege management is implemented depends on the model of access control being used (discretionary, role-based, or mandatory). A discretionary system tends towards decentralized management; role-based tends to be centrally managed.

Protocol Analyzer

Software that intercepts network traffic (packet sniffer) and displays the captured packets for analysis, allowing inspection of the packet headers and payload (unless the communications are encrypted).

Proxy Server

A server that mediates the communications between a client and another server. The proxy server can filter and often modify communications as well as providing caching services to improve performance.

Public Key

See: *Private Key*.

Quantum Cryptography

Quantum cryptography refers to using quantum computing for cryptographic tasks, such as distributing keys or cracking (traditional) cryptographic systems. Quantum computing works on the principle that its units (qubits) have more properties than the bits used in "classical" computers, notably (and very crudely) that a qubit can be both 1 and 0 at the same time and that the value of one qubit can depend on another (entanglement). These properties offer the promise of tamper-proof key distribution but also of fruitful attacks against traditional cryptographic systems.

RA (Registration Authority)

In PKI, the functions of registering and identity proofing users may be devolved from the Certificate Authority (CA) to a Registration Authority (RA). The function of signing and issuing certificates is always reserved by the CA.

RAD (Rapid Application Development)

A programming environment that helps developers to create software quickly.

RADIUS (Remote Authentication Dial-in User Service)

Remote Authentication Dial-in User Service was used by ISPs to authenticate and audit internet access by account holders. RADIUS is now also widely used to manage remote and wireless authentication infrastructure. Users supply authentication information to RADIUS client devices, such as wireless access points. The client device then passes the authentication data to an AAA server, which processes the request.

RAID (Redundant Array of Independent Disks)

Using RAID technology, users can deploy multiple hard disks to provide a backup measure for network servers and workstations. Several levels of backup are suggested by this system, ranging from level 0 to level 6, each level representing a particular type of fault tolerance.

RAS (Remote Access Server)

A server configured to process remote connections. Historically, this meant dial-up connections. These days, remote connections are more likely to be created via a VPN. Remote access policies define how users are able to connect to the server (media, protocols, authentication method, time of day restrictions, and so on) and rights and accessibility of resources over the connection.

RDP (Remote Desktop Protocol)

Microsoft's protocol for operating remote connections to a Windows machine (Terminal Services). The protocol sends screen data from the remote host to the client and transfer mouse and keyboard input from the client to the remote host. It uses TCP port 3389.

Recovery Agent

A user configured to restore encrypted data in the event that the original key is lost. The recovery agent is granted access to a backup of the key, stored in some secure location. Recovery access is often subject to "M of N" control, requiring more than one user to authorize the recovery, to deter fraud.

Redundancy Planning

Most disaster recovery plans call for the presence of redundant systems and backed up data. One goal is to eliminate Single Points of Failure. At the high end, these plans may involve alternate sites. These can be classified as cold, warm, or hot, depending on their state of readiness. Redundancy is also provided by spare parts for key systems, servers that can provide for failover (clusters), redundant network links, disk arrays (RAID), power supply, and backup ISP services (internet connection and web hosting).

Remote Authentication

When a user authenticates with a remote server, it is particularly important that the communications be kept confidential through the use of encryption (though in fact, the use of packet sniffing on LANs means that all password communications, local and remote, are routinely encrypted).

Remote Wipe / Kill Switch

A feature of newer cell phones and smartphones that allows personal data to be deleted (for example if the phone is suspected stolen) by sending a command to the device from a remote server.

Removable Storage

Over the years, several different types of removable storage have been developed to archive and transfer files. The main security concerns with removable media are its durability and longevity (from the point of view of archiving data), whether it is tamper-proof, and the ease with which files can be copied and removed from a site without authorization.

Replay

Where the attacker intercepts some authentication data and reuses it to try to re-establish a session.

Risk Assessment / Calculation

Risk assessment is the process of assessing threats and vulnerabilities to an organization's assets and processes. The first steps are to identify and document assets and threats. The next step is to quantify the degree of risk associated with each asset and procedure. Purely quantitative risk assessment assigns concrete values to each risk factor, depending on variables such as the likelihood of the threat being realized and the impact (factors such as the value of the asset or the cost of disruption if the asset is compromised). This is very hard to do, so many risk assessments use a qualitative approach, in which the assessor makes a more generalized assessment. Risk and the threat of loss make a vulnerability. Each vulnerability must be controlled. Risk can be removed, mitigated, assigned, or accepted, but not ignored.

Rogue Devices

The attachment of rogue network devices and services, including access points, DHCP servers, and DNS servers, can allow very effecting spoofing or Man-in-the-Middle attacks to be launched. Various scanning and monitoring software is available to detect rogues.

Role Management

See: User Management.

Role-Based Access Control

Access control model where resources are protected by ACLs. However, management of ACLs is reserved to administrators rather than owners and users are assigned permissions according to job function rather than personally.

Rootkit

A class of malware (typically a Trojan, which is to say the user believes they are installing something else) that modifies system files, often at the kernel level, to conceal its presence.

Router

Devices that provide network interconnectivity on the internet. Routers can be implemented as dedicated hardware or run as a service of an NOS. Access to the router must be carefully restricted to authorized personnel only.

RPO / RTO

Recovery Point Objective (RPO) is the amount of data loss that a system can sustain, measured in time. Recovery Time Objective (RTO) is the period following a disaster that a system may remain offline.

Rule-Based Access Control

Any access control model that follows system-enforced rules that cannot be countermanded can be described as "rule-based". A firewall is a good example of rule-based access control but the MAC and role-based models can also be described as rule-based. DAC is not rule-based as decisions are made by the resource owner.

S/MIME

Email encryption standard (Cryptographic Message Standard) using PKI (X.509) certificates for confidentiality (digital envelopes) and integrity (digital signatures). S/MIME provides extensions for standard MIME (Multipurpose Internet Mail Extensions) headers.

SAN (Storage Area Network)

Network dedicated to data storage, typically consisting of storage devices and servers connected to switches via Host Bus Adapters. Data access in a SAN is handled at block level.

SCAP (Security Content Automation Protocol)

Allows compatible scanners to determine whether a computer meets a particular configuration baseline from NIST's database (scap.nist.gov).

SCEP (Simple Certificate Enrollment Protocol)

A protocol developed by Cisco to provision users and appliances (such as routers and switches or smartphones) with certificates more easily. SCEP uses HTTP to submit a Certificate Signing Request (CSR) then monitors the status of the request. It can also automatically renew certificates that are about to expire.

SCP (Secure Copy)

Version of the UNIX Remote Copy (RCP) program utilizing SSH to encrypt transmissions.

Scripting

A programming language is used to create compiled (binary) executables. A scripting language is executed "on the fly" by an interpreter. Despite this, scripting languages can control most aspects of OS configuration and file access. Consequently, browsers run scripts within a sandbox, theoretically preventing access to the file system and OS configuration. Exploitable vulnerabilities in the interpreter can overcome these restrictions though.

SDLC (Software Development LifeCycle)

The processes of planning, analysis, design, implementation, and maintenances that often govern software and systems development.

Secure Disposal

See: *Disposal / Destruction Policy*.

Security Baseline

When performing auditing, performance monitoring, or configuring software such as intrusion detection, it is necessary to establish a baseline of "normal" activity. Any variation from the baseline is then treated as an incident, which may need investigation or remediation.

Security Control

A technology or procedure put in place to mitigate vulnerabilities and risk and to ensure the Confidentiality, Integrity, and Availability (CIA) of information. Control types are often classed in different ways, such as technical, operational, and management.

Security Policy

Each organization should have a documented security policy backed by senior management. The policy should set out requirements for protecting technology and information assets from threats and misuse. The policy should be communicated effectively to all levels of the organization and backed up with procedures and resources to put it into effect.

Security Template

Settings for services and policy configuration for a server operating in a particular application role (web server, mail server, file/print server, and so on). In Windows, the current configuration can be compared to the baseline defined in a security template using the Security Configuration and Analysis tool.

Security Zone

A zone is an area of the network (or of a connected network) where the security configuration is the same for all hosts within it.

SEH (Structured Exception Handler)

A mechanism in Windows for allowing software developers to account for unexpected error conditions that might arise during code execution. Effective error handling reduces the chances that a program could be exploited.

Separation of Duties

For a critical business function to be secure, it may be necessary to ensure that no one person can perform that function.

Servers

Servers must be kept secure by careful configuration (running only necessary services) and maintenance (OS and application updates, malware/intrusion detection, and so on). Where a network is connected to the internet, servers storing private information or running local network services should be protected by firewalls so as not to be accessible from the internet.

Service Pack

A collection of software updates, hotfixes, and in some cases new features and enhancements.

SFTP (Secure File Transfer Protocol)

A type of FTP using SSH for confidentiality.

Shielding

Most network media leak signals to some extent, with wireless radio being the easiest to intercept (eavesdrop). Shielding can counteract this risk. Twisted-pair cabling can be shielded or screened; whole rooms can be shielded using metal paint or wire mesh.

Shoulder Surfing

Social technique to gain access to a building by following someone else (or persuading them to "hold the door") or to obtain someone's password or PIN by observing them as they type it in.

Signature-based Monitoring

Software that monitors a system for malware infection, intrusion detection, or performance may be configured to recognize threat signatures or definitions based on known malware or attack patterns. This sort of system is quite simple to install but cannot provide any defense against unknown threats (zero-day exploits) and requires its signature database to be kept up-to-date.

Signed Applet

Java applets can be used as web page plug-ins to provide extra functionality. As with ActiveX, Java is a powerful programming language and can be used to create malware. Vendors can sign applets using certificates to validate their authenticity.

Single Versus Dual-sided Certificates

A digital certificate provides proof of identity through PKI or a Web of Trust (PGP). In most cases, a server authenticates itself to a client; this can be described as "single-sided". In some cases, the server may require the client or a peer server to authenticate itself too; this can be described as "dual-sided". The client and server must establish a trust relationship for their certificates, either directly or using the same root CA.

SIM (Subscriber Identity Module)

A small chip card that identifies the user and phone number of a mobile device, via an International Mobile Subscriber Identity (ISMI). A SIM card also provides a limited amount of local storage, for contacts.

Site Survey

Planning a wireless deployment by identifying optimum locations for antenna and access point placement to provide the required coverage for clients and identifying sources of interference.

SLA (Service Level Agreement)

Operating procedures and standards for a service contract.

SLE (Single Loss Expectancy)

The amount that would be lost in a single occurrence of the risk factor.

Smart Card

A smart card is a credit card with a microchip. The microchip can be programmed with a small amount of data, such as a digital certificate for authentication. A card can be interfaced with a PC using a reader. A special device is required to reprogram a smart card.

SMS (Short Message Service)

A system for sending text messages between cell phones. SMS has been one of the world's most popular communications methods but is now under some threat from messaging apps.

SMTP Open Relay

TCP/IP suite application protocol used to send mail between hosts on the internet. Messages are sent over TCP port 25. An SMTP server typically handles mail for its own domain. Some servers are left configured as open relays, meaning that anyone can use the server to send mail. This can be exploited by spammers and disguises the true source of the messages.

SNMP (Simple Network Management Protocol)

See: *Network Monitoring*.

Social Engineering

An attack that focuses on exploiting human users of the network. Typical social engineering methods include impersonation, domination, and charm.

Software Exploitation

Most software contains vulnerabilities caused by bugs or poor design. Exploits can be used by attackers to crash or gain control of the system.

Spam

Junk messages sent over email (or instant messaging [SPIM]). Filters and blacklists are available to block spam and know spam servers. It is also important to ensure that any mail servers you operate are not open relays, allowing a spammer to leverage your server to distribute spam and making it likely that it will be blacklisted.

Spare Parts

See: *Redundancy Planning*.

SPoF (Single Point of Failure)

A component or system that would cause a complete interruption of a service if it failed. SPoFs are mitigated by providing redundant parts, connections, or services that either provide failover (the replacement is automatically switched in) or swift replacement.

Spoofing

Where the attacker disguises their identity. Some examples include IP spoofing, where the attacker changes their IP address, or phishing, where the attacker sets up a false website.

Spyware

Software that monitors a user's activity. Spyware is distinguished from adware either by installing itself without the user's informed consent or by collecting data for criminal purposes (key logging authentication information for instance).

SSH (Secure Shell)

A remote administration and file copy program that is flexible enough to support VPNs too (using port forwarding). SSH runs on TCP port 22.

SSID Broadcast

The Service Set ID identifies a particular Wireless LAN (WLAN). This "network name" can be used to connect to the correct network. Nominally, broadcasting the SSID makes the network publicly visible but WLANs are quite easy to detect even if the SSID is not advertised. Disabling SSID broadcast is no substitute for enforcing authentication and encryption.

SSL / TLS (Secure Sockets Layer / Transport Layer Security)

Session-layer protocol providing security for TCP-based applications, notably HTTP (HTTPS, running over port 443). Client and server set up a secure connection through PKI (X.509) certificates (optionally, both client and server can authenticate to one another).

SSO (Single Sign-on)

Resources on a network may be hosted by multiple software applications from different vendors. Each application may have a different log on method, requiring administrators to create multiple user accounts and for users to have to remember and input multiple logons. A single sign-on system, such as Kerberos, centralizes user authentication in one module then negotiates with applications on behalf of the user to obtain service tickets.

Standards and Guidelines

Policy sets the overall tone for how something should be done and is usually intended for a general audience. More detailed guidance and standards may be produced for different audiences, such as end users and technical staff. In addition to internal standards, many job tasks may be guided by external standards, legislation, and "best practice" guidance. External standards may come from industry practice, professional organizations, or legislation.

Steganography

Steganography (literally meaning "hidden writing") is a technique for obscuring the presence of a message. Typically, information is embedded where you would not expect to find it (a message hidden in a picture for instance). This technique is used for counterfeit deterrence and detection and in the creation of "covert channels" (embedding messages in IP headers).

Storage and Retention Policies

Many security systems focus on the protection of data that is in use on a "live" or "production" system. When data reaches the end of its useful life, it may either be destroyed or archived. A retention policy will dictate which is the case and for how long information needs to be retained (this may be subject to legislative requirements). The storage facility needs to have similar security mechanisms to the production system, to ensure that the data is kept securely and accessed only by authorized users. Another storage security consideration is data copied to backup media, especially when it is stored offsite.

Subnetting

An IP network can be divided into a number of subnets using different subnet masks. Communications between any two subnets must be channeled via a router. This segmentation of the network is useful for both performance and security. Each subnet is a separate broadcast domain.

Succession Planning

Businesses can only depend so far on written procedures. Many tasks, especially at management level, require skill and experience to conduct properly. Succession planning is the task of identifying ways in which a business could cope if a disaster led to loss of key staff.

Switch

An advanced type of hub used to connect network segments. Switches improve performance by creating temporary virtual circuits between communicating hosts, reducing collisions. Switches can also be used to create VLANs. Access to a switch must be carefully restricted to authorized personnel only.

Symmetric Algorithm

See: *Cryptographic Algorithm*.

System Scanning

Regular scanning (or penetration testing or ethical hacking) is vital to ensure the security of a computer system and network. There are many types of scanners, notably anti-virus and Intrusion Detection software.

Systems Architecture

See: *Documentation*.

Systems Monitor

Software that tracks the health of a computer's subsystems using metrics reported by system hardware or sensors. This provides an alerting service for faults such as high temperature, chassis intrusion, and so on.

TACACS+ (Terminal Access Controller Access Control System)

An alternative to RADIUS developed by Cisco. The version in current use is TACACS+; TACACS and XTACACS are legacy protocols.

Tailgating

A "social engineering" means of gaining unauthorized access to a building by following someone through a door or getting them to hold a door open.

Tap

A device used to eavesdrop on communications at the physical layer. An Ethernet tap can be inserted between a switch and a node while a passive tap can intercept emanations from unshielded cable.

Tape Media

Tape is mostly used for security backups and archiving on larger networks. There are many different formats, supporting multiple gigabytes or even terabytes of storage. Tape is a reliable and secure long term storage option, so long as the tapes are stored in a suitable environment and maintained properly.

TCP/IP Hijacking

A type of spoofing attack where the attacker disconnects a host then replaces it with his or her own machine, spoofing the original host's IP address.

Telecoms

See: *PBX (Private Branch Exchange)*.

Telephony

Telephony refers to carrying voice traffic over data networks (Voice over IP [VoIP]). A network carrying both voice and data is said to be converged. Converged networks introduce a whole new class of devices whose security implications need to be considered. There is also a greater vulnerability to DoS (without redundancy the network is a single point of failure for both voice and data traffic) and eavesdropping on voice communications.

Telnet

Telnet provides terminal emulation software that supports a remote connection to another computer. When you connect, your computer acts as if your keyboard is attached to the remote computer and you can use the same commands as a local user. Often used for router configuration. Telnet communications are not secured.

TFTP (Trivial File Transfer Protocol)

A simplified form of FTP supporting only file copying (FTP can also enumerate directory contents, create directories, remove files and directories, and so on). TFTP works over UDP port 69.

Time of Day Restrictions

Time of day restrictions applied to a user account mean that the account may only be accessed at proscribed times. This is useful in preventing abuse of the account.

Token

A one-time password used for authentication. Tokens (or tickets) may be used in authentication software transparently to the user. A hardware token, such as RSA SecurID, generates a random code synchronized to a server and displayed on a key fob. The user inputs the code displayed at the correct time (along with a PIN to protect against theft of the fob).

TPM (Trusted Platform Module)

Trusted Platform Module (TPM) is a specification for hardware-based storage of digital certificates, keys, hashed passwords, and other user and platform identification information. Essentially it functions as an embedded smart card.

Trojan

Malware that is disguised as another program to trick the user into installing it.

Trust Model

See: *PKI (Public Key Infrastructure)*.

Trojan

Malware that is disguised as another program to trick the user into installing it.

TSIG (Transaction Signature)

Allows a client providing an update to a dynamic DNS server to be authenticated by a password (MD5 HMAC).

Twisted Pair Cable

See: *UTP / STP*.

UAT (User Acceptance Testing)

Usually one of the last stages in software development before release (beta testing), UAT proves that a program is usable and fit-for-purpose in real-world conditions.

Updates

Updates are made freely available by the software manufacturer to fix problems in a particular software version, including any security vulnerabilities. Updates can be classified as hotfixes (available only to selected customers and for a limited problem), patches (generally available), and service packs (installable collections of patches and software improvements).

UPS (Uninterruptible Power Supply)

Uninterruptible Power Supplies (UPS) provide an alternative AC power supply from a bank of DC batteries in the event of power failure and are able to eliminate the effects of power surges and spikes.

USB Devices

The ease of connection and relative difficulty of controlling USB devices makes them a useful tool for stealing data or running unauthorized software or services (a computer can be configured to boot from a USB device).

Use of Proven Technologies

It is very difficult for end-users to determine the actual protection afforded by a particular encryption product. Consequently, use of particular algorithms tends to follow either government standards (such as FIPS and Suite B) or market adoption.

User Access and Rights Review

Part of privilege management is auditing the use users make of privileges that they have been allocated. This may reveal whether privileges are insufficient or too generous. One common problem is "rights creep", where a user acquires more-and-more privileges over time. Another problem is that of disabling expired or unused accounts.

User Awareness

Security systems can be improved cost-effectively by improving user awareness at all levels of the organization. This can be achieved through education and online resources and training.

User Management

In order to control access to resources and perform proper auditing, every user of a computer system must be uniquely identified and allocated appropriate privileges. Different access control models (discretionary, role-based, or mandatory) can be adopted to suit different networks. Many networks use groups or roles to simplify privilege management. Instead of allocating privileges directly to user accounts, they are allocated to group accounts or roles and then users placed in the appropriate security groups.

Username/Password

Widely-used type of authentication based on the idea of a secret (password) known only to one user.

Utilities

Businesses depend on utility suppliers and infrastructure (power, heating, water, telecommunications, and transportation). These can be affected by choice of site or by severe disasters. Larger organizations may have the resources to be self-sufficient (emergency generators, satellite communications links, and so on). Less well-resourced businesses should try to formulate contingency plans and workarounds to cope as well as possible.

UTM (Unified Threat Management)

Security appliances and software that provide a wide range of security controls, including malware scanning, firewall, IPS, NAC, DLP, content filtering, VPN, and load balancing.

UTP / STP

Twisted-pair cable is widely used for LANs. Cabling is rated for different Ethernet products, with Cat5e or Cat6 current. Most installations use unshielded cabling, which does not provide much protection against eavesdropping and is more susceptible to interference. Shielded (or more commonly screened) cable provides better protection but costs more.

Vampire Tap

A connector used on old Ethernet networks for joining a host to a thicknet cable via a drop cable.

Video Surveillance

Surveillance is an important element of physical security and an effective psychological deterrent. CCTV cameras come in various types designed to monitor different locations and require appropriate lighting and positioning (monitoring a doorway and monitoring an open space require different camera types for instance).

Virtualization Technology

Software allowing a single computer (the host) to run multiple "guest" operating systems (or Virtual Machines [VM]). The VMs are configured via a hypervisor or VM Monitor (VMM). VMs can be connected using virtual networks (vSwitch) or leverage the host's network interface(s). It is also possible for the VMs to share data with the host (via shared folders or the clipboard for instance). VT is now used as major infrastructure in data centers as well as for testing and training.

Virus

Code designed to infect computer files (or disks) when it is activated. A virus may also be programmed to carry out other malicious actions, such as deleting files or changing system settings.

VLAN (Virtual LAN)

A virtual LAN is a separate network, created using switching technology. Even though hosts on two VLANs may be physically connected to the same cabling, traffic is restricted to each VLAN. This provides traffic management and protection against packet sniffing.

VoIP

See: *Telephony*.

VPN (Virtual Private Network)

A secure tunnel created between two endpoints connected via an insecure network (typically the internet). VPNs are typically created using PPTP, L2TP, or IPsec.

VPN Concentrator

Appliance-based solution to supporting from 10s to 1000s of VPN connections.

Vulnerability Assessment

Scanning a network and analyzing its configuration, user behavior, policies, and documentation to identify any weaknesses and/or poor practice.

Vulnerability Scanner

Software configured with a list of known exploits and can scan for their presence in a host OS or particular application.

WAP (Wireless Application Protocol)

The Wireless Application Protocol (WAP) suite defines standards for mobile access based on adaptations of HTTP and TLS. Wireless Markup Language (WML) is a variant of HTML that can be used to write handheld-friendly sites; there is also a scripting language (WMLScript). There are two versions of WAP. WAP2 uses more regular versions of web protocols.

War Driving

Using a laptop with suitable software to detect unsecured or poorly secured Wireless LANs (WLAN).

Weak Encryption

If a cryptographic function (or its implementation in a particular product) has faults, such as known weak keys or insufficient bit strength), an attack can be formulated to exploit this (for example, to decrypt a document, fake a digital signature, or intercept wireless communications).

Weak Passwords

Weak passwords are a fruitful exploit for attackers, whether used to access web services, networks, or the administration interface of network devices such as switches and access points. A strong password does not use dictionary words or part of the username, is complex (combines upper and lower case and alphanumeric and non-alphanumeric characters), and is sufficiently long (8 characters or more).

Web Application Firewall

Specialized host firewall designed to prevent attacks against web applications, such as SQL injection or XSS.

Web Security Gateway

An appliance or proxy server that mediates client connections with the internet by filtering spam and malware and enforcing access restrictions on types of sites visited, time spent, and bandwidth consumed.

Web Servers

HTTP servers host websites. A basic website consists of static HTML pages but many sites are developed as front-end applications for databases. Web servers are popular targets for attack, particularly DoS, spoofing, and software exploits. Many companies use hosted web servers but if not, the server should be located in a DMZ. Web servers are also commonly used for intranet services, especially on Microsoft networks.

WEP (Wired Equivalent Privacy)

WEP is the original security mechanism for Wi-Fi. It uses a much criticized encryption technology and only supports pre-shared keys for authentication. WEP has now mostly been replaced by WPA.

Whole Disk Encryption

Encryption of all data on a disk (including system files, temporary files, and the pagefile) can be accomplished via a supported OS, third-party software, or at the controller level by the disk device itself. Used with a strong authentication method, this mitigates against data theft in the event that the device is lost or stolen. The key used to encrypt the disk can either be stored on a USB stick or smart card or in a Trusted Platform Module.

Wireless Cells

Cell phone coverage is achieved through a network of transmitters (or base stations) arranged in a cell-like structure. Mobile devices are a security risk as they can be used to transfer data and (potentially) to spread malware. This risk will only grow as data rates for mobiles increase (3G). Signals can be blocked by metal shielding, but this is rarely practical.

Wireless Devices

Wireless communications are used to support both Personal Area Network and Local Area Network products. PANs are created by IrDA (infrared) and Bluetooth (radio) devices. LANs are created by Wi-Fi (radio) adapters and access points. Wireless communications are easy to intercept and so require the use of encryption for confidentiality.

Workstations

Client devices connecting to the network represent one of the most vulnerable points as they are usually harder to monitor than centrally located equipment, such as servers and switches. As well as secure configuration of the OS and applications, workstations should be protected with anti-malware software. Users should be trained in security best practices and educated about common threats.

Worm

A type of malware that spreads through memory and network connections rather than infecting files.

WPA (Wi-Fi Protected Access)

Improved security mechanism for Wi-Fi. The original version was a patched version of WEP (using the Temporal Key Integrity Protocol [TKIP] to mitigate known attacks) with added support for Extensible Authentication Protocol, allowing better integration with wired authentication on enterprise networks. Version 2 was released as the 802.11i standard and adds support for AES encryption (within the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol [CCMP]).

WTLS (Wireless Transport Layer Security)

A version of SSL developed for portable devices such as smartphones and cell phones. WTLS is part of the original version of the Wireless Application Protocol (WAP). The latest version uses a modified version of TLS.

Xmas Attack

A type of fingerprinting where the scanner probes a server or router with packets that have unusual flags set in the header (FIN, PUSH, and URG) for instance. The way a server responds to such packets can reveal information about it (OS type and version for instance).

XSRF (Cross-site Request Forgery)

A malicious script hosted on the attacker's site that can exploit a session started on another site in the same browser.

XSS (Cross-site Scripting)

A malicious script hosted on the attacker's site or coded in a link injected onto a trusted site designed to compromise clients browsing the trusted site, circumventing the browser's security model of trusted zones.

Zero Day Exploit

An attack that exploits a vulnerability in software that is unknown to the software vendor and users. Most vulnerabilities are discovered by security researchers and the vendor will have time to create a patch and distribute it to users before exploits can be developed so zero day exploits have the potential to be very destructive.

Zombie

See: Botnet.

Index

Where a term or phrase is abbreviated, the acronym is the form listed in the index. Note that index references are made to the nearest main heading for the topic in which the term appears.

3

3DES..... 82

8

802.11i 214
802.1X..... 215, 281

A

AAA..... 9
AAA Server 137
Acceptable Use Policy 400, 451
Acceptance 413
Access Control . 9, 74, 143
Access Lists 365, 372
Access Log 207
Access Point 211
Account Expiration 161
Account Policy Enforcement..... 158
Accounting 18, 206
ACL... 9, 14, 15, 145, 189, 316
Active Directory 149
ActiveX..... 338
Add-ons..... 338
Adherence to Corporate Policies..... 398
Administrative Control 8
Administrator..... 153
Adware..... 33
AES..... 82
AGDLP 156
Agents..... 249
Air Conditioning..... 377
Air Gap..... 180
Alarms..... 209, 369, 380
ALE 410
Alert..... 209
Algorithm..... See Cipher
Alternate Sites..... 431
Amplification Attack..... 58
Analysis Engine..... 204
Android..... 388

Anomaly-based Detection	207
..... 205	
Antenna Placement	219
Antenna Types	219
Anti-Malware Software .	36
Antiquated Protocols ..	328
Anti-spam Software	38
Anti-spyware Software..	37
Anti-Virus Software.....	35,
399	
Apache	315
Applets	338
Application Aware Devices	192, 203
Application Control	398
Application Firewalls....	392
Application Hardening	243,
270, 275, 315, 328	
Application Layer	44
Application Patch	
Management	280
Application Service Ports	
..... 268	
Application Virtualization	
..... 348	
Application Whitelisting	
..... 398	
Arbitrary Code Execution	
..... 330	
Architecture / Infrastructure	
Considerations	398
Archive Attribute	297
Archiving.....	296
Armored Virus	37
ARO.....	410
ARP Poisoning	48
ASP	325
Assessment Technique	
..... 335	
Assessment Types (Risk, Threat, Vulnerability) ..	407
Asset Tracking.....	397
Assets.....	4, 407
Asymmetric Encryption.	83
Attachments	337
Attack Surface	335
Attacks.....	22
Audit Log.....	207
Auditing.....	18, 162, 206
Authentication ..	12, 14, 74,
128, 402	
Authority.....	26
Authorization.....	14
AutoComplete	341
Availability.....	419
Avoidance	413
B	
Backdoors.....	32
Backout Contingency Plan	
..... 301	
Backup.....	296, 297, 304
Backup Generator.....	427
Backup Security	303
Banner Grabbing	56
Bare Metal Backup	300
Bare Metal Hypervisor	346
Barricades.....	366
Baseline	207, 268, 420
Baseline Reporting	274
Bastion Hosts.....	171
bcrypt	126
Behavioral Technologies	
..... 134	
Behavior-based Detection	
..... 205	
Best Practice.....	453
BGP	182
BIA	406, 409
Big Data	295
Big Data Analysis.....	444
BIND	246
Biometrics	14, 131, 367
Birthday Attack.....	125
Black Box.....	62
Block Cipher	81
Blowfish	83
Bluetooth.....	403
Botnets.....	32, 57
BPA.....	415
Browser.....	336
Brute Force Attack	124
BTU.....	377

- Buffer Overflows .329, 334
 Business Continuity406
 BYOD Concerns398
-
- C**
- CA.....93, 97, 100
 Cable Lock.....373
 Cabling378
 Cache Pollution...245, 247
 Caching Engine193
 Callback.....234
 Camera vs.Guard371
 CAPTCHA11
 Captive Portals216
 Capture System Image442
 Capture Video.....441
 CCMP214
 CCTV370, 371
 Centralized Privilege Management.....143
 CERT22
 Certificate Authorities....97
 Certificate Policies98
 Certificates.....85, 93
 Certification Path107
 CGI324
 Chain of Custody443
 Change Management .421
 CHAP121
 CIA Triad5
 CIO / CISO / CTO6
 Cipher75
 Circuit-Level Firewall ..191
 Clean Desk Policy.....451
 Client-side Attacks331, 338
 Cloud Computing355
 Cloud Storage.....358
 Clusters428
 CMP111
 CMS.....327
 Code Review335
 Code Signing338
 Cold Site431
 Collection of Evidence 440
 Collision.....79, 125
 Command Injection....330
 Common Access Card 134
 Common Criteria.....266
 Communication.....455
 Community Cloud355
- Comparative Strength of Algorithms78
 Compensating Control ... 8
 Compliance24, 454
 Confidentiality74
 Configuration Baseline273
 Configuration Management420
 Conflict of Interest449
 Consensus / Social Proof25
 Content Inspection 197
 Continuity of Operations406
 Continuous Security Monitoring163, 414
 Control Redundancy and Diversity391
 Control Types.....7
 Convergence.....259
 Cookies340
 Cookies332
 Counterfeit Deterrence. 91
 Countermeasure7
 Covert Channel32
 CP425
 Cracker3
 Credential Management159, 402
 Credentialed versus Non-credentialed66
 CRL105
 CRLF Injection333
 Crossover Error Rate . 132
 Cross-Site Scripting ... 331
 Cryptographic Standards111
 Cryptography74
 CSIRT434
 CSR98
 CVE.....67
-
- D**
- DAC15, 143
 Damage Control. 436, 438
 Data Backups (Integrating Systems)414
 Data Breach.....437
 Data De-duplication ... 349
 Data Disposal.....306
 Data Emanation212
 Data Encryption290
 Data In-transit / At-rest / In-use289
 Data Labeling287
 Data Ownership.. 399, 416
 Data Policies287
 Database326
 Database Encryption ..293
 DDoS57
 Decentralized Privilege Management143
 Defense in Depth.....174
 Delta CRL.....105
 DES82
 Destruction107
 Detection Controls vs. Prevention Controls....201
 Detective Control.....8
 Deterrence.....413
 Deterrent Control.....8
 Device Access Control393
 Device Removal . 436, 437
 DHCP218, 243
 DHE86
 Dictionary Attack125
 Differential Backup297
 Diffie-Hellman86
 Digital Certificates .13, 93, 94, 111, 128, 342
 Digital Envelopes.....85
 Digital Signatures84
 Directory Information Tree147
 Directory Services145, 149
 Directory Traversal330
 Disable SSID Broadcast217
 Disable Unnecessary Accounts.....163
 Disablement161
 Disabling Unnecessary Services.....268
 Disabling Unused Features398
 Disabling Unused Interfaces / Service Ports268, 281
 Disaster Recovery423
 Disclosure.....439
 Disposal (Data Policies)289, 306
 Distance Requirements431
 DLP293
 DMZ.....171, 316
 DNAT.....187
 DNS.....245

DNS Poisoning..... 247
 DNS Spoofing 245
 Document Management 287
 Domain Controller 149
 Door Access System.. 367
 DoS 57, 351
 DRDoS..... 58
 Drills 381
 DSA..... 84
 Due Process..... 439
 Dumpster Diving... 26, 305
 Dust..... 375

E

EAL 266
 EAP 135, 215
 EAPoL..... 281
 ECC 87
 ECDHE 87
 Education 455
 ElGamal 84
 Elliptic Curve 87
 EMI Shielding..... 379
 Encryption 74
 Encryption (Mobile Apps) 401
 Endpoint Security..... 281
 Environmental Controls 375
 Environmental Monitoring 376
 Ephemeral Key..... 89
 Error / Exception Handling 335
 Escalation 162, 437
 Escape Plans 381
 Escape Routes..... 381
 Escrow 104
 Ethical Hacker..... 61
 Event Log 207
 Everyone Group..... 157
 Evil Twin..... 221
 Execution Control..... 270
 Expiration 107, 159
 Exploit 61, 175, 328
 Extensions 96
 Extranet..... 170

F

Facial Recognition..... 133
 Fail-safe 368
 Fair Use Policy 451

Fake A-V 32
 False Negative 206
 False Positive65, 132, 206
 Familiarity / Liking..... 25
 Fault Tolerance 425
 FCIP 254
 FCoE 254
 Federation 139
 Fencing..... 366
 Fibre Channel..... 253
 File Download..... 337
 File Sharing 322
 File Transfer 320
 Fingerprint Recognition 133
 Fingerprinting 53
 FIPS 112
 Fire 380, 381
 Firewall171, 189, 191, 194
 Firewall Rules.... 189, 195
 Firmware 280
 Firmware Version Control 392
 First Responder..... 436
 Flash Cookies..... 341
 Flood Guard 191
 Follow Up and Gather
 Training Metrics..... 457
 Footprinting 53, 246
 Forensic Procedures .400,
 439, 440
 Forest 149
 Fragle Attack 58
 FTP..... 320
 FTPS 322
 Full Backup..... 297
 Full Device Encryption 395
 Full Disk Encryption.... 291
 Fuzzing..... 334

G

Gain..... 219
 Game Consoles..... 391
 Generic Account
 Prohibition 153
 GLBA..... 454
 GPG 113
 GPO 158, 273
 GPS Tracking 396
 Grandfather, Father, Son
 302
 Gray Box 62
 GRE..... 229
 Group Account 144

Group Authentication ..215
 Group Policies158, 273
 Group-based Privileges
144
 Guards..... 370
 Guest Account153, 157
 Guidelines..... 453

H

Hacker 3
 Handling Big Data295
 Hard Drive Sanitation..306
 Hardening ..238, 266, 272,
 274
 Hardware (Spares)427
 Hardware Security373
 Hardware Utilization....348
 Hardware-based
 Encryption Devices291
 Hardware-based Key
 Storage 101
 Hashing..... 79
 Header Manipulation...333
 Heuristics 205
 High Assurance SSL...314
 High Availability ..419, 425
 Hijacking 245
 HIPAA 454
 HMAC 80
 Hoaxes..... 31
 Honeypot 68
 Host Availability / Elasticity351
 Host Software Baselingin
 269
 Host-based Firewall196
 Host-based Intrusion
 Detection..... 203
 HOSTS 245
 Hot and Cold Aisles378
 Hot Site 431
 Hotfix..... 276
 HOTP 130
 HR Policy 448
 HSM 101
 HTML 309
 HTTP 309
 HTTP Response Splitting
 333
 HTTPS 310
 Humidity..... 376
 HVAC 377
 HVAC..... 386
 Hybrid Attack125
 Hybrid Cloud355

Hypervisor	346
I	
ICMP-based Attacks	52, 58
ID Badges	365
Identification	10
Identification of Critical Systems.....	407
Identification vs Authentication vs Authorization.....	9
Identify Proofing.....	10
Identifying Common Misconfigurations.....	66
Identifying Lack of Controls	66
Identifying Vulnerabilities	64
Identity Theft	12
IDS vs. IPS	201
iFrame	331
IIS	315
IKE	232
IMAP4.....	199
Impact.....	409, 411
Impersonation	24
Implicit Deny	17, 195
In-band Management..	271
In-band vs. Out-of-Band Key Exchange	88
Incident Identification ..	436
Incident Isolation.....	436
Incident Reporting.....	19
Incident Response	433
Incremental Backup....	297
Individual File Encryption	290
Information Classification	287
Infrastructure as a Service	356
Initialization Vectors.....	77
Input Validation ...	328, 334
Integer Overflow	329
Integrity.....	75
Interference	222
Internet	170
Internet Use	451
Interoperability Agreements	415
Interpret Results of Security Assessment Tools.....	67
Intimidation	26
Intranet.....	170
Intrusion Detection Systems	201
Intrusive versus Non-intrusive.....	65
In-vehicle Computing Systems	386
Inventory Control	397, 407
iOS	387
IP Spoofing	50
IPS	203
IPsec.....	231
IPv4 vs. IPv6	256
Iris Scan	133
ISA	415
ISAKMP	232
iSCSI.....	254
ISO.....	41
ISSO	6
IT Contingency Planning	425
IV Attack.....	213
J	
Jamming	222
Java	325, 338
JavaScript	338
Job Log	421
Job Rotation.....	449
JSON	326
K	
Kerberos	118
Key Escrow	104
Key Exchange.....	88
Key Management	100, 104
Key Management (Mobile Apps).....	401
Key Pairs.....	101
Key Recovery Agent ..	103
Key Storage	101
Key Stretching.....	126
Key Usage	96, 101
Keys	77
KPI	419
L	
L2TP	230
land.c	58
Laws.....	454
Layered Security	174
LDAP.....	146
LDAP Injection	148
LEAP	136
Least Privilege.....	17
Legal Concerns	400
Legislation	440
Lessons Learned.....	439
Lighting.....	370, 372
Likelihood	409
Link Layer.....	43
Linux.....	274
LM Authentication.....	116
Load Balancer	319, 426
Local Security Policy ..	158
Location.....	375
Locking Cabinets.....	373
Lockout.....	161, 394
Locks	367
Log Analysis	209
Logic Bomb	30
Logical Access Token	118
Logs	18, 206, 317
Loki.....	32
Loop Protection ..	178, 183
Loss Control	436, 438
LSO	341
LUN	253
Lunchtime Attack.....	27
M	
MAC	16, 143
MAC Filtering.....	218, 281
MAC Flooding.....	49
Mail Gateway.....	199
Mainframes.....	390
Malicious Add-ons	338
Malicious Insider Threats	22
Malware	29
Malware Inspection	197
Management	271
Management Control.....	7
Management Interfaces	272
Mandatory Vacations..	449
Man-in-the-Middle Attack	49, 90
Mantraps	368
Manual Bypass	368
Manual Updates	392
Mathematical Attacks ...	89
MD5.....	80
MDM.....	397
Media Types	301
Message Digest.....	79

MIB.....	248	OCSP	105	PCI DSS	454
Mitigation.....	413	Off-site Storage	303	PEAP	136
Mitigation Steps.....	438	Omnidirectional Antenna	219	Penetration Testing.....	61
Mobile Application Security	401	On-board Camera / Video	400	Perfect Forward Secrecy	89, 312
Mobile Device Encryption	395	On-boarding / Off-boarding	399	Perform Routine Audits	414
Mobile Device Security	393	On-boarding and Off-boarding Business	399	Perimeters	364
Modems	225	Partners.....	416	Permissions / ACL	155, 289, 290
M-of-N Control....	102, 449	On-demand Application	355	Personal Firewall	196
Monitoring System Logs	206	One-Time Pad	78	Personal Identification Verification Card	134
Motion Detection	369	Online Resources	455	Personally Identifiable Information.....	See PII
MOU.....	415	Onsite versus Offsite	355	Personally Owned Devices	452
MTBF / MTTF.....	351, 419	Open File.....	299	PGP	113
MTTR	420	OpenID	141	Pharming	28, 245
Multifactor Authentication	14, 128	Operating System Security and Settings..	268	Phishing	27
Multiple Key Pairs	101	Operational Control	7	PHP	325
Mutual Authentication	110,	Operational Security	6, 446	Physical Access Log...	372
118		Order of Volatility	440	Physical Barriers	.364, 366
N		OS Hardening.....	268	Physical Port Security	.281
NAC	283	OS Restore.....	300	Physical Security	364
Name Resolution.....	245	OSI Model	41	Physical Tokens.....	367
NAPT	186	OSPF.....	182	PII	12, 290
NAS.....	252	OTP	13, 129	PIN	12
NAT.....	184	Out-of-band Management	271	Ping of Death	58
Near Field Communications (NFC)	404	OVAL.....	67	PKCS	94, 111
Need To Know Policy... <td>16</td> <td>P</td> <td></td> <td>PKI</td> <td>93, 100</td>	16	P		PKI	93, 100
NetBIOS.....	242	P2P File Sharing	322	PKIX.....	94, 111
Network Firewall.....	189	Packet Filtering.....	189	Plaintext	75
Network Layer.....	43	Packet Sniffing	212	Platform as a Service..	357
Network Mapper.....	53	PAP	121	Plug-ins.....	338
Network Segmentation	391	Passive vs. Active Tools	64	Policies to Prevent Data Loss	287
Network Separation....	180	Passively Testing Controls	64	Policy	421
Network Traffic and Logs	442	Password Complexity	122, 159	Polymorphic Malware....	37
New Threats and Security Alerts.....	455	Password Cracker	124	POP3	198
NIDS and NIPS ..	201, 203	Password History / Length / Reuse	159	Pop-up Blockers	38
NIST.....	4, 82, 112	Password Protection....	12, 159, 450	Port 110	198
Nmap	55	PAT	186	Port 139	243
Non-repudiation..	5, 10, 75	Patch Compatibility.....	354	Port 143	199
NoSQL	326	Patch Management ...	275, 399	Port 21	320
Notification .	288, 434, 437	PBKDF2	126	Port 22	236
NTLM	116	PBX	258, 259	Port 25	198
NTLMv2	117	PCAP	45	Port 3389	237
NTP	442			Port 443	310
O				Port 53	245
OAuth.....	141			Port 80	309

Portmapper	243	RDBMS	326	Rogue VM	354
Power Level Controls	223	RDP	237	Rogueware	32
PPP	226	Recovery	103	Role	144
PPTP	229	Recovery (Passwords)	161	Role-based Training	456
Preparation	434	Recovery Agent	103	Root CA	107
Preservation of Evidence	443	Recovery Procedures	438	Root User	153
Pre-shared Key	215	Recovery Window	298	Rootkits	34, 39
Prevent Tailgating	450	Redundancy	425	ROSI	412
Preventive Control	8	Redundant Servers	430	Rotation and Retention	302
Principles/Reasons for Effectiveness	24	Registration	98	Rounds	81
Printer	386	Remediation	413	Routers	180, 183
Privacy	340, 341	Remnant Removal	306	RPC	243
Privacy Considerations	416	Remote Access	225	RPO / RTO	412
Privacy Policy	452	Remote Access Technologies	234, 238	RSA Security	82, 83
Private Cloud	355	Remote Administration	237	Rule-based Access Control	16
Private Key	93	Remote Code Execution	330	Rule-based Management	189, 195
Private Key Protection	101	Remote Wiping	394		
Privilege Escalation	175, 329	Removable Media		S	
Privilege Policy	143, 162	Encryption	292	S/MIME	111
Probability	409	Removable Storage (Mobile Devices)	396	Safes	374
Procedures	421, 453	Renewal	106	Safety Controls	364
Proper Lighting	372	Replay Attack	49, 90, 213		
Protected Distribution	374	Replication	431		
Protecting Management Interfaces and Applications	271	Reporting	209, 439		
Protocol Analyzer	45	Repositories	101		
Proven Technologies	89	Resource Contention	351		
Proxies	171, 193	Restoring Data	304		
Proximity Reader	367	Retention (Data Policies)	289, 298		
PTZ	371	Retinal Scan	133		
Public Cloud	355	Reverse Proxy Servers	194		
Public Key	83, 93	Review Agreement Requirements	415		
		Review Architecture / Designs	335		
Q		Revocation	104		
Qualitative Risk Assessment	410	Revoking Privileges	163		
Quantitative Risk Assessment	410	RFI	379		
Quantum Cryptography	87	RIP	182		
Quarantine	436, 437	RIPEMD	80		
		Risk Assessment	406		
R		Risk Awareness (Integrating Systems)	414		
RADIUS	137	Risk Calculation	409		
RAID	428	Risks	21		
Rainbow Tables	125	Risks (Cloud Computing)	358		
Ransomware	34	Risks (Virtualization)	350		
RAS	234, 239	Rogue AP	221		
RBAC	15, 143	Rogue Machine Detection	282		
RC4	82				

Security Policy.....	446	Software-based Key	
Security Policy		Storage.....	101
(Integrating Systems)	. 414	Something You Are	132
Security Policy Training		Something You Do	134
.....	455	Something You Have..	128
Security Template	161,	Something You Know ..	115
273		Source Routing.....	183
Security Zone	170	SOX.....	454
Separation of Duties...	449	Spam	31
Server Consolidation..	348	Spam Filters	199
Servers.....	427, 430	Spare Parts	427, 430
Server-side versus Client-side Validation.....	334	Spear Phishing	27
Service Packs	276	Spim	31
Services	274	Spoofing	50
Session Hijacking.....	332	Spyware	33
Session Key	89	SQL	326
SFTP	236, 321	SQL Injection.....	330
SHA.....	79	SSH.....	236
Shadow Volumes	300	SSID	211, 217
Shared Accounts.....	145	SSL.....	310
Shared Hardware.....	351	SSL VPN	231
Shielding	219	Standards	453
Shoulder Surfing	26	Stateful Inspection	
Side Channel Attacks... 90		Firewall	191, 192
SIEM	209	Static Environments... 385,	
Signal Strength.....	219	391	
Signature Algorithm.....	95	Status Checking	105
Signature Matching	134	Steganography	91
Signature-based Detection	204	Storage (Data Policies)	
Signed Applet.....	338	289, 303
Signs	366	Storage (Keys)	101
Single Point of Failure	351,	Storage Segmentation	399
425		Storage Virtualization .	349
Single Sign-on	11, 17, 118	Stream Cipher	81
Site Security	364, 375	Strong Authentication ..	14,
Site Surveys.....	219	128	
SLA	415, 418	Strong vs. Weak Ciphers	
SLE	410	78
Smart Cards.....	13, 128	Subnetting	169
Smart TV.....	390	Succession Planning ..	424
SMTP	198	Suite B.....	112
Smurf Attack.....	58	Support Ownership....	399
Snapshots	300, 346	Surveillance.....	370, 452
Sniffer.....	45	Suspension.....	104
SNMP.....	248	Switches	175, 176
SOAP	327	Symmetric Encryption... 81	
Social Engineering	24, 370	Symmetric vs. Asymmetric	
Social Media Networks	417	83
Social Networking / P2P		SYN Flood	58
Use.....	451	Systems Architecture..	407
Socket	44		
Software as a Service	357	T	
Software Exploitation .	328	Tabletop Exercise.....	424
		TACACS+.....	138
		Tailgating	27, 450
		Take Hashes.....	442
		Target of Evaluation....	266
		TCP/IP	43
		TCP/IP Hijacking.....	50
		TCP-based Attacks.....	58
		Technical Control.....	7, 8
		Telephony	258
		Telnet.....	235
		Temperature	376
		Template.....	14, 132
		Temporary Internet Files	
		341
		Terminal Server	349
		Terminal Services	237
		Testing Controls.....	372
		TFTP	322
		Thin Client.....	348
		Threat Awareness.....	455
		Threat Vectors	21
		Threats.....	21, 408
		Threshold.....	208, 249
		Throttling.....	317
		Ticket	118
		Time of Day Restrictions	
		161
		Time Offset	442
		Timing / Interrupt Attack	
		352
		TKIP	214
		TLS	310
		Tokens	128, 129
		TOTP	130
		TPM	285, 291
		Track Man Hours and	
		Expense.....	444
		Training.....	455
		Transference.....	413
		Transitive Access.....	330
		Transitive Trust... 139, 402	
		Transmission Encryption	
		213
		Transport Encryption....	88
		Transport Layer	43
		Traps.....	249
		Trends.....	209
		Triangulation	396
		Trojans	32, 39
		Trunking.....	177
		Trust.....	26
		Trust Models	100
		Trusted OS	266
		Tunneling	174, 228
		Twofish	83

Typosquatting	246	Video Surveillance	371		
U					
UAC	153	Virtual Desktop	348		
UDP-based attacks.....	58	Virtual Networks.....	349		
Unauthorized Data Sharing	416	Virtual Switches	349		
UNIX	274	Virtualization	345		
Unsuccessful Backup .	304	Virus.....	29, 35, 39		
Update Server	277	Vishing	28		
Updates	276, 280	VLAN Management....	176		
UPS	427	VM Escaping.....	352		
Uptime	419	VoIP	259		
Urgency	26	VPN.....	228, 234		
URI	309	VPN Concentrator.....	235		
URL Filter	197	VPN over Open Wireless	216		
URL Hijacking	246	Vulnerabilities.....	21, 412		
USB Encryption ..	291, 292	Vulnerability Scanner ...	64		
Use of Proven Technologies	111	Vulnerability Scanning..	60		
User Acceptance	398	W			
User Access Review...	162	War Dialing	225		
User Account	144, 153	War Driving	212		
User Education	455	Warm Site	431		
User Habits	455	Watering Hole Attack ...	28		
User Rights and Permissions Review ...	162	WCMS.....	327		
User-assigned Privileges	144	Weak Encryption.....	213		
Username	115	Weak Key Attack.....	126		
Users with Multiple Accounts/Roles.....	144	Weak Password	175		
Utilities	408	Web Application Firewall	197		
UTM Security Appliances	194, 203	Web Browsers....	336, 340		
V					
VBScript.....	338	Web of Trust	110		
Ventilation.....	377	Web Security Gateway	193, 197		
Video Surveillance	371	Web Servers	315		
Virtual Desktop	348	WEP.....	213		
Virtual Networks.....	349	Whaling	27		
Virtual Switches	349	Whistleblower....	435, 450		
Virtualization	345	White Box.....	62		
Virus.....	29, 35, 39	X			
Vishing	28	X.500	146		
VLAN Management....	176	X.509	94, 111		
VM Escaping.....	352	Xmas Attack	55		
VoIP	259	XML	327		
VPN.....	228, 234	XML Injection.....	330		
VPN Concentrator.....	235	XSRF	332		
VPN over Open Wireless	216	XSS	331		
Vulnerabilities.....	21, 412	XSS / XSRF Prevention	335		
Vulnerability Scanner ...	64	XTACACS	138		
Vulnerability Scanning..	60	Y			
WWN.....	253	Yagi Antenna.....	219		
Z					
Zero-day Attack	328	Zombie	57		



**CompTIA Security+ Certification
Support Skills (Exam SY0-401)**

Labs

G634eng ver094

Acknowledgements

Course Developer.....gtslearning



EditorJames Pengelly

This courseware is owned, published, and distributed by **gtslearning**, the world's only specialist supplier of CompTIA learning solutions.

sales@gtslearning.com

+44 (0)20 7887 7999 +44 (0)20 7887 7988

Unit 127, Hill House, 210 Upper Richmond Road,
London SW15 6NP, UK

COPYRIGHT

This courseware is copyrighted © 2014 *gtslearning*. Product images are the copyright of the vendor or manufacturer named in the caption and used by permission. No part of this courseware or any training material supplied by the publisher to accompany the courseware may be copied, photocopied, reproduced, or re-used in any form or by any means without permission in writing from the publisher. Violation of these laws will lead to prosecution.

All trademarks, service marks, products, or services are trademarks or registered trademarks of their respective holders and are acknowledged by the publisher.

LIMITATION OF LIABILITY

Every effort has been made to ensure complete and accurate information concerning the material presented in this course. Neither the publisher nor its agents can be held legally responsible for any mistakes in printing or for faulty instructions contained within this course. The publisher appreciates receiving notice of any errors or misprints.

Information in this course is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted.

Where the course and all materials supplied for training are designed to familiarize the user with the operation of software programs and computer devices, the publisher urges the user to review the manuals provided by the product vendor regarding specific questions as to operation.

There are no warranties, expressed or implied, including warranties of merchantability or fitness for a particular purpose, made with respect to the materials or any information provided herein. Neither the author nor publisher shall be liable for any direct, indirect, special, incidental, or consequential damages arising out of the use or the inability to use the contents of this course.

Warning All gtslearning products are supplied on the basis of a single copy of a course per student. Additional resources that may be made available from gtslearning may only be used in conjunction with courses sold by gtslearning. No material changes to these resources are permitted without express written permission from gtslearning. These resources may not be used in conjunction with content from any other supplier.

If you suspect that this course has been copied or distributed illegally,
please telephone or email gtslearning.

Table of Contents

Introduction	1
Lab 1 / Using Hyper-V	2
Lab 2 / Trojans and Malware Protection	7
Lab 3 / Network Vulnerabilities	15
Lab 4 / Baseline Security Analyzer	23
Lab 5 / Steganography	25
Lab 6 / Configuring Certificate Services.....	29
Lab 7 / Password Sniffing.....	41
Lab 8 / Configuring a VPN	46
Lab 9 / Telnet and FTP	55
Lab 10 / Attacks Against DHCP and DNS.....	61
Lab 11 / Network Access Protection	65
Lab 12 / Data Leakage Prevention	74
Lab 13 / HTTP and HTTPS.....	77
Lab 14 / Web Application Vulnerabilities.....	81
Lab 15 / Computer Forensic Tools.....	86

This page left blank intentionally.



Introduction

The following conventions have been used in the course practical lab exercises.

- Bullet and number lists - steps for you to follow in the course of completing a task or hands-on exercise.
- File and command selection - files, applets, dialogs and other information that is displayed on the screen by the computer is shown in sans serif bold. For example: Click **OK**, Select **Control Panel**, and so on.
- Sequences of commands - a sequence of steps to follow to open a file or activate a command are shown in bold with arrows. For example, if you need to access the system properties in Windows, this would be shown in the text by: **Start > Control Panel > System**.
- Commands - commands or information that you must enter using the keyboard are shown in Courier New Bold. For example: Type **webadmin@somewhere.com**. Courier New Bold-Italic represents some sort of variable, such as your student number. For example, if your student number is "5", you would follow the instruction **ping 10.0.0.x** by entering **ping 10.0.0.5**.
- Using the mouse - when instructed to click, use the main mouse button; when instructed to alt-click, use the secondary button (that is, the button on the right-hand side of the mouse, assuming right-handed use). Sometimes you need to use both the keyboard and the mouse - for example, **Ctrl+click** means hold down the **Ctrl** key and click the main mouse button.

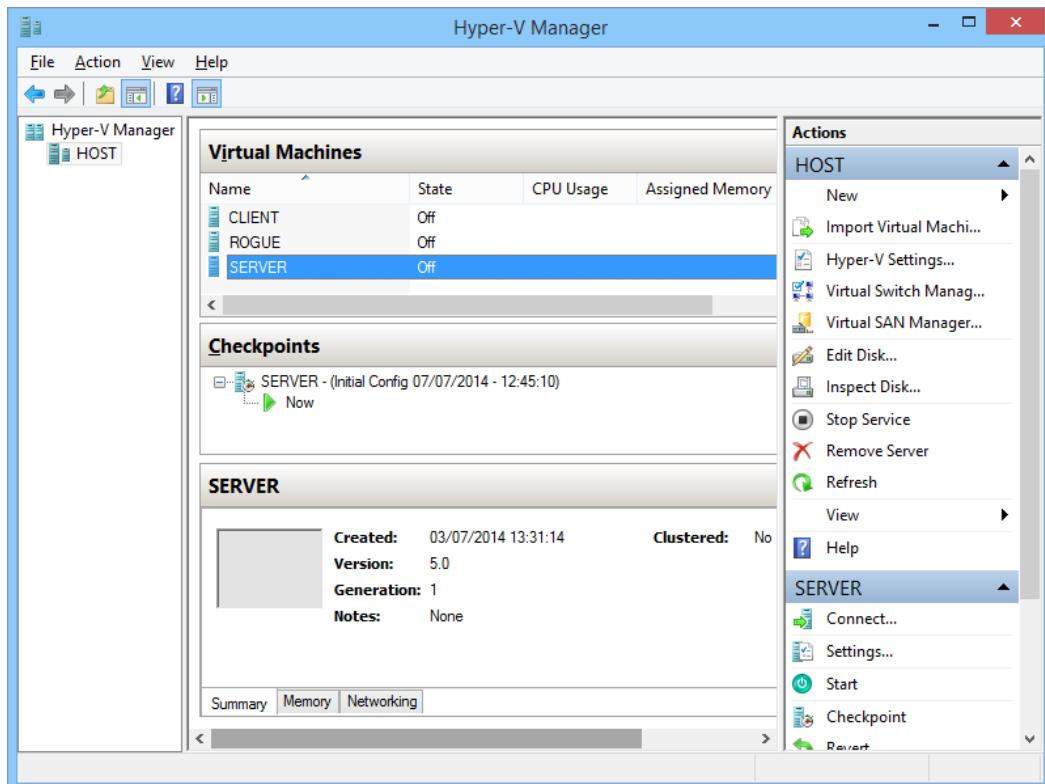


Lab 1 / Using Hyper-V

Many of the practical labs in this course use Microsoft's host virtualization product Hyper-V. In this lab, you will learn how to configure the Virtual Machines (VM) and about the VMs that you will use.

- 1) On the **HOST PC**, press **Start** then type **Hyper-V Manager** then press **Enter**.

The Hyper-V Manager console is loaded. This shows the VMs available to you. Selecting a VM displays more information about it.



Hyper-V console

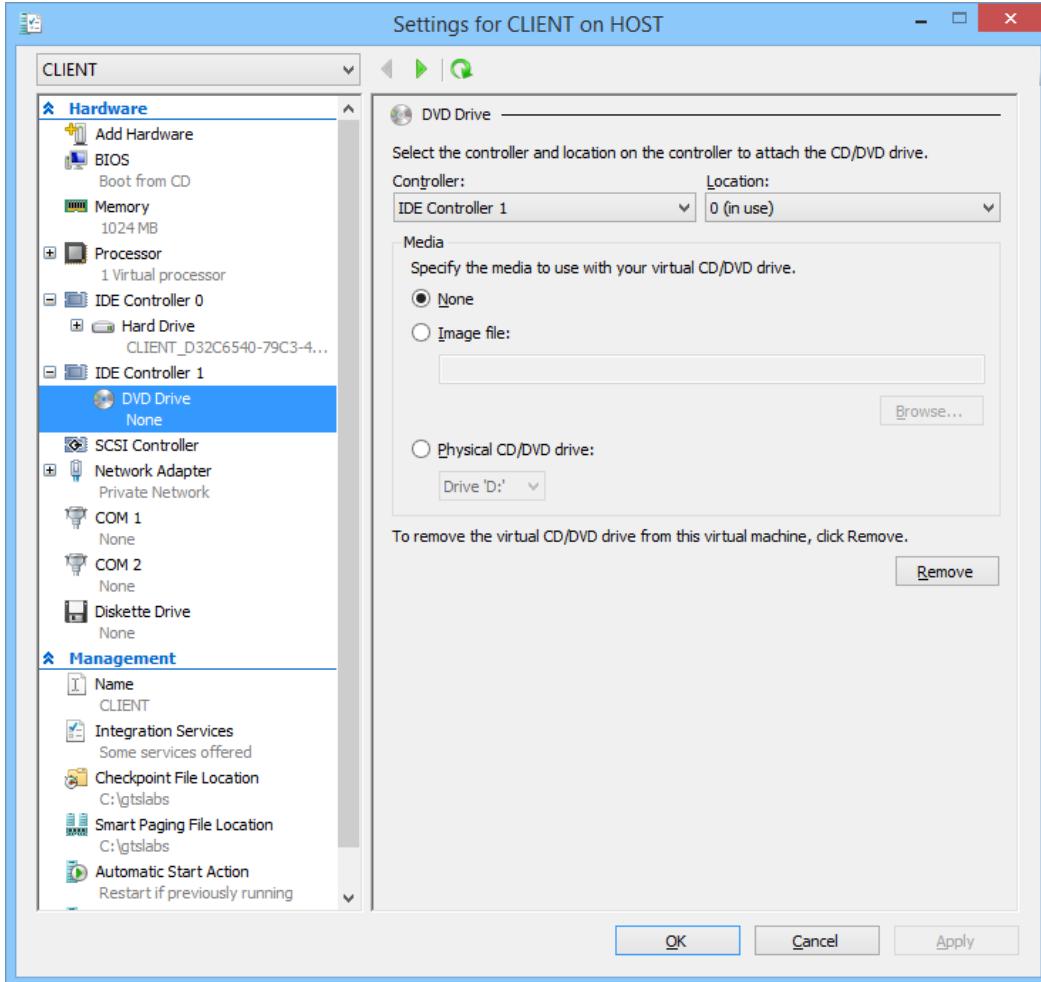
You have 3 VMs:

- SERVER is a Windows Server 2012 R2 Enterprise server configured as a domain controller.
- CLIENT is a Windows 8 Enterprise workstation, configured as a domain client.
- ROGUE is a malicious host running Windows 8 Enterprise workstation, which is outside the domain.

- 2) Alt-click the **CLIENT** VM then select **Settings**.

This dialog allows you to configure the VM's hardware. Some settings can only be changed when the VM is powered off; others you can change from the VM's window menu when it is running.

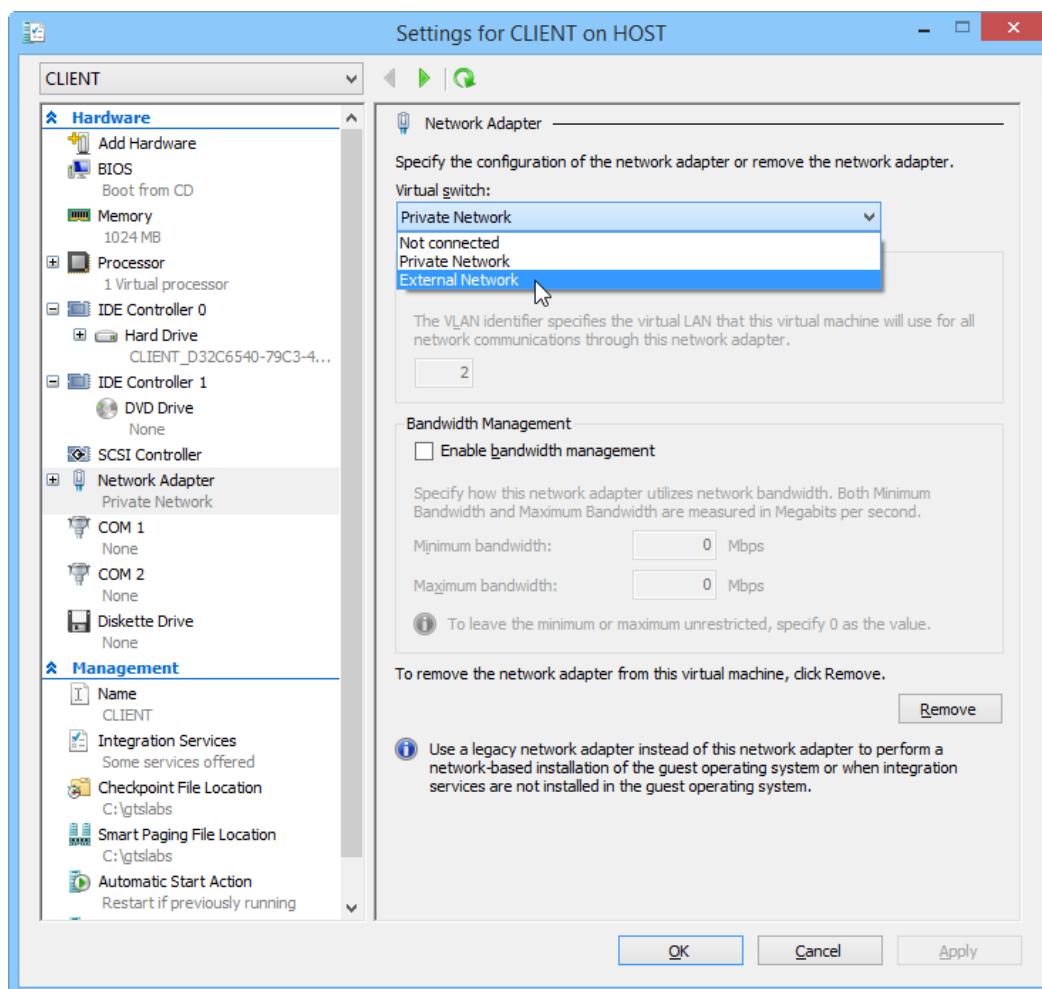
- 3) Observe the IDE and SCSI controller nodes.



Configuring VM storage options

These nodes allow you to add hard drives to the VM and to use disc images (ISOs) in the optical drive (or share the HOST's drive).

- 4) Click the **DVD Drive** node, then on the opposite pane select **Image file** and click **Browse**. Locate the Windows 8 ISO image in **c:\GTLABS** and click **Open**.
- 5) Click the **Network Adapter** node.



Configuring network options

This page allows you to choose which network switch the adapter is connected to. In these labs, the switches will be configured so that each VM can "see" only other VMs installed on the host but not the host itself or the physical network. The VMs can be put on separate internal networks by giving the networks names, much like a Virtual LAN (VLAN). The CLIENT VM is on a network named "Private Network".

You can also "install" additional adapters in a VM. This is an option we will use later in the labs.

- 6) Click **OK**.
- 7) With the **CLIENT** VM still selected, observe the **Checkpoints** pane.

A checkpoint is an image of the VM's disk at a particular point. You can use checkpoints to discard the changes in a particular lab or reset the lab if you need to attempt it again from the start.

These checkpoints can be used to revert any VM easily to its initial configuration if necessary.

- 8) Double-click the **CLIENT** VM to connect to it. A new window will open. Click the **Start** button  to boot the VM.

When the VM has booted, you may be asked to choose a desktop size. If so, choose a setting that is smaller than your host desktop resolution, so that the entire VM desktop will be easily visible.



*To change the console window size, when the VM is running, alt-click the icon in the Hyper-V management window and select **Edit Session Settings**.*

9) Click on **CLIENT\Admin** to log in.

10) Enter the password **Pa\$\$w0rd**.

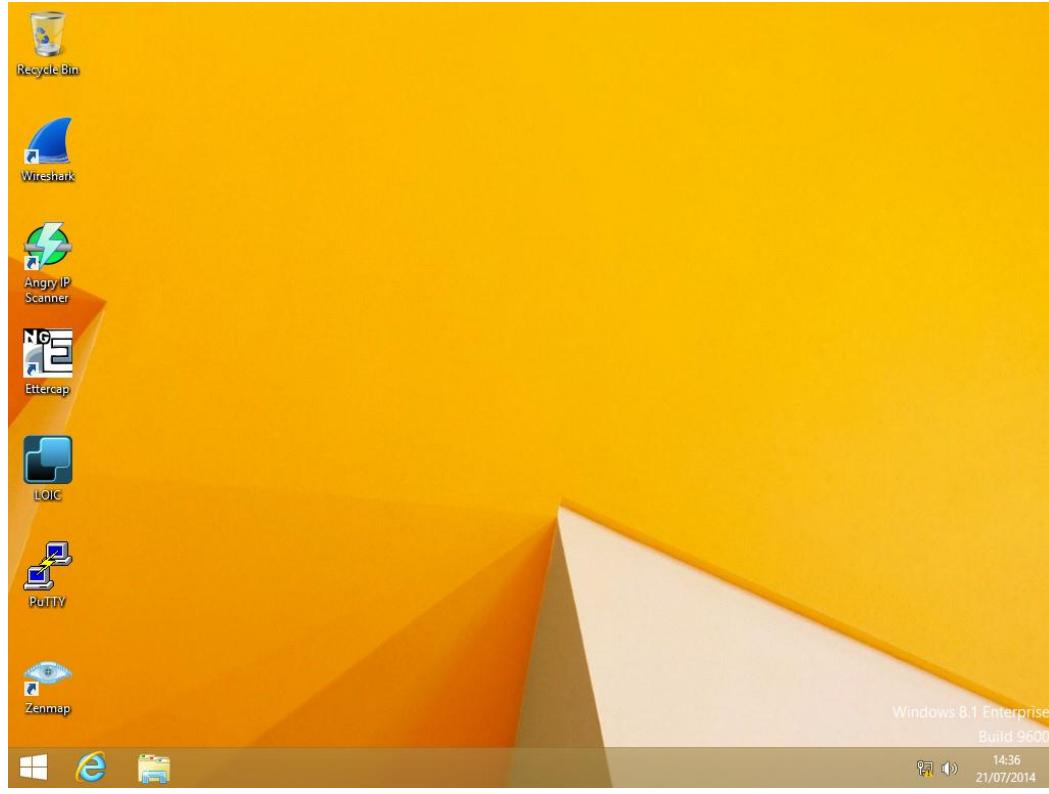


That's a zero between the "w" and the "r".

- 11) On the VM window, click the **File > Settings** menu. You can configure some settings here (though you cannot change the installed hardware without shutting down the VM).
- 12) On the VM window, click the **Media > DVD Drive** menu. You can select a different ISO or choose the host drive here (or just eject the current image).
- 13) In the CLIENT VM, alt-click the Start button and select **Shut down or sign out > Shut down**.

During the labs you will use another Windows 8 VM. The ROGUE VM contains a selection of tools that we will use in the labs to demonstrate various exploits.

- 14) Double-click the **ROGUE** VM to establish a connection in a new window.
Click the **Start** button  to boot the VM.
- 15) The user name Admin will already be selected. Log in with the password **Pa\$\$w0rd**.



The ROGUE desktop

16) Various tools are available on the VM's desktop. These tools will be used throughout the labs. Take a few minutes to familiarize yourself with the tools available:

- Ettercap is a tool used to enable man-in-the-middle (MitM) attacks.
- Angry IP Scanner is a ping sweeper and port scanner.
- LOIC (Low Orbit Ion Cannon) is a tool used in Distributed Denial of Service (DDoS) attacks.
- Zenmap is ping sweeper and port scanner, similar to Angry IP Scanner.
- PuTTY is a Telnet/SSH client, which can be used to for remote command execution.
- Wireshark is a packet capture and analysis utility.

17) When you have finished, alt-click the Start button and select **Shut down or sign out > Shut down**.



The tools and procedures demonstrated in these labs are for use in a learning context only. You MUST NOT replicate any of these exercises outside the training center without the express permission of the system owner. Attempting to run probes or exploits against systems you do not own is a criminal offence in many countries.



Lab 2 / Trojans and Malware Protection

In this lab, you will investigate some malware threats and the use of an enterprise malware protection suite.

Exercise 1: Activating a Trojan

In this exercise, you will run a setup program that has unintended consequences...

- 1) In the Hyper-V management console, alt-click the **SERVER** VM icon and select **Start**.



The VM will run even without an open console window.

- 2) Alt-click the **CLIENT** VM icon and select **Start**. Double-click the icon to open a console window for it.
- 3) At the login screen, click **Other user**.
- 4) Enter **CLASSROOM\Administrator**, in the "User name" box.
- 5) Enter **Pa\$\$w0rd** in the "Password" box and press **Enter**.



If there is an error, wait a little longer for the SERVER VM to complete booting before trying to log on.

- 6) At the Start Screen, type **file explorer** and press **Enter** to open a File Explorer window.
- 7) Browse to the **c:\GTSLABS** folder and run **setup**.

We will pretend that you are installing this program thinking it is a legitimate piece of software.

- 8) Complete the setup process, accepting the defaults.

The program runs at the end of setup. But what else might have changed on the computer?

- 9) Press **Ctrl+Shift+Esc** to open Task Manager and click **More details** to view the full interface. Inspect the list of processes. Can you spot anything unusual?

- 10) Press the **Start** key then type **event viewer** and open the **View event logs** link that appears.

- 11) In **Event Viewer**, expand **Windows Logs** and view the **Application** and **System** logs. Can you spot anything unusual?
-

- 12) Press the **Start** key then type **firewall** and open the **Windows Firewall** link that appears.
- 13) Click the **Advanced settings** link then view the **Inbound Rules** node. Can you spot anything unusual?
-

Exercise 2: Exploiting the Trojan

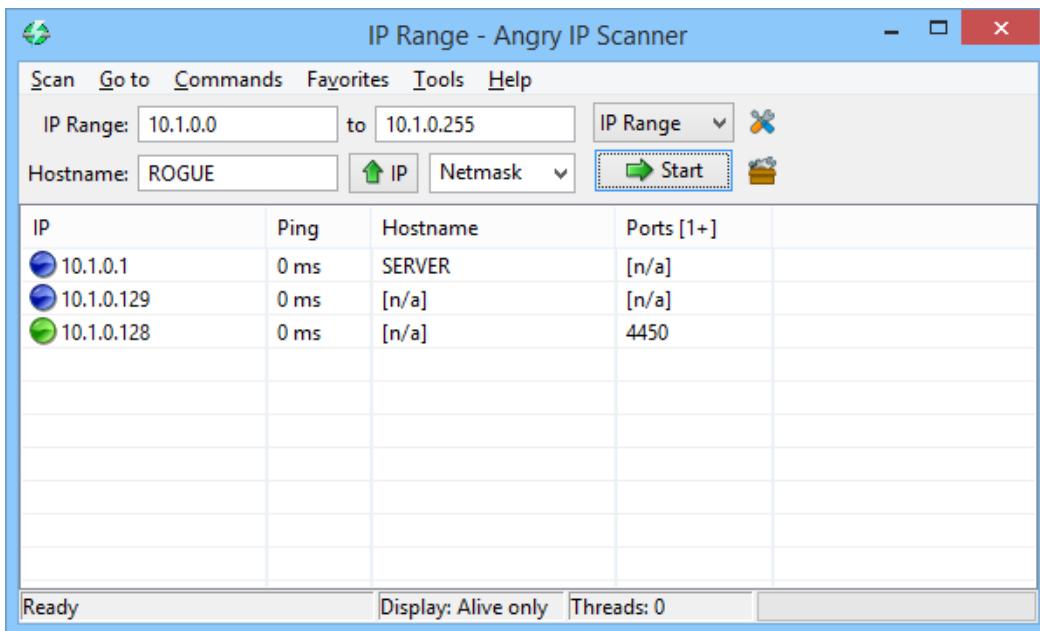
The "Odysseus" software has installed a backdoor application called Netcat on the computer. This runs with the privileges of the logged-on user (currently administrator) and allows a remote machine to access the command prompt on CLIENT. In this exercise, you will use the ROGUE VM to exploit the backdoor. This contains numerous penetration testing and forensic tools.

- 1) Start and connect to the **ROGUE** VM.
- 2) Log in as **Admin** with the password **Pa\$\$w0rd**.
- 3) Firstly, to discover the target host, you can use a network scanner called **Angry IP Scanner**. Double-click the **Angry IP Scanner** icon on the desktop to open the tool.
- 4) In the "Getting Started" dialog, optionally read the help information then click **Close** when you have finished.

We will scan the local subnet for hosts with port 4450 open, as the Trojan listens on this port. Note that the IP Range settings have automatically pre-configured to the local subnet addresses.

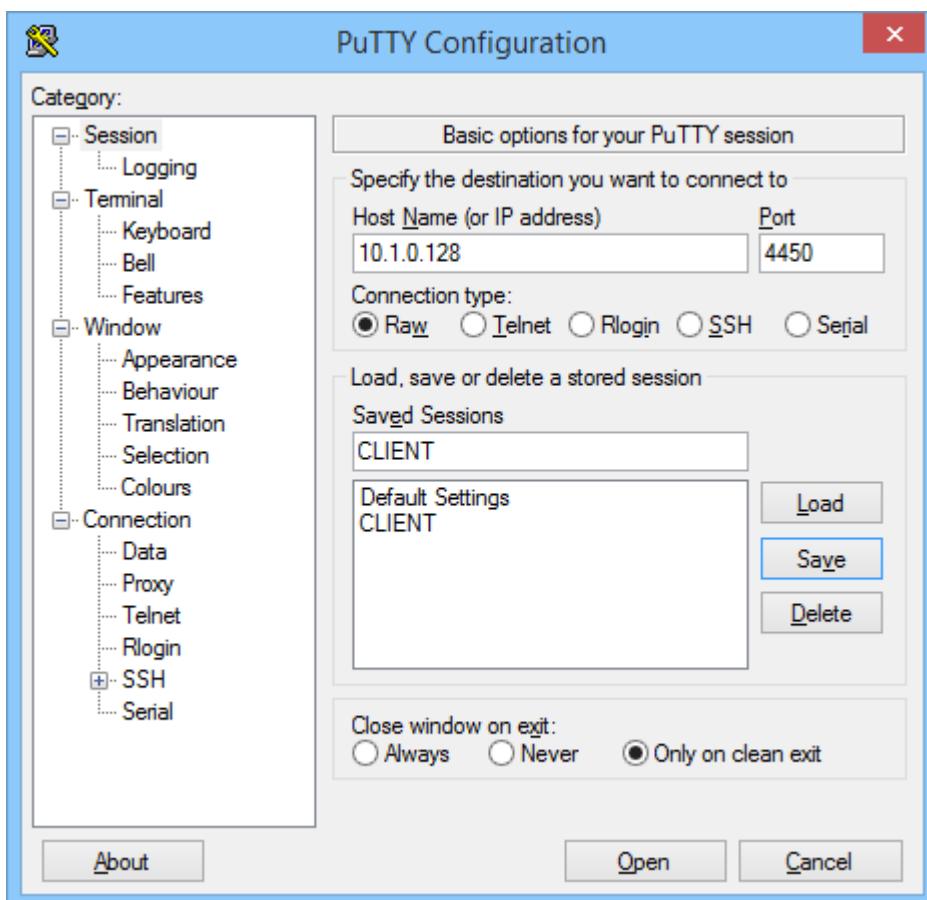
- 5) Click the **Preferences** icon  to open the **Preferences** dialog. Tick the **Scan dead hosts** check box.
- 6) Select the **Ports** tab and enter **4450** in the "Port selection" box.
- 7) Select the **Display** tab, and select **Alive hosts**. Click **OK**.
- 8) Click the **Start** button to perform the scan.
- 9) When the scan is complete, click **Close**.
- 10) The scan should find 3 hosts and 1 host where 4450 is open. This is the CLIENT VM. Make a note of the IP address (CLIENT has obtained this from a DHCP server running on SERVER):

-
- 11) Close the **Angry IP Scanner** window.



Angry IP Scanner

- 12) To connect to the backdoor on CLIENT, we will use a terminal emulation client called **PuTTY**. Double-click the **PuTTY** icon on the desktop.
- 13) In the "Host name (or IP address)" box, type the IP address of CLIENT, as noted above. In the "Port" box, enter **4450**. Set the "Connection type" to **Raw**.
- 14) In the "Saved Sessions" box, type **CLIENT** then click the **Save** button.
Click **Open**.



Connecting to port 4450 using PuTTY

- 15) After a few seconds, you will be connected to the command prompt on CLIENT. Enter the following series of commands to demonstrate that you can access CLIENT with administrator privileges:

```
cd \windows\system32
dir
copy c:\GTSLABS\eicar.com %homepath%\documents\diary.exe
shutdown /r
```

- 16) Note the effect this has on the CLIENT VM.
- 17) Click **OK** on the "Putty Fatal Error" message then close the PuTTY window.

Exercise 3: Blocking the Trojan

In this exercise, you will make further investigations about the changes that the Trojan has made and explore ways to remove it.

- 1) When the CLIENT VM has restarted but is still logged off, attempt to use PuTTY on the ROGUE VM to connect again (select the **CLIENT** saved session and click **Load** then **Open**).
- This backdoor only runs in "user" mode. More powerful Trojans would run at system or kernel level, making them available even when no user is logged in.
- 2) Switch to CLIENT and sign back in as **CLASSROOM\Administrator**. Press **Ctrl+Shift+Esc** to start Task Manager.
 - 3) Click the **Start-up** tab. Notice the entry "ini" has been added to the Registry by Odysseus. This entry executes a script at log on.
 - 4) Alt-click the "ini" entry and select **Open file location**. Open **ini.vbs** in Notepad (alt-click and select **Edit**). Note the actions that the script performs.
 - 5) Click **Start** and type **firewall** then click on the **Windows Firewall** icon. Click on the **Advanced settings** link.
 - 6) Select the **Inbound Rules** node, alt-click any "Service Firewall" rules, and select **Disable Rule**.
 - 7) Try connecting to CLIENT from ROGUE - it will not work.
 - 8) Shut down the CLIENT VM.

Exercise 4: Deploying Malware Protection

This "Trojan" is trivially easy to block and remove but most malware is far more sophisticated. Most networks use centrally managed security suites to ensure that servers and client desktops are protected more-or-less automatically. Windows 8.1 contains a full-featured anti-virus product called Windows Defender (known as Microsoft Security Essentials in previous versions).

In this exercise we will use Group Policy to ensure that Windows Defender is enabled on all computers in the domain.

- 1) Open a console windows for the **SERVER** VM then sign in as **CLASSROOM\Administrator** with the password **Pa\$\$w0rd**.
- 2) When **Server Manager** has loaded, select **Tools > Group Policy Management**.
- 3) In the navigation pane, browse to **Forest: classroom.local > Domains > classroom.local > classroom Domain Policy**. If you receive a message telling you that changes here may impact on other locations. Click **OK**.
- 4) Alt-click **classroom Domain Policy** and select **Edit**.
- 5) In the navigation pane of the Group Policy Management Editor window, expand **Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Defender**.
- 6) In the detail pane, double-click **Turn off Windows Defender**, read the help text in the "Turn off Windows Defender" window, then select **Disabled** and click **OK**.



Note that in Group Policy, we often have to use the logic of double negatives. Here, for example, we want to turn on Windows Defender, but there isn't a policy we can enable for that. So, instead of enabling the policy, we disable turning the Windows Defender off, which has the same overall effect.

- 7) Repeat this method to set **Turn off routine remediation** to **Disabled**.
- 8) Expand the **Real-time Protection** node within Windows Defender. Set **Turn off real-time protection** to **Disabled**.



Changes made in Group Policy Editor are saved immediately, so you don't need to save them manually. They can take up to 2 hours to roll out to all clients, but restarting the clients (sometimes twice in a row) is one simple way to force the issue.

- 9) Close all open windows and sign out.

Exercise 5: Using the Anti-Virus Software

In this exercise, you will use the anti-virus software to detect and neutralize malware threats.

- 1) Start the **CLIENT** VM and sign in as **CLASSROOM\Administrator**.
- 2) Open **File Explorer** and navigate to the **Documents** folder. Try to run the **diary** file.

Note that Defender automatically prevents the file from running and deletes it.
- 3) Click **OK**.
- 4) Click **Start** and type **Windows Defender**, then click the **Windows Defender** icon. When the Windows Defender window opens, it should have a green bar at the top with the message **PC status: Protected**.



*If the automatic deployment has failed (which can happen for a number of reasons), there should be a large red button on the Home tab saying **Start**. If so, click it to start Windows Defender manually.*

- 5) Select the **History** tab then click the **View Details** button. Read the information about the threat discovered in "diary.exe".

The detected item should be identified as containing a virus of type "DOS/Eicar_Test_File". EICAR isn't actually a virus. It's a test string that properly configured virus scanners should detect as a virus.

- 6) Click on the **Home** tab. Ensure that **Quick** is selected under "Scan options", and click **Scan now**.
- 7) Allow the scan to complete (about 1 minute). When the scan has completed, you may receive the message "This app detected a potential threat to your PC." Notice there is a large red "Clean PC" button that we can use to resolve the issue, but first we will check the details.



If the quick scan does not find anything, skip ahead to the full scan.

- 8) Click on the **Show details** link below the **Clean PC** button.

The file can't be disinfected so you will just have to delete it.
- 9) Ensure the recommended action for eicar is set to **Remove**, then click **Apply actions**. When the actions have been successfully applied, click **Close**.
- 10) Under "Scan options", select **Full**, then click the **Scan now** button.

This performs a more in-depth scan, which will take significantly longer.

- 11) While the scan is running, switch to ROGUE and attempt to use PuTTY to exploit the netcat backdoor again.

This should work. While Defender detected EICAR it has not marked Netcat as malicious or done anything to remove the startup script that re-enables the backdoor firewall exception. Security software cannot necessarily decide on its own whether a process is malicious or not. Careful configuration (such as execution control to enforce application white or blacklists) is required.

- 12) Close the PuTTY window, then switch back to CLIENT.

We will now use Windows Firewall to block access to the netcat backdoor more permanently.

- 13) Minimize the Windows Defender window, while leaving the scan running.

- 14) Click **Start**, then type **firewall** and click on the **Windows Firewall** icon. Click on the **Advanced settings** link.

- 15) Click on the **Inbound Rules** node, then on the **New Rule** link in the "Actions" pane. Complete the wizard by making the following choices:

- On the "Rule Type" page, ensure **Program** is selected, then click **Next**.
- On the "Program" page, ensure **This program path** is selected, then click the **Browse** button.
- Browse to **c:\windows\sysWOW64\nc.exe** then click **Open**.
- On the "Program" page, click **Next**.
- On the "Action" page, select **Block the connection** then click **Next**.
- On the "Profile" page, ensure all three profiles are ticked then click **Next**.
- On the "Name" page, enter **Block netcat** in the **Name** box then click **Finish**.

- 16) Close the **Windows Firewall with Advanced Security** window then close the **Windows Firewall** window.

- 17) Switch over to ROGUE and try to exploit the backdoor again. It should fail this time.

- 18) Back on CLIENT, check whether the full scan has completed. If you have time, explore the **Update** and **Settings** tabs to view options for updating malware definitions and configuring scanning exceptions.



Note that group policy prevents the user from disabling Windows Defender.

The scan should identify a number of the software tools in c:\GTLABS that we will be looking at later in the course as potentially malicious.

- 19) As we will be undoing all changes in this lab, feel free to experiment with the available options (Remove/Quarantine/Allow) for any items detected, then click **Apply actions**.

Exercise 6: Completing the Lab

You need to discard some of the changes you made during this lab to the VMs' disk images.

- 1) On each VM, from the console window toolbar, select **Action > Revert**.



Make sure you choose "Revert". Take care NOT to select "Reset".

- 2) Confirm by clicking the **Revert** button.



Lab 3 / Network Vulnerabilities

In this lab, you will practice attack strategies such as footprinting, spoofing, and Denial of Service.

Exercise 1: Network Footprinting

A network scan is usually the first step in an attempt to penetrate security (or indeed to establish what needs defending). Footprinting establishes the topology and protocols deployed on the network while fingerprinting determines the services and other configuration details of a particular host.

One of the most popular scanning tools is nmap. This is a command-line program operated using scripts. A GUI version (Zenmap) can perform several very useful pre-configured scans though.

- 1) Start the **SERVER** VM. When the VM has finished booting, boot the **CLIENT** and **ROGUE** VMs.
- 2) Switch to the ROGUE VM, and log in as **Admin** with the password **Pa\$\$w0rd**.
- 3) From the desktop, open the **Zenmap** shortcut icon.
- 4) Enter **10.1.0.0/24** into the "Target" box. Click **Scan**.

The screenshot shows the Zenmap application window. The 'Targets' section at the top has 'Target' set to '10.1.0.0/24' and 'Profile' set to 'Intense scan'. The 'Command' field contains 'nmap -T4 -A -v 10.1.0.0/24'. Below the targets, the 'Hosts' tab is selected, showing a list of hosts from 10.1.0.244 to 10.1.0.129. The main pane displays the Nmap output, which includes:

```
nmap -T4 -A -v 10.1.0.0/24
Nmap scan report for 10.1.0.244 [host down]
Nmap scan report for 10.1.0.245 [host down]
Nmap scan report for 10.1.0.246 [host down]
Nmap scan report for 10.1.0.247 [host down]
Nmap scan report for 10.1.0.248 [host down]
Nmap scan report for 10.1.0.249 [host down]
Nmap scan report for 10.1.0.250 [host down]
Nmap scan report for 10.1.0.251 [host down]
Nmap scan report for 10.1.0.252 [host down]
Nmap scan report for 10.1.0.253 [host down]
Nmap scan report for 10.1.0.254 [host down]
Nmap scan report for 10.1.0.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 12:17
Completed Parallel DNS resolution of 1 host. at 12:17, 11.77s elapsed
Initiating SYN Stealth Scan at 12:17
Scanning 2 hosts [1000 ports/host]
Discovered open port 445/tcp on 10.1.0.1
Discovered open port 53/tcp on 10.1.0.1
Discovered open port 80/tcp on 10.1.0.1
Discovered open port 135/tcp on 10.1.0.1
Discovered open port 135/tcp on 10.1.0.129
Discovered open port 139/tcp on 10.1.0.1
Discovered open port 49154/tcp on 10.1.0.1
Discovered open port 49167/tcp on 10.1.0.1
Discovered open port 3268/tcp on 10.1.0.1
Discovered open port 49158/tcp on 10.1.0.1
Discovered open port 593/tcp on 10.1.0.1
Discovered open port 389/tcp on 10.1.0.1
Discovered open port 49159/tcp on 10.1.0.1
Discovered open port 636/tcp on 10.1.0.1
Discovered open port 49155/tcp on 10.1.0.1
Discovered open port 3269/tcp on 10.1.0.1
Discovered open port 49157/tcp on 10.1.0.1
Discovered open port 88/tcp on 10.1.0.1
Discovered open port 464/tcp on 10.1.0.1
Completed SYN Stealth Scan against 10.1.0.129 in 7.49s (1 host left)
Completed SYN Stealth Scan at 12:17, 7.59s elapsed (2000 total ports)
Initiating Service scan at 12:17
```

nmap scan in progress

The scan will take a few minutes to complete and should finish with an "Nmap done" status message. You may have to scroll down to see this.

- 5) Click the **Topology** tab - this shows the hosts found via the scan, in this case restricted to the local subnet. You should be able to see all three VMs.



nmap can show the topology of hosts located on the local network

- 6) Click the **Host Details** tab. This shows the scan's attempt to identify the OS, which may be inaccurate as the versions of Windows you are using are newer than the version of nmap.
- 7) Click the different hosts in the left-hand panel to view them. Note that the bomb icon shown on the SERVER VM indicates lots of open ports.

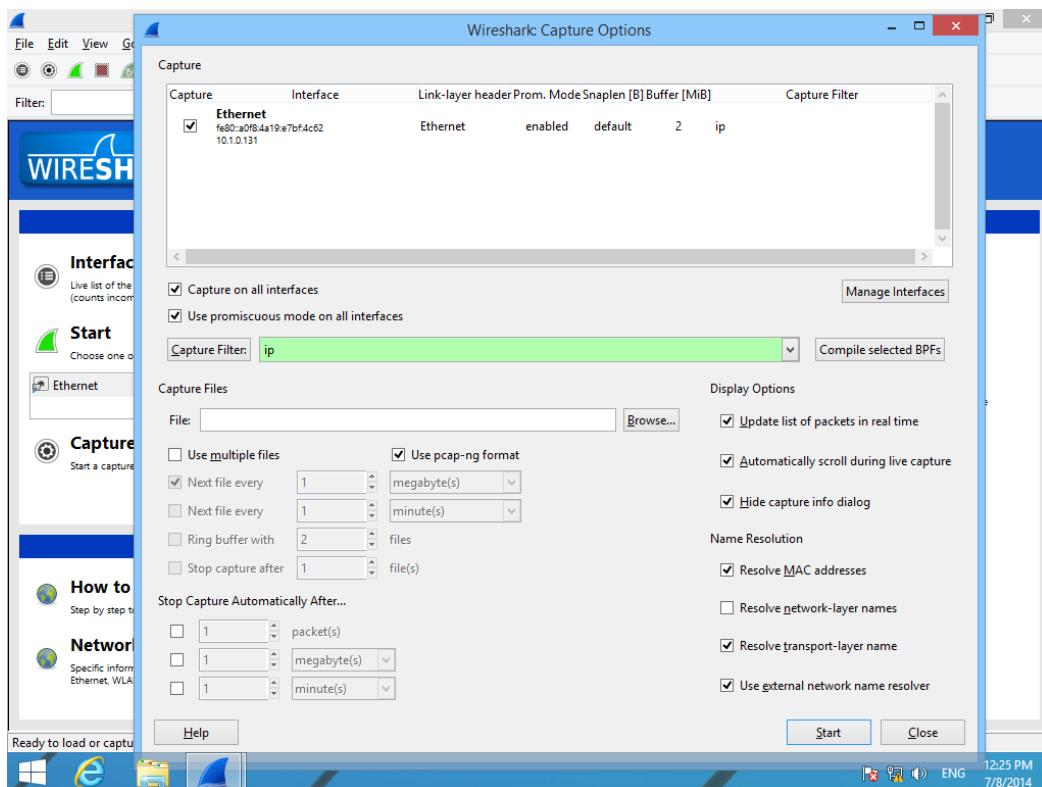
nmap makes a best guess at OS type and version based on its probes but is not always accurate

- 8) Click the **Ports / Hosts** tab. This shows precisely which ports are open on each host and in some cases the model and version of the server hosting them.
- 9) Finally, click the **Services** tab - this sorts the display by service rather than host. For any service you are interested in attacking (or defending) you can see which hosts are running it.
- 10) Close Zenmap, discarding any changes.

Exercise 2: Packet Sniffing

Another critical information gathering tool is a protocol analyzer. This tool works with a network sniffer to capture unicast packets sent to the host and broadcast packets on the same subnet. The most widely used is Wireshark.

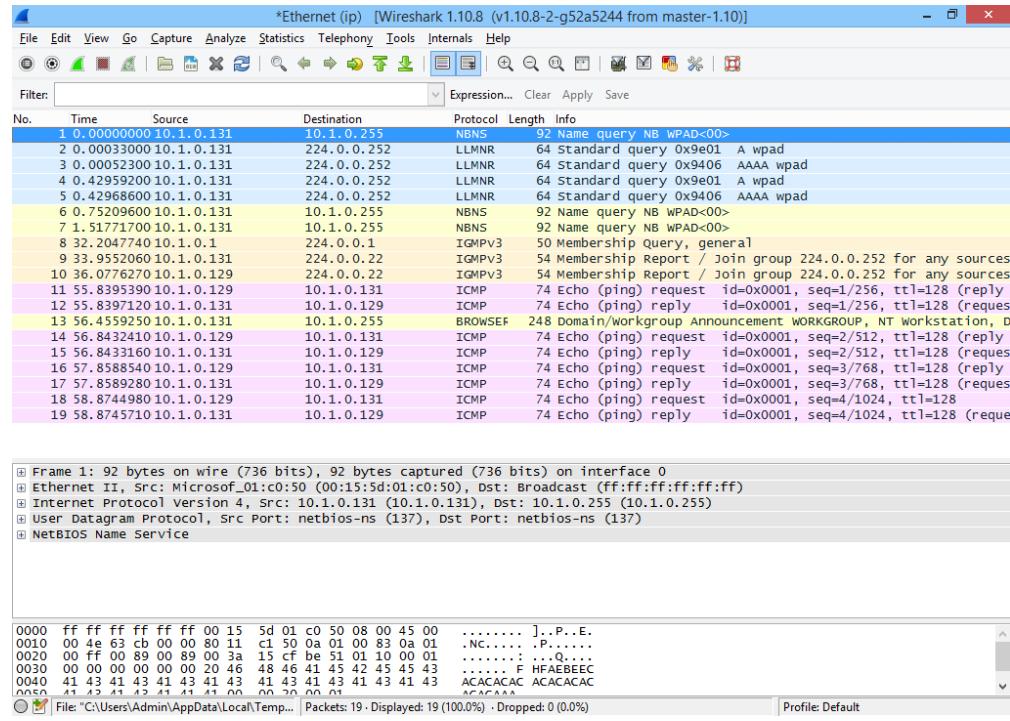
- 1) From the desktop of the ROGUE VM, open **Wireshark**.
- 2) Maximize the window.
- 3) Click the **Capture Options** button .
- 4) In the "Capture Filter" box, type **ip**. Click **Start**.



Enter a capture filter to restrict the type of packets processed by Wireshark

- 5) Switch to the CLIENT VM and log on as **CLASSROOM \Administrator** (password: **Pa\$\$w0rd**).
- 6) Use File Explorer and Internet Explorer to browse resources on SERVER (**start+R**, then **\SERVER** and **http://\SERVER** for instance).
- 7) Open a command prompt and run the command **ping ROGUE**.

8) Close the Command Prompt, Internet Explorer and File Explorer windows.



What do you notice about the packets captured?

9) Switch back to ROGUE and note what has been captured. What do you notice about the packets?

10) Click the **Stop Capture** button in Wireshark to stop the capture.

Exercise 3: MitM with ARP Spoofing

As an attacker, you may be more interested in finding out what information a *different* host on the network is receiving and possibly to modify the transmissions between two hosts - a Man in the Middle (MitM) attack. Ettercap is one of the most widely used tools for launching MitM attacks. On a local network, one of the most powerful techniques is ARP spoofing.

- 1) Log on to the SERVER VM as **CLASSROOM\Administrator**.
- 2) Open File Explorer and copy the **ftproot** and **wwwroot** folders from **c:\GTSLABS**.
- 3) Browse to **c:\inetpub** and paste the folders.
- 4) Switch to the CLIENT VM and open a command prompt.
- 5) Enter **ping 10.1.0.1** to check connectivity with the SERVER VM.
- 6) Open a **Run** box (**start+R**) and type **http://SERVER**, then press **Enter**.

If the web page looks the same as in Exercise 2, use the browser's **Refresh** icon to reload the page.

- 7) In a command prompt, enter `arp -a` to view the ARP cache. Make a note of SERVER's MAC address:
-

- 8) Switch to the ROGUE VM, and open an elevated command prompt (Start button, type `cmd`, alt-click **Command Prompt** icon, select **Run as administrator**, click **Yes** in **User Account Control** dialog if requested).

- 9) Type `ping SERVER`, then press **Enter**. Note SERVER's IP address.
-

- 10) Type `ping CLIENT`, then press **Enter**. Note CLIENT's IP address.
-

- 11) Enter `arp -a` to view the ARP cache. Verify that SERVER's MAC address is the same as previously observed, then note CLIENT's MAC address.
-

- 12) Enter the following command (on a single line): `netsh interface ipv4 add neighbors Ethernet server_IP server_MAC`, replacing `server_IP` with the IP address of SERVER, and `server_MAC` with the MAC address of SERVER.

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window contains the following text:

```
C:\>Windows\system32>arp -a
Interface: 10.1.0.129 --- 0x3
  Internet Address      Physical Address          Type
  10.1.0.1              00-15-5d-01-c0-5c        dynamic
  10.1.0.128             00-15-5d-01-c0-5d        dynamic
  10.1.0.255             ff-ff-ff-ff-ff-ff        static
  224.0.0.22              01-00-5e-00-00-16        static
  224.0.0.252             01-00-5e-00-00-fc        static
  239.255.255.250         01-00-5e-7f-ff-fa        static
  255.255.255.255         ff-ff-ff-ff-ff-ff        static

C:\>Windows\system32>netsh interface ipv4 add neighbors ethernet 10.1.0.1 00-15-5d-01-c0-5c

C:\>Windows\system32>_
```

Configuring static ARP entries

- 13) Likewise, enter the command `netsh interface ipv4 add neighbors Ethernet client_IP client_MAC`, again replacing the appropriate addresses.

- 14) Enter `arp -a` to view the ARP cache again. What has changed about the ARP entries for SERVER and CLIENT?
-

- 15) From the desktop, run **Ettercap**. Maximize the window.

- 16) Select **Sniff > Unified Sniffing**.

17) Click **OK** to select the interface "Microsoft Corporation". This should be the only available interface.

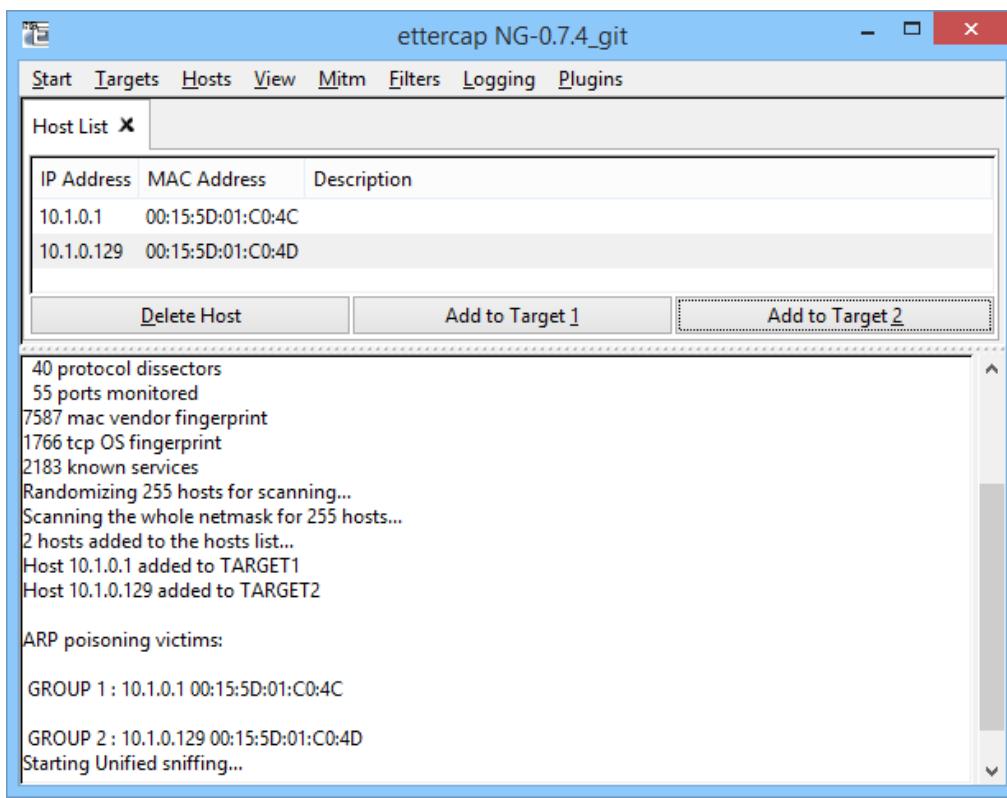
18) Select **Hosts > Scan for hosts**. This should return two results.

19) Select **Hosts > Hosts list**. Select **10.1.0.1** and click **Add to Target 1** then select **10.1.0.x** (CLIENT's IP address) and click **Add to Target 2**.

20) Select **Mitm > Arp poisoning**. Click **OK**.

21) Select **Start > Start sniffing**.

22) Switch to Wireshark and click the **Start Capture** button . Click **Continue without Saving** if asked about an existing capture.



Ettercap

23) Switch to the CLIENT VPC and run `ping 10.1.0.1`.

24) Enter `arp -a` to view the ARP cache. Make a note of SERVER's MAC address:

Note that you can see ROGUE's IP address and MAC and that the MACs for ROGUE and SERVER are identical. The attack we are launching is quite unsophisticated - it is possible to be a lot more subtle.



You may find that performance is a bit unreliable and some requests time out. Use `ping 10.1.0.1 -t` to keep sending if this is the case. Press `ctrl+C` to halt when you have seen some packets.

- 25) Use File Explorer and Internet Explorer to browse resources on SERVER (**start+R**, then `\SERVER` and `http://\SERVER`) again.
- 26) Switch back to the ROGUE VM. In Ettercap, select **Mitm > Stop Mitm attack(s)**.
- 27) Close Ettercap.
- 28) Switch to CLIENT and run `ping 10.1.0.1` again. The first one or two requests may fail but you should eventually see some replies.
- 29) Run `arp -a`. The ARP cache should have been restored.
- 30) On the ROGUE VM, select the Wireshark window and click **Stop Capture** button . Look at the captured packets - what do you notice now?

-
- 31) Close Wireshark, selecting **Quit without Saving** when prompted.

Exercise 4: Denial of Service

The last major class of attack is Denial of Service (DoS). There are any number of ways to prevent a server from responding to clients. We could have used Ettercap to simply discard any packets from client or server for instance.

Flood type attacks really depend on overwhelming the victim system with superior bandwidth, which itself depends on compromising thousands or even millions of "zombie" PCs in a "botnet". This exercise just illustrates how simple it is to craft the sort of malformed packets that can be used to try to flood a server.

- 1) On the SERVER VM, start Wireshark using the icon on the desktop.
- 2) In the **Capture** pane, click on **Ethernet** in the list of interfaces.
- 3) Open the **Capture Options** dialog. In the "Filter options" box, enter `tcp port 80` then start the capture.
- 4) From the CLIENT VM, connect to `http://server` and open the various pages on the site, making a mental note of how quick they are to load (there should be no noticeable delay).
- 5) Close the browser then open the **Internet Options** applet (press **Start**, type `internet options`, then click on the **Internet Options** icon)
- 6) Under "Browsing history", click **Delete**. Ensure **Temporary Internet files and website files** is ticked, then click **Delete**. Wait for the process to complete, then click **OK**.
- 7) Switch to the SERVER VM and note the SYN > SYN/ACK > ACK sequence in the first few packets. The remainder of the capture shows the CLIENT VM retrieving the page using HTTP.
- 8) On the ROGUE VM, run **LOIC** from the icon on the desktop.

Low Orbit Ion Cannon is a program that can be used to launch Distributed Denial of Service attacks against servers, if used by multiple attackers simultaneously.

- 9) In the URL box, type **server.classroom.local**, then click the **Lock on** button. The server's IP address should appear in the "Selected target" box.
- 10) Under "Attack options", in the **Method** dropdown select **HTTP**.



LOIC

- 11) Click the **IMMA CHARGIN MAH LAZER** button.
- 12) Note the flood of packets captured by Wireshark on SERVER. Stop the capture and close Wireshark, discarding the changes.
- 13) On the CLIENT VM, browse the site again - you may find that background graphics and buttons take slightly longer to load.

Clearly you would need a lot more bandwidth to overwhelm the server completely.
- 14) Switch to the Rogue VM and click **Stop flooding**, then close Low Orbit Ion Cannon.

Exercise 5: Completing the Lab

You need to discard some of the changes you made during this lab to the VMs' disk images.

- 1) On each VM, from the console window toolbar, select **Action > Revert**.



Make sure you choose "Revert". Take care NOT to select "Reset".

- 2) Confirm by clicking the **Revert** button.



Lab 4 / Baseline Security Analyzer

There are a number of tools produced by Microsoft to validate OS and application "baseline" configurations. The "superset" tool is now the Microsoft Security Compliance Manager. The tools allow you to test installations against pre-configured or customized templates (lists of which services and configuration options should be enabled).

As the Security Compliance Manager is complex to install, in this lab we will look at the Baseline Security Analyzer, which provides a simple means of testing whether an OS conforms to a basic security configuration.

- 1) Start the **SERVER** and **CLIENT** VMs.
- 2) Sign into the **CLIENT** VM as **CLASSROOM\Administrator** with the password **Pa\$\$w0rd..**
- 3) Browse to **c:\GTSLABS** and run **MBSASetup-x64-EN**.
- 4) Complete the setup wizard then use the desktop shortcut to start the program.
- 5) Select **Scan multiple computers**.
- 6) Enter **CLASSROOM** in the "Domain name" box.
- 7) *Uncheck* the **Check for security updates** box.
- 8) Click **Start Scan**.
- 9) When the scan is complete, click **Pick a security report to view**.

Report Details for classroom - CLIENT (2014-07-10 13:49:47)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name: classroom\CLIENT
IP address: 10.1.0.129
Security report name: classroom - CLIENT (7-10-2014 1:49 PM)
Scan date: 7/10/2014 1:49 PM
Scanned with MBSA version: 2.3.2208.0
Catalog synchronization date: Security updates scan not performed

Sort Order: Score (worst first) ▾

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
!	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
!	Password Expiration	All user accounts (3) have non-expiring passwords. What was scanned Result details How to correct this
!	Incomplete Updates	No incomplete software update installations were found. What was scanned
!	Local Account Password Test	Some user accounts (2 of 3) have blank or simple passwords, or could not be analyzed. What was scanned Result details
!	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details

Print this report Copy to clipboard Previous security report Next security report OK

Microsoft Baseline Security Analyzer

10) Read through both reports.

You need to discard the changes you made during this lab to the VMs' disk images.

11) On each VM, from the console window toolbar, select **Action > Revert**.

12) Confirm by clicking the **Revert** button.



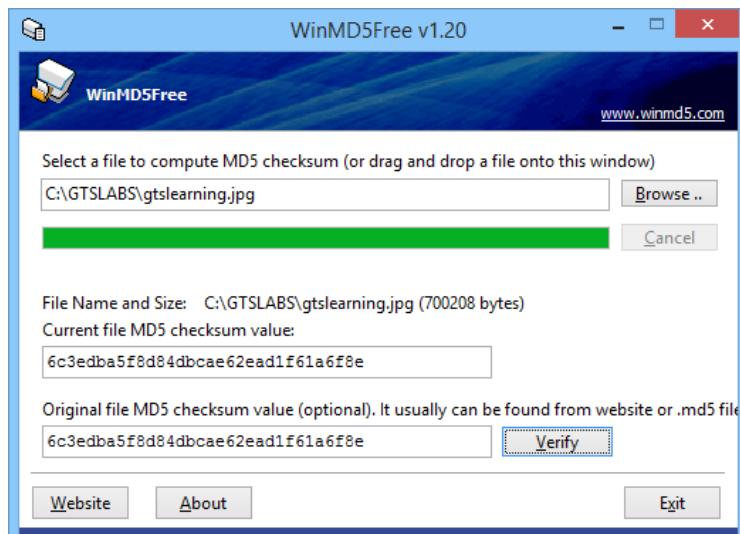
Lab 5 / Steganography

In this lab, you will investigate a couple of techniques for concealing information within the Windows file system.

Exercise 1: Hiding Information within a File

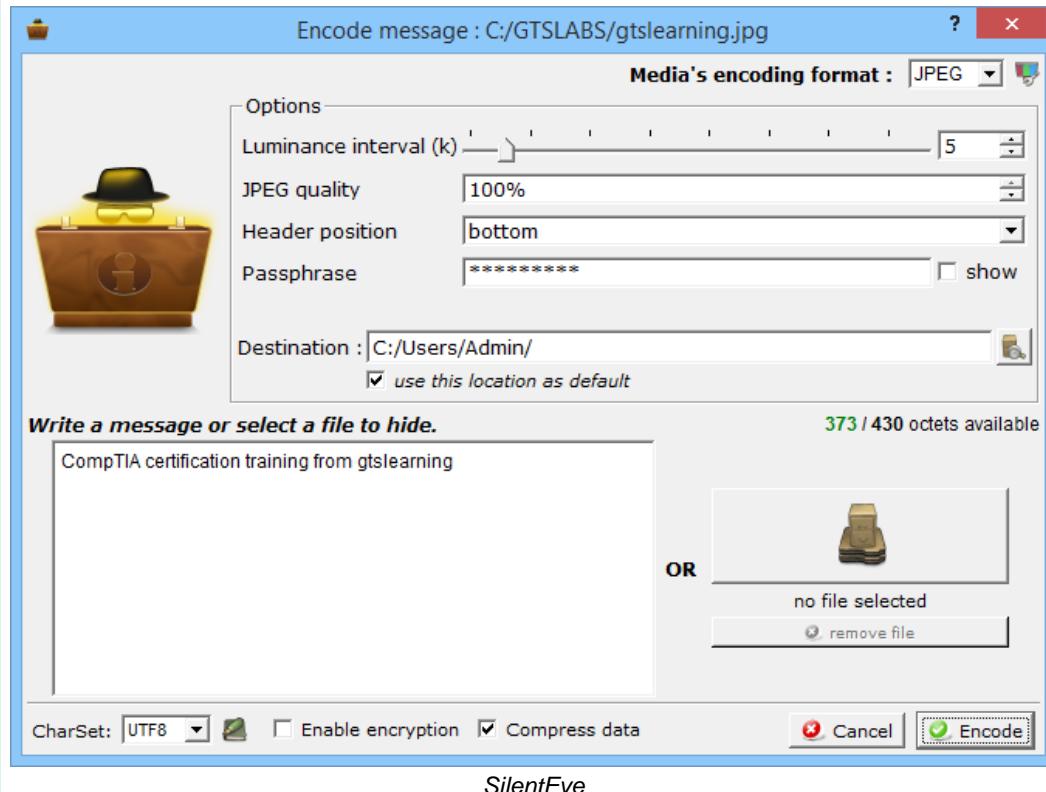
A basic steganography tool encodes information within another file, typically a media file such as a picture or audio/video file. A typical technique is to encode information in the least significant bit of the image or audio data. This does not materially affect the picture or sound and does not alter the file header (though it can change the file size).

- 1) Start the **CLIENT** VM and sign in as **CLIENT\Admin** using the password **Pa\$\$w0rd**
 - 2) Browse to **c:\GTSLABS** and run **silenteye-0.4.1-win32**. Confirm the "User Account Control" dialog, then install the program using the defaults.
 - 3) In the **c:\GTSLABS** folder, alt-click the **gtslearning.jpg** image file and select **Properties**, then make a note of the size and created / modified / accessed dates and times.
-
- 4) Close the "Properties" dialog.
 - 5) In the **c:\GTSLABS** folder, double-click **WinMD5**. Drag the **gtslearning.jpg** file into the "Select a file" box in the WinMD5 window.
- This causes the program to generate a file checksum.
- 6) Copy the value from the **Current file MD5 checksum** box to the **Original file MD5 checksum** box. Leave the WinMD5 window open (you may want to minimize it to the taskbar though).



WinMD5

- 7) In the Silent Eye window, select **File > Open** and select the **gtslearning.jpg** image file from the c:\GTLABS folder.
- 8) Click the **Encode** button.
- 9) In the "message" box, type some message that you want to hide. Note that the message length is limited to the "octets available".



- 10) In the "JPEG quality" box, set the value to **100%**.
- 11) Click the **Encode** button.
- 12) Close Silent Eye.
- 13) In File Explorer, type **%homepath%** in the address bar then press **Enter** to open the folder where the Silent Eye output was saved.
- 14) View the new file's properties in File Explorer and note what has changed:

- 15) Drag the new **gtslearning.jpg** file into the "Select a file" box in the WinMD5 window to generate the new file's checksum.

Exercise 2: Detecting Steganography

If an analyst has access to both the original file and the covertext version, it will be obvious from the file properties that something has changed. There are also steganography analysis tools that can try to perform this sort of detection.

- 1) Open previews of both images and see if you can detect any change visually.

- 2) Browse to **c:\GTSLABS** and extract the contents of the **stegdetect-0.4** zipped folder.
 - 3) In the extracted folder, open the **stegdetect** folder, then run the **xsteg** application.
 - 4) From the **File** menu, select **Open**. Browse to select the image file in **c:\USERS\ADMIN** and click **OK**.
 - 5) Does the tool locate the presence of a message?
-

- 6) Close the **xsteg** window.

Exercise 3: Alternate Data Streams

Alternate Data Streams (ADS) are a feature of NTFS allowing data to be linked to a file or folder but stored "outside" it. ADS are not accessible to most Windows system tools. They represent a way for attackers to conceal data (including executable code) within a file system.

- 1) Create a new Rich Text Document file in **c:\GTSLABS** named **MEMO**. Add some text then save and close it.
 - 2) Alt-click the file and select **Properties**. Make a note of the size and date properties:
-
- 3) Click **Cancel**.
 - 4) Drag the **MEMO.rtf** file into the "Select a file" box in the WinMD5 window.
 - 5) Copy the value from the **Current file MD5 checksum** box to the **Original file MD5 checksum** box. Leave the WinMD5 window open (you may want to minimize it to the taskbar though).
 - 6) Press **Start** then type **cmd** and press **Ctrl+Shift+Enter** to open an elevated command prompt. Click **Yes** to confirm the "User Account Control" dialog.
 - 7) Enter **cd \GTSLABS** to change the current directory.
 - 8) Enter the following commands to put the file "setup.exe" into an ADS associated with the MEMO file then delete the original setup.exe file:

```
type setup.exe>memo.rtf:odysseus.exe
erase setup.exe
```

- 9) In Explorer, check **MEMO.rtf**'s file properties and checksum again - is there any difference?

- 10) Move **MEMO.rtf** to your **Documents** library. Double-click to open the file - the executable will not run.

In previous versions of Windows, the **start** command could be used to launch executable code hidden in an ADS. This ability has been removed but code can still be executed using a symbolic link.

- 11) In the elevated command prompt, execute the following commands:

```
cd %homepath%\Documents  
mklink memo.lnk memo.rtf:odysseus.exe  
memo.lnk
```

- 12) Cancel the setup program.

There are various ways to identify what might have been concealed in ADS. One example is the GUI browser ADS Spy.

- 13) Run **c:\GTSLABS\adsspy**.

- 14) Select **Full scan (all NTFS drives)**.

- 15) Click **Scan the system for alternate data streams**.

The scan should locate Odysseus.exe in both **memo.rtf** and **memo.lnk**.

- 16) Check the boxes then click **Remove selected streams**.

- 17) Click **Yes** to confirm.

- 18) Close **ADS Spy**.

- 19) In the command prompt, try to execute the **memo.lnk** shortcut again.

You will get a "File not found" error. The symbolic link file still exists in the Documents folder (as does MEMO.rtf) but the stream it linked to has been erased.

Exercise 3: Completing the Lab

You need to discard some of the changes you made during this lab to the VM's disk image.

- 1) From the console window toolbar, select **Action > Revert**.



Make sure you choose "Revert". Take care NOT to select "Reset".

- 2) Confirm by clicking the **Revert** button.



Lab 6 / Configuring Certificate Services

In this lab, we will install certificate services on SERVER and configure a recovery agent.

Exercise 1: Installing Certificate Services

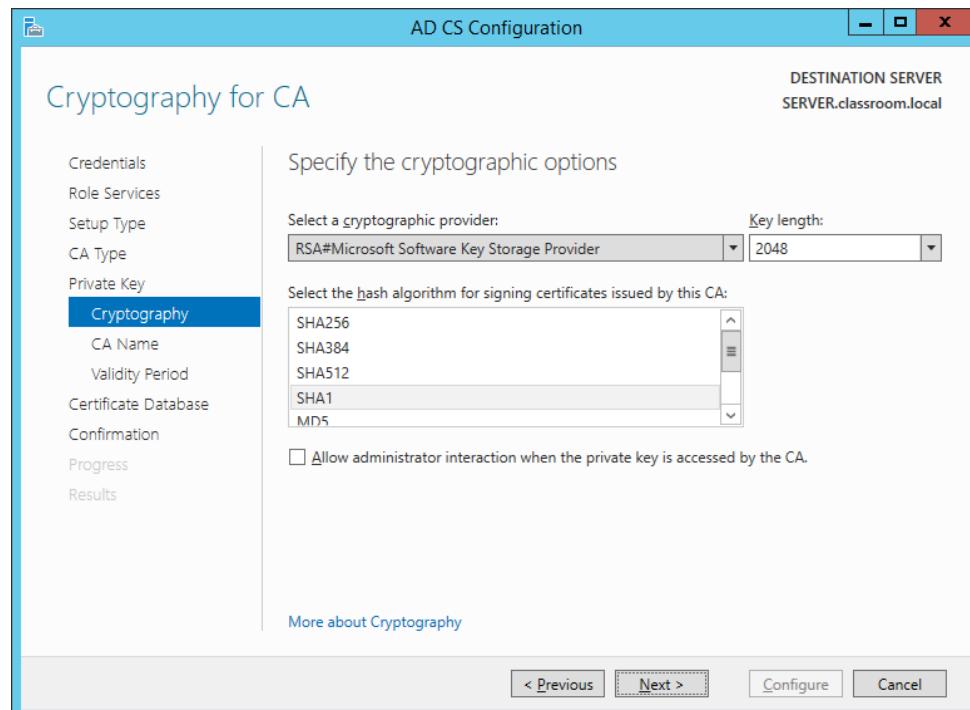
In this exercise, you will install and configure the Certificate Services server bundled with Windows Server.

- 1) Start the **SERVER** VM and sign in as **CLASSROOM\Administrator** with the password **Pa\$\$w0rd**.
- 2) From **Server Manager**, click the **Add roles and features** link. Complete the wizard by making the following choices:
 - o If the "Before you begin" page appears, click **Next**.
 - o On the "Select installation type" page, ensure **Role-based or feature-based installation** is selected, then click **Next**.
 - o On the "Select destination server" page, ensure **Select a server from the server pool** is selected, and **SERVER.classroom.local** is selected in the "Server Pool" list, then click **Next**.
 - o On the "Select server roles" page, check the **Active Directory Certificate Services** check box.
 - o In the "Add Roles and Features Wizard" dialog, ensure the **Include management tools (if applicable)** check box is ticked then click the **Add Features** button.
 - o On the "Select server roles" page, click **Next**.
 - o On the "Select features" page, click **Next**.
 - o On the "Active Directory Certificate Services" page, click **Next**.
 - o On the "Select role services" page, ensure that **Certification Authority** is checked already then also tick the **Certification Authority Web Enrollment** check box.
 - o In the "Add Roles and Features Wizard" dialog, ensure the **Include management tools (if applicable)** check box is ticked then click the **Add Features** button.
 - o On the "Select role services" page, click **Next**.
 - o On the "Confirm installation selections" page, click **Install**.
- 3) Wait for the installation to complete. When the installation has finished, click **Close**.

- 4) In Server Manager, select the **AD CS** node.
- 5) Click the **More** link next to the "Configuration required for Active Directory Certificate Services on SERVER" alert.
- 6) In the "All Servers Task Details" window, click the **Configure Active Directory Certificate Services** link. Complete the **AD CS Configuration** wizard by making the following choices:
 - o On the "Credentials" page, click **Next**.
 - o On the "Role Services" page, tick the **Certification Authority** and **Certification Authority Web Enrollment** check boxes, then click **Next**.
 - o On the "Setup Type" page, ensure **Enterprise CA** is selected, then click **Next**.
 - o On the "CA Type" page, ensure **Root CA** is selected, then click **Next**.
 - o On the "Private Key" page, ensure **Create a new private key** is selected, then click **Next**.

This is the key that secures the integrity of the whole certificate service. In a production network, it is *critical* that this key be kept securely.

- o On the "Cryptography for CA" page, leave the default options selected and click **Next**.



Selecting a cryptographic provider in AD CS Configuration

Note the cryptographic storage providers and supported algorithms. Selecting the most recent algorithms can offer better security but sometimes causes problems with older client OS versions.

- o Select the default options for the remainder of the wizard by clicking **Next** then **Configure** at the end.

7) Click **Close** when the operation has completed.

8) Close the **All Servers Task Details** window.

Exercise 2: Exploring the Certificate Server

In this exercise, you will examine the certificate server.

1) In **Server Manager**, select **Tools > Certification Authority**

2) Expand **classroom-SERVER-CA**.

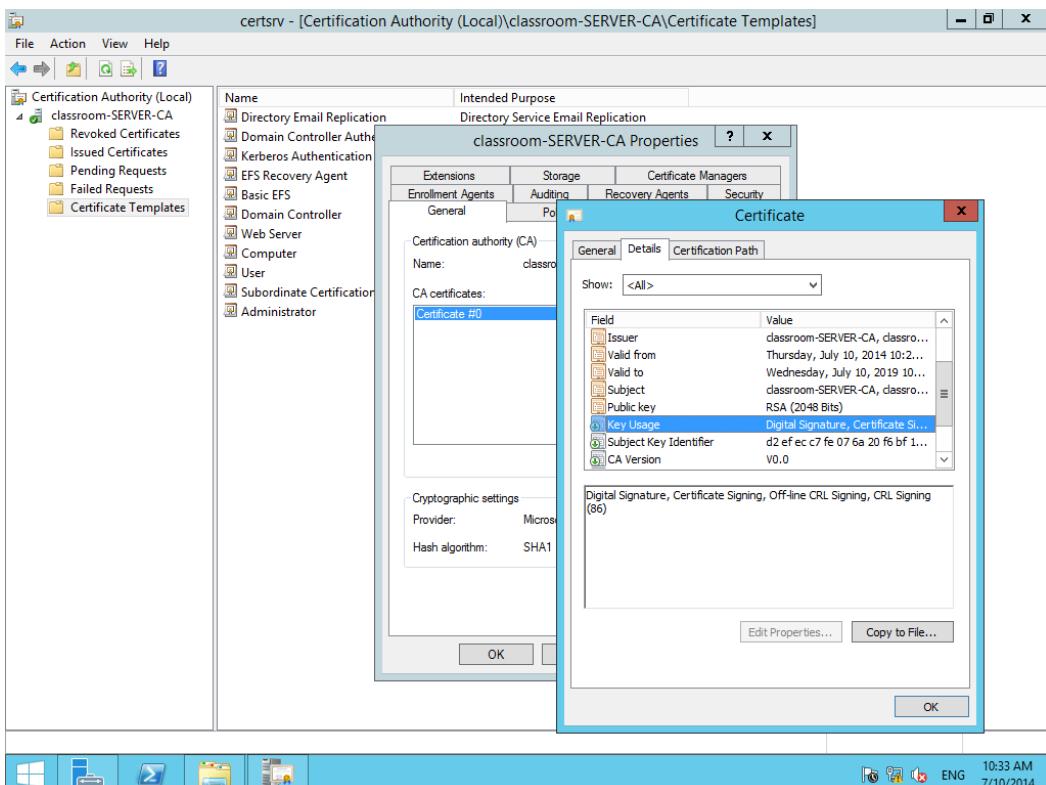
Note that there are folders for revoked and issued certificates and pending and failed requests. These are currently empty.

3) Select the **Certificate Templates** folder.

This snap-in shows the various kinds of certificates that can be issued – such as for server authentication, user authentication, and other specialist uses.

4) Alt-click your server (**classroom-SERVER-CA**) and select **Properties**.

5) On the **General** tab, click **View Certificate**. This is the CA server's proof of identity. Note that it is self-signed because this is the root certification authority. If you were to create subordinate CAs, they would be issued with certificates signed by this server. Look at the "Key Usage" field on the **Details** tab and confirm that the purpose of the certificate is to sign other certificates.



Examining the root certificate

- 6) Click **OK** to close the certificate then in the **Properties** dialog, click the **Extensions** tab.

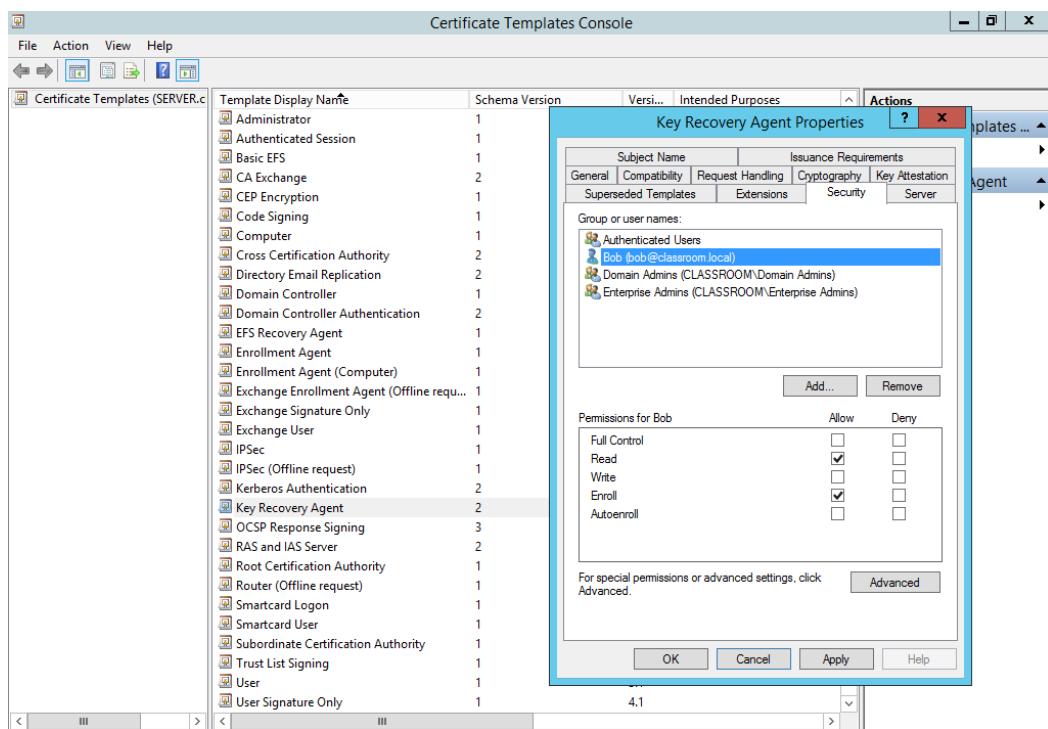
Note the locations of Certificate Revocation Lists (CRLs).

- 7) Click **Cancel** to close the dialog.

Exercise 3: Configuring an EFS Recovery Agent

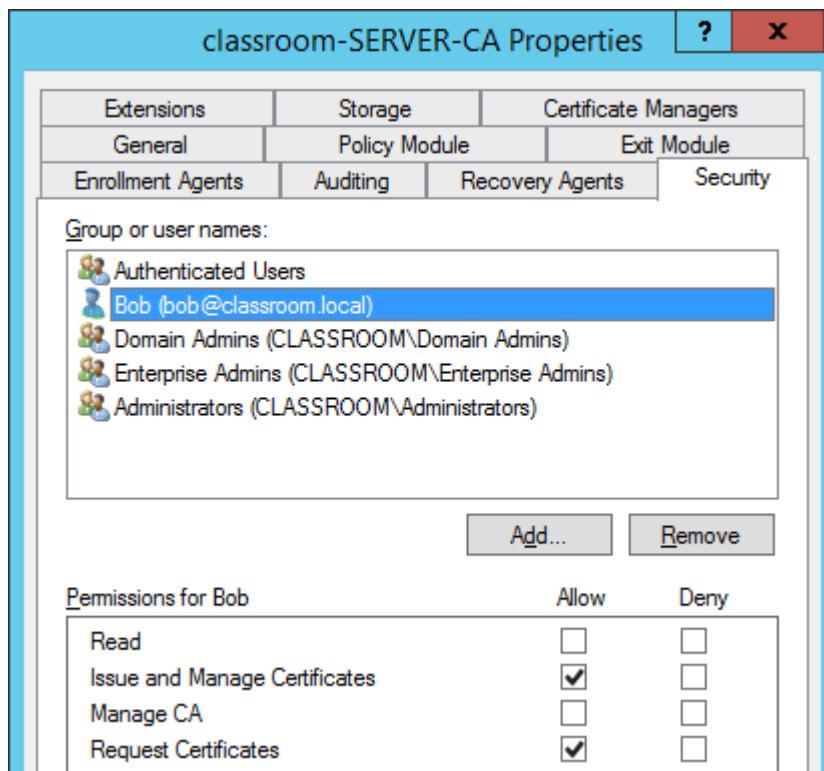
If a private key is lost, any data encrypted using that key will become completely inaccessible. To avoid this, it is usually necessary to configure EFS recovery agents, who have the ability to restore the data.

- 1) In **Server Manager**, select **Tools > Active Directory Users and Computers**.
- 2) Expand **classroom.local** and select the **Users** folder. Alt-click **Users** and select **New > User**.
- 3) Enter **Bob** in the "Full name" and "User logon name" fields. Click **Next**.
- 4) Enter and confirm the password **Pa\$\$w0rd** and uncheck **User must change password at next logon**.
- 5) Click **Next** then **Finish**.
- 6) In the "Users" folder, double-click the **Domain Admins** group. Select the **Members** tab, and click **Add**.
- 7) Enter **Bob** then click **Check Names** and **OK**.
- 8) Click **OK** to confirm the group membership change.
- 9) Switch back to the **Certificate Services** window and navigate to the **Certificate Templates** folder.
- 10) Alt-click the **Certificate Templates** folder and select **Manage**.
- 11) In the "Certificate Templates Console" window, alt-click the **Key Recovery Agent** template and select **Properties**.
- 12) Click the **Security** tab. Click the **Add** button.
- 13) Enter **Bob** then click **Check Names** and **OK**.
- 14) Add the **Enroll** permission to Bob's account.



Configuring a key recovery agent certificate

- 15) Click **OK** then close the **Certificate Templates Console** window.
- 16) In the "Certificate Services" window, alt-click your **classroom-SERVER-CA** server and select **Properties**.
- 17) Click the **Security** tab. Click the **Add** button.
- 18) Enter **Bob** then click **Check Names** and **OK**.
- 19) Add the **Issue and Manage Certificates** permission to Bob's account.



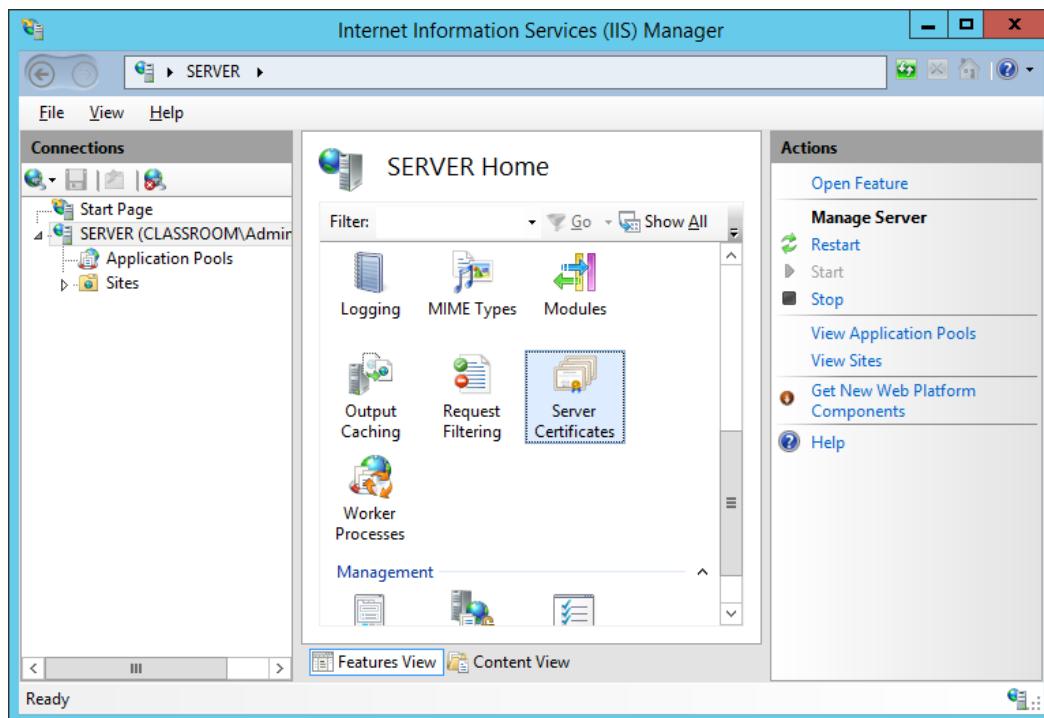
Configuring permissions on the CA server

20) Click **OK**.

Exercise 4: Configuring a Certificate Enrollment Website

Ordinary computer and user certificates can be issued without requiring user intervention but for some types of certificate you may want users to manually choose to request one. You can configure the **CA Web Enrollment** site to facilitate this. The web enrollment server must itself be identified by a certificate however, which we will configure in this exercise.

- 1) Switch to the **Server Manager** window.
- 2) Select **Tools > Internet Information Services (IIS) Manager**.
- 3) Expand **SERVER (CLASSROOM\Administrator)**. If a dialog appears asking about Microsoft Web Platform, click **No**.
- 4) In the "SERVER Home" pane, double-click **Server Certificates**.



Configuring Server Certificates in IIS

- 5) In the "Actions" pane, click the **Create Domain Certificate** link. Complete the wizard by making the following choices:
 - Enter **server.classroom.local** in the **Common name** box, and any values you wish in the other boxes, then click **Next**.
 - On the "Online Certification Authority" page, click **Select**.
 - In the "Select Certification Authority" dialog, select **classroom-SERVER-CA** and click **OK**.
 - In the "Friendly name" box, enter **server.classroom.local**, then click **Finish**.



*Optionally, check the **Issued Certificates** folder in the **Certificate Services** console - you will see the certificate you have just requested for the web server has appeared.*

- 6) Back in IIS Manager, expand **Sites**, then navigate to the **Default Web Site** node.
- 7) In the "Actions" pane, click the **Bindings** link.
- 8) In the "Site Bindings" dialog, click **Add**.
- 9) Set the "Type" drop-down to **HTTPS**, then select **server.classroom.local** in the "SSL Certificate" drop-down and click **OK**.



Note that the host name and friendly name must match for a browser to trust the certificate.

- 10) In the "Site Bindings" dialog, click **Close**.

Exercise 5: Obtaining a Key Recovery Certificate

In this exercise, you will sign in as Bob to request the new certificate from the CA Web Enrollment server.

- 1) Start the **CLIENT** VM and sign in as **CLASSROOM\Bob** with the password **Pa\$\$w0rd**.
- 2) From the desktop, open the **Internet Explorer** browser or a **Run** dialog and go to the address **https://SERVER.classroom.local/certsrv**.
- 3) Enter the user name **Bob** and the password **Pa\$\$w0rd**. Check the **Remember my credentials** box to save the password. Click **OK**.
- 4) Click **Request a certificate** then **advanced certificate request** then **Create and submit a request to this CA**.
- 5) In the "Message from webpage" dialog, click **OK**. In the yellow "Run control" alert box, click **Run Control**.
- 6) In the "Windows Security" dialog, enter the password **Pa\$\$w0rd** again and click **OK**.
- 7) In the "Web Access Confirmation" dialog, click **Yes**.

The "Advanced Certificate Request" web form will be displayed.

The screenshot shows the 'Advanced Certificate Request' page of the Microsoft Active Directory Certificate Services. The URL in the browser is <https://server.classroom.l...>. The page title is 'Microsoft Active Directory Certificate Services -- classroom-SERVER-CA'. The 'Home' button is visible in the top right corner.

Certificate Template: EFS Recovery Agent

Key Options:

- Create new key set Use existing key set
- CSP: Microsoft Enhanced Cryptographic Provider v1.0
- Key Usage: Exchange
- Key Size: 1024 Min: 384 Max: 16384 (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))
 - Automatic key container name User specified key container name
 - Mark keys as exportable
 - Enable strong private key protection

Additional Options:

Request Format: CMC PKCS10

Hash Algorithm: sha1

Only used to sign request.
 Save request

Attributes: [List box with arrows]

Friendly Name: [Text input field]

Submit >

Requesting a certificate

- 8) Under "Certificate Template", choose **EFS Recovery Agent**. Review the settings for cryptographic provider, key size, and request format but just click **Submit** to use the default options.
- 9) Click **Yes** in the "Web Access Confirmation" dialog.
- 10) Click **Install this certificate**.
- 11) When the "New certificate installed" message is displayed, close the browser.

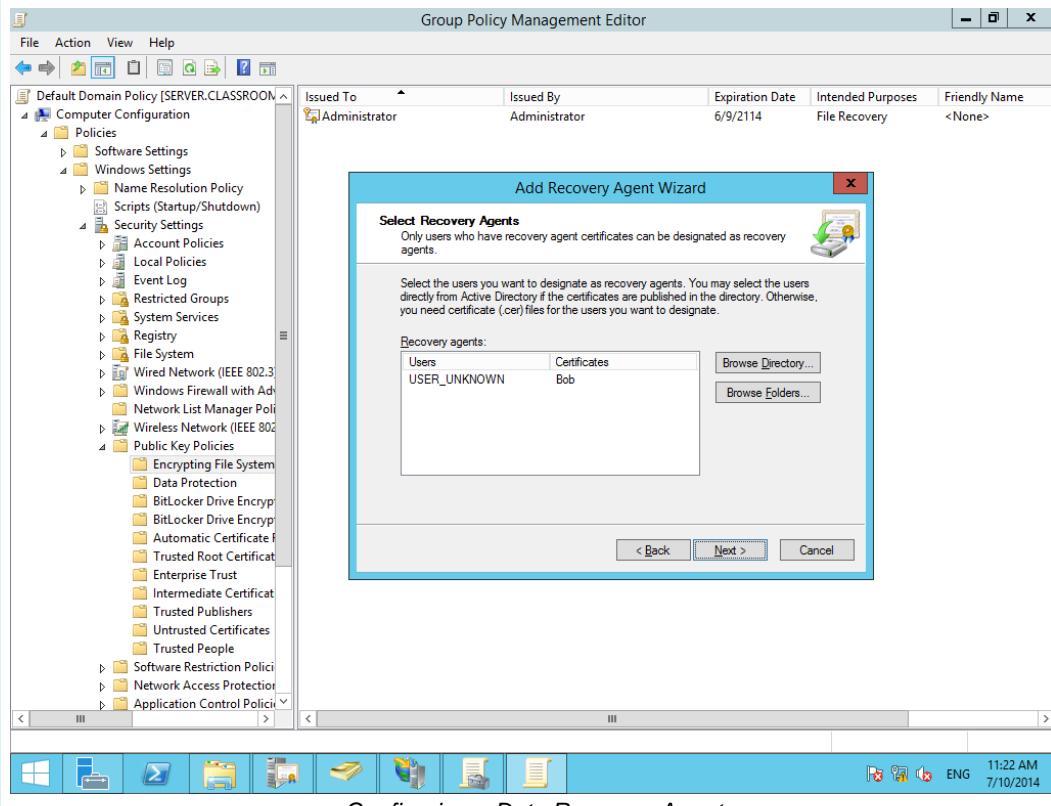


*Optionally, check the **Issued Certificates** folder in the **Certificate Services** console on the SERVER VM. You will see the certificate you have just requested for the key recovery (though you may need to refresh the view first). You will also see that a certificate has been issued for SERVER's domain controller role plus a CAExchange certificate (used for key archiving).*

Exercise 6: Configuring Domain EFS Recovery

Having created Bob's EFS recovery certificate, the next step is to use Group Policy to ensure all encrypted files in the domain can be recovered using this certificate.

- 1) In the CLIENT VM, click the Start button, type `mmc` and click the **mmc** icon. Confirm the "User Account Control" dialog.
- 2) In the console, select **File > Add/Remove Snap-in**.
- 3) Select the **Certificates** snap-in and click **Add** then **Finish**. Click **OK** to close the dialog.
- 4) Browse to **Certificates – Current User > Personal > Certificates**.
- 5) Alt-click the **Bob** certificate and select **All Tasks > Export**. Complete the wizard by making the following choices:
 - Click **Next**.
 - On the "Export Private Key" page, ensure **No, do not export the private key** is selected, then click **Next**.
 - On the "Export File Format" page, click **Next** to accept the default.
 - On the "File to Export" page, in the "File name" box, type `\server\netlogon\bobcert.cer`.
 - Click **Next** then **Finish** then **OK**.
- 6) Sign out of the CLIENT VM.
- 7) On the SERVER VM, in **Server Manager** select **Tools > Group Policy Management**.
- 8) In the "Group Policy Management" window, alt-click the **classroom Domain Policy** node, and select **Edit**.
- 9) In the "Group Policy Management Editor" window, browse to the **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Encrypting File System** node.
- 10) Alt-click the **Encrypting File System** node and select **Add Data Recovery Agent**. Complete the wizard by making the following choices:
 - Click **Next** to start the wizard.
 - On the "Select Recovery Agents" page, click the **Browse Folders** button.
 - In the "File name" box, type `\server\netlogon\bobcert.cer` then click **Open**.
 - Click **Next** then **Finish**.



- 11) Switch to the **CLIENT** VM and sign in as **CLASSROOM\Administrator** with the password **Pa\$\$w0rd**.
- 12) Open a command prompt and enter the command **gpupdate /force**.
- 13) Restart the **CLIENT** VM.
- 14) On the SERVER VM, create a new user named **Sue** using **Domain Users and Computers**. You can use the same **Pa\$\$w0rd** for the account (make sure you untick **User must change password**).
- 15) Alt-click the **Sue** user object and select **Add to a group**. In the "Enter the object names" box, type **remote desktop users** then click the **Check Names** button. Confirm the dialogs by clicking **OK**.



Sue needs to be in this group for you to be able to sign on as her in the CLIENT VM.

Exercise 7: Using Encryption

In this exercise, you will create an ordinary domain user named Sue, who will encrypt some private documents and then get into a bit of a situation.

- 1) Switch to the **CLIENT** VM and click **Other user**.
- 2) Enter the name **Sue** and the password **Pa\$\$w0rd** then press **Enter**.
- 3) Open **File Explorer** and browse to **c:\GTSLABS**, then create a subfolder called **SECRETS** and add and edit a few text and picture files.

- 4) Alt-click the **SECRETS** folder and select **Properties**.
- 5) Click the **Advanced** button and check **Encrypt contents to secure data**. Click **OK** to the prompts.

Note that SECRETS and its child objects are color-coded green for encrypted.

- 6) Confirm that you can still open the files in the **SECRETS** folder.
- 7) Sign out from the Sue account. Sign on as **CLIENT\Admin** (the local administrator account for the computer) and try to view the files that Sue created.

Note that not even administrators can view encrypted files without the appropriate key.
- 8) Try to remove the encryption property from one of the files in the SECRETS folder.
- 9) When that doesn't succeed, cancel out of any dialogs and sign out from the VM.
- 10) Sign back in as **CLASSROOM\Sue**. From the Start Screen, type **mmc** and click the **mmc** icon.
- 11) In the console, select **File > Add/Remove Snap-in**.
- 12) Select the **Certificates** snap-in and click **Add** then **Finish**.

- 13) Click **OK**.
- 14) Navigate to **Certificates > Personal > Certificates** then alt-click the **Sue** certificate and select **All Tasks > Export**. Complete the wizard by making the following choices:
 - Click **Next**.
 - Select **Yes, export the private key**. Click **Next**.
 - On the "Export File Format" page, check the **Delete the private key if the export is successful** box and click **Next**.

This means that the private key is no longer kept in the user's profile. You would normally export a key to a secure USB thumb drive or to a smart card.

- Check the **Password** box, then enter and confirm the password **Pa\$\$w0rd** and click **Next**.
 - Enter the name **c:\GTSILABS\suecert**.
 - Click **Next** then **Finish** and then **OK**.
- 15) Alt-click the certificate and select **Delete**. Confirm by clicking **Yes**.

- 16) Close the console, choosing **No** when prompted to save settings.
- 17) Sign out from the CLIENT VM.
- 18) Sign back in as Sue and try to access the encrypted documents.
- 19) Sign out from the CLIENT VM.

Exercise 8: Performing Data Recovery

At this point, we will assume that Sue moved her exported key to a USB stick and put the USB stick somewhere safe. A few months later ... the stick is gone! Sue approaches the technical support department.

- 1) Sign into the CLIENT VM as **CLASSROOM\Bob**.
- 2) Open **File Explorer** and browse to **c:\GTSLABS**.
- 3) Alt-click the **SECRETS** folder and select **Properties**.
- 4) Click the **Advanced** button and uncheck **Encrypt contents to secure data**. Click **OK**.
- 5) Click **OK** to the prompts.

Note that SECRETS and its child objects are no longer color-coded green for encrypted.

- 6) Sign back in as Sue. Confirm that you can open the files in the SECRETS folder again.



*Optionally, check the **Issued Certificates** folder in the **Certificate Services** console on the SERVER VM. You will see that Sue has two "Basic EFS" certificates. One was generated automatically to replace the one that was deleted but as the replacement certificate has a different key it cannot be used to decrypt files encrypted with the previous one. You could revoke the "lost" certificate to ensure that it is not misused.*

Exercise 9: Completing the Lab

You need to discard some of the changes you made during this lab to the VMs' disk images.

- 1) On each VM, from the console window toolbar, select **Action > Revert**.



Make sure you choose "Revert". Take care NOT to select "Reset".

- 2) Confirm by clicking the **Revert** button.



Lab 7 / Password Sniffing

A password sniffer is a packet capture application optimized to look for packets containing passwords and then decrypt them. A password sniffer can be differentiated on the number of authentication mechanisms it can recognize and the quality of its dictionary.

Exercise 1: Keyloggers

Depending on the authentication method, cracking passwords can be an extremely difficult task. An alternative approach is to install keylogging spyware onto the computer and capture passwords as the user types.

- 1) Start the **SERVER** and **CLIENT** VMs.
- 2) Sign into **CLIENT** as **CLASSROOM\Administrator** with the password **Pa\$\$w0rd..**.
- 3) Browse to **c:\GTSLABS** and run **actualspy**. Complete the setup wizard using the defaults, choosing to create a desktop icon on the **Select Additional Tasks** page.
- 4) Double-click the program icon to start. Click **OK** to continue with the trial version.
- 5) Click **Settings**. Note the hotkey combination for opening ActualSpy.

- 6) Check **Start at the system loading** and all the boxes under "Hiding".
- 7) Select the **Logs** tab and note the PC activity that can be logged.
- 8) Click **Apply** then click the **Start monitoring** button on the toolbar.
- 9) Click the **Hide** button on the toolbar then click **OK** to the warning dialog.
- 10) Sign out from the **CLIENT** VM then log back on as **CLIENT\Admin** (the password is **Pa\$\$w0rd**).
- 11) Look for any sign that ActualSpy is installed or running - can you see any suspicious processes in Task Manager for instance?

- 12) Open a Run dialog (**Start+R**) and address enter the **\server.classroom.local.**

As you are not logged in as a domain user, you will be prompted for credentials.

- 13) Enter **Administrator** and **Pa\$\$w0rd**, and click **OK**.

- 14) Take a few minutes to complete some other activities on the VM - such as creating a couple of documents.
 - 15) Sign out of the CLIENT VM then sign back on as **CLASSROOM\Administrator**.
 - 16) From the desktop, use the hotkey combination previously noted to open ActualSpy.
 - 17) Look through the entries in the Keystrokes tab. Can you find any usernames or passwords?
-
- 18) Look through the other tabs to see what additional information has been logged.
 - 19) Close ActualSpy then sign out from the CLIENT VM.

Exercise 2: Cain and Abel

In this exercise, we will look at the Windows password sniffer Cain and Abel. Cain is the sniffer part of the program; Abel is a server that can redirect network traffic from a remote computer to be processed by Cain.

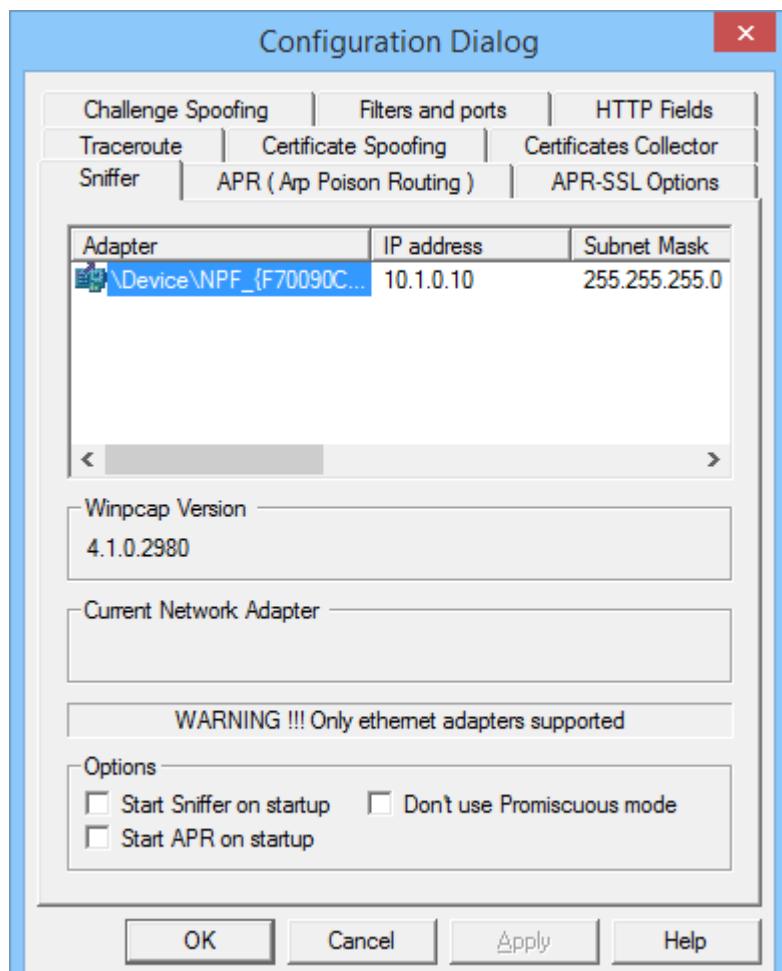
- 1) Sign in to the SERVER VM as **CLASSROOM\Administrator**.
- 2) In **Server Manager**, select **Tools > Internet Information Services (IIS) Manager**.
- 3) Expand **SERVER (CLASSROOM\Administrator)**. If a dialog appears asking about Microsoft Web Platform, click **No**.
- 4) Expand **Sites** and select the **Default Web Site** node.
- 5) In the "Default Web Site Home" pane, double-click **Authentication**.
- 6) Alt-click **Anonymous Authentication** and select **Disable**.
- 7) Alt-click **Basic Authentication** and select **Enable**.
- 8) Log on to the CLIENT VM as **CLASSROOM\Administrator**.

Cain requires a static IP address to be configured on the Ethernet adapter.

- 9) From the desktop, alt-click the **Network** icon in the system notification area and select **Network and Sharing Center**.
- 10) Click the **Ethernet** icon then select the **Properties** button. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
- 11) Select the **Use the following IP address** radio button, then enter **10.1.0.10** for IP address, **255.255.255.0** for "Subnet mask", and **10.1.0.1** for "Default gateway" and "Preferred DNS server".
- 12) Click **OK** and **Close** to close all the dialogs.

- 13) Browse to **c:\GTSLABS** and run **ca_setup**. Install using the defaults.
When prompted to install WinPcap, select **Don't install**.
- 14) Start **Cain** using the desktop shortcut. Note the warning and click **OK**.
- 15) Close Cain. Click the **Start** button, then type **firewall** and click the **Windows Firewall** icon. Click the **Turn Windows Firewall on or off** link, select all three **Turn off Windows Firewall (not recommended)** options, then click **OK** to disable the firewall.
- 16) Close the **Windows Firewall** window and run **Cain** again.

- 17) Click the **Start Sniffer** button  and check that the adapter and IP address have been identified.
- 18) Take a few moments to go through the tabbed options - Cain can perform ARP poisoning to launch MitM attacks on a switched network and perform digital certificate spoofing. Click **OK**.



Cain Configuration Dialog

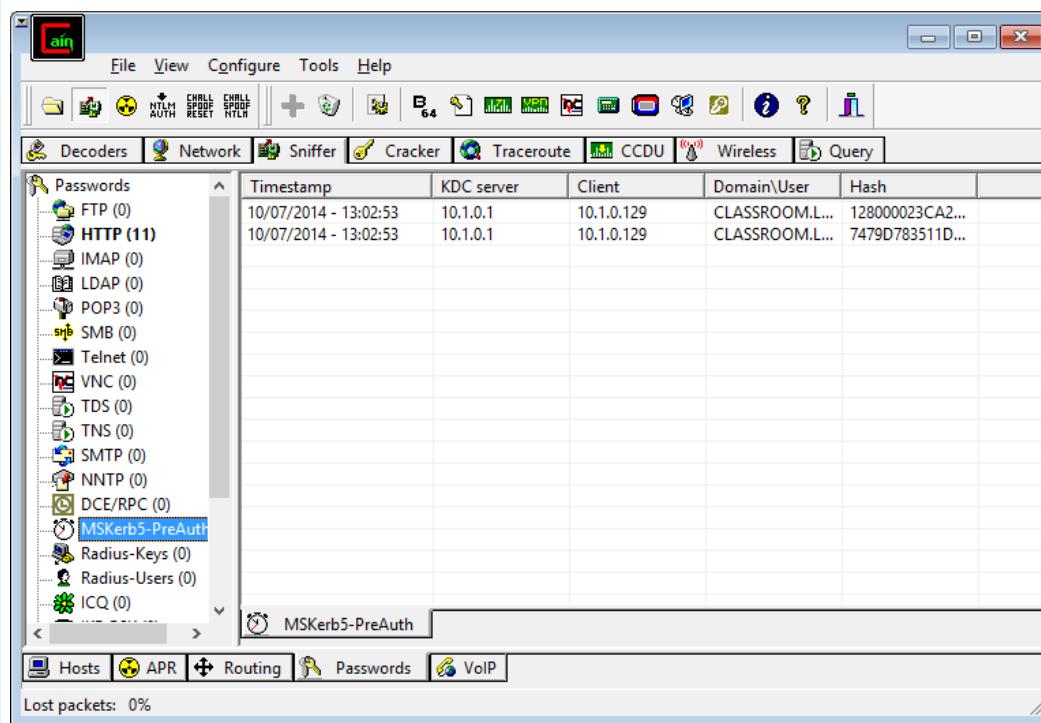
- 19) Click the **Start Sniffer** button  again. If a warning appears, click **OK**.
- 20) Open **http://server.classroom.local** in the browser, and log on (without saving credentials)

- 21) In the browser, open the **Internet Options** dialog, and check the **Delete browsing history on exit** box, then click the **Delete** button. Check all the boxes.
- 22) Click the **Delete** button.
- 23) Click **OK** then close the browser.

Exercise 3: Cracking Windows Passwords

Sniffing a password sent in plaintext is trivial. Cain can also be used to try to crack encrypted passwords.

- 1) Switch to the SERVER VM and open the **Authentication** options for the default site again.
- 2) Alt-click **Basic Authentication** then click **Disable**.
- 3) Alt-click **Windows Authentication** then click **Enable**.
- 4) On the CLIENT, open `http://server.classroom.local` in the browser, log on (without saving credentials), then close the browser.



Capturing passwords using Cain

- 5) Switch to Cain and click the **Sniffer** tab at the top then the **Passwords** tab at the bottom. Select **HTTP**. Note that the password supplied using Basic Authentication has been decoded. The credentials supplied when the website was using Windows Authentication are located under MSKerb5-PreAuth. The password hash has not been decoded automatically.
- 6) Alt-click one of the MSKerb5-PreAuth records and select **Send to Cracker**.
- 7) Click the **Cracker** tab and select **Kerb5 PreAuth Hashes**. Alt-click the **Administrator** account and select **Brute-Force Attack**.

8) Click **Start**. Note the time remaining. Click **Stop**.

9) Select the **Custom** option and type the following:

pPaAssWoOrRdD05\$@

10) Under "Password length", set both **Min** and **Max** boxes to **8**.

11) Click **Start**. Note the time remaining - still a substantial coffee break unless you get lucky! Click **Stop**. Click **Exit**.

As well as sniffing passwords over the network an attacker can also attempt to obtain the password storage file.

12) With the **Cracker** tab still selected, in the left-hand pane select **LM & NTLM Hashes**. Click the **Add to List** icon  on the toolbar.

13) With **Import Hashes from local system** selected click **Next**.

14) Alt-click the **Admin** account and select **Brute-Force Attack > NTLM Hashes**. Click **Start**.

15) Note the time remaining - let it run for a few minutes then click **Stop**.

16) Click **Exit**.

17) Alt-click **Admin** and select **Cryptanalysis Attack > NTLM Hashes > via RainbowTables (RainbowCrack)**.

Rainbow tables are multi-gigabyte databases of precomputed hashes. If a match for a hash is found in the table, the password can be decoded (this approach would not work if stored Windows passwords were "salted" with a random value).

18) Click **Exit**.

Exercise 4: Completing the Lab

You need to discard some of the changes you made during this lab to the VMs' disk images.

1) On each VM, from the console window toolbar, select **Action > Revert**.



Make sure you choose "Revert". Take care NOT to select "Reset".

2) Confirm by clicking the **Revert** button.



Lab 8 / Configuring a VPN

A Virtual Private Network (VPN) can allow two sites to be networked together over the internet or allow remote users to "dial-in" to a site over the internet.

VPN protocols support some sort of encryption mechanism to prevent eavesdropping, replay, or modification attacks. There also has to be a secure authentication mechanism to ensure that only authorized users can connect.

Exercise 1: Installing a Network Adapter

In this exercise you will add a second network adapter to the SERVER VM to support the configuration of RRAS later in the lab.

- 1) In the Hyper-V Manager, click **Virtual Switch Manager**.
- 2) If "External Network" is already listed under "Virtual Switches" click Cancel. Otherwise, complete the following steps to configure a new switch:
 - In the "Virtual Switches" pane, ensure **New virtual network switch** is selected.
 - In the "Create virtual switch" pane, select **External** and then click **Create Virtual Switch**.
 - In the Virtual Switch Properties pane, enter **External Network** in the **Name** box, then click **OK**.
- 3) In the Hyper-V Manager, alt-click the **SERVER** icon in the "Virtual Machines" pane, and select **Settings**.
- 4) In the "Settings for SERVER" dialog box, select **Add Hardware** in the Hardware pane.
- 5) In the "Add Hardware" pane, select **Network Adapter**, then click **Add**.
- 6) In the "Network Adapter" pane, select **External Network** from the "Virtual switch" drop-down list.
- 7) Click **OK** to confirm and close the **Settings for SERVER** dialog.

Exercise 2: Examining Unsecured Traffic

Before we set up a VPN connection, we will examine the risks involved in unsecured network traffic.

- 1) Start the **SERVER** VM and log on as **CLASSROOM\Administrator**.
- 2) In File Explorer, browse to the **c:\GTSLABS** folder, create a new subfolder and name it **SECRET**.

- 3) Within the SECRET folder, create a new text document and name it **CONFIDENTIAL**.
- 4) Open the CONFIDENTIAL file, and enter the following text:
The password is Courage!
- 5) Save and close the file.
- 6) In Server Manager, select **File and Storage Services > Shares**.
- 7) In the dropdown menu above the "SHARES" pane, select **TASKS > New Share**. Complete the wizard by making the following choices:
 - On the "Select Profile" page, ensure **SMB Share – Quick** is selected then click **Next**.
 - On the "Share Location" page, select **Type a custom path** and click **Browse**.
 - Browse to **c:\GTLABS\secret** then click **Select Folder**.
 - On the "Share Location" page, click **Next**.
 - On the "Share Name" page, change the share name to **secret\$** then click **Next**.
 - On the "Other Settings" page, clear the **Allow caching of share** check box, then click **Next**.
 - On the "Permissions" page, click **Next** then click **Create**.
 - When the share has been created, click **Close**.
- 8) Start the **CLIENT** VM and log on as **CLASSROOM\Administrator**.
- 9) Run Wireshark from the desktop icon, and click the **Start Capture** button 
- 10) Open a **Run** dialog (**Start+R**) and enter **\SERVER**. Does the secret\$ share appear?

- 11) In the File Explorer window's address bar, enter **\SERVER\secret\$**
- 12) Open the **Confidential** file and read the text, then close the file and the File Explorer window.
- 13) In Wireshark, click the **Stop Capture** button . Resize the panes so that the packet list (top) and packet data (bottom) panes are more clearly visible.
- 14) Look through the captured packets until you find one with a description (info field) starting **NetShareEnumAll Response**. This is the packet that the server uses to send its share list to the client.

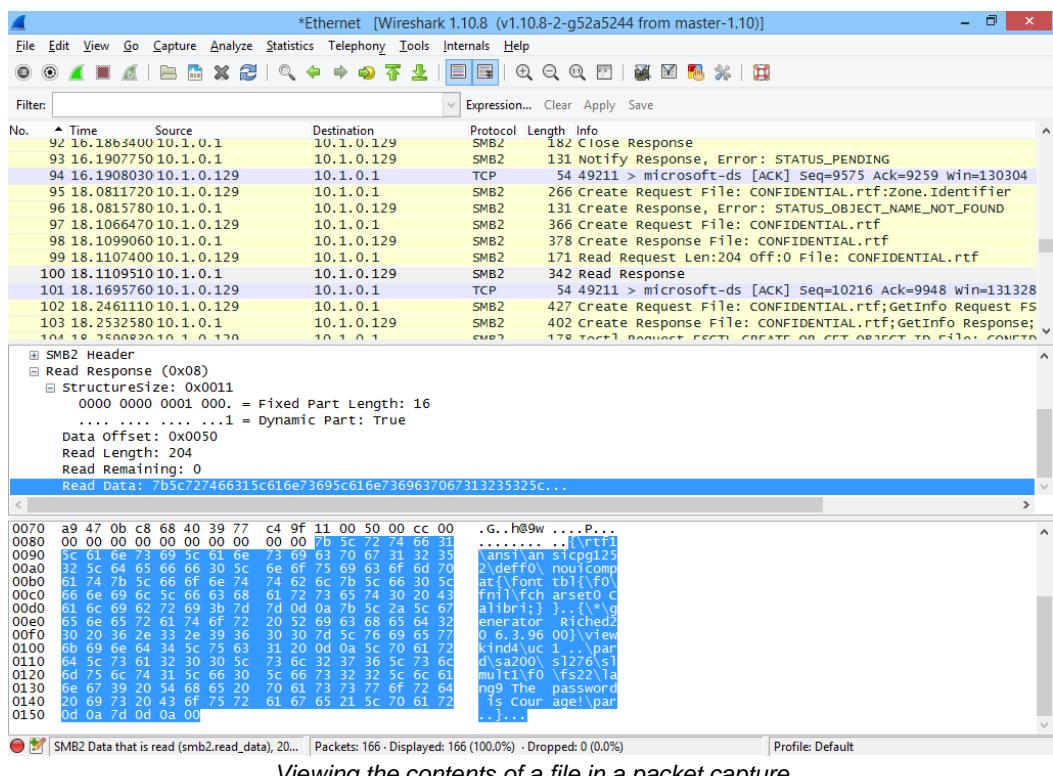
Enumerating shares in the SMB protocol

- 15) Click on this packet, and read its contents in the Packet Data frame. You may have to scroll down to view all the data. Does the secret\$ share appear in the data?



*Sort the capture by the Info field to make viewing the packets easier. Also, you can alt-click in the packet data frame and select **Expand All** to view all fields.*

- 16) Search further through the packets until you find a packet with an info field beginning **Create Response File: ;Find Response;**. This is packet is used by the server to transfer a list of the files contained in the folder to the client.
 - 17) Click on this packet, and read its contents in the Packet Data frame. You may have to scroll down to view all the data. You should see the file name Confidential.txt in the data.
 - 18) Search further through the packets until you find a packet with the info field **Read Response**, immediately after a Read Request for confidential.txt. This is packet is used by the server to transfer the file's contents to the client.
 - 19) Click on this packet, and read its contents in the Packet Data frame. Does the secret message appear in the data?



Viewing the contents of a file in a packet capture

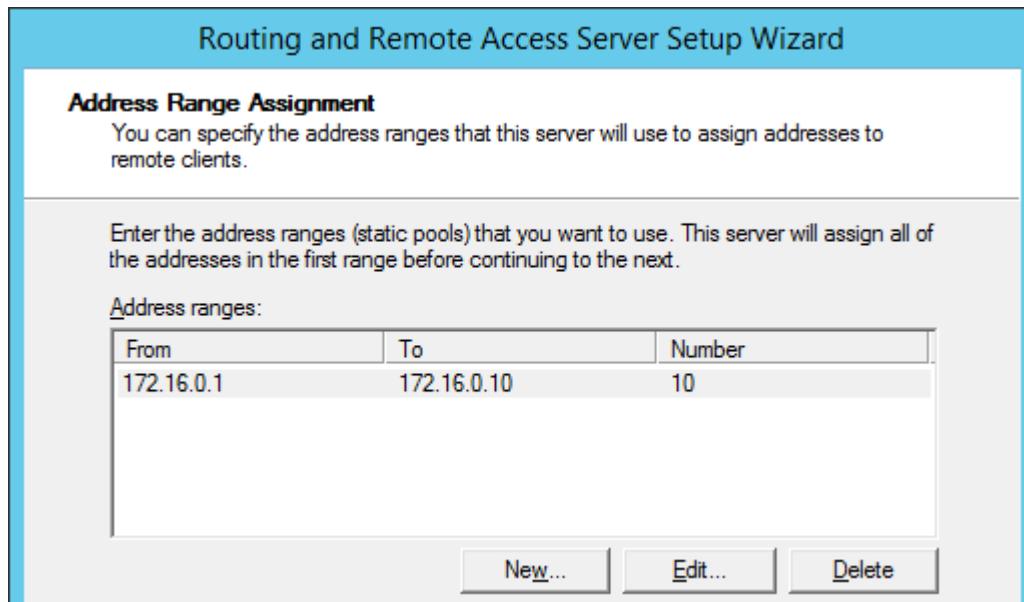
20) Close Wireshark, discarding the captured data.

Exercise 3: Configuring a VPN

We will now configure the SERVER VM to operate as a VPN gateway.

- 1) On the SERVER VM, from in **Server Manager**, select the **Dashboard** node then click the **Add roles and features** link. Complete the wizard by making the following choices:
 - o If the "Before you begin" page appears, click **Next**.
 - o On the "Select installation type" page, ensure **Role-based or feature-based installation** is selected, then click **Next**.
 - o On the "Select destination server" page, ensure **Select a server from the server pool** is selected, and **SERVER.classroom.local** is selected in the "Server Pool" list, then click **Next**.
 - o On the "Select server roles" page, tick the **Remote Access** check box and click **Next**.
 - o On the "Select features" page, click **Next**.
 - o On the "Remote Access" page, click **Next**.
 - o On the "Select role services" page, tick **DirectAccess and VPN (RAS)** then in the "Add Roles and Features" dialog, ensure that **Include management tools** is checked and click **Add Features**.
 - o On the "Select role services" page, click **Next**.
 - o On the "Confirm installation selection" page, click **Install**.

- 2) When installation is complete, click **Close**.
- 3) In **Server Manager**, select **Tools > Routing and Remote Access**.
- 4) Alt-click the **SERVER (local)** node and select **Configure and Enable Routing and Remote Access**. Complete the wizard by making the following choices:
 - On the "Welcome" page, click **Next**.
 - On the "Configuration" page, ensure **Remote access (dial-up or VPN)** is selected, then click **Next**.
 - On the "Remote Access" page, select the **VPN** checkbox, then click **Next**.
 - On the "VPN Connection" page, select **Ethernet** (the adapter configured with the 10.1.0.1 IP address), then click **Next**.
 - On the "IP Address Assignment" page, select **From a specified range of addresses**, then click **Next**.
 - On the "Address Range Assignment" page, click **New**.
 - Enter the start address **172.16.0.1** and the end address **172.16.0.10**. Click **OK**.



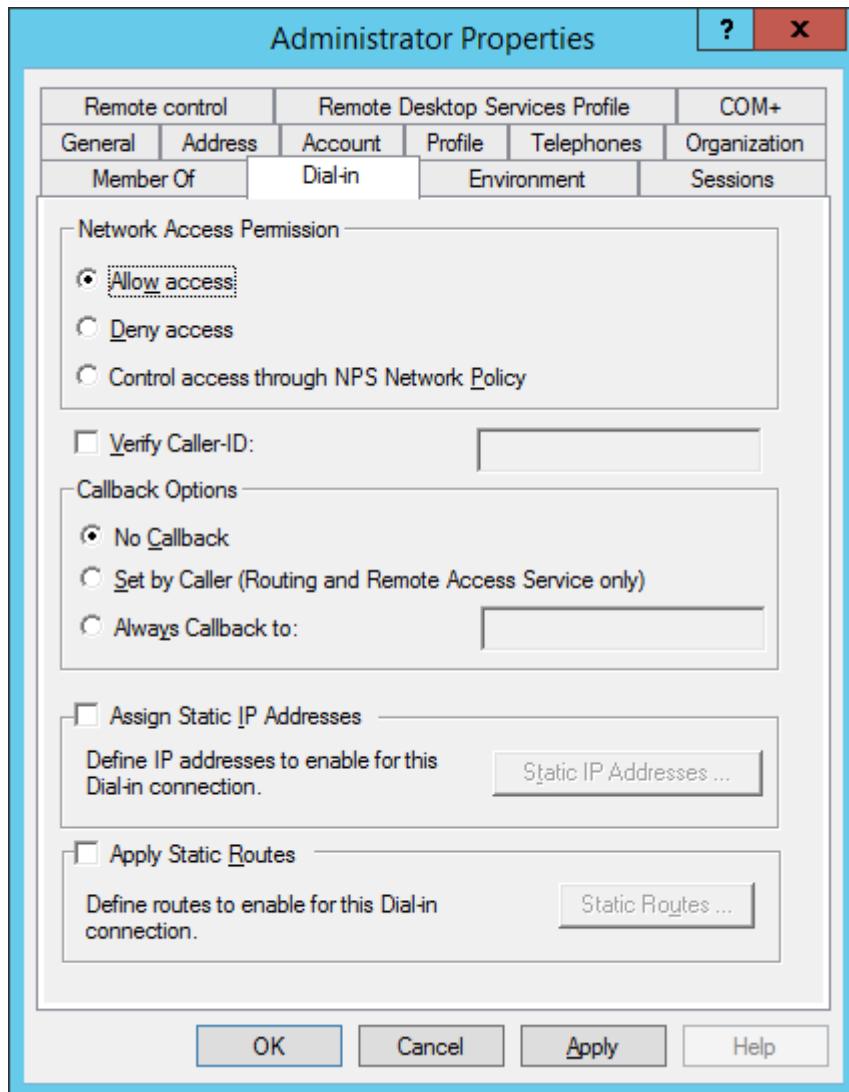
Configuring an address pool for remote clients

- On the "Address Range Assignment" page, click **Next**.
- On the "Managing Multiple Remote Access Servers" page, ensure **No, use Routing and Remote Access to authenticate connection requests** is selected, then click **Next** then **Finish**.
- 5) Read the warning about Windows Firewall then click **OK**.
- 6) Press **Start**, then type **Windows Firewall**, and click the **Windows Firewall with Advanced Security** icon.

- 7) Select the **Inbound Rules** node then in the middle pane, locate the **Routing and Remote Access (GRE-In)**, **(L2TP-In)**, and **(PPTP-In)** rules. Alt-click each rule and select **Enable Rule**.
- 8) Close the **Windows Firewall with Advanced Security** console.

The final step is to configure user rights to join the VPN. For this lab, we will simply enable dial-in rights for a user account.

- 9) Switch back to **Server Manager** and select **Tools >Active Directory Users and Computers**.
- 10) Expand **classroom.local** and select the **Users** node.
- 11) Double-click **Administrator** and select the **Dial-in** tab.
- 12) In the "Network Access Permission" pane, select **Allow access**, then click **OK**.

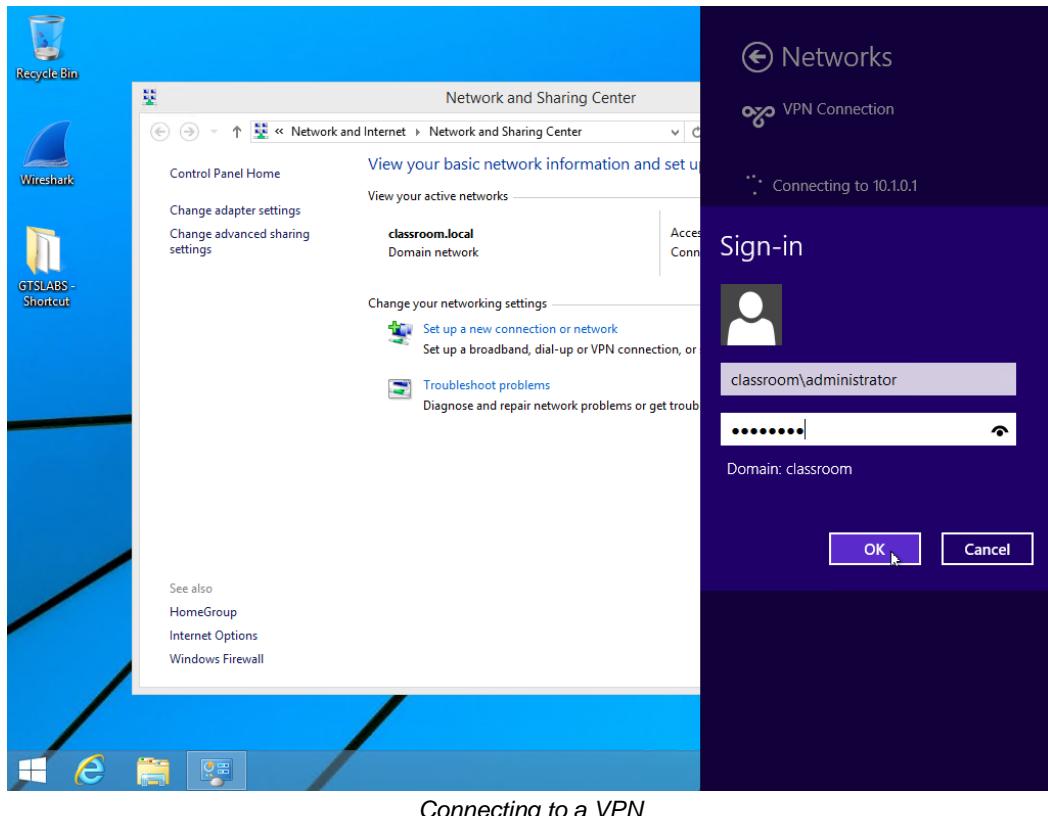


Configuring dial-in permission

Exercise 4: Joining a VPN

In this exercise you will connect to the VPN from the CLIENT PC.

- 1) On the **CLIENT** VM, alt-click the **Network** icon in the system notification area and select **Open Network and Sharing Center**.
- 2) Under "Change your network settings", click the **Set up a new connection or network** link. Complete the wizard by making the following choices:
 - o Select **Connect to a workplace** and click **Next**.
 - o Click **Use my Internet connection (VPN)**.
 - o If prompted, click **I'll set up an Internet connection later**.
 - o Under "Internet address", type **10.1.0.1**. Make sure that the **Remember my credentials** check box is ticked.
 - o Click **Create**.
- 3) In the **Networks** panel, click **VPN Connection** then click **Connect**.
- 4) Enter the user name as **CLASSROOM\Administrator** and the password as **Pa\$\$w0rd**, then click **OK**.



- 5) Click the **VPN Connection** icon again and select **Disconnect**.

Exercise 5: Examining VPN Traffic

In this exercise we will connect to the server via the VPN again and capture the authentication and data traffic generated to see whether any confidential information has been compromised.

- 1) On the CLIENT VM, run **Wireshark** from the desktop icon, and click the **Start Capture** button .

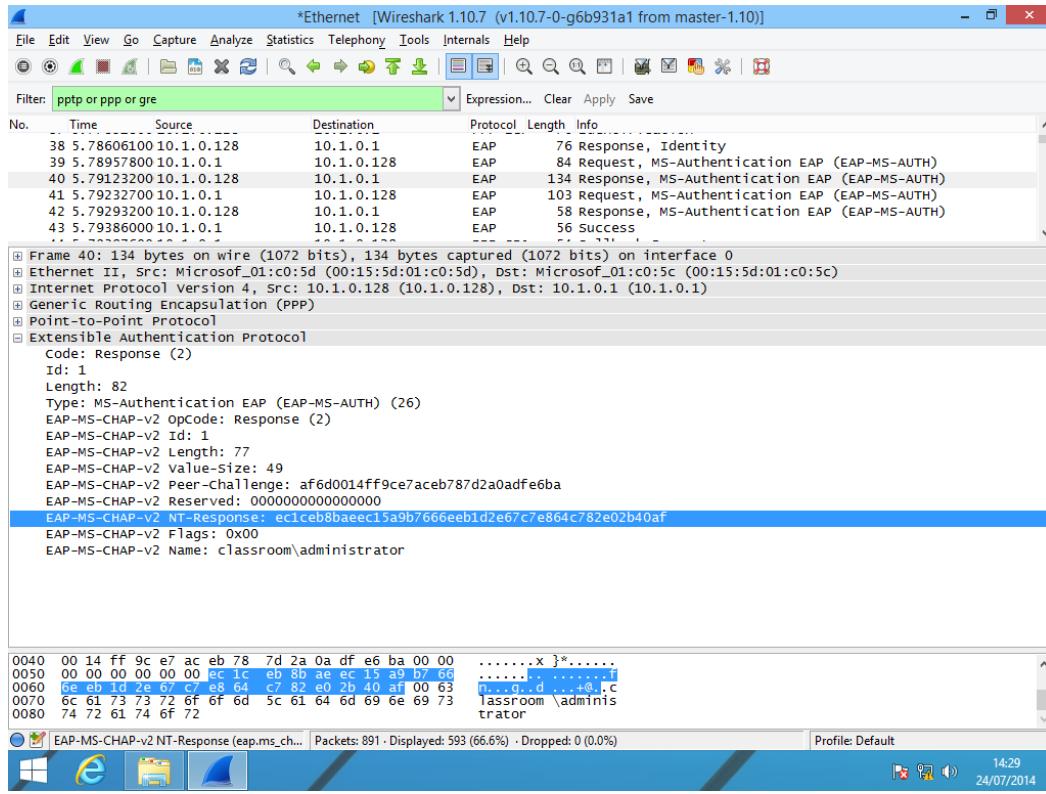
- 2) Click the **Network** icon then click the **VPN Connection** icon and select **Connect**.

You are not prompted for a user name and password as Windows has cached the credentials.

- 3) Open a **Run** dialog (**Start+R**) and enter `\\"172.16.0.1`
- 4) In the File Explorer window's address bar, enter `\\"172.16.0.1\\secret$`
- 5) Open the **CONFIDENTIAL** file and read the text. Close the file and the File Explorer window.

- 6) In Wireshark, click the **Stop Capture** button .

- 7) In the "Filter" box, type **pptp or ppp or gre** and click **Apply**.



- 8) Browse through the PPTP, PPP LCP, and EAP packets used to set up the tunnel and authenticate. What information is revealed?

- 9) Click the **Clear** button to remove the filter. Scroll down through the packet list pane. Are there any SMB packets?
-

- 10) Clicking through the individual PPP and GRE packets, can you see any intelligible data in the packet data pane?
-

Exercise 6: Completing the Lab

You need to discard some of the changes you made during this lab to the VMs' disk images.

- 1) On each VM, from the console window toolbar, select **Action > Revert**.



Make sure you choose "Revert". Take care NOT to select "Reset".

- 2) Confirm by clicking the **Revert** button.



Lab 9 / Telnet and FTP

Exercise 1: Configuring Telnet and FTP

Telnet and FTP are insecure protocols. To demonstrate this you will configure the Telnet and FTP services then connect to them, and view the data packets.

- 1) Start the **SERVER** VM and log on as **CLASSROOM\Administrator** (with the password **Pa\$\$w0rd**).
- 2) From **Server Manager**, click the **Add roles and features** link. Complete the wizard by making the following choices:
 - o If the "Before you begin" page appears, click **Next**.
 - o On the "Select installation type" page, ensure **Role-based or feature-based installation** is selected then click **Next**.
 - o On the "Select destination server" page, ensure **Select a server from the server pool** is selected, and **SERVER.classroom.local** is selected in the "Server Pool" list.
 - o Click **Next**.
 - o On the "Select server roles" page, expand **Web Server (IIS)** and select the **FTP Server** check box, then click **Next**.
 - o On the "Select features" page, select the **Telnet Server** check box, then click **Next**.
 - o On the "Confirm installation selection" page, click **Install**.
- 3) Wait for the installation to complete, then click **Close**.
- 4) In **Server Manager**, select **Tools > Services**.
- 5) Alt-click **Telnet** and select **Properties**. From the "Startup type" box, select **Manual** then click **OK**.
- 6) Alt-click **Telnet** again and select **Start**.
- 7) Using File Explorer, copy the **c:\GTLABS\ftproot** folder to **c:\inetpub**.
- 8) In **Server Manager**, select **Tools > Internet Information Services (IIS) Manager**.
- 9) Expand **SERVER (CLASSROOM\Administrator)**. If a dialog appears asking about Microsoft Web Platform, click **No**.
- 10) In the "SERVER Home" pane, double-click **FTP Authentication**.
- 11) Alt-click **Basic Authentication** then select **Enable**.

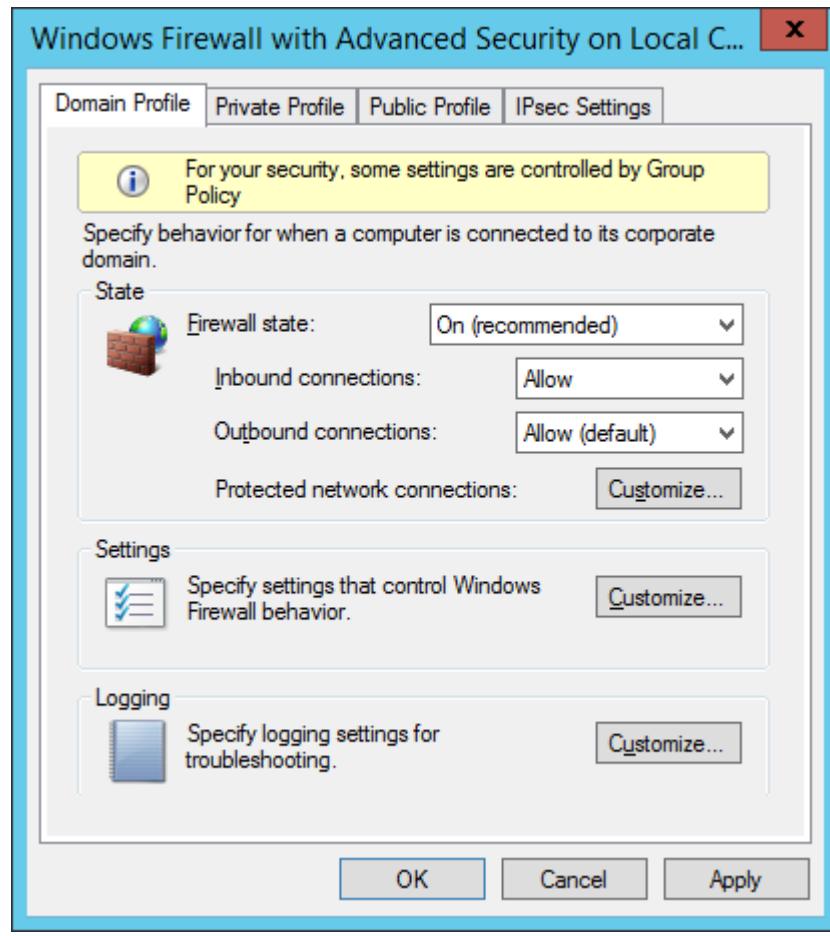
12) Alt-click the **Sites** node and select **Add FTP Site**. Complete the wizard by making the following choices:

- In the "FTP site name" box, enter **server.classroom.local**.
- Click the ... (browse) button, and browse to **c:\inetpub\ftproot**, then click **OK**. Click **Next**.
- On the "Binding and SSL Settings" page, select **No SSL**, then click **Next**.
- On the "Authentication and Authorization Information" page, select **All users** in the "Allow access to" dropdown, check the **Read** and **Write** boxes, and click **Finish**.

13) Click the **Start** button, then type **firewall**. Click the **Windows Firewall with Advanced Security** icon.

14) Alt-click on the **Windows Firewall with Advanced Security on Local Computer** node, and select **Properties**.

15) On the "Domain Profile" tab, select **Allow** in the **Inbound Connections** dropdown, then click **OK**.



Configuring Windows Firewall

Exercise 2: Examining Telnet Traffic

We will now connect to the Telnet service and examine the data packets that are produced.

- 1) Start the **CLIENT** VM and log in as **CLASSROOM\Administrator** (with the password **Pa\$\$w0rd**).
 - 2) On the Start Screen, type **windows features** and click the **Turn Windows features on or off** icon.
 - 3) Select the **Telnet Client** checkbox, then click **OK**.
 - 4) Wait for the installation to complete, then click **Close**.
 - 5) Run **Wireshark** from the desktop icon. When the program has loaded, click the **Start Capture** button .
 - 6) Open a command prompt window, and enter the following command:
telnet server.classroom.local
 - 7) Wait for the welcome message to appear, and note the escape character sequence.
-

- 8) When asked whether you want to continue with automatic authentication, type **n** and press **Enter**.
- 9) At the "login:" prompt, type **administrator** and press **Enter**.
- 10) At the password: prompt, type **Pa\$\$w0rd** and press **Enter**.
- 11) Enter the command **dir**, to confirm that you have connected to the server and are able to execute commands successfully.
- 12) Press the escape sequence previously noted.
- 13) At the "Microsoft Telnet>" prompt, type **quit**
- 14) Close the command prompt window.

- 15) In Wireshark, click the **Stop Capture** button . Resize the panes so that the Packet List (top) and Packet Data (bottom) panes are more clearly visible.
- 16) In the "Filter" box, type **telnet** and press **Enter**.
- 17) Use the cursor keys to scroll down through the telnet data packets, watching the text data in the Packet Data pane, until you find a packet ending in the text "login:"

*Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: telnet Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
17	28.8063240	10.1.0.1	10.1.0.129	TELNET	75	Telnet Data ...
18	28.8064780	10.1.0.129	10.1.0.1	TELNET	57	Telnet Data ...
19	28.8066610	10.1.0.1	10.1.0.129	TELNET	62	Telnet Data ...
20	28.8066830	10.1.0.129	10.1.0.1	TELNET	81	Telnet Data ...
21	28.8079200	10.1.0.1	10.1.0.129	TELNET	69	Telnet Data ...
23	36.6334260	10.1.0.129	10.1.0.1	TELNET	62	Telnet Data ...
24	36.6347170	10.1.0.1	10.1.0.129	TELNET	92	Telnet Data ...
25	36.6347510	10.1.0.129	10.1.0.1	TELNET	99	Telnet Data ...
26	36.6350150	10.1.0.1	10.1.0.129	TELNET	63	Telnet Data ...
28	38.0254370	10.1.0.129	10.1.0.1	TELNET	55	Telnet Data ...
29	38.0256550	10.1.0.1	10.1.0.129	TELNET	55	Telnet Data ...
31	38.2172540	10.1.0.129	10.1.0.1	TELNET	55	Telnet Data ...
32	38.2174610	10.1.0.1	10.1.0.129	TELNET	55	Telnet Data ...
34	38.3772230	10.1.0.129	10.1.0.1	TELNET	55	Telnet Data ...
35	38.3773810	10.1.0.1	10.1.0.129	TELNET	55	Telnet Data ...

Frame 26: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on interface 0
 Ethernet II, Src: Microsoft_01:c0:4c (00:15:5d:01:c0:4c), Dst: Microsoft_01:c0:4d (00:15:5d:01:c0:4d)
 Internet Protocol Version 4, Src: 10.1.0.1 (10.1.0.1), Dst: 10.1.0.129 (10.1.0.129)
 Transmission Control Protocol, Src Port: telnet (23), Dst Port: 49200 (49200), Seq: 103, Ack: 84, Len: 9
 Telnet
 Data: \n
 Data: \rlogin:

0000 00 15 5d 01 c0 4d 00 15 5d 01 c0 4c 08 00 45 00 .].M..].L..E.
 0010 00 31 4c e1 40 00 80 06 99 62 9a 01 00 01 0a 01 .l. @... b.....
 0020 00 81 00 17 c0 30 35 9d df ee bb f5 86 bd 50 18o.....P.
 0030 02 00 14 99 00 00 0a 0d 6c 6f 67 69 6e 3a 20:Login:

Data (telnet.data), 8 bytes Packets: 130 - Displayed: 63 (48.5%) · Dropped: 0 (0.0%) Profile: Default

Locate the Telnet packet that starts the login process

- 18) From this packet, scroll through the next 26 packets, making a note of the final text character in the Packet Data pane of each frame.



Note that the frames are in pairs, the first of each pair coming from the client, and the second from the server. You need only note each character once.

- 19) Next, use the cursor keys to scroll further through the telnet data packets, watching the text data in the Packet Data pane, until you find a packet ending in the text "password:". It should follow almost immediately after the 26 packets you just examined.
- 20) From this packet, scroll through the next 8 packets, making a note of the final text character in the Packet Data pane of each frame.
-
- 21) Examine the contents of the final captured telnet data packet. Can you gain any information from its contents?
-

Exercise 3: Examining FTP Traffic

Next, we will connect to the FTP service and examine the contents of the data packets.

- 1) In Wireshark, click the **Clear** button to remove the contents of the "Filter" box.
- 2) Click the **Start Capture** button  and select **Continue without Saving** to discard the previous capture.
- 3) Open a **Run** dialog, and type `ftp://server`
- 4) In the **Internet Explorer** login dialog, enter **Administrator** as the user name and **Pa\$\$w0rd** as the password, then click **Log on**.
- 5) Click on the **Contact.rtf** link, then click **Open** when prompted.
- 6) Close WordPad and Internet Explorer.

- 7) In Wireshark, click the **Stop Capture** button .
- 8) In the "Filter" box, type `ftp` and press **Enter**.
- 9) Use the cursor keys to scroll down through the ftp packets, paying particular attention to packets where the info field starts "Request: USER"



You will see that Internet Explorer has made several attempts to authenticate anonymously, but these attempts are rejected.

- 10) Find the first "Request: USER" packet where the user name is not "anonymous". Note the user name.
-

- 11) Examine the next two packets following this. Note the password in the "Request: PASS" packet.
-

- 12) Change the contents of the "Filter" box to `ftp-data` and press **Enter**. There should now be only two packets displayed.

- 13) Examine the contents of the first ftp-data packet in the Packet Data pane. What does this packet contain?
-

- 14) Examine the contents of the second ftp-data packet in the Packet Data pane. What does this packet contain?
-

Exercise 4: Completing the Lab

You need to discard some of the changes you made during this lab to the VMs' disk images.

- 1) On each VM, from the console window toolbar, select **Action > Revert**.



Make sure you choose "Revert". Take care NOT to select "Reset".

- 2) Confirm by clicking the **Revert** button.



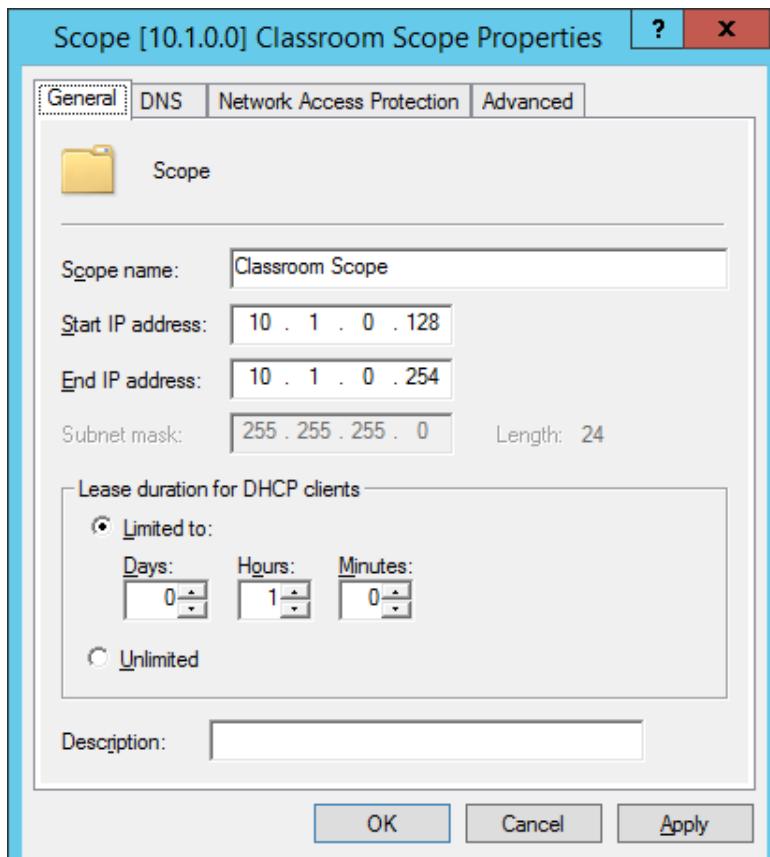
Lab 10 / Attacks Against DHCP and DNS

Attacks against core network services such as DHCP and DNS can represent powerful exploits. In this lab, we will use a rogue DHCP server to misconfigure DNS settings on clients, thereby gaining the ability to hijack other services. We will demonstrate this by a website defacing attack, but it could as easily be used to facilitate a Man in the Middle attack against web services.

Exercise 1: Setting Up the Scenario

In this scenario, the SERVER VM will play the role of a busy DHCP and DNS server in a network with lots of mobile clients (thus short DHCP lease times, and no expectation of clients maintaining the same IP address over multiple visits). It will also host the website to be attacked, although in a real-world situation this website could be anywhere on the internet.

- 1) Start the **SERVER** VM and log on as **CLASSROOM\Administrator** (with the password **Pa\$\$w0rd**).
- 2) In **Server Manager**, select **Tools > DHCP**.
- 3) When the DHCP console opens, expand the **server.classroom.local** node, then expand **IPv4**.
- 4) Click on the **Scope [10.1.0.0] Classroom scope** node, then alt-click this node, and select **Properties**.



Configuring DHCP lease duration

- 5) On the **General** tab, under "Lease duration for DHCP clients", set **Days** to 0 and **Hours** to 1.
- 6) On the **Advanced** tab, under "Delay configuration", set **Subnet delay** to 100, then click **OK**.
- 7) Using File Explorer, copy the **c:\GTSLABS\wwwroot** folder to **c:\inetpub**.

Exercise 2: Preparing the Attack

Now that the scenario is in place, we will first connect to the website, then create and modify a copy, and then use an open source DHCP and DNS server to redirect traffic to our modified site.

- 1) Start the **ROGUE** VM and log on as **Admin** (with the password **Pa\$\$w0rd**).
- 2) Using File Explorer, browse to the **c:\GTSLABS** folder and create a subfolder called **website**.
- 3) Open Internet Explorer, and connect to the server using the address **http://server.classroom.local**.
- 4) Click on the tools icon  and select **File > Save as**.
- 5) Ensure that the "Save as type" list box is set to **Webpage, complete (*.htm, *.html)**, then browse to the **c:\GTSLABS\website** folder. Enter the file name **default.htm** and click **Save**.
- 6) In File Explorer, navigate to the **c:\GTSLABS\website** folder. Alt-click the **Default HTML Document** file, and select **Open with > Notepad**.
- 7) Make any changes you wish to the text of the document, and save the file.



This is a particularly unsophisticated attack. In real-world applications, attackers may redirect links or embed malicious code in the page.

- 8) Alt-click the **Network** icon in the system notification area, and select **Open Network and Sharing Center**.
- 9) In the **Network and Sharing Center** window, click the **Ethernet** link.
- 10) In the **Ethernet Status** dialog, click the **Properties** button.
- 11) Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
- 12) Select **Use the following IP address**, and set the **IP address** to **10.1.0.10** and the **Subnet mask** to **255.255.255.0**.
- 13) Set the **Preferred DNS server** to **10.1.0.10**, and ensure **Validate settings upon exit** is unchecked, then click **OK**.

- 14) In the **Ethernet Properties** dialog, click **OK**, then close the **Ethernet Status** dialog and the **Network and Sharing Center** window.
- 15) Click the **Start** button, type **windows features** and click the **Turn Windows features on or off** icon.
- 16) Select the **Internet Information Services** check box. A square dot appears in it, indicating that only some of the components will be installed. Click **OK**.
- 17) When the installation has completed, click **Close**.
- 18) Click the **Start** button, type **iis** and click the **Internet Information Services (IIS) Manager** icon.
- 19) If a dialog appears asking about Microsoft Web Platform, click **No**.
- 20) Navigate to **ROGUE (ROGUE\Admin) > Sites > Default Web Site**.
- 21) In the "Actions" pane, click the **Basic Settings** link.
- 22) Click the ... (browse) button next to "Physical path". Select the **c:\GTSLABS\website** folder, then click **OK**.
- 23) In the "Edit Site" dialog, click **OK** to confirm the new location.
- 24) In File Explorer, navigate to the **c:\GTSLABS** folder and run **DualServerInstallerV7.12**.
- 25) Click **Yes** to confirm the **User Account Control** dialog.
- 26) Complete the installation using the default settings.
- 27) Using File Explorer, copy the **DualServer** configuration settings file from the **c:\GTSLABS** folder to **c:\DualServer**, choosing to replace the existing file.



Configuration of DualServer is a relatively complex procedure, compared with native Windows services and beyond the scope of this lab. The DualServer.ini file contains the appropriate settings for the exploit used in the lab. If you are familiar with DHCP and DNS configuration concepts, feel free to review the contents of the file.

- 28) Click the **Start** button, type **services** and click the **View local services** icon.
- 29) Alt-click **Dual DHCP DNS Service** and select **Start**.

Exercise 3: Falling for the Attack

We will now start the CLIENT VM and check whether it has been caught by the exploit. Windows clients use an inbuilt mechanism to try to maintain their previously used IP address, so it may not be captured straight away. In a busy environment with lots of clients and a high turnover of IP addresses, this mechanism is likely to fail. However, in the lab setup, we may have to force CLIENT to forget its old IP address in order for the exploit to work.

- 1) Start the **CLIENT** VM and log on as **CLASSROOM\Administrator** (with the password **Pa\$\$w0rd**).
- 2) From the desktop, alt-click the **Network** icon in the system notification area, and select **Open Network and Sharing Center**.
- 3) In the **Network and Sharing Center** window, click the **Ethernet** link.
- 4) In the **Ethernet Status** dialog, click the **Details** button.
- 5) If the final octet of the "IPv4 Address" is less than 128, then skip to the next numbered step; otherwise, complete the following sub-steps to renew the lease.
 - Click the **Start** button, type **services** and click the **View local services** icon.
 - Alt-click **DHCP Client** and select **Restart**.
 - Click **Yes** to confirm restarting dependent services.
 - Open an elevated command prompt and run **ipconfig** to check the IPv4 address.



The authorized DHCP server for the network is configured with a scope beginning 10.1.0.128. Any IP addresses lower than this were not issued by this server.

- 6) Open Internet Explorer, and attempt to connect to the server using the address **http://server.classroom.local**. Which version of the website do you see, and why?
-

Exercise 4: Completing the Lab

You need to discard some of the changes you made during this lab to the VMs' disk images.

- 1) On each VM, from the console window toolbar, select **Action > Revert**.
- 2) Confirm by clicking the **Revert** button.



Lab 11 / Network Access Protection

In this lab, you will install Windows' Network Access Protection feature to investigate the features of a Network Access Control (NAC) solution.

Exercise 1: Installing Network Access Protection

In this exercise, you will configure SERVER with the Network Access Protection role. As this role relies on Certificate Services, we must first configure a certification authority.

- 1) Start the **SERVER** VM and log on as **CLASSROOM\Administrator** (with the password **Pa\$\$w0rd**).
- 2) From **Server Manager**, click the **Add roles and features** link. Complete the wizard by making the following choices:
 - If the "Before you begin" page appears, click **Next**.
 - On the "Select installation type" page, ensure **Role-based or feature-based installation** is selected, then click **Next**.
 - On the "Select destination server" page, ensure **Select a server from the server pool** is selected, and **SERVER.classroom.local** is selected in the "Server Pool" list, then click **Next**.
 - On the "Select server roles" page, tick the **Active Directory Certificate Services** check box.
 - In the "Add Roles and Features Wizard" dialog, ensure the **Include management tools (if applicable)** check box is ticked, then click the **Add Features** button.
 - On the "Select server roles" page, click **Next**.
 - On the "Select features" page, click **Next**.
 - On the "Active Directory Certificate Services" page, click **Next**.
 - On the "Select role services" page, click **Next**.
 - On the "Confirm installation selection" page, click **Install**.
- 3) When the installation has completed, click **Close**.
- 4) In Server Manager, select the **AD CS** node.
- 5) Click the **More** link next to the "Configuration required for Active Directory Certificate Services on SERVER" alert.

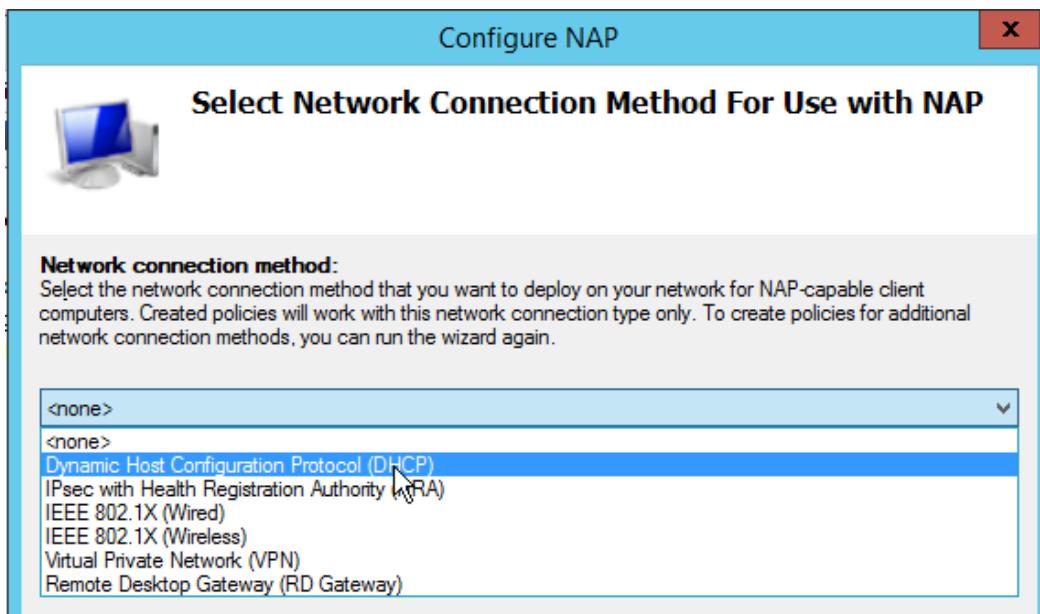
- 6) In the "All Servers Task Details" window, click the **Configure Active Directory Certificate Services** link. Complete the wizard by making the following choices:
 - On the "Credentials" page, click **Next**.
 - On the "Role Services" page, tick the **Certification Authority** check box, then click **Next**.
 - Select the default options for the remainder of the wizard by clicking **Next** then **Configure** at the end.
- 7) Click **Close** when the operation has completed.
- 8) Close the **All Servers Task Details** window.
- 9) In Server Manager, select the **Dashboard** node, then click the **Add roles and features** link. Complete the wizard by making the following choices:
 - If the "Before you begin" page appears, click **Next**.
 - On the "Select installation type" page, ensure **Role-based or feature-based installation** is selected, then click **Next**.
 - On the "Select destination server" page, ensure **Select a server from the server pool** is selected, and **SERVER.classroom.local** is selected in the "Server Pool" list, then click **Next**.
 - In the "Select server roles" page, tick the **Network Policy and Access Services** check box.
 - In the "Add Roles and Features Wizard" dialog, ensure the **Include management tools (if applicable)** check box is ticked, then click the **Add Features** button.
 - On the "Select server roles" page, click **Next**.
 - On the "Select features" page, click **Next**.
 - On the "Network Policy and Access Services" page, click **Next**.
 - On the "Select role services" page, ensure the **Network Policy Server** check box is selected, then select the **Health Registration Authority** check box.
 - In the "Add Roles and Features Wizard" dialog, ensure the **Include management tools (if applicable)** check box is ticked, then click the **Add Features** button.
 - On the "Select role services" page, click **Next**.
 - On the "Certification Authority" page, select **Use the local CA to issue health certificates for this HRA server**, then click **Next**.
 - On the "Authentication Requirements" page, select **No, allow anonymous requests for health certificates**, then click **Next**.

- On the "Server Authentication Certificate" page, ensure **Choose an existing certificate for SSL encryption** is selected, then click **Next**.
 - On the "Confirm installation options" page, click **Install**.
- 10) When the installation has completed, click **Close**.

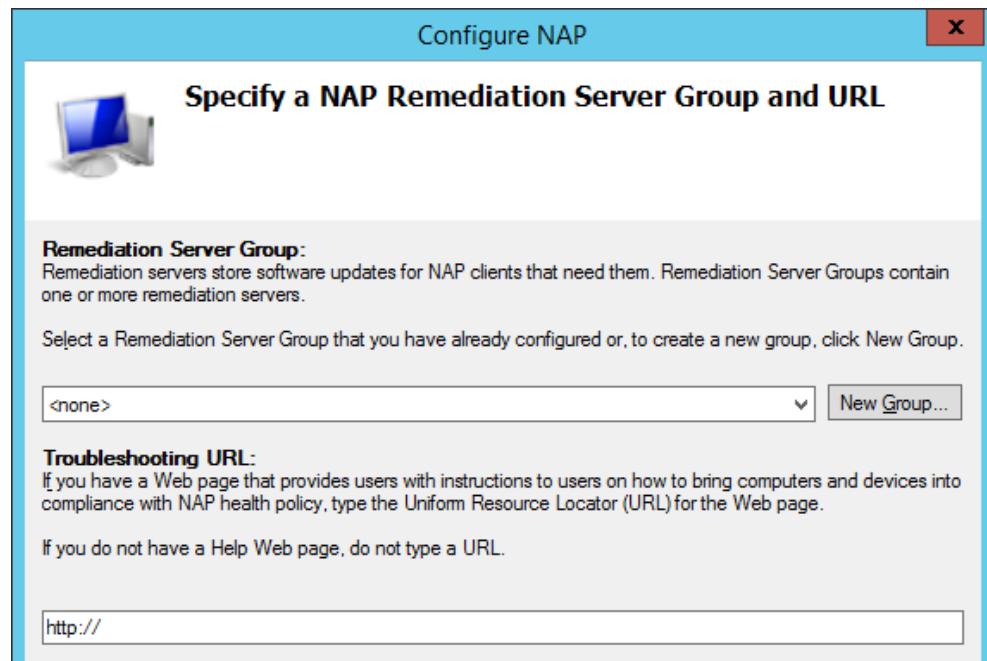
Exercise 2: Configuring Network Access Protection

In this exercise you will configure NAP admission control settings and health policies.

- 1) In **Server Manager**, select **Tools > Network Policy Server**.
- 2) In the **Network Policy Server** window, click the **Configure NAP** link.
Complete the wizard by making the following choices:
 - Under "Network connection method", select **Dynamic Host Configuration Protocol (DHCP)**. Click **Next**.

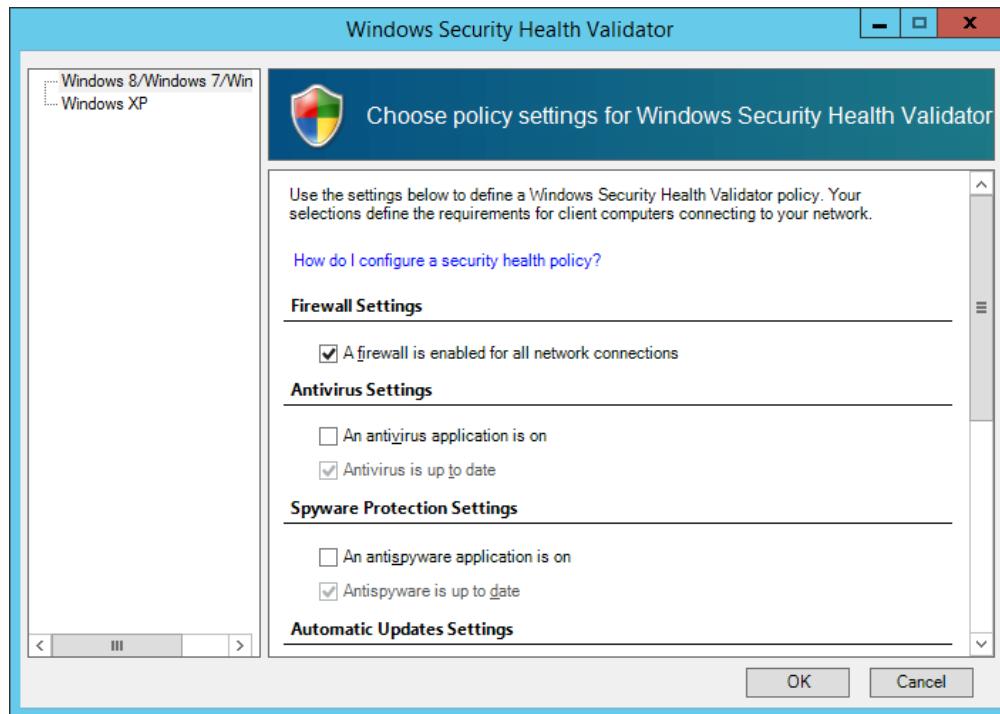


- On the "RADIUS Clients" page, click **Next** (this is the only server accepting authentication requests).
- On the "DHCP Scopes" page, click **Next** (to check all scopes).
- On the **Machine Groups** page, click **Next** (to apply the policy to all users).
- Note the options for creating a remediation portal. This would contain servers that allow the client to access patches and anti-virus software or updates that can allow them to pass the health policy. Click **Next**.



NAP remediation options

- On the **NAP Health Policy** page, note that the default option is "deny all", unless the computer passes the health policy. Leave this selected and click **Next**.
 - Click **Finish**.
- 3) Navigate to **NPS (Local) > Network Access Protection > System Health Validators > Windows Security Health Validator > Settings**.
- 4) Alt-click **Default Configuration** and select **Properties**.



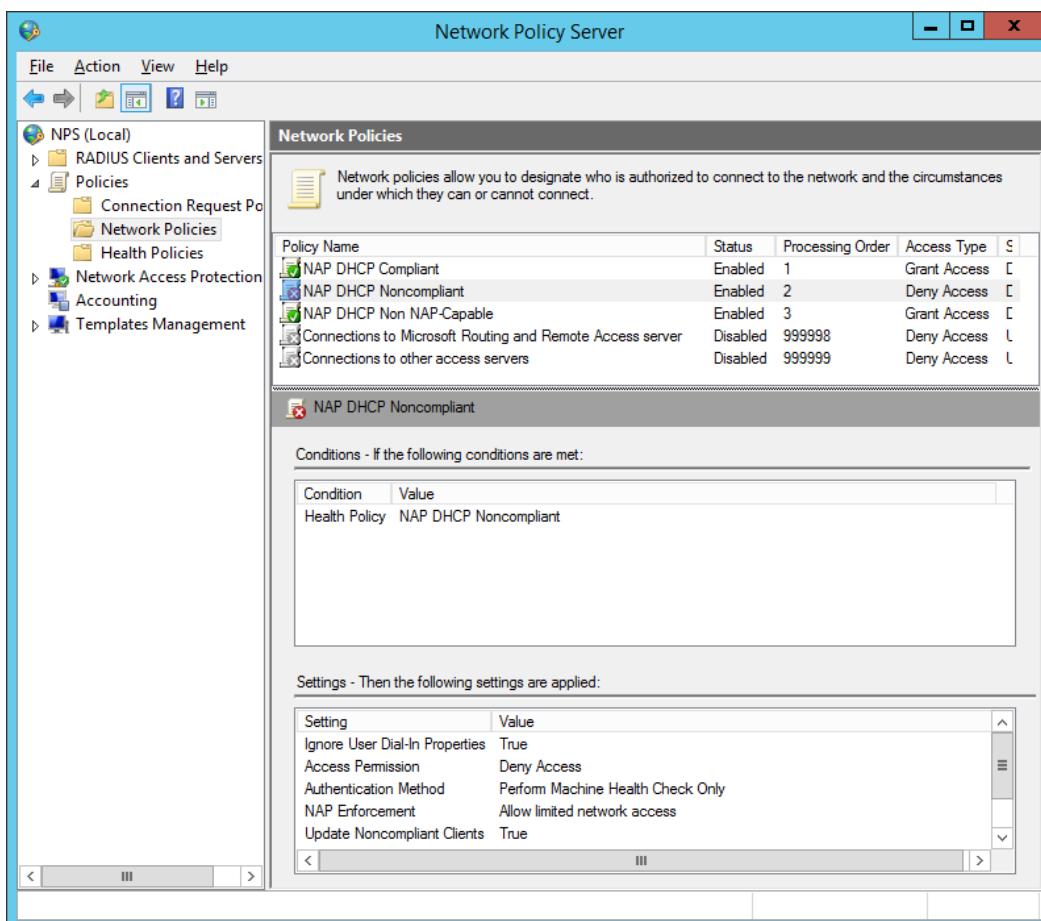
NAP policy settings for a Windows client

Note that this validator only works for Windows clients. By default, the clients must have a firewall, anti-virus, and automatic updating enabled. Note that you can also require clients to have updated to the latest patches.

- 5) Uncheck all the options except for "A firewall is enabled". Click **OK**.

Ideally you would configure a remediation portal to deal with non-compliant non NAP-capable clients but for this exercise we will simply deny them access.

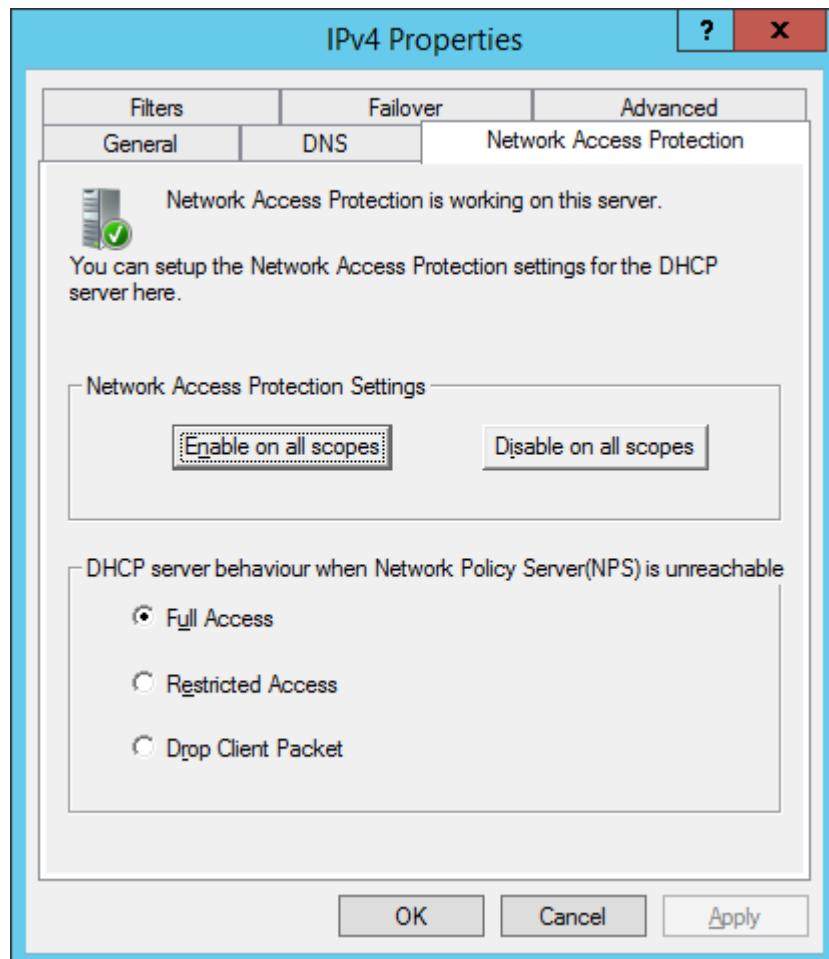
- 6) Expand **NPS (Local) > Policies > Network Policies**.
- 7) Double-click **NAP DHCP Noncompliant**. Select **Deny access** then click **OK**.
- 8) Alt-click the **Connections to Microsoft Routing and Remote Access server** policy and select **Disable**.
- 9) Alt-click the **Connections to other access servers** policy and select **Disable**.



Configuring network policies to allow or deny access to compliant and non-compliant clients

- 10) Select the **Connection Request Policies** node. Alt-click **Use Windows authentication for all users** and select **Disable**.
- 11) Click the **Accounting** node. Note that NPS is configured to log events to a text file.

- 12) In **Server Manager**, select **Tools > DHCP**.
- 13) When the DHCP console opens, expand the **server.classroom.local** node, then click on the **IPv4** node.
- 14) Alt-click **IPv4** and select **Properties**.
- 15) Select the **Network Access Protection** tab. Click **Enable on all scopes** and click **Yes**, then click **OK**.



Configuring NAP on the DHCP server

Exercise 3: Configuring a NAP Client

Having configured a policy and a network connection server (the DHCP server), the final step is to ensure that the NAP client is deployed to client machines in the domain.

- 1) Switch back to **Server Manager** and select **Tools > Group Policy Management**.
- 2) Expand **Forest > Domains > classroom.local**. Alt-click **classroom Domain Policy** and select **Edit**.
- 3) Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Network Access Protection > NAP Client Configuration > Enforcement Clients**.

- 4) Alt-click **DHCP Quarantine Enforcement Client** and select **Enable**.
- 5) Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > System Services** then double-click **Network Access Protection Agent**.
- 6) Check the **Define this policy setting** box and select the **Automatic** option button. Click **OK**.
- 7) Navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > Security Center**.
- 8) Double-click **Turn on Security Center**. Select **Enabled** then click **OK**.
NAP alerts are displayed via the Action (Security) Center.
- 9) Close the GPO windows.
- 10) In an elevated command prompt window, run **gpupdate /force**.

Exercise 4: Testing Network Access Protection

In this exercise, you will test NAP by trying to connect a Windows domain client to the network.

- 1) Start the **CLIENT** VM and log on as **CLASSROOM\Administrator** (with the password **Pa\$\$w0rd**).
- 2) Open a command prompt and run **ipconfig /release** then **ipconfig /renew**.

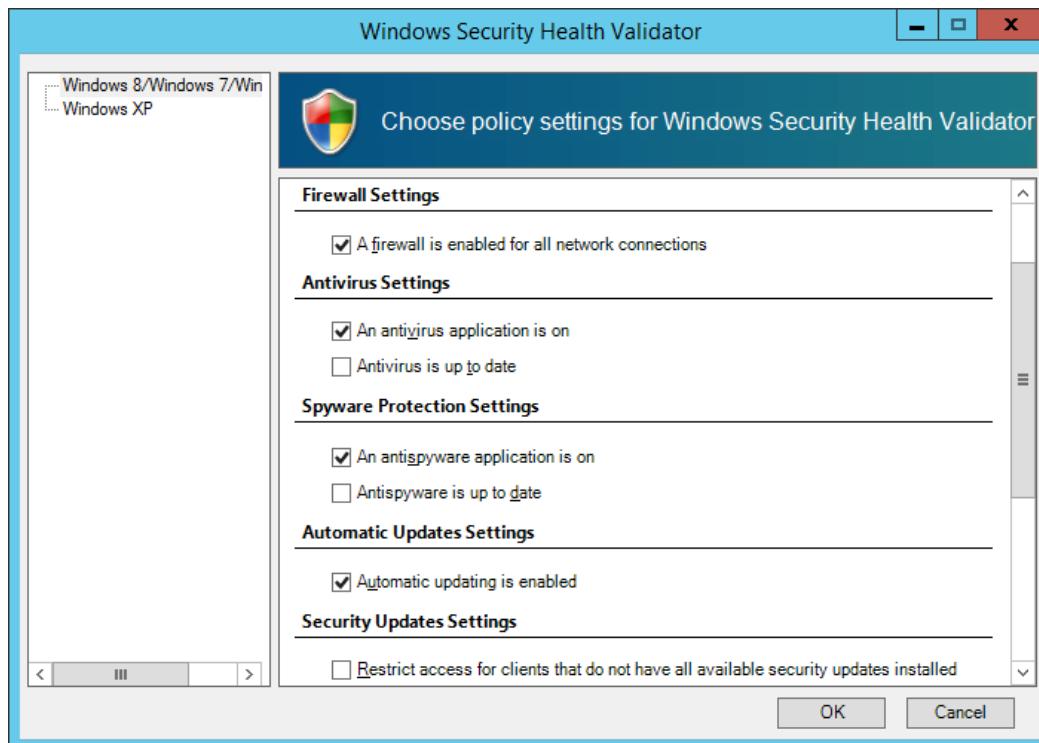
You should still have access to the DHCP server and obtain a lease for a 10.1.0.0/24 address.



*This should work. If it does not, try **ipconfig /renew** again or restart the **CLIENT** VM.*

- 3) Press **Start**, type **action center**, then click the **Action Center** icon.
Observe the alerts (it may take a minute or two for more to appear).
- 4) Alt-click the **Start** button and select **Event Viewer**. Expand **Applications and Services > Microsoft > Windows > Network Access Protection > Operational**. Note that the logs show the NAP server sending system health policies to the client and the client responding with health statements.
- 5) Switch to the **SERVER** VM. In **Server Manager**, from the **Tools** menu, select **Event Viewer**. Expand **Windows Logs > Security**. Look for "Audit Success" logs for the "Network Policy Server" category (event ID 6278).
- 6) In **Server Manager**, from the **Tools** menu, select **Network Policy Server**. Expand **Policies > Network Policies**.

- 7) Double-click **NAP DHCP Non NAP-Capable**. Select the **Deny access** radio button and click **OK**.
- 8) Navigate to **NPS (Local) > Network Access Protection > System Health Validators > Windows Security Health Validator > Settings**.
- 9) Alt-click **Default Configuration** and select **Properties**.



Reconfiguring NAP policy settings for a Windows client

- 10) Check all the boxes for firewall, antivirus, spyware, and automatic updates but then uncheck the "up to date" boxes. Click **OK**.
- 11) Switch back to the CLIENT VM. At an elevated command prompt, use **ipconfig /release** and **ipconfig /renew** to try to obtain an address. What happens?

- 12) Open the Action Center and remediate all the critical alerts (by activating Defender, Automatic Update, and so on).
- 13) Try to obtain a new DHCP lease again.



This should work. If it does not, try ipconfig /renew again or restart the CLIENT VM.

- 14) Observe the events in the **Network Access Protection (Operational)** log again.
- 15) On the **SERVER** VM, observe the Network Policy Server category events in the **Security** log.

Exercise 5: Circumventing Network Access Protection

In this exercise, we will show a PC can be connected to the network even if it does not meet the health policy.

- 1) Start the **ROGUE** VM and log on as **Admin** (with the password **Pa\$\$w0rd**).
 - 2) Attempt to ping SERVER, then check your IP address. What happens, and why?
-
- 3) Open ROGUE's network properties and change to a static IP configuration:
 - IP address: **10.1.0.10**
 - Subnet mask: **255.255.255.0**
 - Default gateway: **10.1.0.1**
 - DNS: **10.1.0.1**
 - 4) Try to ping the SERVER and browse network resources.

You can join the network simply by specifying a static IP address. DHCP is not really the best place for policy enforcement. It is better to perform validation at the switch (for local clients) or remote access server (for remote clients).

Exercise 6: Completing the Lab

You need to discard some of the changes you made during this lab to the VMs' disk images.

- 1) On each VM, from the console window toolbar, select **Action > Revert**.
- 2) Confirm by clicking the **Revert** button.



Lab 12 / Data Leakage Prevention

Data Leakage (or Loss) Prevention allows users to tag digital data with a security classification. The system then enforces rules to control the way that data may be used (in terms of printing, copying, and so on).

Exercise 1: Installing Rights Management Services

- 1) Start the **SERVER** VM and log on as **CLASSROOM\Administrator** (with the password **Pa\$\$w0rd**).
- 2) In **Server Manager**, select **Tools > Active Directory Users and Computers** tool. Expand **classroom.local**, alt-click the **Users** folder, and select **New > User**.
- 3) Set the first name, full name and user name to **ADRMS**, and the password to **Pa\$\$w0rd**. Uncheck **User must change password at next logon**.
- 4) Open the **Users** folder. Alt-click the **ADRMS** user object and select **Add to a group**. Type the group name **Domain Admins** then click **Check Names**. Click **OK**. Click **OK** again to confirm.
- 5) From **Server Manager**, click the **Add roles and features** link. Complete the wizard by making the following choices:
 - o If the "Before you begin" page appears, click **Next**.
 - o On the "Select installation type" page, ensure **Role-based or feature-based installation** is selected, then click **Next**.
 - o On the "Select destination server" page, ensure **Select a server from the server pool** is selected, and **SERVER.classroom.local** is selected in the "Server Pool" list, then click **Next**.
 - o On the "Select server roles" page, tick the **Active Directory Rights Management Services** check box.
 - o In the "Add Roles and Features Wizard" dialog, ensure the **Include management tools (if applicable)** check box is ticked, then click the **Add Features** button.
 - o Click **Next** through the rest of the wizard until you get to the "Confirm installation selection" page, then click **Install**.
- 6) Wait for the installation to complete, then click **Close**.
- 7) In Server Manager, select the **AD RMS** node.
- 8) Click the **More** link next to the "Configuration required for Active Directory Rights Management Services on SERVER" alert.

- 9) In the **All Servers Task Details** window, click the **Perform additional configuration** link. Complete the wizard by making the following choices:
 - On the "AD RMS" and "AD RMS Cluster" pages, click **Next**.
 - On the "Configuration Database" page, select **Use Windows Internal Database on this server**, then click **Next**.
 - On the "Service Account" page, click the **Specify** button then enter the name **ADRMS** and the password **Pa\$\$w0rd**.
 - Click **OK** then **Next**.
 - On the "Cryptographic Mode" and "Cluster Key Storage" pages, click **Next**.
 - On the "Cluster Key Password" page, use **Pa\$\$w0rd** again, then click **Next** (anyone breaking into this network is going to have a field day).
 - On the "Cluster Web Site" page, click **Next**.
 - On the "Cluster Address" page, select **Use an unencrypted connection** and enter **server.classroom.local** as the "Fully-Qualified Domain Name", then click **Next**.
 - Enter the name **SERVER** and click **Next**.
 - Click **Next** through the final screens of the wizard then click **Install**.
- 10) When installation is complete, click **Close**, then restart the server.

Exercise 2: Exploring DLP Options

While it is beyond the scope of this lab to fully implement DLP (in terms of issuing licenses to users and installing compatible applications such as Microsoft Office), you can configure a typical policy template.

- 1) Sign back in as **CLASSROOM\Administrator** then in Server Manager, select **Tools > Active Directory Rights Management Services**.
- 2) Expand the server and select **Rights Policy Templates**.
- 3) Click the **Create Distributed Rights Policy Template** link. Complete the wizard by making the following choices:
 - Click the **Add** button then type the "Name" **classroom** and "Description" **Default policy** and click **Add**.
 - Click **Next** then click the **Add** button.
 - Type **editors@classroom.local** then click **OK**.
 - Check all the rights boxes apart from "Full Control".
 - Add a **reviewers@classroom.local** group with "View" and "Print" rights only, then click **Next**.

- 4) Note that you can expire content (documents) or user licenses. Check the **Expires after the following duration** box and change the time to 365.
- 5) Click **Next** to view the other options then click **Finish**.

Exercise 3: Completing the Lab

You need to discard some of the changes you made during this lab to the VM's disk image.

- 1) From the console window toolbar, select **Action > Revert**.
- 2) Confirm by clicking the **Revert** button.



Lab 13 / HTTP and HTTPS

HTTP transfers are all in plain text or use simple encoding methods. This makes the protocol extremely vulnerable to packet sniffing. HTTP transfers can be protected by encrypting them with SSL/TLS (though even this is vulnerable to attack).

Exercise 1: Sniffing HTTP

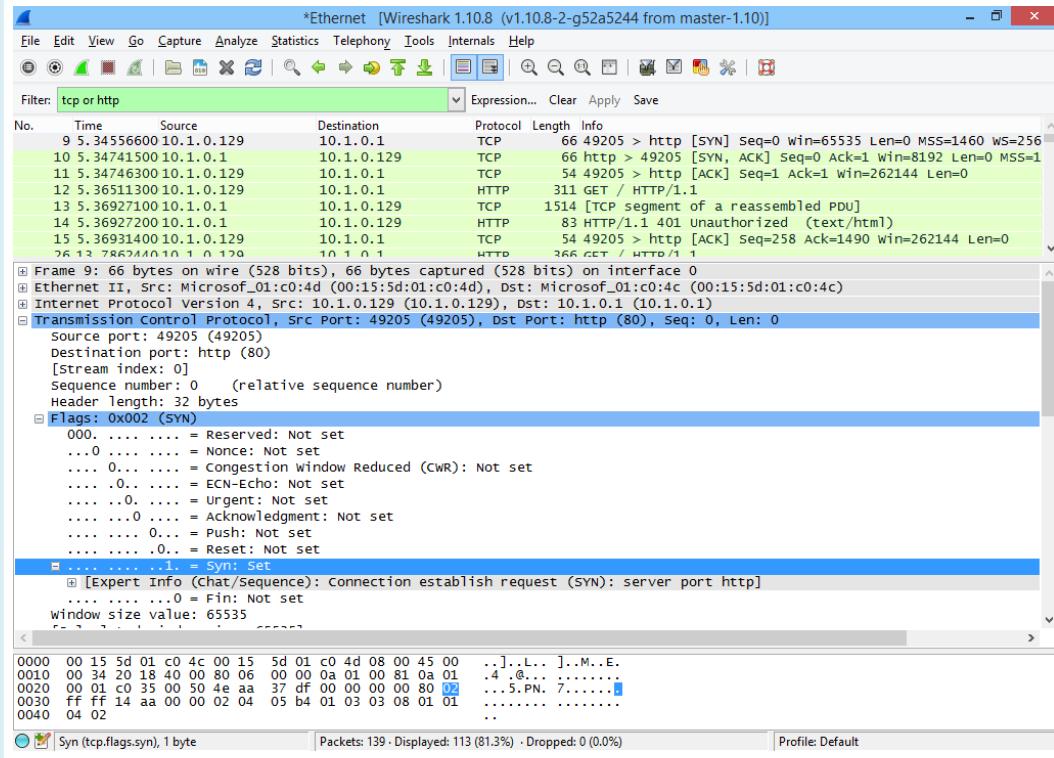
In this exercise, we will run a packet capture on an HTTP session between CLIENT and SERVER VMs. For simplicity, we will capture the packets directly on CLIENT. In real-world attacks, various exploits could be used to sniff the data packets from a third host (for example, those demonstrated in labs 3 and 10).

- 1) Start the **SERVER** VM and log on as **CLASSROOM\Administrator** (with the password **Pa\$\$w0rd**). In **Server Manager**, select **Tools > Internet Information Services (IIS) Manager**.
- 2) Click on **SERVER (CLASSROOM\Administrator)**. If a dialog appears asking about Microsoft Web Platform, click **No**.
- 3) Double-click the **Authentication** icon under "IIS" in the "SERVER Home" pane.
- 4) Select **Anonymous Authentication** then click **Disable**.
- 5) Select **Basic Authentication** then click **Enable**.
- 6) Start the **CLIENT** VM and log on as **CLIENT\Admin** (with the password **Pa\$\$w0rd**).



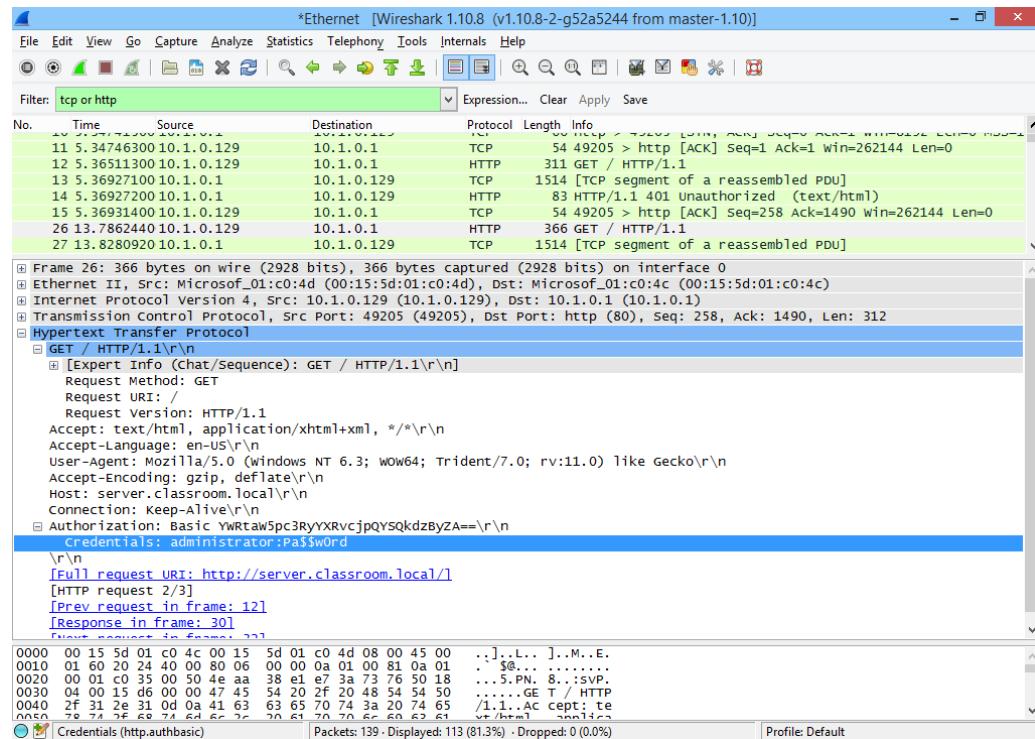
Ensure you sign in to the local computer account (CLIENT\Admin) rather than the domain administrator account.

- 7) Run **Wireshark** from the desktop icon and click the **Start Capture** button .
- 8) Open a **Run** dialog (**Start+R**) and enter the address
http://server.classroom.local
- 9) Enter the user name **Administrator** and password **Pa\$\$w0rd** (but do not save the credentials).
- 10) Close the browser.
- 11) Switch to Wireshark and click the **Stop Capture** button . Observe the following:



Observing the TCP three-way handshake

- The session starts with the TCP three-way handshake.
- The HOST then makes a HTTP GET request (to load the page)
- The SERVER responds with 401 UNAUTHORIZED (at this point the browser displayed the credentials prompt)
- The next HTTP packet contains the credentials - you can see the user name and password in their transmitted form (an encoding method called Base64) and as decoded by Wireshark



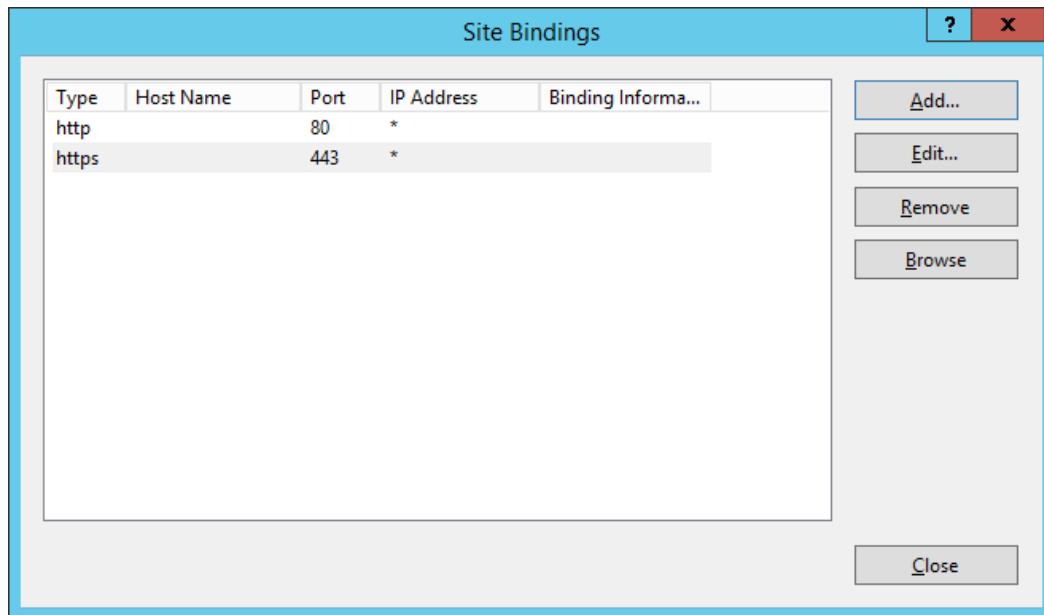
Capturing basic HTTP authentication in Wireshark

Exercise 2: Securing HTTP

Using a server-side certificate means that a secure channel can be created between the server and the client.

The client can also inspect the server's certificate and determine whether it is trustworthy (and if mutual authentication is configured then the server can choose whether to accept the client).

- 1) On the **SERVER** VM, in IIS Manager, click on **SERVER (CLASSROOM\Administrator)**.
- 2) Double-click the **Server Certificates** icon under "IIS" in the "SERVER Home" pane.
- 3) Click the **Create Self-Signed Certificate** link.
- 4) Enter **server.classroom.local** as the friendly name, then click **OK**.
- 5) In the "Connections" pane, navigate to **Sites > Default Web Site**.
- 6) Under the "Actions" panel (on the right-hand side) click **Bindings**.
- 7) Click the **Add** button.
- 8) Select **https** from the "Type" box and the **server.classroom.local** certificate from the "SSL certificate" box, then click **OK**.



Site Bindings dialog

- 9) Click **Close**.

This configuration allows clients to continue to connect via unencrypted HTTP if they choose.

- 10) To force use of SSL, open the **SSL Settings** node.
- 11) Check the **Require SSL** box then in the "Actions" pane, click **Apply**.

12) Switch to the **CLIENT** VM and start a new **Wireshark** capture, discarding the previously captured packets.

13) Open a **Run** dialog (**Start+R**) and enter the address
http://server.classroom.local

14) Press **F5** to refresh the page.

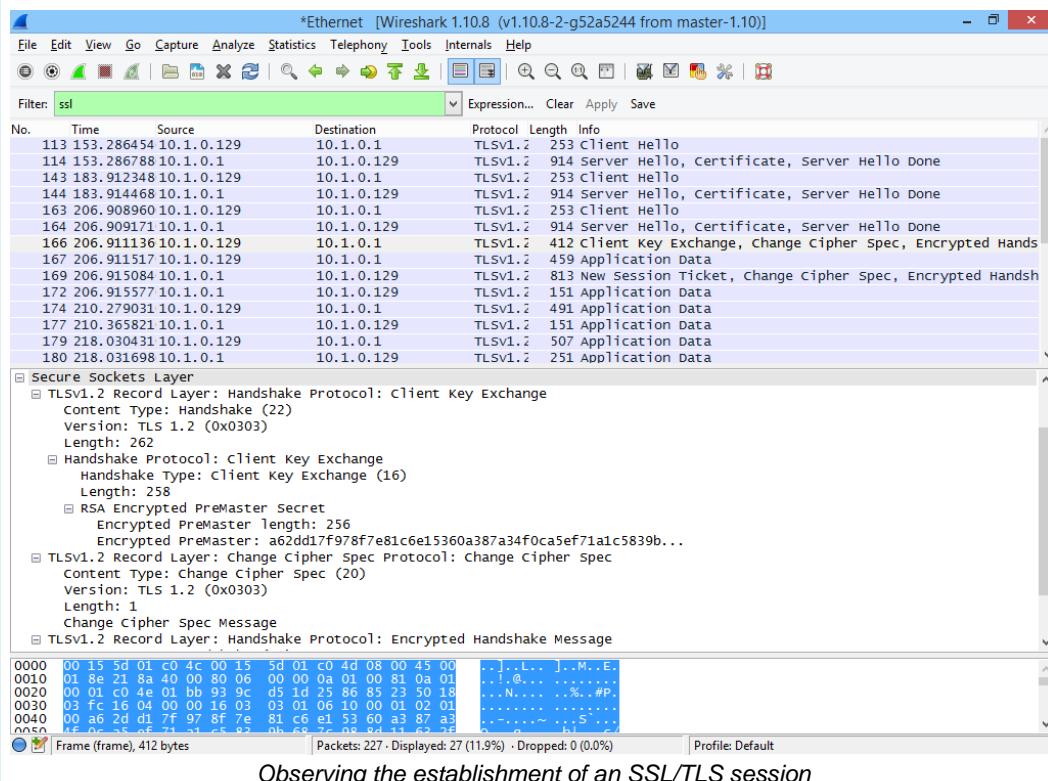
Note that the requested resource is forbidden. When use of SSL is forced, you would normally also use a redirect to send the client to the HTTPS URL instead.

15) Click in the address bar and change the URL to
https://server.classroom.local then press **Enter**.

IE displays a warning about the certificate as it is not signed by a trusted CA.

16) Click the **Continue to this website (not recommended)** link Enter your credentials then close the browser.

17) Switch to the Wireshark capture and stop capturing. Browse through the captured packets to view the TLS handshake. Note that there are no HTTP packets to decode, just TLS application data.



Exercise 3: Completing the Lab

You need to discard some of the changes you made during this lab to the VMs' disk images.

- 1) On each VM, from the console window toolbar, select **Action > Revert**.
- 2) Confirm by clicking the **Revert** button.



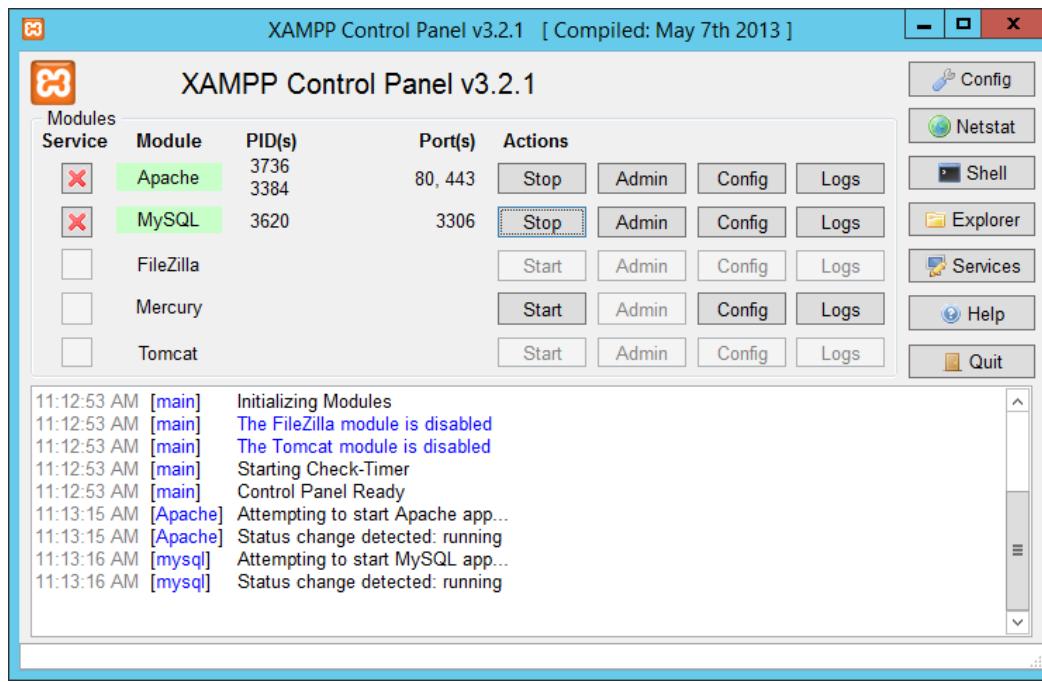
Lab 14 / Web Application Vulnerabilities

DVWA (Damn Vulnerable Web Application) is a web-based application that has been deliberately designed to include various vulnerabilities. In this lab, we will install the application and investigate some of the vulnerabilities.

Exercise 1: Installing XAMPP

DVWA is designed to run on Apache and MySQL, a popular combination of open source platforms commonly used for publishing web-based applications on the internet. We will begin by installing these platforms (replacing IIS) using the XAMPP (Cross-platform Apache, MySQL, PHP, and Perl) package.

- 1) Start the **SERVER** VM and log on as **CLASSROOM\Administrator** (with the password **Pa\$\$w0rd**).
- 2) In **Server Manager**, select **Tools > Services**.
- 3) Alt-click **World Wide Web Publishing Service** and select **Properties**.
- 4) Change the "Startup type" to **Disabled** and click **Stop**. Click **OK**.
- 5) Click the **Windows Start** button, type **uac**, then click the **Change User Account Control settings** icon.
- 6) Move the slider down to the **Never notify** position, and click **OK**.
- 7) In File Explorer, navigate to the **c:\GTSLABS** folder and run **xampp-win32-1.8.3-4-VC11-installer**.
- 8) Note the warning regarding User Account Control and click **OK**. Complete the setup wizard by making the following choices:
 - o On the "Setup - XAMPP" page, click **Next**.
 - o On the "Select Components" page, clear the **FileZilla FTP Server**, **Mercury Mail Server**, and **Tomcat** check boxes, then click **Next**.
 - o On the "Installation folder" page, click **Next >** to accept the default location.
 - o On the "Bitnami for XAMPP" page, clear the **Learn more about Bitnami for XAMPP** check box, then click **Next**.
 - o On the "Ready to Install" page, click **Next**.
 - o Wait for the installation to complete, then click **Finish**.
- 9) In the "XAMPP Control Panel" window, click the **Start** button next to Apache, then click the **Start** button next to MySQL.



XAMPP Control Panel

- 10) Note the three ports used by the two processes:
-

Exercise 2: Installing DVWA

In this exercise we will install the DVWA files to the XAMPP server and configure the Windows Firewall to allow access to the custom server.

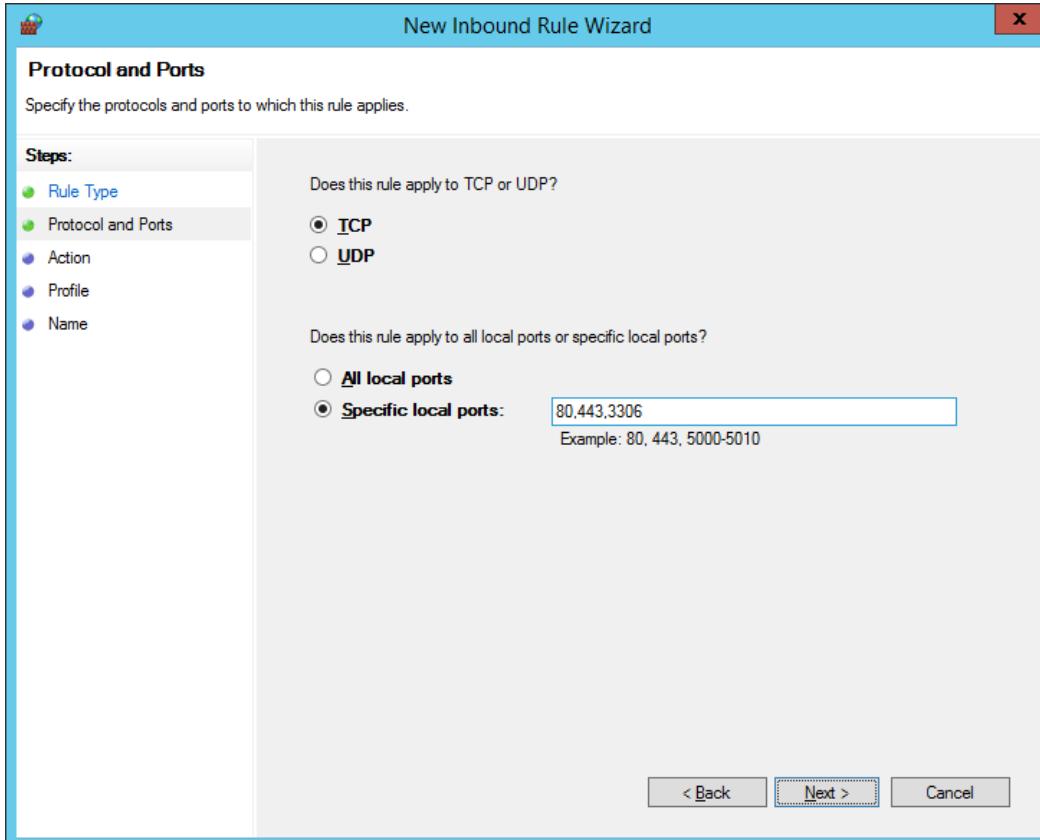
- 1) In File Explorer, navigate to the **c:\GTSLABS** folder. Alt-click **DVWA-1.0.8**, and select **Extract All**.
- 2) Enter the location **c:\xampp\htdocs**, clear the **Show extracted files when complete** check box, and click **Extract**.
- 3) In File Explorer, navigate to **c:\xampp\htdocs** and rename the "DVWA-1.0.8" folder to **dvwa**.
- 4) Navigate to **c:\xampp\htdocs\DVWA\config** and double-click the **config.inc.php** file.
- 5) Click **Try an app on this PC**, and select **Notepad**.
- 6) Find the following line:

```
$_DVWA[ 'db_password' ] = 'p@ssw0rd' ;
```
- 7) Delete the password text to change the line to:

```
$_DVWA[ 'db_password' ] = '' ;
```
- 8) Close Notepad, saving the changes.
- 9) Click the Windows Start button, type **firewall**, then click the **Windows Firewall with Advanced Security** icon.

10) Select the **Inbound Rules** node and click the **New Rule** link in the "Actions" pane. Complete the wizard by making the following choices:

- On the "Rule Type" page, select **Port**, then click **Next**.
- On the "Protocol and Ports" page, ensure **TCP** and **Specific local ports** are selected, and type the three port numbers you noted earlier, separated by commas, then click **Next**.



Open the ports required by XAMPP on the firewall

- Set the "Action" to **Allow the connection** and click **Next**.
 - On the "Profile" page, ensure all three profiles are checked then click **Next**.
 - In the "Name" box, type **XAMPP**.
 - Click **Finish**.
- 3) In a **Run** dialog, type `http://server/dvwa`, and press **Enter**.
- 11) Click the **here** link to set up the database.
- 12) In the "Security Warning" and "Trusted Sites" dialogs, click **Add**, **Add**, and **Close** to allow access to the site.
- 13) Click the **Create / Reset Database** button.

The screenshot shows a web browser window for the DVWA application. The URL is http://server/dvwa/setup.php#. The title bar says "Damn Vulnerable Web App ...". The main content area is titled "Database setup". It has a sidebar with links: Home, Instructions, Setup (which is highlighted in green), Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. Below the sidebar is a message: "Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in /config/config.inc.php". It also says "If the database already exists, it will be cleared and the data will be reset." Under "Backend Database: MySQL", there is a "Create / Reset Database" button. To the right of the button are several text boxes containing success messages: "Database has been created.", "'users' table was created.", "Data inserted into 'users' table.", "'guestbook' table was created.", "Data inserted into 'guestbook' table.", and "Setup successful!". At the bottom left is a "Username:" field with "Security Level: high" and a "Logout" link. At the bottom center is the "DVWA" logo.

- 14) When complete, click on the **DVWA Security** button. Log in with the username **admin** and the password **password**.
- 15) Click on the **DVWA Security** button again, set the security level to **Low**, and click **Submit**.

Exercise 3: Exploiting a Command Execution Vulnerability

We will now examine some of the vulnerabilities that can be exploited in DVWA, starting with a command execution. In this exercise, we will use a bug in the web application to force the server to execute an arbitrary command.

- 1) Click on the **Command Execution** button.
- 2) Type **server** in the "IP address" box, and click **Submit**. Note the size of the packets sent.

- 3) Type **-l 800 server** in the "IP address" box, and click **Submit**. Again, note the packet size.

- 4) Type **/?** into the "IP address" box, and click **Submit**. What can we tell from these results about how the application works?

- 5) Type **server | dir** into the "IP address" box. What is returned, and why?

Exercise 4: Exploiting a SQL Injection Vulnerability

In a SQL injection attack, we manipulate the application into executing a SQL statement that was not intended as part of the original code. A hacker will often test an application with invalid data, to see what can be learned from the result.

- 1) Click on the **SQL Injection** button.
- 2) Type **2** in the "User ID" box, and click **Submit**. Note that a single record is displayed.
- 3) Type **hello** in the "User ID" box, and click **Submit**. Note that no data is returned.
- 4) Type **'** (a single quote) into the "User ID" box and click **Submit**. What happens, and what does this tell us about how the application works?

- 5) Use the browser's **Back** button to get back to the form. Type the following into the "User ID" box, and click **Submit**:

1' or '1' = '1

Exercise 5: Exploiting a Cross Site Scripting Vulnerability

In this attack, we will cause the site to run a script that is not part of the original code.

- 1) Click on the **XSS Reflected** button.
- 2) Type your name into the text box and click **Submit**.
- 3) Type the following into the box, and click **Submit**:

<script>alert('Hello World!')</script>

- 4) Click **OK** to close the **Message from Website** dialog.

Exercise 6: Completing the Lab

You need to discard the changes you made during this lab to the VM's disk image.

- 1) From the console window toolbar, select **Action > Revert**.
- 2) Confirm by clicking the **Revert** button.



Lab 15 / Computer Forensic Tools

In this lab, you will use some computer forensic tools to mount the ROGUE VM's hard disk and perform some analysis.

Exercise 1: The Scene of the Crime

In this exercise, we will imagine that the ROGUE computer contained some software and documents that an attacker wished to hide.

- 1) Start the **ROGUE** VM and log on as **Admin** (with the password **Pa\$\$w0rd**).
- 2) In the **Documents** library, create a new rich text document called **GAMENET** and add the text **Gamenet password dump**.
- 3) Close the document, saving the changes.
- 4) Alt-click the **GAMENET** document and select **Send to > Compressed (zipped) folder**. Press Enter to accept the same file name.
- 5) Open a command prompt and execute the following commands:

```
cd c:\users\admin\documents  
ren gamenet.zip gamenet.txt  
del gamenet.rtf  
del /s /q c:\GTSLABS
```

- 6) Alt-click the **Start** button and select **Control Panel** then click the **Uninstall a program** link.
- 7) Uninstall **Angry IP Scanner**, **Ettercap**, **Nmap**, and **Wireshark**.
- 8) Shut down the VM.

Exercise 2: Creating a Disk Image

Before any data is examined in an actual forensic investigation, the PC is booted from an OS on an external drive, and the contents of the internal drive cloned sector by sector to separate media. This allows the data to be examined without any changes being made to the original, thus maintaining the integrity of the evidence. In this exercise, we will mimic this operation in the virtual environment by making a checkpoint of the VM and exporting that checkpoint to an alternate location.

- 1) In Hyper-V Manager, verify that the ROGUE VM state is "Off". When it has fully shut down, alt-click the **ROGUE** VM and select **Checkpoint** to create a new checkpoint (named ROGUE and timestamped with the current date and time).
- 2) Alt-click the new checkpoint and select **Export**.

- 3) In the "Location" box, type **c:\GTSLABS** and click **Export**. Wait a few minutes for the export to complete.



The export progress is shown in the "Status" column of the "Virtual Machines" panel - use the scroll bar or maximize the Hyper-V window to see this clearly.

Exercise 3: Mounting the Disk Image and Creating a Disk Signature

In this exercise, you will make the disk image you have created available to the host PC, then use forensic software to start a new case and create a disk signature. This can be used later to prove the integrity of the data on the disk.

- 1) On the HOST PC, open File Explorer and navigate to **c:\GTSLABS\ROGUE\Virtual Hard Disks**.
- 2) Alt-click **ROGUE** and select **Properties**. Check the **Read-only** box and click **OK**.
- 3) Alt-click **ROGUE** and select **Mount**. Note the drive letter that has been assigned to the mounted "Local Disk" image (ignore the "System Reserved" disk).
- 4) Double-click the **OSForensics** icon on the HOST PC's desktop and click **Yes** to confirm the User Account Control dialog.



If OSForensics is not available on the HOST PC, install it using the setup file in c:\GTSLABS\osf_v2.2.1000.

- 5) When OSForensics loads (it may take a few seconds), click **Continue Using Free Version**.
- 6) Under "Case Management", click the **Create Case** icon.
- 7) In the **Case Name** box, enter **ROGUE Investigation**.
- 8) Type your name in the **Investigator** box.
- 9) Under **Acquisition Type**, select **Investigate Disk(s) from Another Machine**.
- 10) Click **OK**.
- 11) Select the **Start** node, and under "Hashing & File Identification", click the **Create Hash** icon.
- 12) Under "Verify / Create Hash", select **Volume**.

- 13) In the **Volume** drop-down, select the entry corresponding to the drive letter you noted earlier. It should appear in the format **\.\PhysicalDrive1: Partition 2, D: [63.66GB NTFS]**
- 14) Under the **Hash Function** drop-down, select each function in turn and note its description in the "Selected Hash Function Description" panel. After viewing all available functions, select **MD5** then click **Calculate**.
- 15) When the calculation has completed (about ten minutes), select all the text in the **Calculated Hash** box then alt-click the text and select **Copy**.
- 16) Select the **Manage Case** node and click the **Add Note** button.
- 17) In the **Name** box, type **Initial MD5 hash**.
- 18) Alt-click the note area and select **Paste** to paste the MD5 hash value, then click **Save**.

Exercise 4: Analyzing the Image

In this exercise, you will take a quick look at some tools that can be used to recover information from the image without using the usual file access tools of the OS (data carving).

- 1) Click on the **Recent Activity** node.
- 2) Select the **Scan Drive** radio button then choose the drive letter you noted earlier. Click the **Scan** button.
- 3) Review the list of results. Near the top you should see at least one entry for "Gamenet.rtf". Alt-click this entry, and select **Add to Case > List of Selected Items**.
- 4) In the **Title** box, type **Gamenet document accessed**, then click **OK**.
- 5) Alt-click the entry again and select **Add to Case > List of All Items**.
- 6) In the **Title** box, type **All recent activity** then click **OK**.
- 7) Select the **Deleted Files Search** node.
- 8) In the **Disk** drop-down, select the entry corresponding to the drive letter you noted earlier, then click **Search**.
- 9) Review the list of results. Check whether you can find an entry for "Gamenet.rtf". If so, alt-click this entry and select **Add to Case > File(s)**, then enter in the **Export Title** box **Deleted Gamenet document**, and click **Add**.



Not all deleted files will be available, particularly with a virtual disk image.

- 10) In the "Filter String" box, type **.exe** then click the **Apply Filter** button.

- 11) Click on the first file found, hold down **Shift**, then click on the last file. Alt-click any of these entries, and select **Add to Case > List of Selected Items**.
- 12) In the **Title** box, type **Programs deleted**, then click **OK**.
- 13) Clear the "Filter String" box then click **Apply Filter** again.
- 14) In the **Sorting** drop-down (bottom right corner) select **Folder**.
- 15) Review the results to check whether you can find any evidence of any files deleted from the **GTSLABS** folder.
- 16) If you find any, click on the first file in the GTSLABS folder, hold down **Shift**, then click on the last GTSLABS file. Alt-click any of these entries, and select **Add to Case > List of Selected Items**.
- 17) In the **Title** box, type **Deleted from GTSLABS**, then click **OK**.
- 18) Alt-click any entry, and select **Add to Case > List of All Items**.
- 19) In the **Title** box, type **All deleted files**, then click **OK**.
- 20) Select the **Mismatch File Search** node.

This node locates file types that do not match their file extension.

- 21) Change the contents of the **Start Folder** box to reference the root of the drive you noted previously, then click **Search**.
- 22) The search will take a few minutes. When complete, select **Name** from the **Sorting** drop-down, and review the results for a GAMENET file.

Note that while the file's name is GAMENET.txt, OSForensics identifies the file type as a zip archive.

- 23) Alt-click **gamenet.txt** and select **Add to Case > File(s)**, then enter in the **Export Title** box **Disguised Gamenet document**, and click **Add**.
- 24) Click on the **Manage Case** node and review the case notes.
- 25) Close **OSForensics**.

Exercise 5: Completing the Lab

You need to discard the changes you made during this lab.

- 1) On the HOST PC, alt-click the **Start** button and select **Disk Management**.
- 2) In the lower pane, alt-click the VHD disk and select **Detach VHD**. Confirm by clicking **OK**.



The VHD disk will be marked "Read Only" and will be 64GB in size.

- 3) Open File Explorer and navigate to **c:\GTLABS\ROGUE\Virtual Hard Disks**.
- 4) Alt-click **ROGUE** and select **Delete**.
- 5) In the Hyper-V Manager console, select the **ROGUE** VM.
- 6) In the "Checkpoints" pane, alt-click **ROGUE Initial Config** and select **Apply**. Click the **Apply** button to confirm.
- 7) Alt-click the **ROGUE (*Today's Date*)** checkpoint that you created and select **Delete Checkpoint**. Confirm by clicking **Delete**.



Uninstall OSForensics if your instructor asks you to.