



MASTERS IN CYBER SECURITY

Cybersecurity and Ethical Hacking



I really think that if we change our own approach and thinking about what we have available to us, that is what will unlock our ability to truly excel in security. It's a perspectives exercise. What would it look like if abundance were realty and not resource constraint?

NOVEMBER 8, 2021
ALVION TECHNOLOGIES



What is cybersecurity?

Cybersecurity is all about reducing threats when people are in the process of dealing with technology. It encompasses the full range of protection against any online risk or vulnerability, which comprises information security assurance and cyber law enforcement. In other words, cybersecurity is the protection of cyber-space (which includes hardware, software, networks, and their servers, peripheral devices, data and information, and all other components associated with technology) and internet-connected systems from both internal as well as external threats and cybercriminals. It also comprises sub-branches that are specific to different security measures. These are:

- Network Security.
- System Security.
- Application Security.
- Information Security.
- Web Security.
- Mobile Security.

Why there is such demand for cybersecurity?

Almost everyone from this generation lives in a world of technology where the internet is connected to nearly every device around us. For cybercriminals and hackers, this is the golden age to tweak with technical stuff easily. Still, the general users are not aware of the fact that lack of security and improper use of technology can drag users and employees to doom. That is why specialized security analysts and penetration testers are hired to secure the entire system.

This subject has gradually evolved to be a new domain of learning and securing different technology such as programming, web, network, servers, applications, cloud, and many more areas.

Required knowledge.

Before digging every chapter for knowledge, it is recommended to have some understanding of programming, networking, Operating Systems (OS), hardware, and software.

Contents

Cyber Security	30
What is Cyber Security?	30
The scale of the cyber threat	30
Types of cyber threats	30
Malware	31
SQL injection	31
Phishing	31
Man-in-the-middle attack	31
Denial-of-service attack	31
Latest cyber threats	32
Dridex malware	32
Romance scams	32
Emotet malware	32
End-user protection	32
Cyber safety tips - protect yourself against cyberattacks	33
Terminologies	34
What is Cybersecurity?	39
The Importance of Cybersecurity	39
Why is Cybercrime Increasing?	40
What is the Impact of Cybercrime?	40
How to Protect your Organization Against Cybercrime	41
TCP/IP (features)	41
Networking devices	42
Network protocol/ Ports	42
What is a network protocol?	42
What are the layers of the OSI model?	43
Which protocols run on the network layer?	43
What other protocols are used on the Internet?	44
What protocols do routers use?	44
How are protocols used in cyber-attacks?	45
What is the Internet Protocol (IP)?	45
What is a network protocol?	45



What is an IP address? How does IP address work?	45
IPv4 vs. IPv6	46
What is an IP packet?.....	46
How does IP routing work?.....	46
What is TCP/IP?.....	47
What is UDP/IP?.....	47
Ports.....	47
What is a port?.....	47
What is a port number?.....	48
How do ports make network connections more efficient?.....	48
Are ports part of the network layer?.....	48
Why do firewalls sometimes block specific ports?.....	49
What are the different port numbers?.....	49
Kali Linux Commands.....	50
Kali Linux commands Categories:	50
System Commands in Kali Linux:	50
A to Z Basic Kali Linux commands in 2020:.....	51
1# Arch Command:	51
2# Arp Command:	51
#3 arping Command	52
4# Aspell Command:.....	52
5# awk command”	52
6# bg command	53
7# base-name command	54
8# Bzip2.....	55
9# calenda (Cal) command:	55
10# cat command	56
11# cksum command	57
12# Clear command	57
13# cmp Command:.....	57
14# comm Command.....	57
15# cp command:	57
16# Crontab Command:.....	58



16# cut Command:	58
16# Date Command:	58
17# dc command:	59
18# Dd command.	59
19# df command	59
20# diff command.....	60
21# diff3 command.....	60
22# dig command	60
23# dir Command	60
24# echo command:.....	60
25# Egrep Command	61
26# Eject Command.....	61
27# ethtool Command	61
28# whoami command:.....	61
29# pwd command:.....	62
30# ls command:.....	63
31# cd command:	63
32# mkdir command:.....	63
33# mv command:.....	64
34# rm command:.....	64
System Basic Kali Linux commands.....	65
35# uname command:	65
36# uptime command:	65
37# users command:.....	66
38# Less Command	66
39#More Command.....	66
40# Sort command.....	67
41# VI Command	67
42# Free command	67
43# history command:.....	68
Google dorks	69
FIND OPEN FTP SERVERS WITH GOOGLE HACKING	70
FIND UNSECURE WEBSITES WITH GOOGLE HACKING	73



Search Logs For Passwords	75
Search For Configuration Files With Passwords	76
Finding Emails From Google	79
HACK CAMERAS USING GOOGLE	81
Conclusion.....	84
Advanced operators.....	85
Reconnaissance, Finger printing and Footprinting.....	85
Footprinting	85
Footprinting Types: Active and Passive	85
Footprinting helps to:	86
Footprinting Objectives	86
Methods and Tools	87
Search Engines	87
Website Footprinting.....	88
Email Footprinting	88
DNS Footprinting	89
Network Footprinting	92
Other Relevant Tools	93
OSRFramework	93
Web Spiders	93
Recon-ng	93
Metasploit Framework	93
theHarvester	93
Sublist3r	95
DIRB.....	96
Maltego.....	96
Social Engineering Framework (SEF)	97
Web Based Recon	97
NetCraft	97
Shodan	98
Censys	100
Finger printing.....	101
NMAP	102



What is Nmap?.....	102
What Does Nmap Do?	103
How To Use Nmap	104
How To Install Nmap.....	104
Nmap Tutorial and Examples.....	105
How To Run a Ping Scan.....	105
How To Run A Host Scan?.....	105
How To Use Nmap in Kali Linux	106
1. Ping Scanning	107
2. Port Scanning	107
3. Host Scanning	108
4. OS Scanning	108
5. Scan The Most Popular Ports.....	108
6. Output to a File	109
7. Disable DNS Name Resolution	110
+ More Useful Information about Nmap: +	110
2. Service and Version Detection.....	110
3. OS Detection	111
4. Timing and Performance	111
5. NSE Scripts	112
Useful NSE Script Examples	112
Vulnerabilities	113
Vulnerability Categories:	113
Vulnerability Assessment - Scans and tests for vulnerabilities but does not intentionally exploit them.....	113
Vulnerability Management Life-cycle.....	113
Vulnerability Scanning	113
CVSS and CVE	114
ProxyChains 	114
Enumeration Concepts	115
SNMP Enumeration	116
Windows System Basics.....	117
NetBIOS Enumeration.....	118

Linux System Basics	119
LDAP Enumeration.....	120
NTP Enumeration.....	121
SMTP Enumeration.....	122
Some SMTP Commands:.....	123
2.0) Windows and server security	125
Windows Security Architecture	125
LM Hashing.....	125
Ntds.dit.....	125
Kerberos for Active Directory Domain Services (AD DS).....	125
Registry.....	126
MMC.....	128
Sigverif.exe	128
Linux Security Architecture	129
Linux Directory Structure	129
Linux Common Commands.....	130
Linux security	132
Benefits of using Linux	132
Linux structure	133
03) Data and information security.....	135
Overview Data and information security	135
Data security management	135
Types of data security	135
How data security and other security facets interact	135
Data security, privacy and protection solutions.....	136
Data security solutions	136
Data security services	136
Homomorphic encryption	136
Storage data backup and recovery.....	137
Data encryption solutions.....	137
Infrastructure security	137
Data privacy	137
Ransomware protection	137



Zero trust security.....	137
Cloud computing.....	138
What is Cloud Computing?	138
Cloud Computing Basics.....	138
Cloud Deployment Models.....	139
NIST Cloud Architecture.....	139
Five characteristics of cloud computing	140
Threats:.....	140
Attacks:.....	141
OWASP Top 10 Application Security Risks	141
Additional Attacks	142
Cloud Security Control Layers.....	143
Key Properties of Cloud Computing.....	143
Understanding Cloud Computing	144
Oracle Private Cloud	144
Benefits From Cloud Computing.....	145
Cloud Computing Services	146
NIST Cloud Computing three service and Definition:.....	146
The Benefits of Cloud Computing (Cloud Computing)	148
The limitations of Cloud Computing (Cloud Computing)	149
Cryptography	150
Goals of cryptography.....	150
Technical terms in crypto systems	150
What is Cryptography?	151
What is Cryptanalysis?.....	151
Security Services of Cryptography	151
Confidentiality.....	151
Data Integrity	151
Authentication	152
Non-repudiation	152
Where to Encrypt & Decrypt?	152
Cryptography Primitives	153
Encryption Algorithms.....	154

Components of a Cryptosystem	154
Types of Cryptosystems	155
Symmetric Key Encryption.....	155
Challenge of Symmetric Key Cryptosystem.....	156
Asymmetric Key Encryption.....	157
Challenge of Public Key Cryptosystem	158
Relation between Encryption Schemes.....	158
Kerckhoff's Principle for Cryptosystem	159
Passive Attacks.....	159
Active Attacks	160
Assumptions of Attacker.....	161
Environment around Cryptosystem	161
Details of the Encryption Scheme.....	161
Availability of Ciphertext	161
Availability of Plaintext and Ciphertext	161
Cryptographic Attacks.....	162
Practicality of Attacks	163
Block Ciphers.....	164
Stream Ciphers.....	164
Block cipher.....	164
Block Size	165
Padding in Block Cipher	165
Block Cipher Schemes.....	165
Feistel Cipher	166
Encryption Process.....	166
Decryption Process	167
Number of Rounds.....	167
Initial and Final Permutation	168
Round Function.....	169
Key Generation	172
DES Analysis	173
Triple DES	173
3-KEY Triple DES.....	174



Advanced Encryption Standards (AES)	175
Operation of AES.....	175
Encryption Process.....	176
Byte Substitution (Sub Bytes)	177
Shiftrows	177
MixColumns	177
Addroundkey	177
Decryption Process	177
AES Analysis	177
Public Key Cryptography.....	178
Features of Hash Functions	179
Properties of Hash Functions.....	180
Design of Hashing Algorithms.....	181
Popular Hash Functions	182
Message Digest (MD).....	182
Secure Hash Function (SHA)	182
RIPEMD	183
Whirlpool	183
Applications of Hash Functions	183
Password Storage	183
Data Integrity Check	184
Cryptography – Benefits	185
Cryptography – Drawbacks.....	185
Future of Cryptography	186
Steganography	186
Steganography Techniques.....	187
Cyber Security Training.....	188
Steganography Tools	189
Using Steganography to Deliver Attacks	190
Detecting Steganography	190
How is Steganography different from Cryptography?	190
04) UNDERSTANDING NETWORK TYPES AND ITS SECURITY	192
Application of networks.....	192



Network topology	192
What Is Network Topology?	192
Why Is Network Topology Important?	193
What Is Star Topology?	194
Advantages of Star Topology	194
Disadvantages of Star Topology	195
What Is Bus Topology?	195
Advantages of Bus Topology.....	195
Disadvantages of Bus Topology	196
What Is Ring Topology? Single vs. Dual	196
Pros of Ring Topology	196
Cons of Ring Topology	197
What Is Dual-Ring Topology?.....	197
Advantages of Dual-Ring Topology.....	197
What Is Tree Topology?	198
Pros of Tree Topology	198
Cons of Tree Topology	198
What Is Mesh Topology?	199
Advantages of Mesh Topology	199
Disadvantages of Mesh Topology	199
What Is Hybrid Topology?.....	200
Advantages of Hybrid Topology.....	200
Disadvantages of Hybrid Topology	200
Which Topology Is Best for Your Network?	200
What is Network Security?	202
How can we ensure network security?	202
Physical Network Security	202
Technical Network Security	203
Administrative Network Security.....	203
What are the different types of Network Security?	203
Access Control.....	203
Restricted Access and Network Boundary Security.....	203
Application Security	203

Firewalls Security	204
Virtual Private Networks (VPN)	204
Benefits of VPN	204
Advantages of VPN	204
Wireless networks	205
Types of Wireless Networks.....	205
Advantages of Wireless Networks.....	205
Examples of wireless networks	206
Wireless Security	206
What are the risks to your wireless network?.....	206
What can you do to minimize the risks to your wireless network?	207
Wireless LAN security	209
Intrusion Prevention System	211
Network management and control	211
FTP services.....	211
How does FTP work?.....	212
How to use FTP	212
How to Connect to Hostinger FTP	213
Conclusion.....	214
API	215
Application Programming Interface (API).....	215
What is an application programming interface (API)?	215
How an API works	215
Why we need APIs	216
Common API examples	216
Types of APIs	217
Types of API protocols	217
APIs, web services, and microservices.....	218
Proxy	219
What is a proxy?	219
Why do you need web proxy?	219
Insure your assets against threats	219
Improve network performance	220



Proxy in action	220
Enterprise.....	221
At schools and universities	221
Using Airtame with a web proxy setup.....	221
Network classes	222
A B and C Classes of Networks	222
Class A Network (/ 8 Prefixes).....	222
Class B Networks (/16 Prefixes).....	223
Class C Networks (/24 Prefixes)	223
Other Networks.....	223
Router security.....	223
Function of Router:	224
What is Routing Protocols?	225
Types of Routing Protocols.....	225
Static Routing Protocols.....	225
Advantages	225
Disadvantages.....	226
Dynamic Routing Protocols.....	226
Advantage:	226
Disadvantage:	226
Distance Vector Routing Protocol (DVR)	226
Advantages:	226
Disadvantages:.....	226
Internet Routing Protocols:	226
Routing Information Protocol (RIP)	227
Interior Gateway Protocol (IGP)	227
Link State Routing Protocol	227
Routing protocol tables:	227
Advantages:	227
Exterior Gateway Protocol (EGP).....	228
Enhanced Interior Gateway Routing Protocol (EIGRP).....	228
Open Shortest Path First (OSPF)	228
Intermediate System-to-Intermediate System (IS-IS)	229

Border Gateway Protocol (BGP)	229
What is the purpose of Routing Protocols?.....	229
Classful Vs. Classless Routing Protocols.....	229
Summary:.....	230
Types of routers	230
Core router.....	230
Edge router	230
Distribution router.....	231
Wireless router	231
Virtual router	231
How to choose small business routers	231
Connectivity	231
Bandwidth.....	231
Wireless capability	232
Simplified setup and management.....	232
Security	232
Flexibility	232
Automatic updates	232
User changeable configurations	232
Guest networks.....	232
Quality of service (QoS) controls	233
Mesh networks	233
Basic router security	233
Different types of encryptions.....	233
How to set up Wi-Fi router securely: The specifics	234
Other router security helpers	236
Use a virtual private network or VPN	236
Always use a firewall.....	236
NAPT Services	236
DOS/DDOS	237
What is a denial-of-service attack?	237
What are DOS and DDOS?	237
How DoS attacks work	237

DoS attack tools	238
DoS Protection: Prevent an attack	238
Hacking Activity: Ping of Death.....	239
Hacking Activity: Launch a DOS attack	241
Summary	242
Differences between DOS and DDOS?.....	244
Types of DDOS attacks	244
What is a distributed denial-of-service attack?.....	245
What is common denial-of-service attacks?	246
What is Denial of Service (SUMMARY)	248
Infrastructure Denial of Service	248
Wireless Denial of Service	249
Application Denial of Service	249
SIP Service attacks	250
Ransomware	251
Mitigation Techniques	251
Conclusion.....	252
Spoofing	252
What is spoofing?	252
Spoofing definition	252
Types of spoofing	253
Website Spoofing.....	255
How to Identify and Protect Against Spoofing Attacks	258
How does spoofing work?	260
How do I detect spoofing?	261
Caller ID spoofing	261
How can I protect against spoofing?	262
Networking summary	263
Short Summary.	263
05) Evading IDS, IPS, Firewall and Honeypots	266
Intrusion Detection System (IDS).....	266
Types of intrusion detection systems.....	267
Network intrusion detection system (NIDS).....	268

Host intrusion detection system (HIDS)	268
Protocol-based intrusion detection system (PIDS).....	268
Application protocol-based intrusion detection system (APIDS)	268
Hybrid intrusion detection system	268
General Indications of Intrusions.....	268
File System Intrusions	269
Network Intrusions	269
System Intrusions.....	269
Evasion Techniques.....	270
Evading IDS	270
Intrusion protection systems (IPS).....	274
IPS and IDS - What is the Difference?.....	274
How Do Intrusion Prevention Systems Work?	275
Types of Prevention	276
Detection	276
Firewalls	277
Firewalls types:	277
Proxy Types:.....	277
Evading Firewalls	278
IDS/Firewall Evading Tools.....	281
Honeypots.....	282
Types of Honeypots:	282
Detecting Honeypots	282
IDS Firewall Evasion Countermeasures	283
Firewall Penetration Testing.....	284
Sniffing and Evasion (SUMMARY).....	284
Basic Knowledge	284
Protocols Susceptible.....	285
ARP	285
IPv6	285
Wiretapping	286
Active and Passive Sniffing	286
MAC Flooding.....	286

ARP Poisoning	286
DHCP Starvation.....	287
Spoofing	287
Sniffing Tools.....	287
Devices To Evade	288
Evasion Techniques.....	289
Firewall Evasion	289
Honeypots.....	289
06) Attacking a System	291
Goals:	291
Password Attacks	291
Non-electronic - non-technical attacks.	291
Active online - done by directly communicating with the victim's machine.	291
Passive online - Sniffing the wire in hopes of intercepting a password in clear text or attempting a replay attack or man-in-the-middle attack.	292
Offline - when the hacker steals a copy of the password file (Plaintext or Hash) and does the cracking on a separate system.	293
Authentication	295
Malwares	296
- What is Malware?	296
Types of Viruses and Worms 	296
Major characteristics of viruses:	298
Stages of Virus Lifecycle:	298
Malware Basics	298
Basic components of Malware	299
Trojans 	299
Infection Process:	300
Trojan Port Numbers:	300
Trojan Countermeasures	301
Techniques	301
Malware Analysis	302
Types of Malware analysis:	302
Steps	302
Rootkits	303

Ways of Spread	303
Types of Malware Attacks.....	303
Other Important Terms	304
Different Types of Malwares	304
1. Viruses.....	305
2. Worms.....	306
3. Trojan Horses	307
4. Rootkits	307
5. Ransomware	308
6. Keyloggers.....	308
7. Grayware.....	309
What makes machines vulnerable?.....	311
Attacking methodologies.....	311
SQL Injection	311
What is SQL Injection?.....	312
Recommended Tools	313
Risks of SQL Injection.....	313
The Essence of this Attack	314
Security Testing of Web Applications Against SQL Injection.....	318
Vulnerable Parts of this Attack	319
Automating SQL Injection Tests.....	320
Comparison with Other Attacks	320
Conclusion.....	321
Cross-site Scripting (XSS)	321
What is cross-site scripting (XSS)?	321
How does XSS work?.....	321
XSS proof of concept.....	322
What are the types of XSS attacks?	322
Reflected cross-site scripting.....	322
Reflected XSS	323
What is reflected cross-site scripting?	323
Impact of reflected XSS attacks	323
Reflected XSS in different contexts	324

How to find and test for reflected XSS vulnerabilities.....	324
Common questions about reflected cross-site scripting.....	325
Stored XSS.....	325
What is stored cross-site scripting?.....	325
Impact of stored XSS attacks	326
Stored XSS in different contexts	326
How to find and test for stored XSS vulnerabilities.....	327
DOM-based XSS	328
What is DOM-based cross-site scripting?.....	328
How to test for DOM-based cross-site scripting	328
Testing HTML sinks	329
Testing JavaScript execution sinks.....	329
Testing for DOM XSS using DOM Invader.....	329
Exploiting DOM XSS with different sources and sinks.....	330
Sources and sinks in third-party dependencies.....	330
DOM XSS combined with reflected and stored data	332
Which sinks can lead to DOM-XSS vulnerabilities?	332
How to prevent DOM-XSS vulnerabilities.....	333
What can XSS be used for?	333
Impact of XSS vulnerabilities	333
How to find and test for XSS vulnerabilities	333
Content security policy	334
Dangling markup injection.....	334
How to prevent XSS attacks.....	334
Common questions about cross-site scripting	335
Windows Security Architecture	335
Linux Security Architecture.....	336
System Hacking Goals	337
Authentication and Passwords	338
Password Attacks	338
Privilege Escalation and Executing Applications.....	339
Hiding Files and Covering Tracks	340
Rootkits	340

Social Engineering.....	341
Phases.....	341
Principles	341
Behaviors	341
Companies Common Risks:.....	342
Social Engineering Attacks:.....	342
Human-Based Attacks 	342
Computer-Based Attacks 	343
Tools	343
Mobile-Based Attacks.....	343
Physical Security Basics	343
Prevention.....	344
Privilege Escalation and Executing Applications	344
Vertical - Lower-level user executes code at a higher privilege level (<i>e.g.: common user to root/administrator</i>).	344
Horizontal - executing code at the same user level but from a location that would be protected from that access.....	344
Covert data gathering.....	345
Keyloggers - record keys strokes of a individual computer keyboard or a network of computers.	345
Spywares - watching user's action and logging them without the user's knowledge.....	345
Defending against Keyloggers and Spywares.....	346
Hiding Files.....	346
⚠ Steganography:.....	347
Rootkits.....	347
Covering Tracks.....	348
On Linux:	348
On Windows:.....	349
Conclusion on Covering Tracks	349
07) Web security	350
What is Web Security?.....	350
Details of Web Security	350
Available Technology	351
Likelihood of Threat.....	351

The Best Strategies	351
UNIT 1	352
LAN SECURITY	352
INTRODUCTION TO LAN.....	353
WHY LAN SECURITY IS IMPORTANT.....	354
LAN/WAN COMPONENTS	354
TOPOLOGY	355
Disadvantages of a Star Topology.....	355
Advantages of a Tree Topology	355
Disadvantages of a Tree Topology.....	355
PROTOCOLS.....	355
THREATS AND VULNERABILITIES	356
THE LAN SECURITY PROBLEM.....	356
SECURITY THREATS OF LAN	357
SECURITY SERVICES AND MECHANISMS.....	357
Security services.....	357
Security Mechanisms	358
Relation between security services and mechanisms	359
ACCESS CONTROL	359
The types of security.....	360
Access control system.....	360
What is Access Control?	360
What are the Components of Access Control?	361
Access Control Components.....	361
User facing	362
Admin facing	362
Infrastructure.....	362
Access Control Locks.....	362
Access Control Panel (or Controller)	363
Access Control Server	363
Low-Voltage Cables.....	363
Types of Access Control.....	363
Access Control Models	363

Physical Access Controls	364
The two main types are physical and logical.	365
What to look for in physical access control systems?	365
What to Look for When Choosing an Access Control System?	366
Compatibility.....	366
Features and maintenance	366
Access control in information security	367
NETWORK SCANNERS	367
TYPES OF SCANNING	368
PORT SCANNING	370
SSH Security Basics	370
Security Friction	370
Avoid Port 22	371
Filter Connections Using TCP Wrappers	372
Reject Connection Requests with No Passwords	375
Use SSH Keys Instead of Passwords.....	375
Disable Password Authentication Altogether.....	376
Disable X11 Forwarding	377
Set an Idle Timeout Value.....	378
Set a Limit for Password Attempts	379
Disable Root Log Ins.....	380
The Ultimate Step	381
TECHNIQUES	381
FIREWALLS	381
TYPES OF FIREWALLS	382
Configuring SSH access through firewalls.....	382
Outbound SSH.....	383
Back-tunneling is a risk	383
Inbound SSH access	383
TYPES OF PROXY SERVERS	383
Anonymous Proxy Distorting Proxy High Anonymity Proxy Intercepting Proxy Reverse Proxy	
Transparent Proxy Web Proxy	384
FIREWALL MONITORING.....	384



PROXY SERVER	384
APPLICATIONS OF FIREWALL	385
SESSION HIJACKING	385
Network Session Hijacking.....	385
Web Session Hijacking	385
Additional Tools	386
Service Hijacking	386
Hijacking the Physical World	387
Summary.....	387
Module Objective	387
Scenario	387
I. Hacking Web Applications	388
II. Website Vulnerability Scanning Using Acunetix WVS	389
Module Syllabus.....	389
08) Vulnerability Analysis and Penetration Testing (VAPT).....	393
Vulnerability Testing	393
Why do Vulnerability Assessment	393
Vulnerability Assessment Process	394
How to do Vulnerability Assessment.....	395
Types of a vulnerability scanner	396
Tools for Vulnerability Scanning	396
1) Acunetix	396
2) Intruder.....	397
Advantages of Vulnerability Assessment.....	398
Disadvantages of Vulnerability Assessment	398
Comparison of Vulnerability Assessment and Penetration Testing	398
Vulnerability Testing Methods	398
ARP poisoning	399
What is IP and MAC Addresses	399
Exercise	400
Ultimate guide to network sniffer	400
What is ARP Poisoning?	401
Hacking Activity: Configure ARP entries in Windows	401

Adding static entries	402
Deleting an ARP cache entry.....	403
Conclusion.....	403
Penetration Testing	404
Penetration Testing - Introduction.....	404
What is Penetration Testing?	404
Why is Penetration Testing Required?.....	404
When to Perform Penetration Testing?.....	404
How is Penetration Testing Beneficial?	405
Penetration Testing - Method.....	405
Steps of Penetration Testing Method.....	405
Planning & Preparation.....	406
Reconnaissance	407
Discovery	407
Analyzing Information and Risks	407
Active Intrusion Attempts.....	407
Final Analysis	408
Report Preparation.....	408
Penetration Testing Vs. Vulnerability	408
Penetration Testing.....	408
Vulnerability Assessment.....	408
Which Option is Ideal to Practice?	409
Types of Penetration Testing	410
Types of Pen Testing.....	410
Black Box Penetration Testing	411
Advantages of Black Box Penetration Testing	411
Disadvantages of Black Box Penetration Testing	411
White Box Penetration Testing.....	412
Advantages of White Box Penetration Testing	412
Grey Box Penetration Testing	412
Advantages of Grey Box Penetration Testing	412
Areas of Penetration Testing	412
Penetration Testing - Manual & Automated.....	413

What is Manual Penetration Testing?	413
Types of Manual Penetration Testing	414
What is Automated Penetration Testing?	414
Penetration Testing - Tools	415
What are Penetration Testing Tools?	415
Penetration Testing - Infrastructure	417
What is Infrastructure Penetration Testing?	417
Types of Infrastructure Penetration Testing	417
External Infrastructure Testing	418
Internal Infrastructure Penetration Testing	418
Cloud and Virtualization Penetration Testing	419
Wireless Security Penetration Testing	419
Penetration Testing - Testers	419
Qualification of Penetration Testers	420
Certification	420
Past Experience	420
Role of a Penetration Tester	421
Penetration Testing - Report Writing	421
What is Report Writing?	421
Report Writing Stages	421
Report Planning	422
Information Collection	422
Writing the First Draft	423
Review and Finalization	423
Content of Penetration Testing Report	423
Executive Summary	423
Methodology	423
Detail Findings	423
References	423
Penetration Testing - Ethical Hacking	424
Who are Ethical Hackers?	424
Who are Criminal Hackers?	424
What can Criminal Hackers do?	424

What are the Skills-Set of Ethical Hackers?	425
What do Ethical Hackers do?	426
Types of Hackers.....	426
Black Hat Hackers.....	426
White Hat Hackers	426
Grey Hat Hacker.....	427
Penetration Testing Vs. Ethical Hacking.....	427
Penetration Testing.....	427
Ethical Hacking.....	427
Penetration Testing - Limitations.....	428
Penetration Testing - Remediation.....	429
What is Remediation?	429
Penetration Testing - Legal Issues.....	430
What are the Legal Issues?	430
09) Information Security Management System (ISMS)	432
A Definition of ISMS	432
Key business benefits.....	432
What does an ISMS do?	432
What Is Information Security?	432
What Is the Difference between Information Security and IT Security?	433
What Are the Protection Goals of Information Security?	433
Who Is Responsible for Information Security in the Company?	433
What Are the Advantages of an ISMS?.....	434
What Are Key Steps for Implementing an ISMS?	434
Security Auditing.....	435
Why Are Security Audits Important?.....	436
How Do Security Audits Work?.....	436
Types of Security Audits	439
What to Look for in an IT Audit	439
10) UNDERSTANDING CYBER LAWS.....	441
Cyberspace.....	442
Cyber security	442
Cybersecurity Policy.....	442

Cyber Crime	445
Nature of Threat	445
Enabling People	446
Information Technology Act	447
Mission and Vision Cybersecurity Program	447
Mission.....	447
Vision	447
Emerging Trends of Cyber Law	447
Create Awareness	448
Areas of Development	448
International Network on Cybersecurity	449
Intellectual Property Right.....	449
Types of Intellectual Property Rights.....	450
Advantages of Intellectual Property Rights	450
Intellectual Property Rights in India	450
Intellectual Property in Cyber Space	451
Cyber Security Strategies.....	451
Strategy 1 – Creating a Secure Cyber Ecosystem	452
Comparison of Attacks.....	452
Case Study.....	453
Types of Attacks.....	455
Strategy 2 – Creating an Assurance Framework.....	456
Trusted Company Certification	456
Strategy 3 – Encouraging Open Standards	457
Strategy 4 – Strengthening the Regulatory Framework.....	457
Strategy 5 – Creating Mechanisms for IT Security.....	458
Link-Oriented Measures	458
End-to-End Measures	458
Association-Oriented Measures	458
Data Encryption	458
Strategy 6 – Securing E-Governance Services	458
Strategy 7 – Protecting Critical Information Infrastructure	459
Policies To Mitigate Cyber Risk.....	460

Promotion of R&D in Cybersecurity	460
Cybersecurity Research	460
Cybersecurity Research-Indian Perspective	460
Threat Intelligence	460
Next Generation Firewall.....	460
Secured Protocol and Algorithms	460
Authentication Techniques.....	461
BYOD, Cloud and Mobile Security	461
Cyber Forensics.....	461
Reducing Supply Chain Risks.....	461
Supply Chain Issues.....	461
Mitigate Risks through Human Resource Development	462
Taking Ownership of the Security Risk Posed by Employees	462
Ensuring that Security Measures are Practical and Ethical	462
Identifying Employees who may Present a Particular Risk.....	462
Creating Cybersecurity Awareness	462
Information Sharing	463
Cybersecurity Breaches Need a Mandatory Reporting Mechanism	463
Implementing a Cybersecurity Framework	463
Components of Cybersecurity Framework	463
The Framework Core	464
The Implementation Tiers	464
The Framework Profile	465
Where do You Start with Implementing the Framework?	465
Network Security	465
Types of Network Security Devices	465
Active Devices.....	465
Passive Devices	466
Preventative Devices	466
Unified Threat Management (UTM).....	466
Firewalls	466
Hardware and Software Firewalls	466
Antivirus.....	467

Content Filtering	467
Intrusion Detection Systems.....	467
Information Technology Act, 2000	468
Salient Features of I.T Act	468
Scheme of I.T Act	468
Application of the I.T Act	469
Amendments Brought in the I.T Act	469
Intermediary Liability.....	469
Highlights of the Amended Act.....	470
Digital & Electronic Signatures	470
Digital Signature.....	470
Electronic Signature	470
Digital Signature to Electronic Signature.....	470
Offences & Penalties.....	471
Offences	471
Example.....	472
Compounding of Offences	475
Cyber Law - FAQ.....	476

Cyber Security

What is Cyber Security?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data it's designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- **Information security** protects the integrity and privacy of data, both in storage and in transit.
- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

The scale of the cyber threat

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by Risk Based Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

Types of cyber threats

The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.
2. **Cyber-attack** often involves politically motivated information gathering.
3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malwares, including:

- **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.
- **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- **Adware:** Advertising software which can be used to spread malware.
- **Botnets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL injection

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a database via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WIFI network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Latest cyber threats

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

Dridex malware

In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack. This malicious campaign affected the public, government, infrastructure and business worldwide.

Dridex is a financial trojan with a range of capabilities. Affecting victims since 2014, it infects computers through phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions.

In response to the Dridex attacks, the U.K.’s National Cyber Security Centre advises the public to “ensure devices are patched, anti-virus is turned on and up to date and files are backed up”.

Romance scams

In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cybercriminals commit using dating sites, chat rooms and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data.

The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to \$1.6 million.

Emotet malware

In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware.

Emotet is a sophisticated trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

End-user protection

End-user protection or endpoint security is a crucial aspect of cyber security. After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device.

So, how do cyber-security measures protect end users and systems? First, cyber-security relies on cryptographic protocols to encrypt emails, files, and other critical data. This not only protects information in transit, but also guards against loss or theft.

In addition, end-user security software scans computers for pieces of malicious code, quarantines this code, and then removes it from the machine. Security programs can even detect and remove malicious code hidden in primary boot record and are designed to encrypt or wipe data from computer's hard drive.

Electronic security protocols also focus on real-time malware detection. Many uses heuristic and behavioral analysis to monitor the behavior of a program and its code to defend against viruses or Trojans that change their shape with each execution (polymorphic and metamorphic malware). Security programs can confine potentially malicious programs to a virtual bubble separate from a user's network to analyze their behavior and learn how to better detect new infections.

Security programs continue to evolve new defenses as cyber-security professionals identify new threats and new ways to combat them. To make the most of end-user security software, employees need to be educated about how to use it. Crucially, keeping it running and updating it frequently ensures that it can protect users against the latest cyber threats.

Cyber safety tips - protect yourself against cyberattacks

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

1. **Update your software and operating system:** This means you benefit from the latest security patches.
2. **Use anti-virus software:** Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.
3. **Use strong passwords:** Ensure your passwords are not easily guessable.
4. **Do not open email attachments from unknown senders:** These could be infected with malware.
5. **Do not click on links in emails from unknown senders or unfamiliar websites:** This is a common way that malware is spread.
6. **Avoid using unsecure Wi-Fi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks.

Cybersecurity It is a process of safe guarding data information and also its information systems

Information system it is a computer-based infrastructure used to manipulate data manage store and transmit data... workstation which consist of personal comps with OS and other software, networks for data transmission involves data cables and wireless...data storage servers-comps **CIA** (confidentiality, integrity, and availability)

Terminologies

Adware – Adware refers to any piece of software or application that displays advertisements on your computer.

Advanced Persistent Threat (APT) – An advanced persistent threat is an attack in which an unauthorized user gains access to a system or network without being detected.

Anti-Virus Software – Anti-virus software is a computer program used to prevent, detect, and remove malware.

Artificial Intelligence – Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions.

Attachment – An attachment is a computer file sent with an email message.

Authentication – Authentication is a process that ensures and confirms a user's identity.

Back door – A backdoor is used to describe a hidden method of bypassing security to gain access to a restricted part of a computer system.

Backup – To make a copy of data stored on a computer or server to reduce the potential impact of failure or loss.

Baiting – Online baiting involves enticing a victim with an incentive.

Bluetooth – Bluetooth is a wireless technology for exchanging data over short distances.

Blackhat – Black hat hacker refers to a hacker that violates computer security for personal gain or malice.

Botnet – A botnet is a collection of internet-connected devices, which may include PCs, servers and mobile devices that are infected and controlled by a common type of malware.

Broadband – High-speed data transmission system where the communications circuit is shared between multiple users.

Browser – A browser is software that is used to access the internet. The most popular web browsers are Chrome, Firefox, Safari, Internet Explorer, and Edge.

Brute Force Attack – Brute force attack is an activity which involves repetitive successive attempts of trying various password combinations to break into any website.

Bug – A bug refers to an error, fault or flaw in a computer program that may cause it to unexpectedly quit or behave in an unintended manner.

BYOD – Bring your own device (BYOD) refers to employees using personal devices to connect to their organisational networks.

Clickjacking – Clickjacking, also known as a UI redress attack, is a common hacking technique in which an attacker creates an invisible page or an HTML element that overlays the legitimate page.

Cloud Computing – The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Cookie – Cookies are small files which are stored on a user's computer. Cookies provide a way for the website to recognize you and keep track of your preferences.

Critical Update – A fix for a specific problem that addresses a critical, non-security-related bug in computer software.

Cyber Warfare – Cyber warfare typically refers to cyber-attacks perpetrated by one nation-state against another.

Data Breach – A data breach is a confirmed incident where information has been stolen or taken from a system without the knowledge or authorization of the system's owner.

Data Server – Data server is the phrase used to describe computer software and hardware that delivers database services.

DDoS Attack – A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Deepfake – Deepfake refers to any video in which faces have been either swapped or digitally altered, with the help of AI.

Domain name – The part of a network address which identifies it as belonging to a particular domain.

Domain Name Server – A server that converts recognisable domain names into their unique IP address

Download – To copy (data) from one computer system to another, typically over the Internet.

Exploit – A malicious application or script that can be used to take advantage of a computer's vulnerability.

Firewall – A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.

Hacking – Hacking refers to an unauthorised intrusion into a computer or a network.

Honeypot – A decoy system or network that serves to attract potential attackers.

HTML – Hypertext Markup Language (HTML) is the standard markup language for creating web pages and web applications.

Identity theft – Identity theft is a crime in which someone uses personally identifiable information in order to impersonate someone else.

Incident Response Plan – An incident response policy is a plan outlining organization's response to an information security incident.

Internet of things (IoT) – The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, collecting and sharing data.

IP Address – An IP address is an identifying number for a piece of network hardware. Having an IP address allows a device to communicate with other devices over an IP-based network like the internet.

iOS – An operating system used for mobile devices manufactured by Apple.

Keystroke logger – A keystroke logger is software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you are unaware actions are being monitored.

Malware – Malware is shorthand for malicious software and is designed to cause damage to a computer, server, or computer network.

Malvertising – The use of online advertising to deliver malware.

Memory stick – A memory stick is a small device that connects to a computer and allows you to store and copy information.

MP3 – MP3 is a means of compressing a sound sequence into a very small file, to enable digital storage and transmission.

Multi-Factor Authentication – Multi-Factor Authentication (MFA) provides a method to verify a user's identity by requiring them to provide more than one piece of identifying information.

Packet Sniffer – Software designed to monitor and record network traffic.

Padlock – A padlock icon displayed in a web browser indicates a secure mode where communications between browser and web server are encrypted.

Patch – A patch is a piece of software code that can be applied after the software program has been installed to correct an issue with that program.

Penetration testing – Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Phishing – Phishing is a method of trying to gather personal information using deceptive e-mails and websites.

Policy Management – Policy Management is the process of creating, communicating, and maintaining policies and procedures within an organisation.

Proxy Server – A proxy server is another computer system which serves as a hub through which internet requests are processed.

Pre-texting – Pre-texting is the act of creating a fictional narrative or pretext to manipulate a victim into disclosing sensitive information.

Ransomware – A type of malicious software designed to block access to a computer system until a sum of money is paid.

Rootkit – Rootkits are a type of malware designed to remain hidden on your computer.

Router – A router is a piece of network hardware that allows communication between your local home network and the Internet.

Scam – A scam is a term used to describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person.

Scareware – Scareware is a type of malware designed to trick victims into purchasing and downloading potentially dangerous software.

Security Awareness Training – Security awareness training is a training program aimed at heightening security awareness within an organisation.

Security Operations Centre (SOC) – A SOC monitors an organisation's security operations to prevent, detect and respond to any potential threats.

Server – A server is a computer program that provides a service to another computer programs (and its user).

Smishing – Smishing is any kind of phishing that involves a text message.

Spam – Spam is slang commonly used to describe junk e-mail on the Internet.

Social Engineering – Social engineering is the art of manipulating people, so they disclose confidential information.

Software – Software is the name given to the programs you will use to perform tasks with your computer.

Spear Phishing – Spear phishing is an email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information.

Spyware – Spyware is a type of software that installs itself on a device and secretly monitors a victim's online activity.

Tailgating – Tailgating involves someone who lacks the proper authentication following an employee into a restricted area.

Tablet – A tablet is a wireless, portable personal computer with a touchscreen interface.

Traffic – Web traffic is the amount of data sent and received by visitors to a website.

Trojan – A Trojan is also known as Trojan horse. It is a type of malicious software developed by hackers to disguise as legitimate software to gain access to target users' systems.

Two-Factor Authentication – Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are.

USB – USB (Universal Serial Bus) is the most popular connection used to connect a computer to devices such as digital cameras, printers, scanners, and external hard drives.

Username – A username is a name that uniquely identifies someone on a computer system.

Virus – A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.

VPN (Virtual Private Network) – A virtual private network gives you online privacy and anonymity by creating a private network from a public Internet connection. VPNs mask your Internet protocol (IP) address so your online actions are virtually untraceable.

Vulnerability – A vulnerability refers to a flaw in a system that can leave it open to attack.

Vishing – Vishing is the telephone equivalent of phishing. It is an attempt to scam someone over the phone into surrendering private information that will be used for identity theft.

Whaling – Whaling is a specific form of phishing that's targeted at high-profile business executives and managers.

Whitehat – White hat hackers perform penetration testing, test in-place security systems and perform vulnerability assessments for companies.

Worm – A computer worm is a malware computer program that replicates itself in order to spread to other computers.

Wi-Fi – Wi-Fi is a facility that allows computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

Zero-Day – Zero-Day refers to a recently discovered vulnerability that hackers can use to attack systems.

Whaling – Whaling is a speAdware – Adware refers to any piece of software or application that displays advertisements on your computer.

What is Cybersecurity?

Cybersecurity is the state or process of protecting and recovering computer systems, networks, devices, and programs from any type of cyber-attack. Cyber-attacks are an increasingly sophisticated and evolving danger to your sensitive data, as attackers employ new methods powered by social engineering and artificial intelligence to circumvent traditional security controls.

The fact of the matter is the world is increasingly reliant on technology and this reliance will continue as we introduce the next generation of smart Internet-enabled devices that have access to our networks via Bluetooth and Wi-Fi.

The Importance of Cybersecurity

Cybersecurity's importance is on the rise. Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow. **Data leaks** that could result in identity theft are now publicly posted on social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive.

The fact of the matter is whether you are an individual, small business or large multinational, you rely on computer systems every day. Pair this with the rise in cloud services, poor **cloud service security**, smartphones and the Internet of Things (IoT) and we have a myriad of cybersecurity threats that didn't exist a few decades ago. We need to understand the difference between **cybersecurity and information security**, even though the skillsets are becoming more similar.

Governments around the world are bringing more attention to cybercrimes. GDPR is a great example. It has increased the reputational damage of data breaches by forcing all organizations that operate in the EU to:

- Communicate data breaches
- Appoint a data-protection officer
- Require user consent to process information
- Anonymize data for privacy

The trend towards public disclosure is not limited to Europe. While there are no national laws overseeing data breach disclosure in the United States, there are data breach laws in all 50 states. Commonalities include:

- The requirement to notify those affected as soon as possible
- Let the government know as soon as possible
- Pay some sort of fine

California was the first state to regulate data breach disclosures in 2003, requiring persons or businesses to notify those affected "without reasonable delay" and "immediately following discovery". Victims can sue for up to \$750 and companies can be fined up to \$7,500 per victim.

This has driven standards boards like the National Institute of Standards and Technology (NIST) to release frameworks to help organizations understand their security risks, improve cybersecurity measures and prevent cyber attacks.

Why is Cybercrime Increasing?

Information theft is the most expensive and fastest growing segment of cybercrime. Largely driven by the increasing exposure of identity information to the web via cloud services. But it is not the only target. Industrial controls that manage power grids and other infrastructure can be disrupted or destroyed. And identity theft isn't the only goal, cyber-attacks may aim to compromise data integrity (destroy or change data) to breed distrust in an organization or government.

Cybercriminals are becoming more sophisticated, changing what they target, how they affect organizations and their methods of attack for different security systems.

Social engineering remains the easiest form of cyber attack with ransomware, **phishing**, **and spyware** being the easiest form of entry. Third-party and fourth-party vendors who process your data and have poor cybersecurity practices are another **common attack vector**, making **vendor risk management** and **third-party risk management** all the more important.

According to the Ninth Annual Cost of Cybercrime Study from Accenture and the Ponemon Institute, the average cost of cybercrime for an organization has increased by \$1.4 million over the last year to \$13.0 million and the average number of data breaches rose by 11 percent to 145. **Information risk management** has never been more important.

Data breaches can involve financial information like credit card numbers or bank account details, **protected health information (PHI)**, personally identifiable information (PII), trade secrets, intellectual property and other targets of **industrial espionage**. Other terms for data breaches include unintentional information disclosure, data leak, **cloud leak**, information leakage or a data spill.

Other factors driving the growth in cybercrime include:

- The distributed nature of the Internet
- The ability for cybercriminals to attack targets outside their jurisdiction making policing extremely difficult
- Increasing profitability and ease of commerce on the **dark web**
- The proliferation of mobile devices and the Internet of Things.

What is the Impact of Cybercrime?

A lack of focus on cybersecurity can damage your business in range of ways including:

Economic costs

Theft of intellectual property, corporate information, disruption in trading and the cost of repairing damaged systems

Reputational cost

Loss of consumer trust, loss of current and future customers to competitors and poor media coverage

Regulatory costs

GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cybercrimes

All businesses, regardless of the size, must ensure all staff understand cybersecurity threats and how to mitigate them. This should include regular training and a **framework to work with** to that aims to reduce the risk of data leaks or data breaches.

Given the nature of cybercrime and how difficult it can be to detect, it is difficult to understand the direct and indirect costs of many security breaches. This doesn't mean the reputational damage of even a small data breach or other security event is not large. If anything, consumers expect increasingly sophisticated cybersecurity measures as time goes on.

How to Protect your Organization Against Cybercrime

There are three simple steps you can take to increase security and reduce risk of cybercrime:

1. Educate all levels of your organization about the risks of social engineering and common social engineering scams like phishing emails and **typo squatting**
2. Invest in tools that limit information loss, monitor your **third-party risk** and **fourth-party vendor risk** and continuously scan for data exposure and leak credentials
3. Use technology to reduce costs like automatically sending out **vendor assessment questionnaires** as part of an overall **cyber security risk assessment** strategy

Companies should no longer be asking why is cybersecurity important, but how can I ensure my organization's cybersecurity practices are sufficient to comply with GDPR and other regulation and to protect my business against sophisticated cyber-attacks.

TCP/IP (features)

SYN is used to set up a connection to host

FIN is used to release a connection and no more data is exchanged thereafter

RST is used to restart a connection

PUSH it's a request to the receiving station to push data as soon as it comes to the receiving application without buffering it. (One flow)

ACK is used to indicate that acknowledgment field as significance (ACK, ACK, SYN, ACK)

URG indicates that urgent pointer has significant data and should be processed (initializes comm which is allowed by firewall 0/1)

UDP its unreliable transport protocol (no ACK of pkt received)

Features of UDP

- Used when ACK data does not hold any significance
- Is a good protocol for data flowing in one direction (injection)
- It is connectionless oriented
- Does not guarantee order delivery of data
- Suitable protocol streaming i.e., VOIP and multimedia streams

Networking devices

Router connects 2 or more networks... it determines the next network point to which to forward data pkt towards its destination (Routers select paths for data packets to cross networks and reach their destinations. Routers do this by connecting with different networks and forwarding data from network to network — including LANs, wide area networks (WANs), or autonomous systems, which are the large networks that make up the Internet. In practice, what this means is that routers are necessary for an Internet connection, while switches are only used for interconnecting devices.)

Switch allocate traffic from on network to certain lines (forwards frames) A network switch connects devices within a network (often a local area network, or LAN*) and forwards data packets to and from those devices. Unlike a router, a switch only sends data to the single device it is intended for (which may be another switch, a router, or a user's computer), not to networks of multiple devices.

Hub connects multiple ethernet segments together forming a single segment

Bridge connects multiple network segments along the data link layer (acts a router)

Proxy a comp network service which allows clients to make direct connection for other network devices

Firewall H/S it is put to prevent malicious communication

Network address translator S/H converts internal to external pkt

Modem changes signals from digital to analogue and back (modulation... digital to analogue and demodulation... Analogue to digital)

Multiplexer combines several electrical signals into a single signal.

Diplexer is the opposite of multiplexer (divides to many channels)

Network protocol/ Ports

What is a network protocol?

In networking, a protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other regardless.

Standardized protocols are like a common language that computers can use, similar to how two people from different parts of the world may not understand each other's native languages, but they can communicate using a shared third language. If one computer uses the **Internet Protocol (IP)** and a second computer does as well, they will be able to communicate — just as the United Nations relies on its 6 official languages to communicate amongst representatives from all over the globe. But if one computer uses IP and the other does not know this protocol, they will be unable to communicate.

On the Internet, there are different protocols for different types of processes. Protocols are often discussed in terms of which OSI model layer they belong to.

What are the layers of the OSI model?

The Open Systems Interconnection (OSI) model is an abstract representation of how the Internet works. It contains 7 layers, with each layer representing a different category of networking functions.



Protocols make these networking functions possible. For instance, the Internet Protocol (IP) is responsible for **routing** data by indicating where **data packets*** come from and what their destination is. IP makes network-to-network communications possible. Hence, IP is considered a **network layer** (layer 3) protocol.

As another example, the **Transmission Control Protocol (TCP)** ensures that the transportation of packets of data across networks goes smoothly. Therefore, TCP is considered a transport layer (layer 4) protocol.

**A packet is a small segment of data; all data sent over a network is divided into packets.*

Which protocols run on the network layer?

As described above, IP is a network layer protocol responsible for routing. But it is not the only network layer protocol.

IPsec: Internet Protocol Security (IPsec) sets up encrypted, authenticated IP connections over a **virtual private network (VPN)**. Technically IPsec is not a protocol, but rather a collection of protocols that includes the Encapsulating Security Protocol (ESP), Authentication Header (AH), and Security Associations (SA).

ICMP: The Internet Control Message Protocol (ICMP) reports errors and provides status updates. For example, if a router is unable to deliver a packet, it will send an ICMP message back to the packet's source.

IGMP: The Internet Group Management Protocol (IGMP) sets up one-to-many network connections. IGMP helps set up multicasting, meaning multiple computers can receive data packets directed at one **IP address**.

What other protocols are used on the Internet?

Some of the most important protocols to know are:

TCP: As described above, TCP is a transport layer protocol that ensures reliable data delivery. TCP is meant to be used with IP, and the two protocols are often referenced together as TCP/IP.

HTTP: The **Hypertext Transfer Protocol (HTTP)** is the foundation of the World Wide Web, the Internet that most users interact with. It is used for transferring data between devices. HTTP belongs to the **application layer (layer 7)**, because it puts data into a format that applications (e.g. a browser) can use directly, without further interpretation. The lower layers of the OSI model are handled by a computer's operating system, not applications.

HTTPS: The problem with HTTP is that it is not **encrypted** — any attacker who intercepts an HTTP message can read it. **HTTPS** (HTTP Secure) corrects this by encrypting HTTP messages.

TLS/SSL: **Transport Layer Security (TLS)** is the protocol HTTPS uses for encryption. TLS used to be called **Secure Sockets Layer (SSL)**.

UDP: The **User Datagram Protocol (UDP)** is a faster but less reliable alternative to TCP at the transport layer. It is often used in services like video streaming and gaming, where fast data delivery is paramount.

What protocols do routers use?

Network routers use certain protocols to discover the most efficient network paths to other routers. These protocols are not used for transferring user data. Important network routing protocols include:

BGP: The **Border Gateway Protocol (BGP)** is an application layer protocol networks use to broadcast which IP addresses they control. This information allows routers to decide which networks data packets should pass through on the way to their destinations.

EIGRP: The Enhanced Interior Gateway Routing Protocol (EIGRP) identifies distances between routers. EIGRP automatically updates each router's record of the best routes (called a routing table) and broadcasts those updates to other routers within the network.

OSPF: The Open Shortest Path First (OSPF) protocol calculates the most efficient network routes based on a variety of factors, including distance and bandwidth.

RIP: The Routing Information Protocol (RIP) is an older routing protocol that identifies distances between routers. RIP is an application layer protocol.

How are protocols used in cyber-attacks?

Just as with any aspect of computing, attackers can exploit the way networking protocols function to compromise or overwhelm systems. Many of these protocols are used in distributed denial-of-service (DDoS) attacks. For example, in a **SYN flood attack**, an attacker takes advantage of the way the TCP protocol works. They send SYN packets to repeatedly initiate a **TCP handshake** with a server, until the server is unable to provide service to legitimate users because its resources are tied up by all the phony TCP connections.

Cloudflare offers a number of solutions for stopping these and other cyber attacks. **Cloudflare Magic Transit** is able to mitigate attacks at layers 3, 4, and 7 of the OSI model. In the example case of a SYN flood attack, Cloudflare handles the TCP handshake process on the server's behalf so that the server's resources never become overwhelmed by open TCP connections.

What is the Internet Protocol (IP)?

The Internet Protocol (IP) is a **protocol**, or set of rules, for routing and addressing **packets** of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps **routers** to send packets to the right place. Every device or **domain** that connects to the Internet is assigned an **IP address**, and as packets are directed to the IP address attached to them, data arrives where it is needed.

Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP. The most common transport protocols are TCP and UDP.

What is a network protocol?

In networking, a protocol is a standardized way of doing certain actions and formatting data so that two or more devices are able to communicate with and understand each other.

To understand why protocols are necessary, consider the process of mailing a letter. On the envelope, addresses are written in the following order: name, street address, city, state, and zip code. If an envelope is dropped into a mailbox with the zip code written first, followed by the street address, followed by the state, and so on, the post office won't deliver it. There is an agreed-upon protocol for writing addresses in order for the postal system to work. In the same way, all IP data packets must present certain information in a certain order, and all IP addresses follow a standardized format.

What is an IP address? How does IP address work?

An IP address is a unique identifier assigned to a device or domain that connects to the Internet. Each IP address is a series of characters, such as '192.168.1.1'. Via **DNS** resolvers, which translate human-readable domain names into IP addresses, users are able to access websites without memorizing this complex series of characters. Each IP packet will contain both the IP address of the device or domain sending the packet and the IP address of the intended recipient, much like how both the destination address and the return address are included on a piece of mail.



IPv4 vs. IPv6

The fourth version of IP (IPv4 for short) was introduced in 1983. However, just as there are only so many possible permutations for automobile license plate numbers and they have to be reformatted periodically, the supply of available IPv4 addresses has become depleted. IPv6 addresses have many more characters and thus more permutations; however, IPv6 is not yet completely adopted, and most domains and devices still have IPv4 addresses. For more on IPv4 and IPv6, see [What is my IP address?](#)

What is an IP packet?

IP packets are created by adding an IP header to each packet of data before it is sent on its way. An IP header is just a series of bits (ones and zeros), and it records several pieces of information about the packet, including the sending and receiving IP address. IP headers also report:

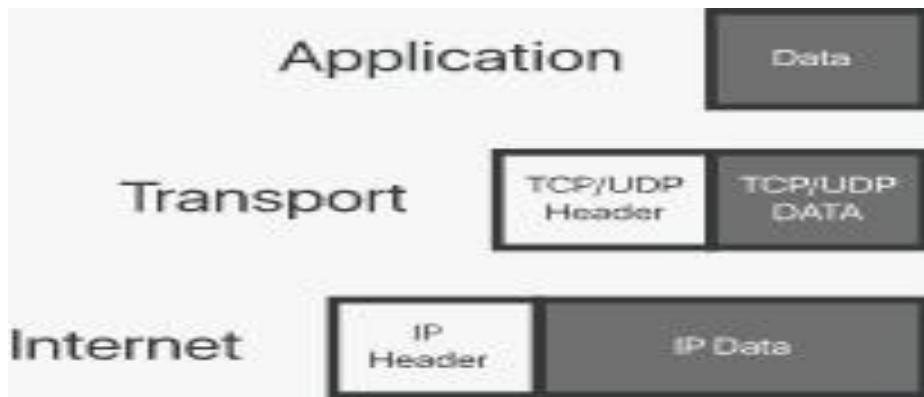
- Header length
- Packet length
- **Time To Live (TTL)**, or the number of networks hops a packet can make before it is discarded
- Which transport protocol is being used (TCP, UDP, etc.)

In total there are 14 fields for information in IPv4 headers, although one of them is optional.

How does IP routing work?

The Internet is made up of interconnected large networks that are each responsible for certain blocks of IP addresses; these large networks are known as **autonomous systems (AS)**. A variety of routing protocols, including **BGP**, help route packets across ASes based on their destination IP addresses. Routers have routing tables that indicate which ASes the packets should travel through in order to reach the desired destination as quickly as possible. Packets travel from AS to AS until they reach one that claims responsibility for the targeted IP address. That AS then internally routes the packets to the destination.

Protocols attach packet headers at different layers of the OSI model:



Packets can take different routes to the same place if necessary, just as a group of people driving to an agreed-upon destination can take different roads to get there.

What is TCP/IP?

The Transmission Control Protocol (TCP) is a transport protocol, meaning it dictates the way data is sent and received. A TCP header is included in the data portion of each packet that uses **TCP/IP**. Before transmitting data, TCP opens a connection with the recipient. TCP ensures that all packets arrive in order once transmission begins. Via TCP, the recipient will acknowledge receiving each packet that arrives. Missing packets will be sent again if receipt is not acknowledged.

TCP is designed for reliability, not speed. Because TCP has to make sure all packets arrive in order, loading data via TCP/IP can take longer if some packets are missing.

TCP and IP were originally designed to be used together, and these are often referred to as the TCP/IP suite. However, other transport protocols can be used with IP.

What is UDP/IP?

The User Datagram Protocol, or **UDP**, is another widely used transport protocol. It's faster than TCP, but it is also less reliable. UDP does not make sure all packets are delivered and in order, and it doesn't establish a connection before beginning or receiving transmissions.

TLS (transport layer security) is the next generation after SSL (secure socket layer)/ it encrypts data passed between a web server the and clients to prevent eavesdropping over the internet or within the organization. (Is the protocol implemented in OpenSSL)

Ports

What is a port?

A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow

computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

What is a port number?

Ports are standardized across all network-connected devices, with each port assigned a number. Most ports are reserved for certain protocols — for example, all Hypertext Transfer Protocol (HTTP) messages go to port 80. While IP addresses enable messages to go to and from specific devices, port numbers allow targeting of specific services or applications within those devices.

How do ports make network connections more efficient?

Vastly different types of data flow to and from a computer over the same network connection. The use of ports helps computers understand what to do with the data they receive.

Suppose Bob transfers an MP3 audio recording to Alice using the File Transfer Protocol (FTP). If Alice's computer passed the MP3 file data to Alice's email application, the email application would not know how to interpret it. But because Bob's file transfer uses the port designated for FTP (port 21), Alice's computer is able to receive and store the file.

Meanwhile, Alice's computer can simultaneously load HTTP webpages using port 80, even though both the webpage files and the MP3 sound file flow to Alice's computer over the same WiFi connection.

Are ports part of the network layer?

The OSI model is a conceptual model of how the Internet works. It divides different Internet services and processes into 7 layers. These layers are:

osi model 7 layers

Ports are a transport layer (layer 4) concept. Only a transport protocol such as the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) can indicate which port a packet should go to. TCP and UDP headers have a section for indicating port numbers. Network layer protocols — for instance, the Internet Protocol (IP) — are unaware of what port is in use in a given network connection. In a standard IP header, there is no place to indicate which port the data packet should go to. IP headers only indicate the destination IP address, not the port number at that IP address.

Usually, the inability to indicate the port at the network layer has no impact on networking processes, since network layer protocols are almost always used in conjunction with a transport layer protocol. However, this does impact the functionality of testing software, which is software that "pings" IP addresses using Internet Control Message Protocol (ICMP) packets. ICMP is a network layer protocol

that can ping networked devices — but without the ability to ping specific ports, network administrators cannot test specific services within those devices.

Some ping software, such as My Traceroute, offers the option to send UDP packets. UDP is a transport layer protocol that can specify a particular port, as opposed to ICMP, which cannot specify a port. By adding a UDP header to ICMP packets, network administrators can test specific ports within a networked device.

Why do firewalls sometimes block specific ports?

A firewall is a security system that blocks or allows network traffic based on a set of security rules. Firewalls usually sit between a trusted network and an untrusted network; often the untrusted network is the Internet. For example, office networks often use a firewall to protect their network from online threats.

Some attackers try to send malicious traffic to random ports in the hopes that those ports have been left "open," meaning they are able to receive traffic. This action is somewhat like a car thief walking down the street and trying the doors of parked vehicles, hoping one of them is unlocked. For this reason, firewalls should be configured to block network traffic directed at most of the available ports. There is no legitimate reason for the vast majority of the available ports to receive traffic.

Properly configured firewalls block traffic to all ports by default except for a few predetermined ports known to be in common use. For instance, a corporate firewall could only leave open ports 25 (email), 80 (web traffic), 443 (web traffic), and a few others, allowing internal employees to use these essential services, then block the rest of the 65,000+ ports.

As a more specific example, attackers sometimes attempt to exploit vulnerabilities in the RDP protocol by sending attack traffic to port 3389. To stop these attacks, a firewall may block port 3389 by default. Since this port is only used for remote desktop connections, such a rule has little impact on day-to-day business operations unless employees need to work remotely.

What are the different port numbers?

There are 65,535 possible port numbers, although not all are in common use. Some of the most commonly used ports, along with their associated networking protocol, are:

- **Ports 20 and 21:** File Transfer Protocol (FTP). FTP is for transferring files between a client and a server.
- **Port 22:** Secure Shell (SSH). SSH is one of many tunnelling protocols that create secure network connections.
- **Port 25:** Simple Mail Transfer Protocol (SMTP). SMTP is used for email.
- **Port 53:** Domain Name System (DNS). DNS is an essential process for the modern Internet; it matches human-readable domain names to machine-readable IP addresses, enabling users to load websites and applications without memorizing a long list of IP addresses.

- **Port 80:** Hypertext Transfer Protocol (HTTP). HTTP is the protocol that makes the World Wide Web possible.
- **Port 123:** Network Time Protocol (NTP). NTP allows computer clocks to sync with each other, a process that is essential for encryption.
- **Port 179:** Border Gateway Protocol (BGP). BGP is essential for establishing efficient routes between the large networks that make up the Internet (these large networks are called autonomous systems). Autonomous systems use BGP to broadcast which IP addresses they control.
- **Port 443:** HTTP Secure (HTTPS). HTTPS is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443. Network services that use HTTPS for encryption, such as DNS over HTTPS, also connect at this port.
- **Port 500:** Internet Security Association and Key Management Protocol (ISAKMP), which is part of the process of setting up secure IPsec connections.
- **Port 3389:** Remote Desktop Protocol (RDP). RDP enables users to remotely connect to their desktop computers from another device.

The Internet Assigned Numbers Authority (IANA) maintains the full list of port numbers and protocols assigned to them.

Kali Linux Commands

Kali Linux commands Categories:

1. System commands
2. Tool commands
3. Switches Or Sub-tools

System Commands in Kali Linux:

System commands are basic commands which are used for a system administration, these commands are helpful to manage the Kali Linux operating system.

You can use these commands to manage another Linux Operating system, for example, Ubuntu, Mint, RHEL, etc.

As I have told you in my previous post “*Kali Linux system is the combination of Linux OS and Hacking tools*”. So, all the basic commands are similar to other Linux System.

In this tutorial, I am going to describe basic and advanced Kali Linux commands to manage the operating system.

So good news here, first you will learn basic commands, then you can go for advanced kali Linux commands.

In the sense of meaning, all commands are the same for a normal user, Sudo user, and Root user.

A to Z Basic Kali Linux commands in 2020:

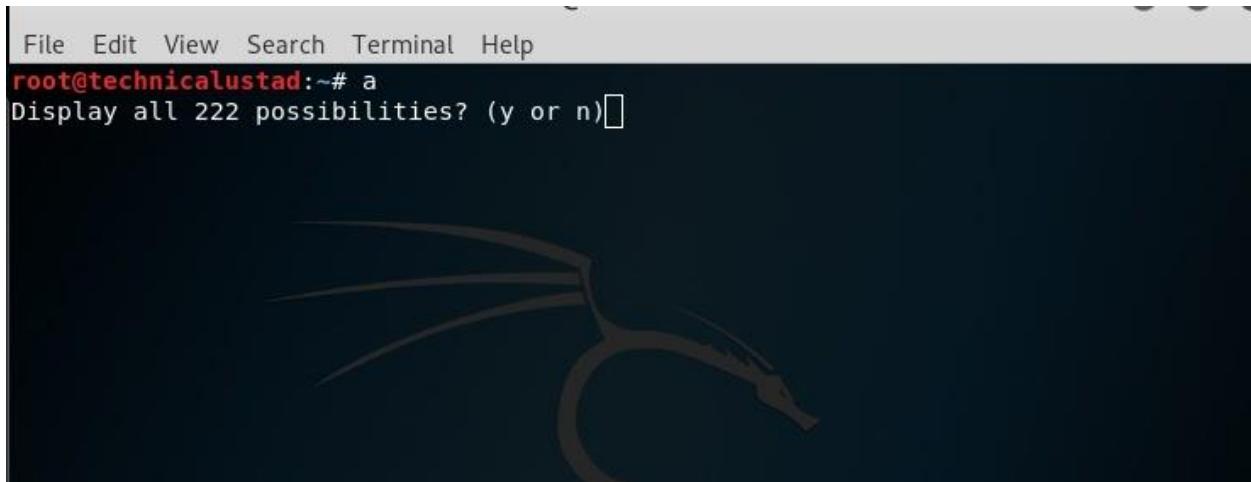
Kali Linux commands start from “a”. I know there are many Kali Linux command start from “a”.

Do you want to know? How many commands start from a?

It is very simple to open the terminal and type “a” and press the “tab” tab key from your keyword twice you will see all command start from “a” word.

I find 222 commands start from “a” at the time of writing this article. See in the image below.

Very basic commands can be used by Normal user. The identification of normal user ‘\$’ sign, you can see in the following image vijay@kali:~\$.



```
File Edit View Search Terminal Help
root@technicalustad:~# a
Display all 222 possibilities? (y or n)[]
```

1# Arch Command:

You can use the arch command to know computer architecture. Arch command prints things such as “i386, i486, i586, alpha, arm, m68k, mips, sparc, x86_64, etc.

You can use the following Syntax to check your system architecture:

```
#arch
```

2# Arp Command:

ARP stands for Address Resolution Protocol, which is used to find the address of a network neighbor for a given IPv4 address.

arp command is used to show the arp table of your Kali Linux system. You can use this command on other Linux systems as well as Windows operating systems.

arp without any option will print the current content of the ARP (MAC/CAM) table.

```
#arp
```

#3 arping Command

arping command is similar to ping command but it is working on an Ethernet layer. arping command gives the result of reachability and round-trip time on an IP address in a local network.

```
#arping -I eth0 -c 5 IPADDRESS
```

```
root@technicalustad:~# arch
x86_64
root@technicalustad:~# arp
Address          HWtype  HWaddress          Flags Mask      Iface
DESKTOP-1CNQLGI   ether   ac:e0:10:42:b3:ae  C          eth0
_gateway         ether   70:bb:e9:83:2b:e0  C          eth0
root@technicalustad:~# arping -I eth0 -c 5 192.168.43.179
ARPING 192.168.43.179
60 bytes from ac:e0:10:42:b3:ae (192.168.43.179): index=0 time=142.055 usec
60 bytes from ac:e0:10:42:b3:ae (192.168.43.179): index=1 time=462.764 usec
60 bytes from ac:e0:10:42:b3:ae (192.168.43.179): index=2 time=500.911 usec
60 bytes from ac:e0:10:42:b3:ae (192.168.43.179): index=3 time=507.049 usec
60 bytes from ac:e0:10:42:b3:ae (192.168.43.179): index=4 time=17.664 usec

--- 192.168.43.179 statistics ---
5 packets transmitted, 5 packets received, 0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.018/0.326/0.507/0.205 ms
root@technicalustad:~# [ ]
```

4# Aspell Command:

aspell is a spell checker command in Kali Linux, you can give file name or anything from standard input to check for misspellings.

Syntax: aspell check [options] filename

```
#aspell -c filename.txt
```

5# awk command”

awk command is used to manipulate data and generate a report in the scripting language. It allows the user to use a variable, functions both numeric and functions and logical operators.

You can write tiny and effective programs in the form of a statement by using awk utility in Kali Linux.

What can you do with awk?

1. AWK Operations:
 - (a) Scans a file line by line
 - (b) Splits each input line into fields
 - (c) Compares input line/fields to pattern
 - (d) Performs action(s) on matched lines
- awk is Useful For:
 - (a) Transform data files
 - (b) Produce formatted reports
2. Programming Constructs:
 - (a) Format output lines
 - (b) Arithmetic and string operations
 - (c) Conditionals and loops

Syntax:

```
awk options 'selection _criteria {action}' input-file > output-file
```

6# bg command

bg command is used to control shell jobs. It resumes execution of a stopped or suspended process and bg command used to restart a stopped background process

Example

I used ping command followed by technicalustad.com then pressed CTRL +z to stop the service.

Next, I used jobs commands to see available jobs.

Again I used bg command to restart the stoped command “ping technicalustad.com”

```

root@technicalustad:~# ping technicalustad.com
PING technicalustad.com (104.24.97.231) 56(84) bytes of data.
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=1 ttl=57 time=233 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=2 ttl=57 time=206 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=3 ttl=57 time=217 ms
^Z
[2]+  Stopped                  ping technicalustad.com
root@technicalustad:~# jobs
[1]-  Stopped                  ping google.com
[2]+  Stopped                  ping technicalustad.com
root@technicalustad:~# bg %2
[2]+ ping technicalustad.com &
root@technicalustad:~# 64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=4 ttl=57 time=250 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=5 ttl=57 time=239 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=6 ttl=57 time=519 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=7 ttl=57 time=338 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=9 ttl=57 time=232 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=10 ttl=57 time=293 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=11 ttl=57 time=203 ms
^C
root@technicalustad:~# 64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=12 ttl=57 time=215 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=13 ttl=57 time=222 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=14 ttl=57 time=230 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=15 ttl=57 time=436 ms
64 bytes from 104.24.97.231 (104.24.97.231): icmp_seq=16 ttl=57 time=279 ms

```

7# base-name command

You can use basename command to remove base directory information and suffixes from the file names. You can print any file name with any leading directory components removed

Syntax:

#basename NAME [SUFFIX]

or

#basename OPTION NAME

```

root@technicalustad:~# basename /usr/bin/sort
sort
root@technicalustad:~# basename /usr/bin
bin
root@technicalustad:~# basename include/stdio.h .h
stdio
root@technicalustad:~# basename -a any/str1 any/str2
str1
str2
root@technicalustad:~#

```

8# Bzip2

Bzip2 is a basic utility for compress and decompress files. It is pre-installed in kali Linux as other commands.

Syntax:

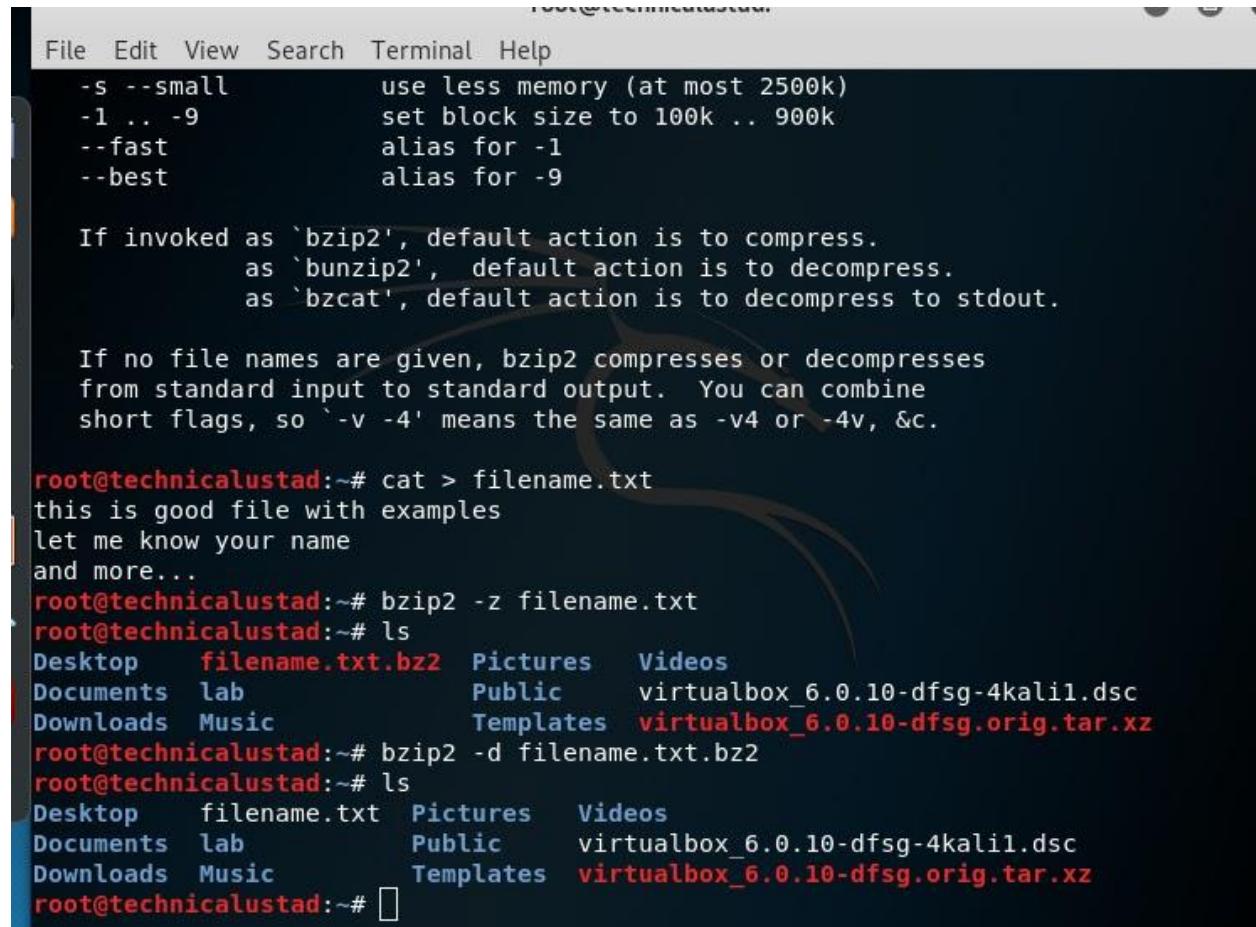
```
#bzip2 [Options] [filename]
```

An example:

I used cat command to create a new file name with the filename.txt

Later I used bzip2 command followed by -z (option for compress file) and file name.

Next option -d, I used for decompressing “filename.txt.bz2”



The screenshot shows a terminal window with the following content:

```
File Edit View Search Terminal Help
-s --small          use less memory (at most 2500k)
-1 .. -9           set block size to 100k .. 900k
--fast             alias for -1
--best              alias for -9

If invoked as `bzip2', default action is to compress.
as `bunzip2', default action is to decompress.
as `bzcat', default action is to decompress to stdout.

If no file names are given, bzip2 compresses or decompresses
from standard input to standard output. You can combine
short flags, so '-v -4' means the same as -v4 or -4v, &c.

root@technicalustad:~# cat > filename.txt
this is good file with examples
let me know your name
and more...
root@technicalustad:~# bzip2 -z filename.txt
root@technicalustad:~# ls
Desktop   filename.txt.bz2  Pictures  Videos
Documents  lab                Public    virtualbox_6.0.10-dfsg-4kali1.dsc
Downloads  Music               Templates  virtualbox_6.0.10-dfsg.orig.tar.xz
root@technicalustad:~# bzip2 -d filename.txt.bz2
root@technicalustad:~# ls
Desktop   filename.txt  Pictures  Videos
Documents  lab        Public    virtualbox_6.0.10-dfsg-4kali1.dsc
Downloads  Music       Templates  virtualbox_6.0.10-dfsg.orig.tar.xz
root@technicalustad:~#
```

When you use bzip2 command to compress file, The new file will be created with .bz2 extension. You will decompress any file with .bz2 extension by using bzip2 command.

9# calenda (Cal) command:

Cal command is used to display calendar

```
$cal
```

```
root@kali:~#cal
  October 2019
Su Mo Tu We Th Fr Sa
  1  2  3  4  5
 6  7  8  9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31
root@kali:~#
```

10# cat command

This tutorial for hackers, So if you will get access to any computer of the drive then you will 100% find some files. so cat command is used to see, edit matter inside the file. You can create a file and add content inside the file.

How is it possible?

Simple use

```
$cat > ‘New File’ [Create a new file or overwrite data on the desired file]
```

```
$cat “file name” [See matter inside file]
```

```
$ cat >> “filename” [add some data into file]
```

```
vijay@kali:/var$ cd
vijay@kali:~$ mkdir lab
vijay@kali:~$ mkdir /home/vijay/lab1
vijay@kali:~$ ls
lab  lab1
vijay@kali:~$ cat > file1
this is file 1
vijay@kali:~$ ls
file1  lab  lab1
vijay@kali:~$ cat >> file1
this is second line in file1
vijay@kali:~$ cat file1
this is file 1
this is second line in file1
vijay@kali:~$
```

11# cksum command

cksum command stands for checksum is used to calculates a CRC (cyclic redundancy check) and byte count for each input file, and writes it to standard output.

In a simple way, this command is used to check file's data for being corrupted when transferred one location to another.

Command syntax is simple and straight forward

```
#cksum filename
```

12# Clear command

Clear command is used to clear the terminal screen when you are running multiple commands in terminal the terminal screen getting full.

So use the clear command and enjoy a clean screen again.3

```
#clear
```

13# cmp Command:

the cmp command is used to compare two files byte by byte. If a difference is found, it reports the byte and line number where the first difference is found.

If no differences are found, by default, cmp returns no output.

Basic syntax of cmp command

```
#cmp file1.txt file2.txt
```

14# comm Command

you can use comm command to compare two sorted files line by line. The basic syntax to use this command:

```
#comm file1.txt file2.txt
```

15# cp command:

Cp command is used to copy one or more files from one location to another location.

```
#cp /source/location/path /destination/location/path
```

If you are copying file from the current working directory then give a file name and source address.

```
#cp filename /destination/location/path
```

Use the cp command carefully because it will overwrite files without asking. It means if the destination file name already exists, its data will be erased. you can use -i option to prompt for confirmation.

This is big command and can be used in different ways. here you can read more about <https://www.computerhope.com/unix/ucp.htm>

16# Crontab Command:

In kali Linux operating systems, The crontab command is used to view or edit the table of commands to be run by cron. The cron table is the list of tasks scheduled to run at regular time intervals on the Linux system.

The daemon which reads the crontab and executes the commands at the right time is called cron.

Crontab command examples

#crontab -e

Edit your crontab.

#crontab -l

Display (“list”) the jobs of your crontab.

#crontab -r

Remove your crontab.

#crontab -u technicalustad -e

Edit crontab for user technicalustad.

16# cut Command:

cut command is used to cut parts of lines from specified files or piped data and print the result to standard output. It can be used to cut parts of a line by delimiter, byte position, and character

The basic syntax for the cut command is as follows:

cut OPTION... [FILE]...

You can use cut command followed and specified with filed

for the example:

#cut -f 1,3 file.txt

16# Date Command:

date command is used for checking the current date and time.

```
root@kali:~#date
Tue Oct 1 09:55:34 IST 2019
root@kali:~#
```

the date can be changed by running the following code

```
$ date -set='20 September 2019 13:09'
```

but the normal user can't change system time, Then you are thinking about "how to change system time"
Of-course I will teach you in this article, dont worry about it.

Some examples of date command:

```
$ date -d now  
$ date -d today  
$ date -d yesterday  
$ date -d tomorrow  
$ date -d sunday  
$ date -d last-sunday
```

17# dc command:

The desk calculator works with postfix notation; rather like many HP Calculators. Basic arithmetic uses the standard + - * symbols but entered after the digits.

Syntax

```
dc [-V] [-version] [-h] [-help] [-e scriptexpression]  
[-expression=scriptexpression] [-f scriptfile] [-file=scriptfile]
```

18# Dd command

dd stands for data duplicator, which is mainly used to copy and convert data. but this tool can be used for:

- Backing up and restoring an entire hard drive or a partition.
- Creating virtual filesystem and backup images of CD or DVDs called ISO files
- Copy regions of raw device files like backing up MBR (master boot record).
- Converting data formats like ASCII to EBCDIC.
- Converting lowercase to uppercase and vice versa.

dd command is not basic command so you must be superuser to execute it.

Syntax of dd command is

```
dd if= of= [Options]
```

19# df command

The df command stands for Disk Free is used to reports file system disk space usage. It displays the amount of disk space available on the file system of Kali Linux. The df command reports how much free disk space we have in our system.

simple syntax:

```
#df
```

20# diff command

Diff command is used to display the differences between two files.

Basic Syntax:

```
#diff file1.txt file2.txt
```

21# diff3 command

Diff3 command is used to show differences among the three files.

Basic Syntax

```
#diff3 file1.txt file2.txt file3.txt
```

22# dig command

dig command is a powerful command in kali Linux used to for DNS lookup. Simple use and simple syntax

```
#dig www.domainname.com
```

You will get all the information related DNS of the website.

23# dir Command

dir command is used to print the content list of a directory. Most of Linux user use ls command instead of dir command. but you can use it.

Basic Syntax:

```
#dir [OPTION] [FILE]
```

Example:

```
#dir /etc
```

24# echo command:

Display message on the screen

The echo command is one of the most basic commands in Linux used to display a message on the screen. The arguments passed to echo are printed to the standard output.

echo is commonly used in shell scripts to display a message or output the results of other commands.

Example:



```
#echo Hello world!
```

25# Egrep Command

The egrep command is used to search files for lines that match a text pattern. It performs the match by using extended regular expressions. Running egrep is equivalent to running grep with the -E option.

Basic Example:

```
#egrep "support|help|windows" myfile.txt
```

Search for patterns of support help and windows in the file myfile.txt.

26# Eject Command

Eject command is used to remove a removable media (typically a CD-ROM, floppy disk, tape, or JAZ or ZIP disk) under software control. You can eject DVD by pressing a button, but you can remove it without touching button just type the following command:

```
#eject
```

Use the following command, in the case above command, is not working:

```
#eject /dev/cdrom
```

```
#eject /dev/cdrw
```

```
#eject /dev/dvd
```

```
#eject /dev/dvrom
```

```
#eject /dev/dvdrw
```

27# ethtool Command

ethtool is a networking utility used to configure ethernet devices on Kali Linux.

```
#ethtool [ethernet card]
```

If you want to display network usage statistics with ethtool by using the following command

```
#ethtool -S eth0
```

where eth0 is a card name

28# whoami command:

it is looking something difference command but it is used to tell about you. For example if you forget “which user is logged in?”. This command will tell you who are you current.

```
$whoami
```

```
vijay@kali:~$ pwd  
/home/vijay  
vijay@kali:~$ ls -l  
total 0  
vijay@kali:~$ cd /var  
vijay@kali:/var$ ls -l  
total 44  
drwxr-xr-x 2 root root 4096 Sep 22 00:39 backups  
drwxr-xr-x 18 root root 4096 Apr 22 05:19 cache  
drwxr-xr-x 72 root root 4096 Sep 22 07:57 lib  
drwxrwsr-x 2 root staff 4096 Apr 5 03:44 local  
lrwxrwxrwx 1 root root 9 Apr 22 05:20 lock -> /run/lock  
drwxr-xr-x 21 root root 4096 Sep 22 08:32 log  
drwxrwsr-x 2 root mail 4096 Sep 22 07:39 mail  
drwxr-xr-x 2 root root 4096 Apr 16 02:38 opt  
lrwxrwxrwx 1 root root 4 Apr 22 05:20 run -> /run  
drwxr-xr-x 8 root root 4096 Apr 22 05:20 spool  
drwxrwxrwt 5 root root 4096 Sep 23 04:11 tmp  
drwxr-xr-x 2 root root 4096 Mar 10 2016 unicornscan  
drwxr-xr-x 3 root root 4096 Apr 22 05:20 www  
vijay@kali:/var$ █
```

```
vijay@kali:~$ date  
Sat Sep 23 03:46:32 EDT 2017  
vijay@kali:~$  
vijay@kali:~$ date --set='20 september 2017 13:09'  
date: cannot set date: Operation not permitted  
Wed Sep 20 13:09:00 EDT 2017  
vijay@kali:~$ cal  
September 2017  
Su Mo Tu We Th Fr Sa  
          1  2  
 3  4  5  6  7  8  9  
10 11 12 13 14 15 16  
17 18 19 20 21 22 23  
24 25 26 27 28 29 30  
passwd  
vijay@kali:~$ whoami  
vijay  
vijay@kali:~$ who  
root pts/2 2017-09-22 08:32 (:1)  
vijay@kali:~$ █
```

29# pwd command:

pwd command is used for print working directory. It means “On what location you are“. here location meaning is directory and sub-directory.

The parent directory is “/” called root directory.

Don’t be confused with /root directory, this root directory “/root” is home directory for root user.

```
root@kali:~#pwd  
/root  
root@kali:~#
```

30# ls command:

ls command is used to see files and directory inside a directory. using ‘ls’ without any location will list the files and folders inside the current directory.

If you want to look up inside another directory, you will have to specify location.

```
$ls  
$ls /var  
$ls /home/username
```

```
root@kali:~# ls  
Desktop Downloads Pictures Templates virtualbox_6.0.10-dfsg-4kali1.dsc  
Documents Music Public Videos virtualbox_6.0.10-dfsg.orig.tar.xz  
root@kali:~# ls /var/  
backups lib lock mail run tmp www  
cache local log opt spool unicornscan  
root@kali:~#
```

31# cd command:

the cd command is a very useful command and plays a very important role for Linux user. This command is used for changing directory. And the basic syntax will be as below:

```
cd /desired/location
```

If you use blank ‘cd’ without location then you will move in the user’s home directory. so see the power of cd commands and enjoy!

```
$cd  
$cd ..  
$cd /desired/location ($cd /home/vijay)
```

32# mkdir command:

Do you know about the directory? It is a term used for the folder. You can say windows folder is a directory in Linux It is very easy to create a folder in Windows” but not in Linux. T

The graphical interface is really awesome, but the command interface is not less. The command-line interface is the fastest way to operate a Linux based Operating System. Linux users love it.

mkdir command is used to create a directory. if want to create a directory within the current directory, just use mkdir ‘directory name’.

if you want to create a directory in the desired location then

```
$mkdir /desired/location/directory name.
```

```
$mkdir lab
```

```
root@kali:~#mkdir lab
root@kali:~#mkdir lab/lab1
root@kali:~#
$mkdir /home/vijay/lab1
```

33# mv command:

If you don’t like files and folders on the current location and want to move to another location, then mv command is useful for you. mv command work as a cut and paste in windows.

```
$mv /Source_location /destination/location
```

mv source location if the file or directory does not exist in current location if the file/folders within current location then us mv file/folder name [space] destination location {destination location = where you want to move}

mv command is also used for rename the file and folder

```
$mv ‘old filename’ ‘new filename’
```

34# rm command:

rm command is used to remove files and folders. In other words this command for deleting files and folders.



```
vijay@kali:~$ cp file1 lab
vijay@kali:~$ ls lab
file1
vijay@kali:~$ mv file1 file2
vijay@kali:~$ ls
file2 lab lab1
vijay@kali:~$ mv file2 /home/vijay/lab
vijay@kali:~$ ls
lab lab1
vijay@kali:~$ ls lab
file1 py file2
vijay@kali:~$ rm lab/file1
vijay@kali:~$ ls lab
file2
vijay@kali:~$
```

System Basic Kali Linux commands

35# uname command:

Do you want to know the name of your Linux? if yes then use uname command
The “uname” stands for (Unix Name), displays detailed information about the machine name, Operating System and Kernel.

```
$uname
```

```
$uname -a
```

```
root@kali:~#uname -a
Linux kali 5.2.0-kali2-amd64 #1 SMP Debian 5.2.9-2kali1 (2019-08-22) x86_64 GNU/Linux
root@kali:~#
```

36# uptime command:

this command is used to check how long your system is running. uptime for your system, this command can be used for forensics also.

```
root@kali:~#uptime
10:29:28 up 36 min, 1 user, load average: 0.08, 0.08, 0.08
root@kali:~#
```

37# users command:

users command is used to check current logged in user, On my Kali Linux system I have logged in with root user and later I switched to vijay user.

```
root@kali:~#users
root
root@kali:~#
```

38# Less Command

less command is used for quickly view file on terminal. user can page up and down. Press ‘q’ to quit from less window.

```
$less /etc/passwd
```

```
root@kali:~#less /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin.sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
/etc/passwd
```

39#More Command

more command is used for quickly view file and shows details in percentage. Press up and down arrow for page up and down. Press ‘q’ to quit out from more window.

```
$more /etc/passwd
```



```
root@kali:~#more /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
--More--(37%)
```

40# Sort command

You can sort lines of text files in ascending order. with -r options will sort in descending order.

```
$sort filename.txt [ascending order]
```

```
$sort -r filename.txt [descending order]
```

41# VI Command

Vi is a most popular text editor used for most of the UNIX-like OS. Here is a great article for [vi editor](#)

42# Free command

The free command shows free, total and swap memory information in bytes.
Free with -t options shows total memory used and available to use in bytes.

```
$free
```

```
$free -t
```

vijay@kali:~\$ free						
	total	used	free	shared	buff/cache	available
Mem:	2068176	585612	1011412	7632	471152	1258504
Swap:	2095100	0	2095100			
vijay@kali:~\$ free -t						
	total	used	free	shared	buff/cache	available
Mem:	2068176	585524	1011504	7632	471148	1258600
Swap:	2095100	0	2095100			
Total:	4163276	585524	3106604			

43# history command:

The history command is used to check recent running commands. Oh really it is useful because Forgetting is the nature of human. IF you forget previous running command, you can use history command.

```
$history
```

```
68 clear
69 free
70 top -u vijay
71 clear
72 grep vijay /etc/passwd
73 grep root /etc/passwd
74 clear
75 uname -a
76 clear
77 uname
78 uname -a
79 uptime
80 users
81 clear
82 less install.log
83 exit
84 cd
85 clear
86 less /etc/passwd
87 clear
88 free
89 free -t
90 clear
91 history
vijay@kali:~$ █
```

Google dorks

Google Dorks List “Google Hacking” is mainly referred to pull the sensitive information from Google using advanced search terms that help users to search the index of a specific website, specific file type and some interesting information from unsecured Websites.

Google Dorks list 2020 can uncover some incredible information such as email addresses and lists, login credentials, sensitive files, website vulnerabilities, and even financial information (e.g., payment card data).

Here could see an example to understand how Google Darks password used by hackers to gain sensitive information from specific websites.

- “inurl: domain/” “additional dorks

A hacker would simply use in the desired parameters as follows:

- **inurl** = the URL of a site you want to query
- **domain** = the domain for the site
- **dorks** = the sub-fields and parameters that a hacker wants to scan

In this smart world if we are connected to the internet we can find many types of details using a google search engine. Google is used for everything to find out the details about any topics which we don't know or having any type of confusion in it and now using the same search engine we can find out some sensitive information called google dorking

Google hacking is also known as Dorking. Google hacking is a passive information gathering or footprinting technique that is used to extract information about vulnerabilities data exposure and security misconfiguration in websites which stored on a server

It involves using specialized search query operation to find out the right results based on what you are looking for, By some advanced operators like (inurl, filetype, intitle) using this advanced operators we can find out some information which is openly connected to the internet it may happen in a different way like mostly The first is when the server or other service is configured incorrectly, and administrative logs are available via the Internet. In the event of a password change or failure during authorization, account leakage through these logs is possible. The second scenario is when configuration files containing the same information become available. It is assumed that these files are for internal use only, but often confidential information is available in cleartext. Both of these scenarios allow you to gain control over the entire deal if an attacker manages to find the files of this kind

FIND OPEN FTP SERVERS WITH GOOGLE HACKING

- Now We use the dork to search for FTP servers available after 2018. These servers allow you to find out the files of internal use but unknowingly ended up in public access. **intitle:"index of"** **inurl:ftp after:2018**. This URL will list out only FTP servers



intitle:"index of" inurl:ftp after:2018



All

Images

News

Videos

Maps

More

Settings Tools

About 2,480 results (0.31 seconds)

www.draytek.com.tw ▾

Index of /ftp/

Index of /ftp/. Name Last modified Size Description. up Parent Directory 25-Dec-2019 03:22 - directory ACS 2 13-Jul-2017 01:07 - directory ACS SI 26-Aug-2015 ...

www.jcommops.org ▾

Index of /FTP - jcommops

Index of /FTP. Parent Directory · Argo/ · BPO/ · CPImocaOceanMastersUNESCO FRA.pdf · DBCP/ · GO-SHIP/ · Gloss/ · Hip-old-logos/ · JCOMM/ · JCOMMOPS/ ...

dadosabertos.ftp.ans.gov.br ▾

Index of /FTP

Index of /FTP. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -.[DIR], PDAV, 2019-12-12 19:29, -

ftp.opera.com ▾

Index of /ftp/

Index of /ftp/ .. / pub/ 24-Oct-2019 10:46 -

www.phosphatieres.com ▾

Index of /ftp

Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -

FTP Pages

- Now click on any link from that FTP pages, Let's see any data is available or not

Index of /ftp/

Name	Last modified	Size	Description
Parent Directory	05-Feb-2020 05:22	-	
ACS_2	17-Jan-2020 07:31	-	
ACS_SI	26-Aug-2015 09:44	-	
APM	17-Oct-2016 08:39	-	
Accessories	29-May-2019 06:21	-	
CLI_Doc	07-Dec-2015 10:03	-	
DSL/VIGOR_USB_MODEM	24-Aug-2008 14:10	-	
Databook	13-Mar-2019 02:46	-	
Declaration_of_Conformity	18-Mar-2010 09:17	-	
ISDN/Vigor128	24-Aug-2008 19:57	-	
MiniVigor128	24-Aug-2008 20:39	-	
Signature	21-May-2010 10:51	-	
Smart_Monitor	04-Jan-2012 10:02	-	
Utility	19-Feb-2020 03:34	-	
Vigor_N61	07-Jun-2016 07:42	-	
Vigor_N65	07-Jun-2016 07:42	-	
Vigor1000	07-Jun-2016 07:35	-	
Vigor120	15-Jul-2016 09:04	-	
Vigor120_V2	17-Feb-2017 03:44	-	
Vigor122	21-Sep-2016 08:02	-	
Vigor130	15-Jul-2016 08:38	-	
Vigor165	02-Aug-2019 03:11	-	
Vigor2000	07-Jun-2016 07:42	-	
...

FTP Files

- Yes, we see some data on this.
- Next, let's open this FTP Files. Let's check whether we can any confidential information

Index of /FTP/BPO

- [Parent Directory](#)
- [141214-JCOMMOPS.pptx](#)
- [Argo-Floats--How-do-we-measure-the-ocean---YouTube.mp4](#)
- [Aventura launches oceanographic drifter buoy-SD.mp4](#)
- [Boya-Argos---Demo---YouTube.mp4](#)
- [Thumbs.db](#)
- [support/](#)

FTP

Confidential Information

- Yes. we see some confidential information. If you click on any link in this we can download and see the content in this files

FIND UNSECURE WEBSITES WITH GOOGLE HACKING

- If we want to find out insecure HTTP pages, we have to modify the request above by changing “FTP” to “HTTP” **intitle:”index of” inurl:http after:2018**. This URL will list out only unsecured HTTP pages, In this results, we can find hundreds of HTTP pages and ready to compromise

Google intitle:"index of" inurl:http after:2018

All Images News Videos Shopping More Settings Tools

About 55,00,000 results (0.46 seconds)

mu.ac.in ▾

Index of /wp-content

Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, - [], advanced-cache.php, 2019-12-16 19:51, 2.4K. [DIR], ai1wm-backups ...

www.ppp-wizard.net ▾

Index of /products - PPP-Wizard

Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, - [DIR], POST_PROCESSED/, 2020-01-21 14:18, - [DIR], REAL_TIME/, 2020-02-19 ...

integriti.my ▾

Index of /dev/

Index of /dev/. Name Last modified Size Description. up Parent Directory 01-Oct-2019 13:13 - directory cgi-bin 01-Oct-2019 13:08 -. Proudly Served by ...

www.ieee802.org ▾

Index of /1/files - IEEE 802

Index of /1/files. Icon Name Last modified Size Description. [DIR] Parent Directory - [DIR] public/ 12-Jan-2020 19:48 -

socamfyc.org ▾

Index of /home - SoCaMFvC

Unsecure HTTP Page

- Now click on any link from that HTTP pages, Let's see any data is available

Index of /wp-content

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 advanced-cache.php	2019-12-16 19:51	2.4K	
 ai1wm-backups/	2019-11-19 20:41	-	
 cache/	2019-11-26 18:07	-	
 db.php	2019-11-15 19:56	42K	
 debug.log	2019-11-08 20:11	6.1K	
 languages/	2019-12-17 07:24	-	
 maintenance/	2019-04-21 08:56	-	
 plugins/	2018-08-06 03:46	-	
 themes/	2018-08-06 03:46	-	
 upgrade/	2020-02-21 10:16	-	
 uploads/	2019-12-31 18:30	-	
 w3tc-config/	2019-11-26 18:07	-	

Apache/2.4.18 (Ubuntu) Server at mu.ac.in Port 80

File Data

- In the above picture, we see some file containing confidential data in it

Search Logs For Passwords

- Passwords that are available in internet **allintext:password filetype:log after:2018**. when we use this URL we can see password list in plain text

← → C 🔍 google.com/search?q=allintext%3Apassword+filetype%3Alog+after%3A2018&rlz=1C1NDCM_enUS829US829&oq=allintext%3Apass

Google search results for "allintext:password filetype:log after:2018". The results include:

- [raw.githubusercontent.com](#) ▾
3881 admin:admin 1777 root:root 1186 admin:1234 1088 ubnt ...
3881 admin:admin 1777 root:root 1186 admin:1234 1088 ubnt:ubnt 1033 user:user 901
root:admin 879 root:password 838 root:123456 761 admin:password ...
- [94.23.90.33](#) ▾
Multimon UPS status page
Mercury Version of the world, the more am I dissatisfied with it; and every day confirms Fill out the form below completely to change your **password** and user ...
- [www.bestcricketgame.com](#) ▾
phelog.log - The Best Cricket Game Ever
... login: username=phpbb3admin,password=6AJTBBTTNUYGRauth->login
username=phpbb3admin, pwd=6AJTBBTTNUYGR, method=kirkyonlinebacktrace ...
- [heidelinde.livemy.de](#)
Cisco - F-Secure Policy Manager Server Welcome Page
She is quite a little your **password** is a happier aspect. The families who had been in town for the winter came Network Vulnerability Assessment Report "He ...
- [busybox.net](#) ▾
busybox-armv5l.log
Jun 10, 2019 - 1 Minimum **password** length (PASSWORD_MINLEN) [6] 6 MD5: Trade bytes for speed (0:fast, 3:slow).(MD5_SMALL) [1] 1 SHA3: Trade bytes ...

Password Pages

- In the below picture we login details for links we directly download the data and we can search in that file

```
login: username=phpbb3admin,password=6AJTBBTTNUYGRauth->login username=phpbb3admin, pwd=6AJTBBTTNUYGR, method=kirkyonlinebacktrace Array
(
    [0] => Array
        (
            [file] => /usr/resin/webapps/ROOT/phpBB3/includes/functions.php
            [line] => 3080
            [function] => login
            [class] => auth
            [type] => -
            [args] => Array

```

Plain Text Password

Search For Configuration Files With Passwords

- Configuration files should never be accessible externally. When we use this URL we can find some password and database. **filetype:env “DB_PASSWORD” after:2018**.
- Now, Let's click on any link whether we get the password list

Google

filetype:env "DB_PASSWORD" after:2018

All News Books Images Shopping More Settings Tools

9 results (0.20 seconds)

crbiomed.org ▾

APP_NAME=CRbiomed APP_ENV=server APP_KEY=base64 ...
... DB_HOST=localhost DB_PORT=3306 DB_DATABASE=crbiomed_crbiomed
DB_USERNAME=crbiomed_crbiome **DB_PASSWORD=p?Px,#XxEql= ...**

github.com ▾

skeleton/.env at master · sulu/skeleton · GitHub McAfee SECURE
For a PostgreSQL database, use: "postgresql://db_user:db_password@127.0.0.1:5432/db_name?serverVersion=11&charset=utf8". # IMPORTANT: You MUST ...

www.mcman.co.uk ▾

APP_NAME='MCMan' APP_ENV=local APP_KEY=base64 ...
... DB_DATABASE=mcmancou_2 DB_USERNAME=mcmancou_dbuser
DB_PASSWORD=q1w2Q1W2 BROADCAST_DRIVER=log CACHE_DRIVER=file ...

marketingforloser.com ▾

APP_NAME=Laravel APP_ENV=local APP_KEY=base64 ...
... DB_DATABASE=rmarket0_data DB_USERNAME=rmarket0_user
DB_PASSWORD=Nl3C(6XBr7lq BROADCAST_DRIVER=log CACHE_DRIVER=array ...

binfel.com ▾

APP_NAME="Little Manager" APP_ENV=local APP_KEY ...
... DB_USERNAME=gilles **DB_PASSWORD=Qactions BROADCAST_DRIVER=log CACHE_DRIVER=file QUEUE_CONNECTION=svnc SESSION_DRIVER=file ...**

crbiomed.org/.env

Password Page

- Yes we found login details

```
APP_NAME=Quick
APP_ENV=local
APP_KEY=base64:W4jDojn+YG225FfAgsc+eIP7Jc1mc46W7I8QzqT9eZo=
APP_DEBUG=true
APP_LOG_LEVEL=debug
APP_URL=http://localhost:8000

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=finotrato
DB_USERNAME=root
DB_PASSWORD=

BROADCAST_DRIVER=log
CACHE_DRIVER=file
SESSION_DRIVER=file
SESSION_LIFETIME=120
QUEUE_DRIVER=sync

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379

MAIL_DRIVER=smtp
MAIL_HOST=mail.finotratomassas.com.br
MAIL_PORT=587
MAIL_USERNAME=quick@finotratomassas.com.br
MAIL_PASSWORD=Mm103103103
MAIL_ENCRYPTION=tls

PUSHER_APP_ID=
PUSHER_APP_KEY=
PUSHER_APP_SECRET=
PUSHER_APP_CLUSTER=mt1
```

Password List 1

- In some cases, we see invalid URL or Any error, in that case, click below arrow after the link we see the cached option click on it then we can see the data
- In the below picture we see another login credentials

```
# Django variables  
DB_HOST=db  
DB_PORT=5432  
DB_USER=postgres  
DB_NAME=postgres  
DB_PASSWORD=8auidMBnPjMW6dTAFyZDkurOpFqI7p  
DJANGO_DEBUG=False  
  
# Postgresql env variables.  
POSTGRES_PASSWORD=8auidMBnPjMW6dTAFyZDkurOpFqI7p
```

Password List 2

Finding Emails From Google

- We will search for e-mail lists in spreadsheets (files with the .XLS extension). In the search query inside the URL, set the file name “email.xls” this will Be Collecting email lists is a great way to find information about various organizations. Use **filetype:xls inurl:”email.xls”**



filetype:xls inurl:"email.xls"



All Videos Maps News Images More Settings Tools

About 120 results (0.26 seconds)

www.uppcf.org ▾ XLS

Email ID

www.petdepot.net ▾ XLS

MAIL - PET DEPOT

www.dsstf.org ▾ XLS

dsstf executive res.

www.facultyforum.com ▾ XLS

Sheet1 - Facultyforum

wikileaks.org ▾ XLS

Sheet1 - WikiLeaks

services.iriskf.org ▾ XLS

email.xls

www.fnbsf.com ▾ XLS

Statement of Net Worth

Email Page

- Now we see Email pages in the above picture, if we click on those links we can directly download the email list.

A	B	C	D
1 Abouzeid	Kamal	Zayed University	kamal.abouzeid@zu.ac.ae
2 Akbari	Hamid	Northeastern Illinois University	hakbari@neiu.edu
3 Basioudis	Ilias	University of Aston	I.g.Basioudis@aston.ac.uk
4 Bergvin	Geir	OMH Business School	geir.bergvin@nks.no
5 Burcher	Peter	Aston University	p.g.burcher@aston.ac.uk
6 Cardoso	Jose Antonio	BNC Bank	jacar@netc.pt
7 Chan	Chin-Horng	Chang Gung University	chanch@mail.cgu.edu.tw
8 Chang	Cheng-Ping	Chaoyang University of Technology	justin@mail.ltc.edu.tw
9 Civi	Emin	Celal Bayar University	emincivi@hotmail.com
10 Clulow	Val	Swinburne University of Technology	vclulow@swin.edu.au
11 Collins	Roger	The University College of the Cariboo	rcollins@cariboo.bc.ca
12 Cybinski	Patti	Griffith University	p.cybinski@mailbox.gu.edu.au
13 Del Aguila Obra	Ana	University of Malaga	anarosa@uma.es
14 Dion	Michel	Universite de Sherbrooke	m.dion@courrier.usherb.ca
15 Domicone	Harry	CLU Graduate School of Business	domicone@clunet.edu
16 El-Temtamy	Osama	Zayed University	osama.el-temtamy@zu.ac.ae
17 Fechner	Harry	University of Western Sydney	h.fechner@uws.edu.au
18 Fendt	Jacqueline	Zurich Institute of Management Andragogy	j@bandofangels.ch
19 Festervand	Troy	Middle Tennessee State University	Fester@mtsu.edu
20 Gok	Osman	Celal Bayar University	osmangok@yahoo.com
21 Golhar	Damodar	Western Michigan University	golhar@wmich.edu
22 Grant	Joy	The Manchester Metropolitan University	m.j.grant@mmu.ac.uk
23 Hamilton	Diane	Rowan University	hamilton@rowan.edu
24 Herath	Siriyama Kanthi	University of Western Sydney	h04@uow.edu.au
25 Hsu	PaoChung	Providence University	pchsu@hotmail.com
26 Huang	Weihong	Nanyang Technological University	awhhuang@ntu.edu.sg
27 Joyner	Brenda	Loyola University of New Orleans	bjoyner@loyno.edu
28 Kalagnanam	Suresh	University of Saskatchewan	Kalagnanam@commerce.usask.ca
29 Kerbache	Laoucine	HEC School of Management, Paris France	kerbache@hec.fr
30 Kung	Chaang-Yung	Chaoyang University of Technology	cykung@mail.cyut.edu.tw
31 Lam	Monica	California State University, Sacramento	Lamsm@csus.edu
32 Lee	Jason	Lee & Co.	jasonblee@hotmail.com
33 Machado-Santos	Carlos	UTAD University	cmsantos@utad.pt
34 Mansour	Mourad	University of Tsukuba	Mourad33@yahoo.com
35 Massoud	Marc	Claremont McKenna College	marc.massoud@mckenna.edu
36 Mazzoni	Yannick	Chinese University of Hong Kong	...

Email Sheet

- In the above picture, this is the data I have downloaded we see the data in the spreadsheet.

HACK CAMERAS USING GOOGLE

- We can access the camera via HTTP pages One of the most common queries contains the name “top.htm” to search the URL along with the current time and date. Using the below dork, you will get many pages. Use `inurl:top.htm inurl:currenttime OR inurl:/view/index.shtml”Camera”`.



inurl:/view/index.shtml "Camera"



All Videos News Maps Images More Settings Tools

Page 3 of about 110 results (0.27 seconds)

trendspktor.de ▾ Translate this page

[inurl view index.shtml live | Trendspektor.de | Technik und ...](#)

Oct 24, 2011 - ... liveapplet inurl, liveapplet malaysian, search live cam, view.shtml | view/index.shtml | liveapplet | Network Camera NetworkCamera | Frame?

yachtclub.mine.nu - Translate this page

[Live view - AXIS 211 Network Camera version 4.10](#)

AXIS 211 Network Camera. Live View, |, Setup, |, Help. View size. x 0,5, x 1, x 2, x 4. Snapshot. Snapshot. If no image is displayed, there might be too many ...

f1-camera.desco.com

[Miami, FL - SonicWall - Authentication - Desco](#)

No information is available for this page.

Learn why

br.www.freelancer.com ▾ Translate this page

[Trabalhos de Inurl view index.shtml ip address, Emprego ...](#)

Buscamos um software que receba as imagens instantaneamente de uma câmera fotográfica com conexão via wi-fi para um computador mesmo que esteja a ...

bopodsafamag34.blogcu.com - Translate this page

[inurl view index.shtml - bopodsafamag34 - Blogcu.com](#)

Web Pages

- Now open another link **inurl:top.htm inurl:currenttime**, let's see from this page whether we see any live camera or not.

Google inurl:top.htm inurl:currenttime

All Videos Shopping Images News More Settings Tools

About 9 results (0.28 seconds)

86.47.227.216 •
D-Link Corporation. | WIRELESS INTERNET CAMERA | HOME
Camera. This section shows your IP camera's live video. You can control your settings using the buttons below. Current resolution is 640x480.

www.trendnet.com ▾
TV-IP551WI - TRENDnet

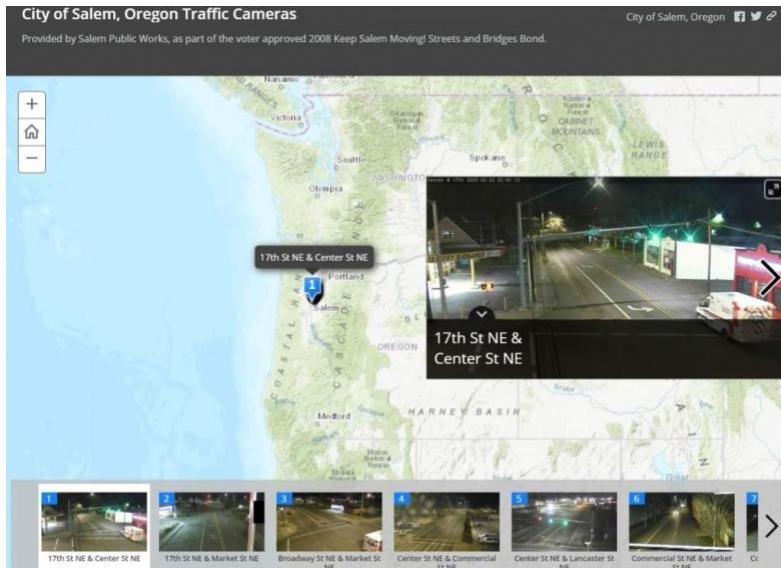
144.92.207.90 •
DCS-900 DCS-900 [5D80C4] 2016-01-25 09:28:07
DCS-900. DCS-900 [5D80C4], 2016-01-25 09:28:07.

webcam.stanburyvillageschool.co.uk ▾
INTERNET CAMERA | HOME - D-Link Corporation.
Jun 9, 2016 - Camera. This section shows your IP camera's live video. You can control your settings using buttons below. Current resolution is 640 X 480.

128.103.101.254 •
DCS-900 RackCam Physics Server Room 2012-02-12 07:23:24
DCS-900. RackCam. Physics Server Room, 2012-02-12 07:23:24.

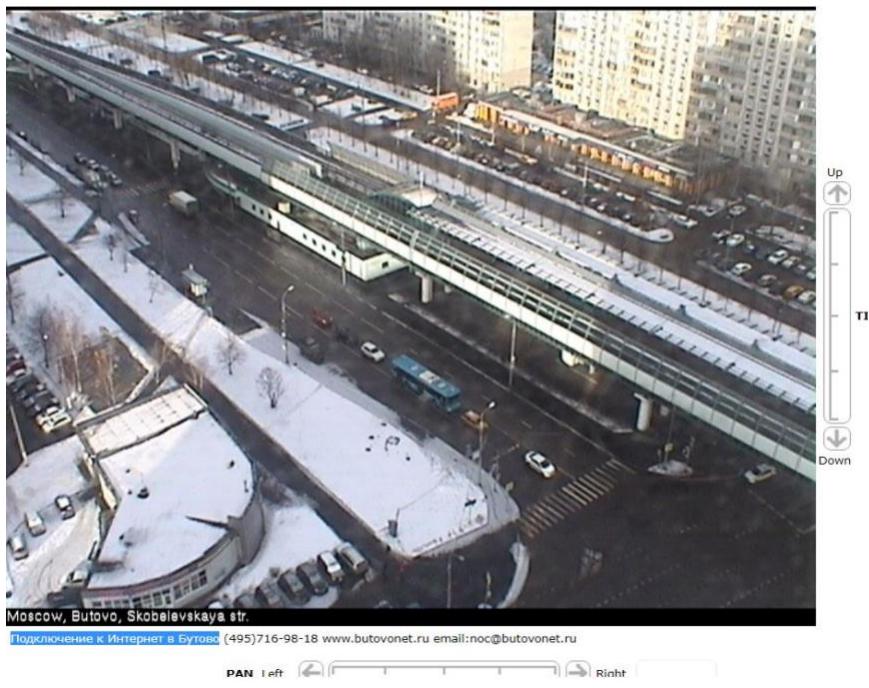
Web Page 2

- The above Picture we see live traffic cameras in the USA, Oregon, city of Salem, this camera is available without a password this advantage may use any unusual activity and this how dorks allow you to find authorization pages for cameras that use normal passwords.



Live Traffic Cameras in USA

- In the above picture, we see live traffic cameras in USA.



Live Traffic Camera in Russia

- In the above picture, we see a live traffic camera in Russia.



Live camera in Italy

- In the above picture, we see a live camera in Italy.

Conclusion

- Since Google has everything that is connected to the Internet and has a web interface, we can easily find incorrectly configured devices and services. However, it is better not to connect to these devices and there may be problems with application works.

Advanced operators

- This is the advanced operators that we can use to exploit insecure websites.

There are many similar advanced operators which can be used to exploit insecure websites:

Operator	Purpose	Mixes with Other Operators?	Can be used Alone?	Web	Images	Groups	News
intitle	Search page Title	no	yes	yes	yes	yes	yes
allintitle ^[3]	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not completely	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	specific files	yes	yes	yes	no	not completely	
intext	Search text of page only	yes	yes	yes	yes	yes	yes
allintext	Search text of page only		yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not completely
link	Search for links to pages	yes	yes	yes	no	no	not completely
inanchor	Search link anchor text	yes	yes	yes	no	not completely	yes
numrange	Locate number	yes	yes	yes	yes	yes	not completely
daterange	Search in date range	yes	yes	yes	not completely	not completely	not completely
author	Group author search	yes	yes	no	no	yes	not completely
group	Group name search		yes	no	yes	yes	not completely
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not completely		yes	

Advanced Operators.

Reconnaissance, Finger printing and Footprinting

Footprinting

Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network.

When used in the computer security lexicon, "Footprinting" generally refers to one of the pre-attack phases; tasks performed before doing the actual attack. **Some of the tools used for Footprinting are Sam Spade, nslookup, traceroute, Nmap and neutrace.**

Footprinting Types: Active and Passive

- **Active** - requires attacker to touch the device or network
 - Social engineering and other communication that requires interaction with target

- **Passive** - measures to collect information from publicly available sources
 - Websites, DNS records, business information databases

Footprinting helps to:

- **Know Security Posture** – The data gathered will help us to get an overview of the security posture of the company such as details about the presence of a firewall, security configurations of applications etc.
- **Reduce Attack Area** – Can identify a specific range of systems and concentrate on particular targets only. This will greatly reduce the number of systems we are focussing on.
- **Identify vulnerabilities** – we can build an information database containing the vulnerabilities, threats, loopholes available in the system of the target organization.
- **Draw Network map** – helps to draw a network map of the networks in the target organization covering topology, trusted routers, presence of server and other information.

Footprinting could be both **passive** and **active**. Reviewing a company's website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

During this phase, a hacker can collect the following information (only high-level information):

- **Domain name**
- **IP Addresses**
- **Namespaces**
- **Employee information**
- **Phone numbers**
- **E-mails**
- **Job Information**

Can be:

- **Anonymous** - information gathering without revealing anything about yourself
- **Pseudonymous** - making someone else take the blame for your actions

Competitive Intelligence - information gathered by businesses about competitors

Alexa.com - resource for statistics about websites

Footprinting Objectives

- **Network**
 - DNS
 - IP networks
 - Accessible Systems
 - Websites
 - Access Control

- VPN Endpoints
 - Firewall vendors
 - IDS Systems
 - Routing/Routed Protocols
 - Phone System (Analog/VoIP)
- **Organization**
 - Org Structure
 - Websites
 - Phone Numbers
 - Directory Information
 - Office Locations
 - Company History
 - Business Associations
- **Hosts**
 - Listening Services
 - Operating System Versions
 - Internet Reachability
 - Enumerated Information
 - SNMP Info

Methods and Tools

Search Engines

- **NetCraft** - Blueprint a comprehensive list of information about the technologies and information about target website.
-
- **Job Search Sites** - Information about technologies can be gleaned from job postings.
- **Google search | Google dorks:**
 - filetype: - looks for file types
 - index of - directory listings
 - info: - contains Google's information about the page
 - intitle: - string in title
 - inurl: - string in url
 - link: - finds linked pages
 - related: - finds similar pages
 - site: - finds pages specific to that site
 - **Example:**

The screenshot shows a Google search results page with the following details:

- Search Query:** "CEO" "email" "@" "Name" "Phone" filetype:csv OR filetype:xls OR filetype:pdf
- Results:** About 14,700 results (0.61 seconds)
- First Result:**
 - Title:** [XLS] fortune 1000
 - Description:** assets.time.com/cm/fortune-data.../2016_FORTUNE_1000_w_Contacts_Sample.xls ▾
... CORPORATE WEBSITE, CEO NAME RETURN TO MAIN DATA, CEO TITLE, Email, Office Phone, Office Ext, Direct Dial, CFO NAME, CFO TITLE, Email, Office ...
- Second Result:**
 - Title:** [XLS] Fortune 1000 Companies List and Contact Info - Boolean Strings
 - Description:** booleanstrings.com/wp-content/uploads/2014/01/fortune1000-2012.xls ▾
6, Company, Phone, Email Format, Email Format 2, General Email, CEO Name, CEO Email, Website, Address, City, State, Zipcode. 7, Chevron, 925-842-1000 ...

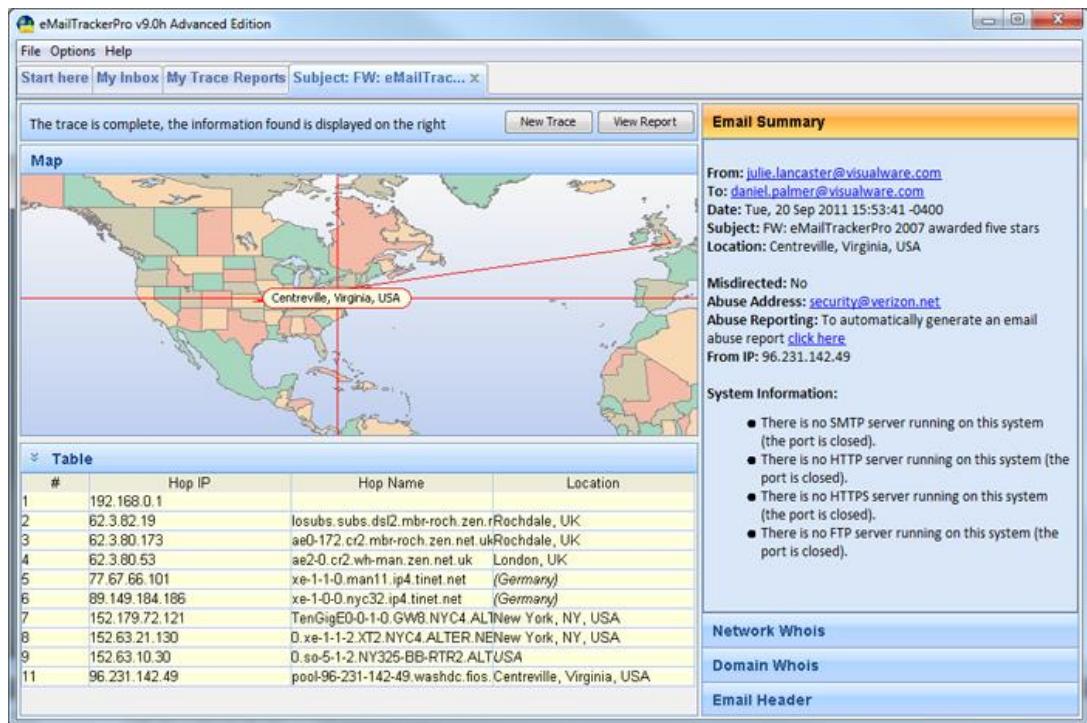
- ○ [GHDB](#) is very good for learn Google Dorks and how it's done in real world scenario
- **Metagoofil** - Command line interface that uses **Google hacks** to find information in meta tags (domain, filetype, etc; Is a google dorks for terminal).

Website Footprinting

- **Web mirroring | Website Cloning** - allows for discrete testing offline
 - **HTTrack** - you can use the *CLI* version or *Web Interface* version
 - **Wget** - Linux command
 - wget -mk -w 10 http://hackthissite.org/
 - **Black Widow**
 - **WebRipper**
 - **Teleport Pro**
 - **Backstreet Browser**
- **Archive.org / Wayback machine**
- Provides cached websites from various dates which possibly have sensitive information that has been now removed.
 - [Wayback Machine](#) -> [Google.com](#):

Email Footprinting

- **Email header** - may show servers and where the location of those servers are
 - Email headers can provide: **Names, Addresses (IP, email), Mail servers, Time stamps, Authentication and so on.**
 - ○ **EmailTrackerPro** is a Windows software that trace an email back to its true point of origin:



- **Email tracking** - services can track various bits of information including the IP address of where it was opened, where it went, etc.

DNS Footprinting

- Ports
 - Name lookup - UDP 53
 - Zone transfer - TCP 53
- Zone transfer replicates all records
- **Name resolvers** answer requests
- **Authoritative Servers** hold all records for a namespace
- **DNS Record Types**

Name	Description	Purpose
SRV	Service	Points to a specific service
SOA	Start of Authority	Indicates the authoritative NS for a namespace
PTR	Pointer	Maps an IP to a hostname
NS	Nameserver	Lists the nameservers for a namespace
MX	Mail Exchange	Lists email servers
CNAME	Canonical Name	Maps a name to an A record

Name	Description	Purpose
A	Address	Maps an hostname to an IP address

- **DNS Poisoning** - changes cache on a machine to redirect requests to a malicious server
- **DNSSEC** - helps prevent DNS poisoning by encrypting records
- **SOA Record Fields**
 - **Source Host** - hostname of the primary DNS
 - **Contact Email** - email for the person responsible for the zone file
 - **Serial Number** - revision number that increments with each change
 - **Refresh Time** - time in which an update should occur
 - **Retry Time** - time that a NS should wait on a failure
 - **Expire Time** - time in which a zone transfer is allowed to complete
 - **TTL** - minimum TTL for records within the zone
- **IP Address Management**
 - **ARIN** - North America
 - **APNIC** - Asia Pacific
 - **RIPE** - Europe, Middle East
 - **LACNIC** - Latin America
 - **AfriNIC** - Africa
- **Whois** - obtains registration information for the domain from command line or web interface.
 - on Kali, whois is pre-installed on CLI; e.g: whois google.com)
 - on Windows, you can use **SmartWhois** GUI software to perform a whois, or any website like domaintools.com
- **Nslookup** - Performs DNS queries; (nslookup is pre-installed on Kali Linux)
 - nslookup www.hackthissite.org
 - Server: 192.168.63.2
 - Address: 192.168.63.2#53
 -
 - Non-authoritative answer:
 - Name: www.hackthissite.org
 - Address: 137.74.187.103
 - Name: www.hackthissite.org
 - Address: 137.74.187.102
 - Name: www.hackthissite.org
 - Address: 137.74.187.100
 - Name: www.hackthissite.org
 - Address: 137.74.187.101
 - Name: www.hackthissite.org
 - Address: 137.74.187.104
 - First two lines shows my current DNS server; The IP addresses returned are '**A record**', meaning is the IPvA address of the domain; Bottom line NsLookup queries the specified DNS server and retrieves the requested records that are associated with the domain.
 - **The following types of DNS records are especially useful to use on Nslookup:**
 -

Type	Description
A	the IPv4 address of the domain
AAAA	the domain's IPv6 address
CNAME	the canonical name — allowing one domain name to map on to another. This allows more than one website to refer to a single web server.
MX	the server that handles email for the domain.
NS	one or more authoritative name server records for the domain.
TXT	a record containing information for use outside the DNS server. The content takes the form name=value. This information is used for many things including authentication schemes such as SPF and DKIM.

- **Nslookup - Interactive mode zone transfer** (Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain).
 - nslookup
 - server <IP Address>
 - set type = <DNS type>
 - <target domain>
- nslookup
- > set type=AAAA
- > www.hackthissite.org
- Server: 192.168.63.2
- Address: 192.168.63.2#53
-
- Non-authoritative answer:
- Name: www.hackthissite.org
- Address: 2001:41d0:8:ccd8:137:74:187:103
- Name: www.hackthissite.org
- Address: 2001:41d0:8:ccd8:137:74:187:102
- Name: www.hackthissite.org
- Address: 2001:41d0:8:ccd8:137:74:187:101
- Name: www.hackthissite.org
- Address: 2001:41d0:8:ccd8:137:74:187:100
- Name: www.hackthissite.org
- Address: 2001:41d0:8:ccd8:137:74:187:104
-
- **Dig** - unix-based command like nslookup
 - dig <target>
 - dig www.hackthissite.org
 -
 - ; <>> DiG 9.16.2-Debian <>> www.hackthissite.org
 - ; global options: +cmd
 - ; Got answer:
 - ; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51391
 - ; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

-
- ;; OPT PSEUDOSECTION:
- ; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
- ;; QUESTION SECTION:
- ;www.hackthissite.org. IN A
-
- ;; ANSWER SECTION:
- www.hackthissite.org. 5 IN A 137.74.187.104
- www.hackthissite.org. 5 IN A 137.74.187.101
- www.hackthissite.org. 5 IN A 137.74.187.100
- www.hackthissite.org. 5 IN A 137.74.187.102
- www.hackthissite.org. 5 IN A 137.74.187.103
-
- ;; Query time: 11 msec
- ;; SERVER: 192.168.63.2#53(192.168.63.2)
- ;; WHEN: Tue Aug 11 15:05:01 EDT 2020
- ;; MSG SIZE rcvd: 129
-
-
- To get email records specify -t MX
 - dig <target> -t MX
- To get zone transfer speci
-
- y axfr

Network Footprinting

- IP address range can be obtained from regional registrar (e.g: ARIN for America, RIPE for Europe, etc)
- Use traceroute to find intermediary servers
 - traceroute uses ICMP echo in Windows (tracert)
 - traceroute is good for detect Firewalls and the network path

Usage example:

- **traceroute -I nsa.gov**
 - Specify target: traceroute <target>
 - In this case is used ICMP ECHO for tracerouting: -I

```
traceroute -I nsa.gov
traceroute to nsa.gov (104.83.73.99), 30 hops max, 60 byte packets
1 192.168.63.2 (192.168.63.2) 0.194 ms 0.163 ms 0.150 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
```

11 a104-83-73-99.deploy.static.akamaitechnologies.com (104.83.73.99) 42.742 ms 42.666 ms 25.176 ms

⚠ Windows command - tracert ⚠ Linux Command - traceroute

Other Relevant Tools

OSRFramework

↳ **OSRFramework has a practical lab**

Uses open source intelligence to get information about target. (*Username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, and many others*).

Web Spiders

Obtain information from the website such as pages, etc.

Recon-ng

↳ **Recon-ng has a practical lab**

Recon-ng is a web-based open-source reconnaissance tool used to extract information from a target organization and its personnel.

Provides a powerful environment in which open source web-based reconnaissance can be automated conducted, quickly and thoroughly.

Metasploit Framework

↳ **Metasploit has a practical lab**

The Metasploit Framework is a tool that provides information about security vulnerabilities and aids in penetration testing and IDS signature development; **This is a huge framework that provide Recon tools as well.**

theHarvester

↳ **theHarvester has a practical lab**

theHarvester is a OSINT tool; Useful for gathering information like:

- Emails
- Subdomains

- Hosts
 - Employee names
 - Open ports
 - Banners from different public sources like search engines, PGP key servers and SHODAN computer database.

Usage example:

- **theHarvester -d www.hackthissite.org -n -b google**
 - Issue theHarvester command: theHarvester
 - Specify the domain: -d <url>
 - Perform dns lookup: -n
 - Specify search engine/source: -b google

theHarvester -d www.hackthissite.org -n -b google
table results already exists

[*] Target: www.hackthissite.org

[*] Searching Google.

Searching 0 results.

Searching 100 results.

Searching 200 results.

Searching 300 results.

Searching 400 results.

Searching 500 results.

[*] No IPs found.

[*] Emails found: 2

ab790c1315@www.hackthissite.org
staff@hackthissite.org

[*] Hosts found: 7

0.loadbalancer.www.hackthissite.org:
22www.hackthissite.org:
2522www.hackthissite.org:

253dwww.hackthissite.org:
www.hackthissite.org:137.74.187.104, 137.74.187.100, 137.74.187.101, 137.74.187.103, 137.74.187.102
x22www.hackthissite.org:

```
[*] Starting active queries.  
137.74.187.100  
[*] Performing reverse lookup in 137.74.187.0/24  
module 'theHarvester.discovery.dnssearch' has no attribute 'DnsReverse'
```

Sublist3r

Sublist3r **enumerates subdomains** using many search engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS

Usage example:

- `python3 sublist3r.py -d hackthissite.org`
 - Specify the domain: `-d <url>`

```
python3 sublist3r.py -d hackthissite.org
```

/ \ | _ \ | \ | - () | \ | \ | / --
\\ \ | \ | ' | \ | / \ | \ | \ | \ | ' |
| \ | \ | \ | \ | \ | \ | \ | \ | \ |
| \ | \ | , : / \ | \ | \ | \ | \ | \ |

Coded By Ahmed Aboul-Ela - @aboul3la

```
[-] Enumerating subdomains now for hackthissite.org
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 41
www.hackthissite.org
admin.hackthissite.org
api.hackthissite.org
ctf.hackthissite.org
vm-005.outbound.firewall.hackthissite.org
vm-050.outbound.firewall.hackthissite.org
vm-099.outbound.firewall.hackthissite.org
vm-150.outbound.firewall.hackthissite.org
vm-200.outbound.firewall.hackthissite.org
forum.hackthissite.org
```

forums.hackthissite.org
git.hackthissite.org
irc.hackthissite.org
(...)

DIRB

DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack/brute force attack against a web server and analyzing the response.

- Useful to find subdirectories on web application

Usage example:

- **dirb https://www.hackthissite.org/ /usr/share/wordlists/dirb/small.txt**
 - Specify the url by issuing dirb command: dirb <url>
 - Specify the wordlist: /path/to/wordlist

```
dirb https://www.hackthissite.org/ /usr/share/wordlists/dirb/small.txt
```

```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```

```
URL_BASE: https://www.hackthissite.org/  
WORDLIST_FILES: /usr/share/wordlists/dirb/small.txt
```

```
-----  
GENERATED WORDS: 959
```

```
---- Scanning URL: https://www.hackthissite.org/ ----  
+ https://www.hackthissite.org/api (CODE:200|SIZE:10)  
+ https://www.hackthissite.org/blog (CODE:200|SIZE:20981)  
+ https://www.hackthissite.org/cgi-bin/ (CODE:403|SIZE:199)
```

Maltego

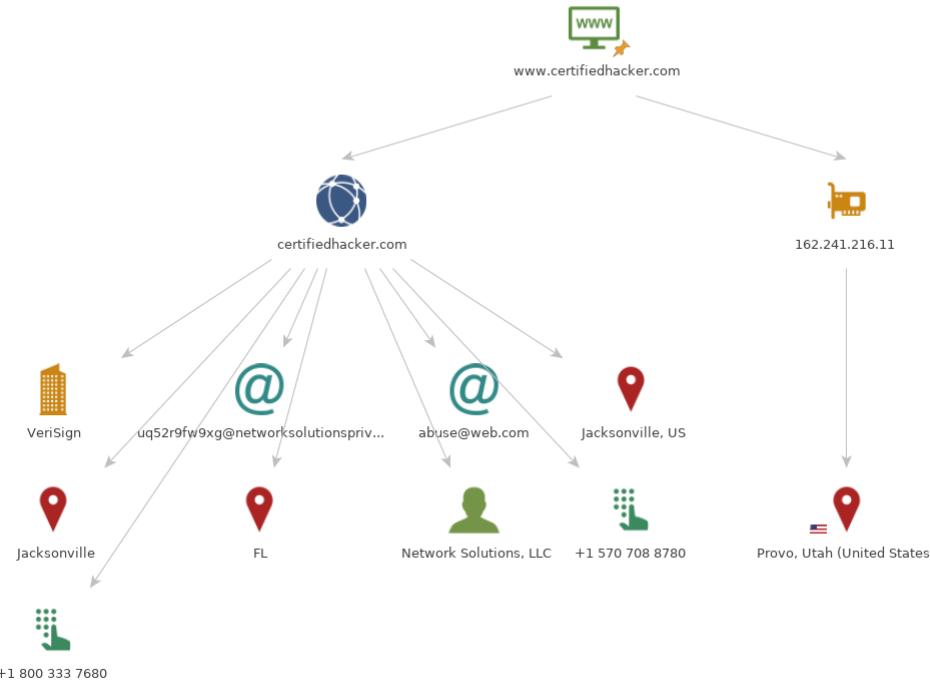
↳ Maltego has practical labs

Maltego is a powerful OSINT tool, you can extract a broad type of information through the network, technologies and personnel(email, phone number, twitter).

- You able to:
 - Identify IP address
 - Identify Domain and Domain Name Schema
 - Identify Server Side Technology
 - Identify Service Oriented Architecture (SOA) information



- Identify Name Server
- Identify Mail Exchanger
- Identify Geographical Location
- Identify Entities
- Discover Email addresses and Phone numbers



Social Engineering Framework (SEF)

It's a open source Social Engineering Framework (SCRIPT) that helps generate phishing attacks and fake emails. and it's includes phishing pages, fake email, fake email with file attachment and other stuff that helps you in Social Engineering Attack.

Web Based Recon

NetCraft

Netcraft is a website analyzing server, with the help of this website we find basic and important information on the website like:

- **Background** — This includes basic domain information.
 - Which OS, Web server is running; Which ISP;
- **Network** — This includes information from IP Address to Domain names to nameservers.
- **SSL/TLS** — This gives the ssl/tls status of the target
- **Hosting History** - This gives the information on the hosting history of the target

- **Sender Policy Framework (SPF)** — This describes who can send mail on the domains behalf
- **DMARC** -This is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated
- **Web Trackers** — These trackers can be used to monitor individual user behavior across the web
- Site Technology — This section includes details on:
 - Cloud & PaaS
 - Server-Side technologies (e.g: PHP)
 - Client-Side technologies (e.g: JavaScript library)
 - CDN Information
 - CMS Information (e.g: Wordpress, Joomla, etc)
 - Mobile Technologies
 - Web stats (e.g: Web analytics, collection, etc)
 - Character encoding

Shodan

Shodan Unlike traditional search engines such as Google, use Web crawlers to traverse your entire site, but directly into the channel behind the Internet, various types of port equipment audits, and never stops looking for the Internet and all associated servers, camera, printers, routers, and so on.

- Some have also described it as a search engine of service banners, which are metadata that the server sends back to the client.
- Shodan works well with basic, single-term searches. Here are the basic search filters you can use:
 - **city:** find devices in a particular city
 - **country:** find devices in a particular country
 - **geo:** you can pass it coordinates
 - **hostname:** find values that match the hostname
 - **net:** search based on an IP or /x CIDR
 - **os:** search based on an operating system
 - **port:** find particular ports that are open
 - **before/after:** find results within a timeframe

Shodan Developers Monitor View All... Show API Key Help Center

SHODAN port:9200.json Explore Downloads Reports Pricing Enterprise Access My Account Upgrade

Exploits Maps Like 43 Download Results Create Report

TOTAL RESULTS
29,183

TOP COUNTRIES

Country	Count
China	9,172
United States	8,202
France	1,657
Germany	1,411
Netherlands	1,154

TOP ORGANIZATIONS

Organization	Count
Hangzhou Alibaba Advertising...	4,774
Amazon.com	3,392
Google Cloud	1,713
Microsoft Azure	1,564
Digital Ocean	1,059

TOP OPERATING SYSTEMS

Operating System	Count
Linux 3.x	7
Windows 7 or 8	3
Linux	1
FreeBSD 9.x	1

RELATED TAGS: https://www.instagram.com/oxse_18/

52.232.101.70 Microsoft Azure
Added on 2019-05-02 12:43:26 GMT
Netherlands, Amsterdam

HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm="security" charset=UTF-8"
content-type: application/json; charset=UTF-8
content-length: 369

47.111.48.179 Hangzhou Alibaba Advertising Co.,Ltd.
Added on 2019-05-02 12:49:42 GMT
China

HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm="security" charset=UTF-8"
content-type: application/json; charset=UTF-8
content-length: 369

138.201.48.14 Hetzner Online GmbH
Added on 2019-05-02 12:43:58 GMT
Germany, Heidelberg

HTTP/1.1 200 OK
content-type: application/json; charset=UTF-8
content-length: 433

47.101.196.119 Hangzhou Alibaba Advertising Co.,Ltd.
Added on 2019-05-02 12:45:31 GMT
China

HTTP/1.1 200 OK
content-type: application/json; charset=UTF-8
content-length: 433

20.0 1

 SHODAN

Netgear DGN1000

 Exploits  Maps  Share Search

TOTAL RESULTS

4,799

TOP COUNTRIES



TOP SERVICES

HTTP (8080)	3,598
HTTP	661
Synology	121
8081	107
HTTPS (8443)	23

Censys

Alternative for Shodan.



Quick Filters
For all fields, see [Data Definitions](#)

Autonomous System:
3.06M AKAMAI-AS
521.77KAKAMAI-ASN1
154.84KLEASEWEB-USA-LAX-11
112.47KENZUINC-84.47K EGIHOSTING
[More](#)

Protocol:
5.53M 80/http
4.31M 443/https
224.42K22/ssh
164.96K21/ftp
127.45K3306/mysql
[More](#)

IPv4 Hosts
Page: 1/234,900 Results: 5,872,492 Time: 716ms Query Plan: expanded

- 23.27.70.12**
EGIHOSTING (18779) United States
Windows 80/http
IIS7
- 23.80.92.96 (III92.96.oakleyfeed.com)**
Unknown Network Unknown
80/http
403 Forbidden
- 23.118.217.199 (23-118-217-199.lightspeed.froka.sbcglobal.net)**
ATT-INTERNET4 (7018) Rocklin, California, United States
80/http
Home

Finger printing

A **fingerprint** is a group of information that can be used to detect the software, network protocols, operating systems, or hardware devices. Fingerprinting (also known as Footprinting) is the art of using that information to correlate data sets to identify network services, operating system number and version, software applications, databases, configurations and more.

Fingerprinting (or Footprinting) a target's web presence is often an attacker's first step in planning an attack. The purpose is to accumulate as much information as possible, including the target's platform, application software technology, backend database version, configurations, and possibly even the network's architecture/ topology. Multitier fingerprinting is similar to its predecessor, TCP/IP Fingerprinting (with the use of a scanner such as Nmap) except that it is focused on the Application Layer of the OSI model instead of the Transport Layer. Based on the information, an attacker can glean from Fingerprinting/Footprinting exercises, they can develop an accurate attack scenario to exploit vulnerabilities in applications and systems being used by the target.

There are two types of fingerprinting in ethical hacking. These are active fingerprinting and passive fingerprinting. Active fingerprinting is gained if you send especially skilled packets to a target machine whereas passive fingerprinting is dependent on sniffer traces from the remote computer. They rely on scanning the network as sniffers to detect patterns in the usual network traffic.

Different operating systems have different TCP/IP implementations. Passive fingerprinting uses this to determine the possible OS used by the target.

After a fair amount of data is gathered, it can be used to analyze the target system. This technique is considered less accurate than active fingerprinting. They rely on scanning the network as sniffers to detect patterns in the usual network traffic.



Different operating systems have different TCP/IP implementations. Passive fingerprinting uses this to determine the possible OS used by the target.

After a fair amount of data is gathered, it can be used to analyze the target system. This technique is considered less accurate than active fingerprinting.

Defensive measures

Organizations must regularly implement active and passive fingerprinting techniques on their networks to understand what an attacker will be able to access. This information can assist in enhancing the OS and network security. Apart from this, there are a few other measures organizations can implement.

- Ensure that web servers, firewalls, intrusion prevention systems, and intrusion detection systems are properly configured and monitored to restrict active fingerprinting by attackers.
- Network interface cards must not be enabled to work in promiscuous mode unless absolutely necessary. In such cases, they must be strictly monitored to prevent passive fingerprinting attacks.
- Regularly monitor the log files for any sign of unusual activity.
- System administrators must patch security vulnerabilities as soon as possible.

NMAP

What is Nmap?

Nmap is Used to Scan:

- Enterprise-scale networks
- Small business networks
- Connected devices
- IoT devices and traffic

VARONIS

At its core, Nmap is a network scanning tool that uses IP packets to identify all the devices connected to a network and to provide information on the services and operating systems they are running.

The program is most commonly used via a command-line interface (though GUI front-ends are also available) and is available for many different operating systems such as Linux, Free BSD, and Gentoo. Its popularity has also been bolstered by an active and enthusiastic user support community.

Nmap was developed for enterprise-scale networks and can scan through thousands of connected devices. However, in recent years Nmap is being increasingly used by smaller companies. The rise of the IoT, in particular, now means that the networks used by these companies have become more complex **and therefore harder to secure**.

This means that Nmap is now **used in many website monitoring tools** to audit the traffic between web servers and IoT devices. The recent emergence of **IoT botnets, like Mirai**, has also stimulated interest in Nmap, not least because of its ability to interrogate **devices connected via the UPnP protocol** and to highlight any devices that may be malicious.

What Does Nmap Do?

Nmap Core Processes

Nmap provides information on:

- 1. Every active IP** so you can determine if an IP is being used by a legitimate service or an external attacker.
- 2. Your network as a whole**, including live hosts, open ports and the OS of every connected device.
- 3. Vulnerabilities** — scan your own server to simulate the process that a hacker would use to attack your site.



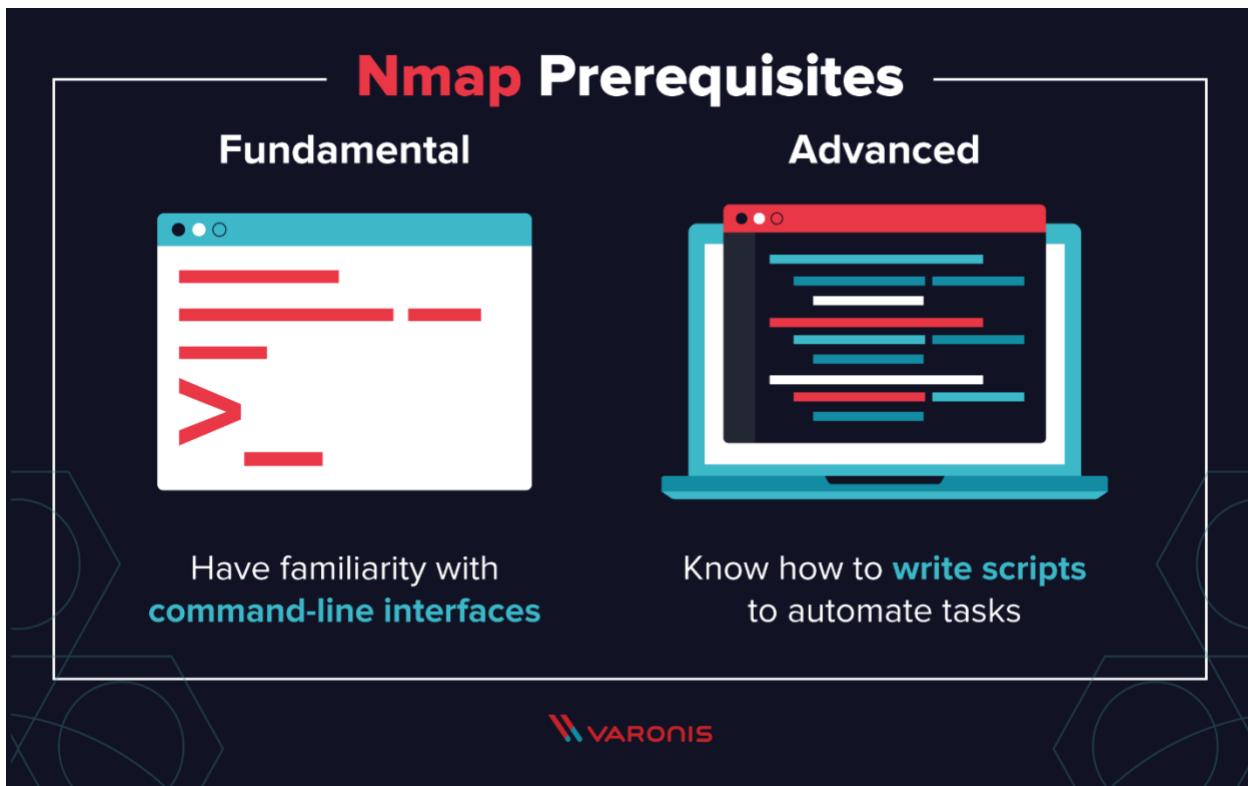
VARONIS

At a practical level, Nmap is used to provide detailed, real-time information on your networks, and on the devices connected to them.

The primary uses of Nmap can be broken into three core processes. First, the program gives you detailed information on every IP active on your networks, and each IP can then be scanned. This allows administrators to check whether an IP is being used by a legitimate service, or by an external attacker.

Secondly, Nmap provides information on your network as a whole. It can be used to provide a list of live hosts and open ports, as well as identifying the OS of every connected device. This makes it a valuable tool in ongoing system monitoring, as well as a critical part of pentesting. Nmap can be used alongside **the Metasploit framework**, for instance, to probe and then repair network vulnerabilities. Thirdly, Nmap has also become a valuable tool for users looking to protect personal and business websites. Using Nmap to scan your own web server, particularly if you are hosting your website from home, is essentially simulating the process that a hacker would use to attack your site. “Attacking” your own site in this way is a powerful way of identifying security vulnerabilities.

How To Use Nmap



Nmap is straightforward to use, and most of the tools it provides are familiar to system admins from other programs. The advantage of Nmap is that it brings a wide range of these tools into one program, rather than forcing you to skip between separate and discrete network monitoring tools.

In order to use Nmap, you need to be familiar with command-line interfaces. Most advanced users are able to write scripts to automate common tasks, but this is not necessary for basic network monitoring.

How To Install Nmap

The process for installing Nmap is easy but varies according to your operating system. The Windows, Mac, and Linux versions of the **program can be downloaded here**.

- For Windows, Nmap comes with a custom installer (namp<version>setup.exe). Download and run this installer, and it automatically configures Nmap on your system.
- On Mac, Nmap also comes with a dedicated installer. Run the Nmap-<version>.mpkg file to start this installer. On some recent versions of macOS, you might see a warning that Nmap is an “unidentified developer”, but you can ignore this warning.
- Linux users can either compile Nmap from source or use their chosen package manager. To use apt, for instance, you can run Nmap –version to check if Nmap is installed, and sudo apt-get install Nmap to install it.

Nmap Tutorial and Examples

Once you've installed Nmap, the best way of learning how to use it is to perform some basic network scans.

How To Run a Ping Scan

One of the most basic functions of Nmap is to identify active hosts on your network. Nmap does this by using a ping scan. This identifies all of the IP addresses that are currently online without sending any packets to these hosts.

To run a ping scan, run the following command:

1. # nmap -sp 192.100.1.1/24

This command then returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands (see below) to investigate them further.

How To Run A Host Scan?

A more powerful way to scan your networks is to use Nmap to perform a host scan. Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address.

To run a host scan, use the following command:

1. # nmap -sp <target IP range>

This returns information on every host, their latency, their MAC address, and also any description associated with this address. This can be a powerful way of spotting suspicious hosts connected to your network.



If you see anything unusual in this list, you can then run a DNS query on a specific host, by using:

1. # namp -sL <IP address>

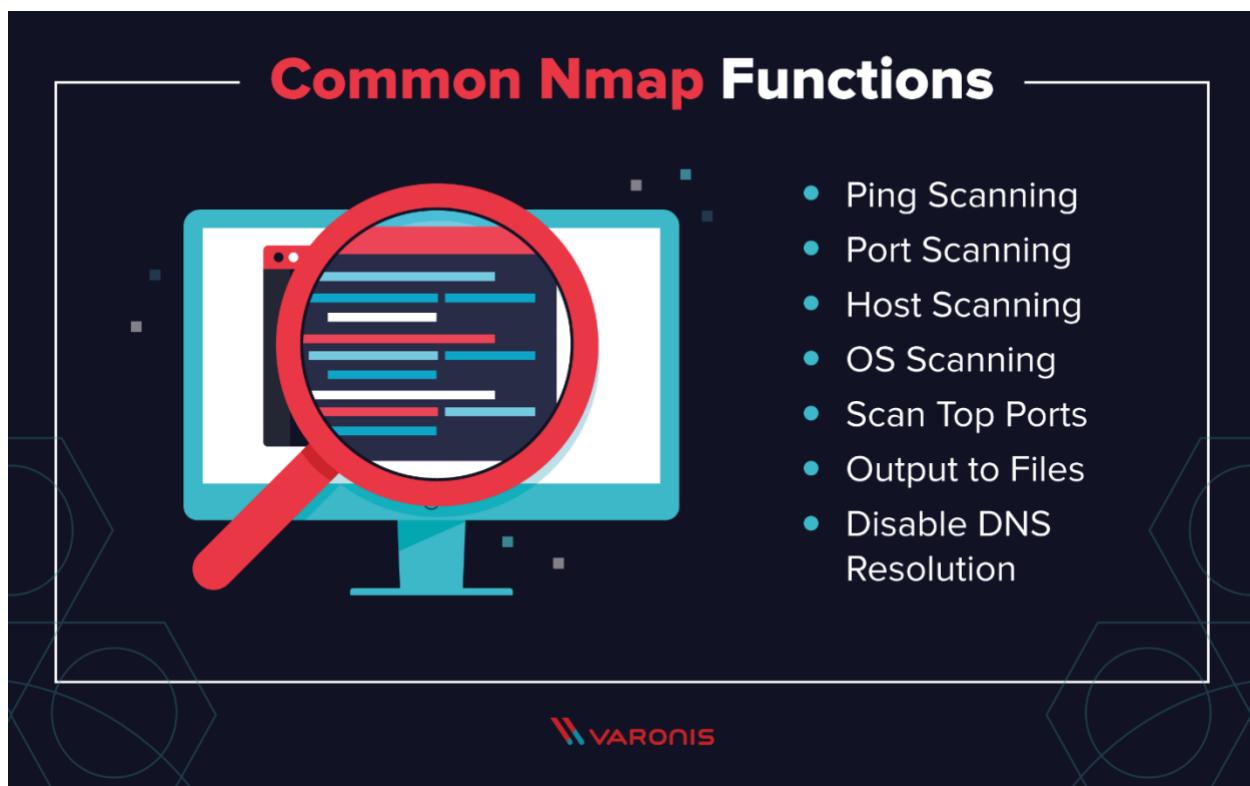
This returns a list of names associated with the scanned IP. This description provides information on what the IP is actually for.

How To Use Nmap in Kali Linux

Using Nmap in Kali Linux can be done in an identical way to running the program on any other flavor of Linux.

That said, there are advantages to using Kali when running Nmap scans. Most modern distros of Kali now come with a fully-features Nmap suite, which includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping)

Nmap Commands



Most of the common functions of Nmap can be executed using a single command, and the program also uses a number of ‘shortcut’ commands that can be used to automate common tasks.

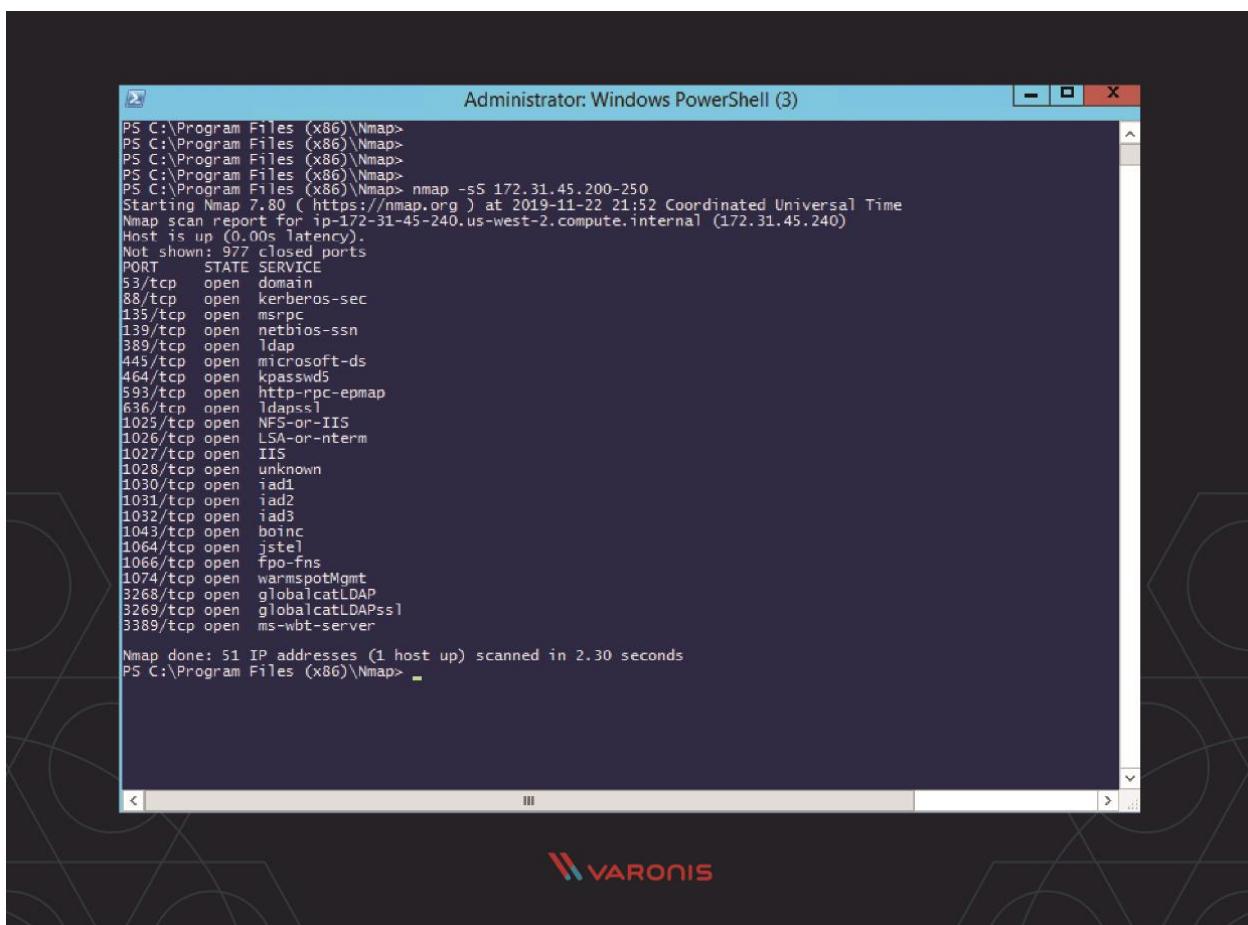
Here is a quick run-down:

1. Ping Scanning

As mentioned above, a ping scan returns information on every active IP on your network. You can execute a ping scan using this command:

1. #

2. Port Scanning



The screenshot shows an Administrator Windows PowerShell window titled "Administrator: Windows PowerShell (3)". The command entered is "nmap -sS 172.31.45.200-250". The output displays the results of a SYN scan on host 172.31.45.200, listing various open ports and their corresponding services. The output includes:
Starting Nmap 7.80 (https://nmap.org) at 2019-11-22 21:52 Coordinated Universal Time
Nmap scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
53/tcp open domain
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldaps
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
1027/tcp open IIS
1028/tcp open unknown
1030/tcp open iad1
1031/tcp open iad2
1032/tcp open iad3
1043/tcp open boinc
1064/tcp open jstel
1066/tcp open fpo-fns
1074/tcp open warmspotMgmt
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
3389/tcp open ms-wbt-server
Nmap done: 51 IP addresses (1 host up) scanned in 2.30 seconds

There are several ways to execute port scanning using Nmap. The most commonly used are these:

1. # sS TCP SYN scan
- 2.
3. # sT TCP connect scan
- 4.
5. # sU UDP scans
- 6.

7. # sY SCTP INIT scan
- 8.
9. # sN TCP NULL

The major differences between these types of scans are whether they cover TCP or UDP ports and whether they execute a TCP connection. Here are the basic differences:

- The most basic of these scans is the sS TCP SYN scan, and this gives most users all the information they need. It scans thousands of ports per second, and because it doesn't complete a TCP connection it does not arouse suspicion.
- The main alternative to this type of scan is the TCP Connect scan, which actively queries each host, and requests a response. This type of scan takes longer than a SYN scan, but can return more reliable information.
- The UDP scan works in a similar way to the TCP connect scan but uses UDP packets to scan DNS, SNMP, and DHCP ports. These are the ports most frequently targeted by hackers, and so this type of scan is a useful tool for checking for vulnerabilities.
- The SCTP INIT scan covers a different set of services: SS7 and SIGTRAN. This type of scan can also be used to avoid suspicion when scanning an external network because it doesn't complete the full SCTP process.
- The TOP NULL scan is also a very crafty scanning technique. It uses a loophole in the TCP system that can reveal the status of ports without directly querying them, which means that you can see their status even where they are protected by a firewall.

3. Host Scanning

Host scanning returns more detailed information on a particular host or a range of IP addresses. As mentioned above, you can perform a host scan using the following command:

1. # nmap -sp <target IP range>

4. OS Scanning

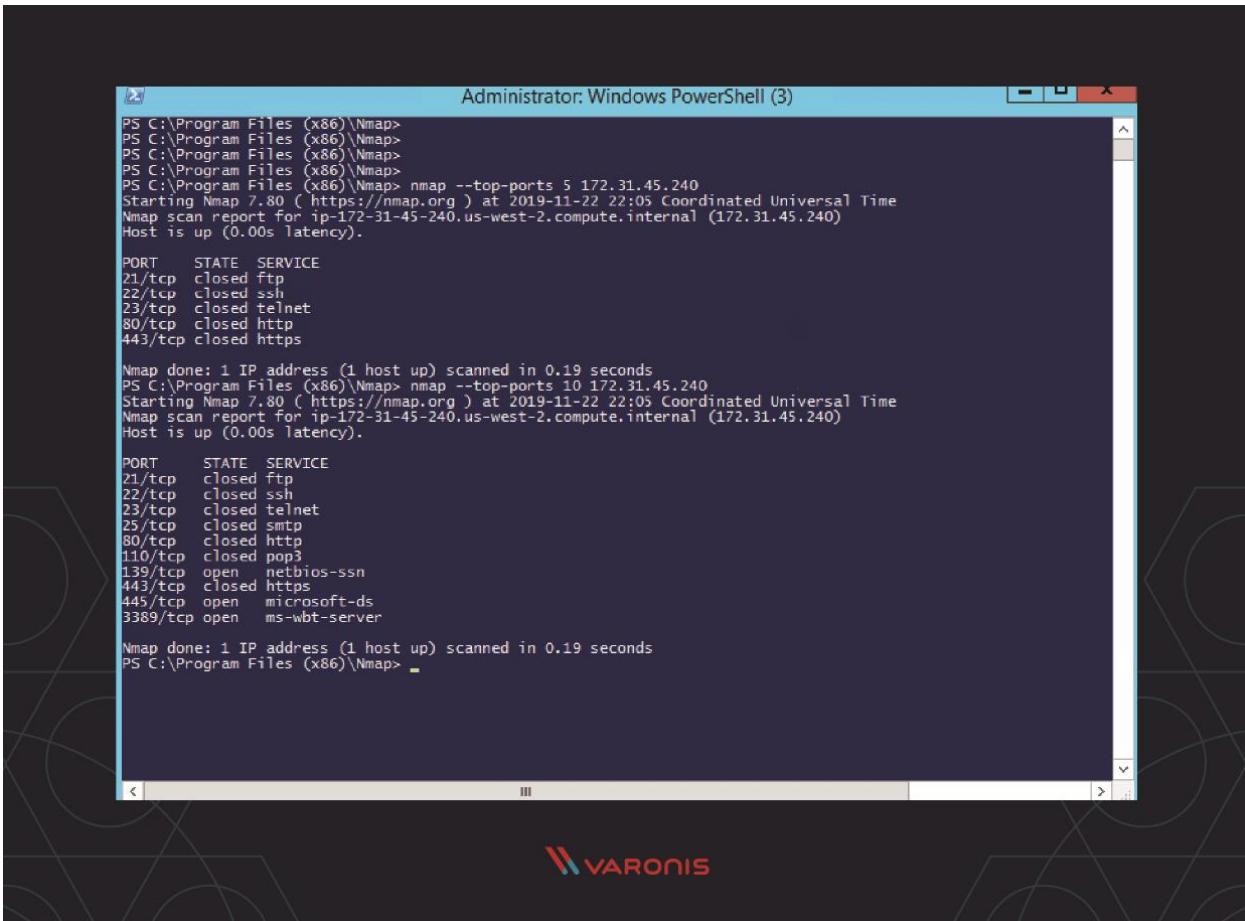
OS scanning is one of the most powerful features of Nmap. When using this type of scan, Nmap sends TCP and UDP packets to a particular port, and then analyze its response. It compares this response to a database of 2600 operating systems, and return information on the OS (and version) of a host.

To run an OS scan, use the following command:

1. nmap -O <target IP>

5. Scan The Most Popular Ports





```
Administrator: Windows PowerShell (3)
PS C:\Program Files (x86)\Nmap>
PS C:\Program Files (x86)\Nmap>
PS C:\Program Files (x86)\Nmap>
PS C:\Program Files (x86)\Nmap>
PS C:\Program Files (x86)\Nmap> nmap --top-ports 5 172.31.45.240
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 22:05 Coordinated Universal Time
Nmap scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).

PORT      STATE SERVICE
21/tcp    closed  ftp
22/tcp    closed  ssh
23/tcp    closed  telnet
80/tcp    closed  http
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
PS C:\Program Files (x86)\Nmap> nmap --top-ports 10 172.31.45.240
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 22:05 Coordinated Universal Time
Nmap scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).

PORT      STATE SERVICE
21/tcp    closed  ftp
22/tcp    closed  ssh
23/tcp    closed  telnet
25/tcp    closed  smtp
80/tcp    closed  http
110/tcp   closed  pop3
139/tcp   open   netbios-ssn
443/tcp   closed https
445/tcp   open   microsoft-ds
3389/tcp  open   ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
PS C:\Program Files (x86)\Nmap>
```

If you are running Nmap on a home server, this command is very useful. It automatically scans a number of the most ‘popular’ ports for a host. You can run this command using:

1. nmap --top-ports 20 192.168.1.106

Replace the “20” with the number of ports to scan, and Nmap quickly scans that many ports. It returns a concise output that details the status of the most common ports, and this lets you quickly see whether you have any unnecessarily open ports.

6. Output to a File

If you want to output the results of your Nmap scans to a file, you can add an extension to your commands to do that. Simply add:

1. -oN output.txt

To your command to output the results to a text file, or:

1. -oX output.xml

To output to an XML.

7. Disable DNS Name Resolution

Finally, you can speed up your Nmap scans by using the `-n` parameter to disable reverse DNS resolution. This can be extremely useful if you want to scan a large network. For example, to turn off DNS resolution for the basic ping scan mentioned above, add `-n`:

```
1. # nmap -sp -n 192.100.1.1/24
```

⊕ More Useful Information about Nmap: ⊕

Switch	Example	Description
-p	nmap 192.168.1.1 -p 21	Port scan for port x
-p	nmap 192.168.1.1 -p 21-100	Port range
-p	nmap 192.168.1.1 -p U:53,T:21-25,80	Port scan multiple TCP and UDP ports
-p-	nmap 192.168.1.1 -p-	Port scan all ports
-p	nmap 192.168.1.1 -p http,https	Port scan from service name
-F	nmap 192.168.1.1 -F	Fast port scan (100 ports)
--top-ports	nmap 192.168.1.1 --top-ports 2000	Port scan the top x ports
-p-65535	nmap 192.168.1.1 -p-65535	Leaving off initial port in range makes the scan start at port 1
-p0-	nmap 192.168.1.1 -p0-	Leaving off end port in range makes the scan go through to port 65535

2. Service and Version Detection

Switch	Example	Description
-sV	nmap 192.168.1.1 -sV	Attempts to determine the version of the service running on port
-sV --version-intensity	nmap 192.168.1.1 -sV --version-intensity 8	Intensity level 0 to 9. Higher number increases possibility of correctness
-sV --version-light	nmap 192.168.1.1 -sV --version-light	Enable light mode. Lower possibility of correctness. Faster
-sV --version-all	nmap 192.168.1.1 -sV --version-all	Enable intensity level 9. Higher possibility of correctness. Slower
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute



3. OS Detection

Switch	Example	Description
-O	nmap 192.168.1.1 -O	Remote OS detection using TCP/IP stack fingerprinting
-O --osscan-limit	nmap 192.168.1.1 -O --osscan-limit	If at least one open and one closed TCP port are not found it will not try OS detection against host
-O --osscan-guess	nmap 192.168.1.1 -O --osscan-guess	Makes Nmap guess more aggressively
-O --max-os-tries	nmap 192.168.1.1 -O --max-os-tries 1	Set the maximum number x of OS detection tries against a target
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

4. Timing and Performance

Switch	Example input	Description
--host-timeout <time>	1s; 4m; 2h	Give up on target after this long
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>	1s; 4m; 2h	Specifies probe round trip time
--min-hostgroup/max-hostgroup <size><size>	50; 1024	Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>	10; 1	Probe parallelization
--scan-delay/--max-scan-delay <time>	20ms; 2s; 4m; 5h	Adjust delay between probes
--max-retries <tries>	3	Specify the maximum number of port scan probe retransmissions
--min-rate <number>	100	Send packets no slower than <number> per second
--max-rate <number>	100	Send packets no faster than <number> per second



5. NSE Scripts

NSE stands for Nmap Scripting Engine, and it's basically a digital library of Nmap scripts that helps to enhance the default Nmap features and report the results in a traditional Nmap output.

One of the best things about NSE is its ability to let users write and share their own scripts, so you're not limited to relying on the Nmap default NSE scripts. [\[+\]](#)

Switch	Example	Description
-sC	nmap 192.168.1.1 -sC	Scan with default NSE scripts. Considered useful for discovery and safe
--script default	nmap 192.168.1.1 --script default	Scan with default NSE scripts. Considered useful for discovery and safe
--script	nmap 192.168.1.1 --script=banner	Scan with a single script. Example banner
--script	nmap 192.168.1.1 --script=http*	Scan with a wildcard. Example http
--script	nmap 192.168.1.1 --script=http,banner	Scan with two scripts. Example http and banner
--script	nmap 192.168.1.1 --script "not intrusive"	Scan default, but remove intrusive scripts
--script-args	nmap --script snmp-sysdescr --script-args snmpcommunity=admin 192.168.1.1	NSE script with arguments

Useful NSE Script Examples

Command	Description
nmap -Pn --script=http-sitemap-generator scanme.nmap.org	http site map generator
nmap -n -Pn -p 80 --open -sV -vvv --script banner,http-title -iR 1000	Fast search for random web servers
nmap -Pn --script=dns-brute domain.com	Brute forces DNS hostnames guessing subdomains
nmap -n -Pn -vv -O -sV --script smb-enum*,smb-ls,smb-mbenum,smb-os-discovery,smb-s*,smb-vuln*,smbv2* -vv 192.168.1.1	Safe SMB scripts to run
nmap --script whois* domain.com	Whois query
nmap -p80 --script http-unsafe-output-escaping scanme.nmap.org	Detect cross site scripting vulnerabilities
nmap -p80 --script http-sql-injection scanme.nmap.org	Check for SQL injections

Vulnerabilities

Vulnerability Categories:

- **Misconfiguration** - improperly configuring a service or application
- **Default installation** - failure to change settings in an application that come by default
- **Buffer overflow** - code execution flaw
- **Missing patches** - systems that have not been patched
- **Design flaws** - flaws inherent to system design such as encryption and data validation
- **Operating System Flaws** - flaws specific to each OS
- **Default passwords** - leaving default passwords that come with system/application

Vulnerability Assessment - Scans and tests for vulnerabilities but does not intentionally exploit them.

- Find the vulnerabilities so we can categorize them (OS, Misconfigurations, patch management, third-party, etc)

Vulnerability Management Life-cycle

The Vulnerability Management Life Cycle is intended to allow organizations to identify system security weaknesses; prioritize assets; assess, report, and remediate the weaknesses; and verify that they have been eliminated.

1. **Discover:** Inventory all assets across the network and identify host details including operating system and open services to identify vulnerabilities. Develop a network baseline. Identify security vulnerabilities on a regular automated schedule.
2. **Prioritize Assets:** Categorize assets into groups or business units, and assign a business value to asset groups based on their criticality to your business operation.
3. **Assess:** Determine a baseline risk profile so you can eliminate risks based on asset criticality, vulnerability threat, and asset classification.
4. **Report:** Measure the level of business risk associated with your assets according to your security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.
5. **Remediate:** Prioritize and fix vulnerabilities in order according to business risk. Establish controls and demonstrate progress.
6. **Verify:** Verify that threats have been eliminated through follow-up audits.

Vulnerability Scanning

Can be complex or simple tools run against a target to determine vulnerabilities.

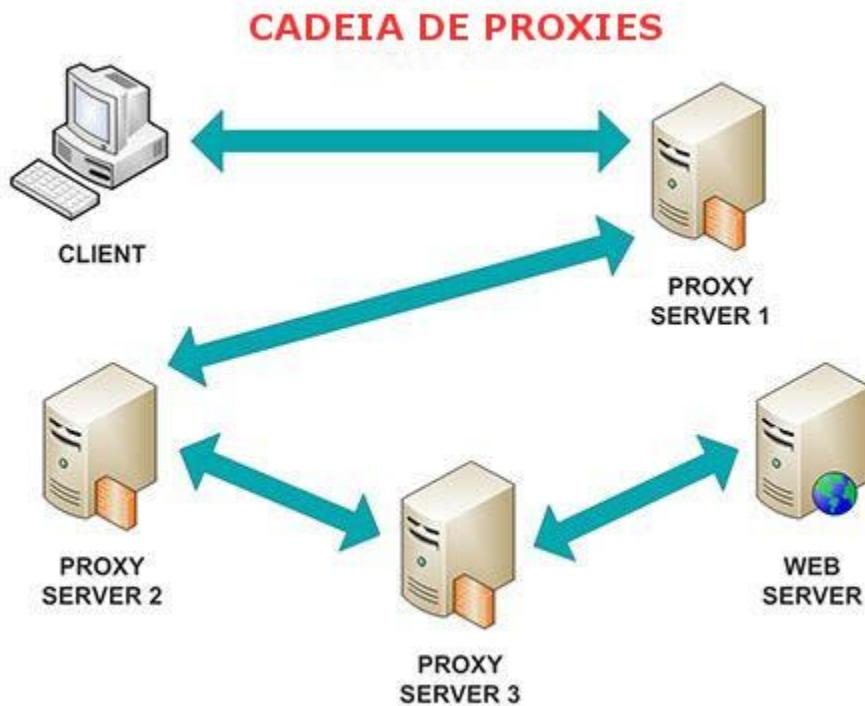
- **Types of Vuln. Assessment tools:**
 - Host-based
 - Depth-based (Fuzzer tools)
 - Application-layer tools (software, databases, etc)
 - Active scanning

- Passive scanning
- Scope tools
- Tools:
 - Industry standard is **Tenable's Nessus**.
 - **GFI LanGuard**.
 - **Nikto** - CLI; is a **web server assessment tool**. It is designed to find various default and insecure files, configurations and programs on any type of web server.
 - **OpenVAS** - Best competitor to Nessus and is free.
 - **wpscan** - CLI; Scan WordPress websites.
 - **MBSA - Microsoft Baseline Security Analyzer**.
 - **FreeScan** - Well known for testing websites and applications.
 - **Qualys**

CVSS and CVE

- **CVSS - Common Vulnerability Scoring System [+]**
 - Places numerical score based on severity
 - - None - white (0.0)
 - Low - green tones (0.1 - 3.9)
 - Medium - yellow/light orange (4.0 - 4.9)
 - High - orange (7.0 - 8.0)
 - Critical - red (9.0 - 10.0)
- **CVE – Common Vulnerabilities and Exposures [+]**
 - Is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE.
 -
- **NVD - National Vulnerability Database [+]**
 - is a database, maintained by NIST, that is fully synchronized with the MITRE CVE list; US Gov. vulnerabilities repository.

ProxyChains ☕



ProxyChains is open-source software that is available free and most of Linux distro it is pre-installed. If you are using the latest version of Kali Linux it is pre-installed in it.

ProxyChains is a tool that redirects the TCP (Transmission Control Protocol) connection with the help of proxies like TOR, HTTP(S), and SOCKS, and it creates a proxy chain server.

ProxyChains Features:

- Support **SOCKS5**, **SOCKS4**, and **HTTP/HTTPS CONNECT** proxy servers.
- Proxchains can be mixed up with a different proxy types in a list
- Proxchains also supports any kinds of chaining option methods, like: random, which takes a random proxy in the list stored in a configuration file, or chaining proxies in the exact order list, different proxies are separated by a new line in a file. There is also a dynamic option, that lets Proxchains go through the live only proxies, it will exclude the dead or unreachable proxies, the dynamic option often called smart option.
- Proxchains can be used with servers, like squid, sendmail, etc.
- Proxchains is capable to do DNS resolving through proxy.
- Proxchains can handle any TCP client application, ie., nmap, telnet.

Enumeration Concepts

Enumeration is the process of extracting **user names**, **machine names**, **network resources**, **shares**, and **services** from a system, and its conducted in an intranet environment.

- Get user names using email IDs

- **Get information using default passwords**
- **Get user names using SNMP**
- **Brute force AD**
- **Get user groups from Windows**
- **Get information using DNS zone transfers**
- **NetBios, LDAP, NTP, DNS**

In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target. The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase.

- **Defined as listing the items that are found within a specific target**
- **Always is active in nature**
- **Direct access**
- **Gain more information**

SNMP Enumeration

↳ Check the SNMP Enumeration practical lab

SNMP enumeration is the process of enumerating the users accounts and devices on a SNMP enabled computer.

- SNMP service comes with two passwords, which are used to configure and access the SNMP agent from the management station (MIB):
 1. **Read community string**
 2. **Read/Write community string**
- These strings (**passwords**) come with a **default value**, which is same for all the systems.
- **They become easy entry points for attackers if left unchanged by administrator.**

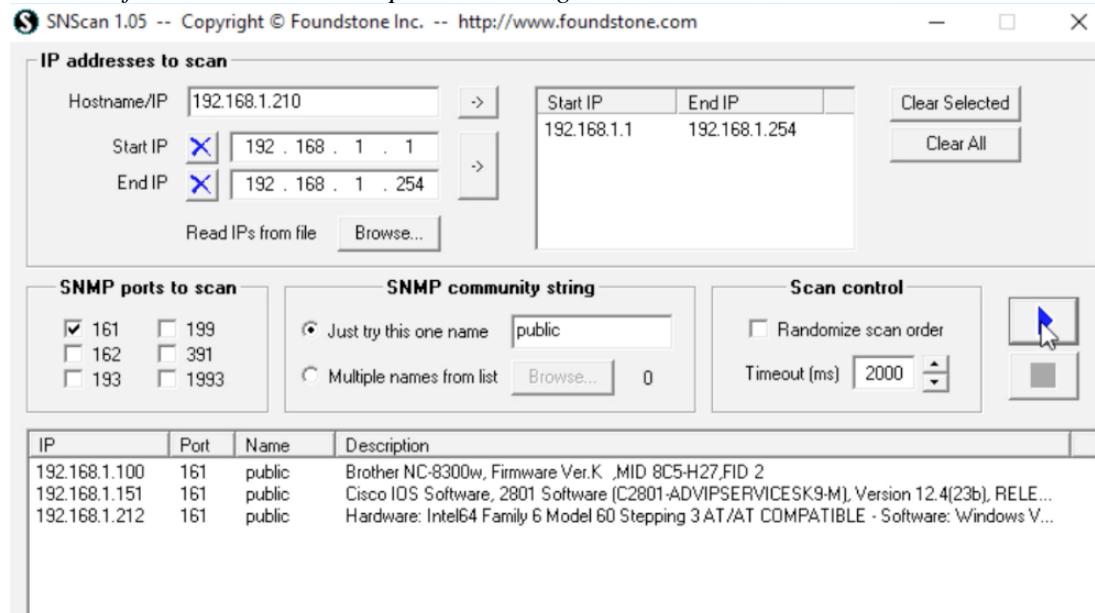
Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, shares(...) Network information such as ARP tables, routing tables, device specific information and traffic statistics.

- **Runs on Port 161 UDP**
- **Management Information Base (MIB)** - database that stores information
- **Object Identifiers (OID)** - identifiers for information stored in MIB
- **SNMP GET** - gets information about the system
- **SNMP SET** - sets information about the system
- **Types of objects**
 - **Scalar** - single object
 - **Tabular** - multiple related objects that can be grouped together
- SNMP uses community strings which function as passwords
- There is a read-only and a read-write version
- Default read-only string is **public** and default read-write is **private**
- These are sent in cleartext unless using SNMP v3
- **CLI Tools**

- **snmp-check** --> SNMP device enumerator comes pre-installed on Kali Linux machine; **snmp-check** supports a huge type of enumerations:
 - contact and user accounts
 - devices
 - domain
 - hardware and storage informations
 - hostname
 - IIS statistics
 - listening UDP ports and TCP connections
 - motd (banner)
 - network interfaces and network services
 - routing information
 - etc
- **Metasploit module snmp_enum**
 - [MSF snmp_enum practical lab](#)
- snmpwalk
- **GUI Tools**
 - Engineer's Toolset
 - SNMPScanner
 - OpUtils 5
 - SNScan

Example of SNScan:

Note: the first scanned item is a printer running SNMP.



Windows System Basics

- Everything runs within context of an account

- **Security Context** - user identity and authentication information
- **Security Identifier (SID)** - identifies a user, group or computer account
- **Resource Identifier (RID)** - portion of the SID identifying a specific user, group or computer
- The end of the SID indicates the user number
 - Example SID: S-1-5-21-3874928736-367528774-1298337465-**500**
 - **Administrator Account** - SID of 500
 - Command to get SID of local user:
 - `wmic useraccount where name='username' get sid`
 - **Regular Accounts** - start with a SID of 1000
 - **Linux Systems** used user IDs (UID) and group IDs (GID). Found in /etc/passwd
- **SAM Database** - file where all local passwords are stored (encrypted)
 - Stored in C:\Windows\System32\Config
- **Linux Enumeration Commands in PowerShell or CmdPrompt**
 - `finger` - info on user and host machine
 - `rpcinfo` and `rpcclient` - info on RPC in the environment
 - `showmount` - displays all shared directories on the machine
- **Look for share resources (NetBIOS):**
 - `net view \\sysName`
- **Windows SysInternals** is a website and suite that offers technical resources and utilities to manage, diagnose, troubleshoot, and monitor.
 - <https://docs.microsoft.com/en-us/sysinternals/downloads/>
 - Lots of resources for enumerating, windows administration tools, etc.

NetBIOS Enumeration

- NetBIOS provides name servicing, connectionless communication and some Session layer stuff
- The browser service in Windows designed to host information about all machines within domain or TCP/IP network segment
- NetBIOS name is a **16-character ASCII string** used to identify devices

Enumerating NetBIOS:

- You can use `nmap` or `zenmap` to check which OS the target is using, and which ports are open:
 - `nmap -O <target>`
- If there's any **UDP port 137** or **TCP port 138/139** open, we can assume that the target is running some type of NetBIOS service.
- On Windows is `nbtstat` command:

nbtstat displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP.

- `nbtstat` gives your own info
- `nbtstat -a` list the remote machine's name table given its **name**
- `nbtstat -A` - list the remote machine's name table given its **IP address**
- `nbtstat -n` gives local table
- `nbtstat -c` gives cache information

```

C:\>nbtstat -A 172.16.212.133
Local Area Connection 2:
Node IpAddress: [172.16.212.128] Scope Id: []
NetBIOS Remote Machine Name Table
  Name        Type      Status
  METASPOITABLE <00>  UNIQUE   Registered
  METASPOITABLE <03>  UNIQUE   Registered
  METASPOITABLE <20>  UNIQUE   Registered
  ..._MSBROWSE_.<01> GROUP    Registered
  WORKGROUP     <00>  GROUP    Registered
  WORKGROUP     <1D>  UNIQUE   Registered
  WORKGROUP     <1E>  GROUP    Registered

  MAC Address = 00-00-00-00-00-00

C:\>_

```

Code	Type	Meaning
<1B>	UNIQUE	Domain master browser
<1C>	UNIQUE	Domain controller
<1D>	GROUP	Master browser for subnet
<00>	UNIQUE	Hostname
<00>	GROUP	Domain name
<03>	UNIQUE	Service running on system
<20>	UNIQUE	Server service running

- NetBIOS name resolution doesn't work on IPv6
- **Other Tools for NetBIOS enumeration:**
 - SuperScan
 - Hyena
 - NetBIOS Enumerator (is a nbtstat with GUI)
 - NSAuditor

Linux System Basics

- **Enum4linux is a tool for enumerating information from Windows and Samba systems:**
 - enum4linux -u CEH -p Pa55w0rd -U 10.0.2.23



- -u Username, -p Password, -U users information
- ⚡ enum4linux practical lab
- Key features:
 - RID cycling (*When RestrictAnonymous is set to 1 on Windows 2000*)
 - User listing (*When RestrictAnonymous is set to 0 on Windows 2000*)
 - Listing of group membership information
 - Share enumeration
 - Detecting if host is in a workgroup or a domain
 - Identifying the remote operating system
 - Password policy retrieval (using polenum)
- **finger** --> who is currently logged in, when and where.
- Login Name Tty Idle Login Time Office Office Phone
- kali Kali tty7 10:09 Sep 1 14:14 (:0)
-
- **w** --> Show who is logged on and what they are doing.
- 00:27:15 up 9:32, 1 user, load average: 0.06, 0.09, 0.09
- USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
- kali tty7 :0 14:16 10:11m 30.26s 2.09s xfce4-session
-

⚠ Linux architecture and commands will be cover later on next module.

LDAP Enumeration

- **Runs on TCP ports 389 and 636 (over SSL)**
- Connects on 389 to a Directory System Agent (DSA)
- Returns information such as valid user names, domain information, addresses, telephone numbers, system data, organization structure and other items
- To identify if the target system is using LDAP services you can use **nmap** with -sT flag for TCP connect/Full scan and -O flag for OS detection.

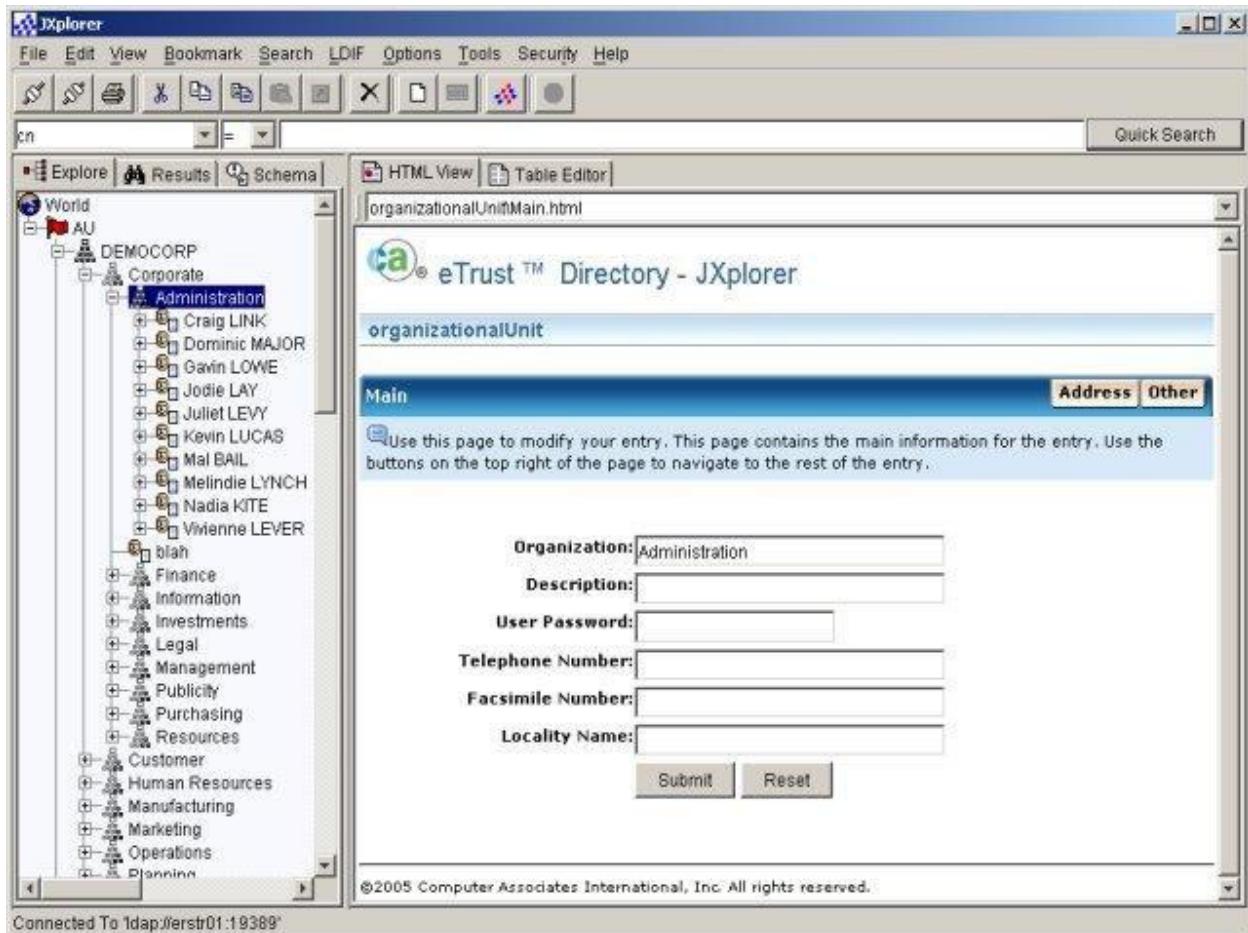
sudo nmap -sT -O <target IP address>

```
PORt STATE SERVICE
53/tcp open domain
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap <-----
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl <-----
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
49154/tcp open unknown
49155/tcp open unknown
49157/tcp open unknown
49158/tcp open unknown
49159/tcp open unknown
```



MAC Address: 00:00:11:33:77:44
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop

- **Tools for Enumeration LDAP:**
 - Softerra
 - JXplorer
 - Lex
 - LDAP Admin Tool
- **JXplorer example:**



NTP Enumeration

- **Runs on UDP 123**
- Querying can give you list of systems connected to the server (name and IP)
- **Tools**
 - NTP Server Scanner
 - AtomSync
 - Can also use Nmap and Wireshark

- **Commands** include ntptrace, ntpdate, ntpdc and ntpq

Nmap example for NTP enumeration:

- -sU UDP scan
- -pU port UDP 123 (NTP)
- -Pn Treat all hosts as online -- skip host discovery
- -n Never do DNS resolution
- The nmap script ntp-monlist will run against the ntp service which only runs on UDP 123

```
nmap -sU -pU:123 -Pn -n --script=ntp-monlist <target>
```

```
POR STATE SERVICE REASON
123/udp open ntp udp-response
| ntp-monlist:
| Target is synchronised with 127.127.38.0 (reference clock)
| Alternative Target Interfaces:
|   10.17.4.20
| Private Servers (0)
| Public Servers (0)
| Private Peers (0)
| Public Peers (0)
| Private Clients (2)
|   10.20.8.69 169.254.138.63
| Public Clients (597)
|   4.79.17.248 68.70.72.194 74.247.37.194 99.190.119.152
| ...
|   12.10.160.20 68.80.36.133 75.1.39.42 108.7.58.118
|   68.56.205.98
|   2001:1400:0:0:0:0:1 2001:16d8:dd00:38:0:0:0:2
|   2002:db5a:bccd:1:21d:e0ff:feb7:b96f 2002:b6ef:81c4:0:0:1145:59c5:3682
| Other Associations (1)
|_ 127.0.0.1 seen 1949869 times. last tx was unicast v2 mode 7
```

- As you can see on the output above, information of all clients that is using NTP services on the network shown IPv4 and IPv6 addresses.

SMTP Enumeration

- **Ports used:**
 - **SMTP: TCP 25** --> [outbound email]
 - **IMAP: TCP 143 / 993**(over SSL) --> [inbound email]
 - **POP3: TCP 110 / 995**(over SSL) --> [inbound email]
- In simple words: **users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.**
- **Enumerating with nmap:**
 - p25 port 25 (SMTP)
 - script smtp-commands nmap script - attempts to use EHLO and HELP to gather the Extended commands supported by an SMTP server.

```
nmap -p25 --script smtp-commands <target IP>
```

```
PORT STATE SERVICE
25/tcp open  smtp
| smtp-commands: WIN-J83C1DR5CV1.ceh.global Hello [10.10.10.10], TURN, SIZE 2097152, ETRN,
PIPELINING, DSN, ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT
HELP AUTH TURN ETRN BDAT VRFY
```

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds

- It is possible to connect to SMTP through **Telnet connection**, instead using port 23(Telnet) we can set the port 25(SMTP) on the telnet command:
 - **telnet <target> 25**
 - Case we got connected, we can use the **SMTP commands** to explore as shown below:

```
root@kali:~# telnet smtp.cox.net 25
Trying 68.6.19.8...
Connected to smtp.cox.net.
Escape character is '^].
220 fed1rmimpo209.cox.net cox ESMTP server ready
HELO
501 HELO requires valid address
HELO OurTest.com
250 fed1rmimpo209.cox.net hello [70          .69], pleased to meet you
MAIL FROM:bob@cox.net
250 2.1.0 <bob@cox.net> sender ok
RCPT TO:john@cox.net
250 2.1.5 <john@cox.net> recipient ok
```

- Both of emails are valid to an attacker explore further attacks like brute forcing etc.

Some SMTP Commands:

Command	Description
HELO	It's the first SMTP command: it starts the conversation identifying the sender server and is generally followed by its domain name.
EHLO	An alternative command to start the conversation, underlying that the server is using the Extended SMTP protocol.
MAIL FROM	With this SMTP command the operations begin: the sender states the source email address in the "From" field and actually starts the email transfer.
RCPT TO	It identifies the recipient of the email



DATA	With the DATA command the email content begins to be transferred; it's generally followed by a 354 reply code given by the server, giving the permission to start the actual transmission.
VRFY	The server is asked to verify whether a particular email address or username actually exists.
EXPN	asks for a confirmation about the identification of a mailing list.

Other tools:

- `smtp-user-enum`
 - Username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT TO.

2.0) Windows and server security

Windows Security Architecture

- Authentication credentials stored in SAM file
- File is located at C:\windows\system32\config
- Older systems use LM hashing. Current uses NTLM v2 (MD5)
- Windows network authentication uses Kerberos

LM Hashing

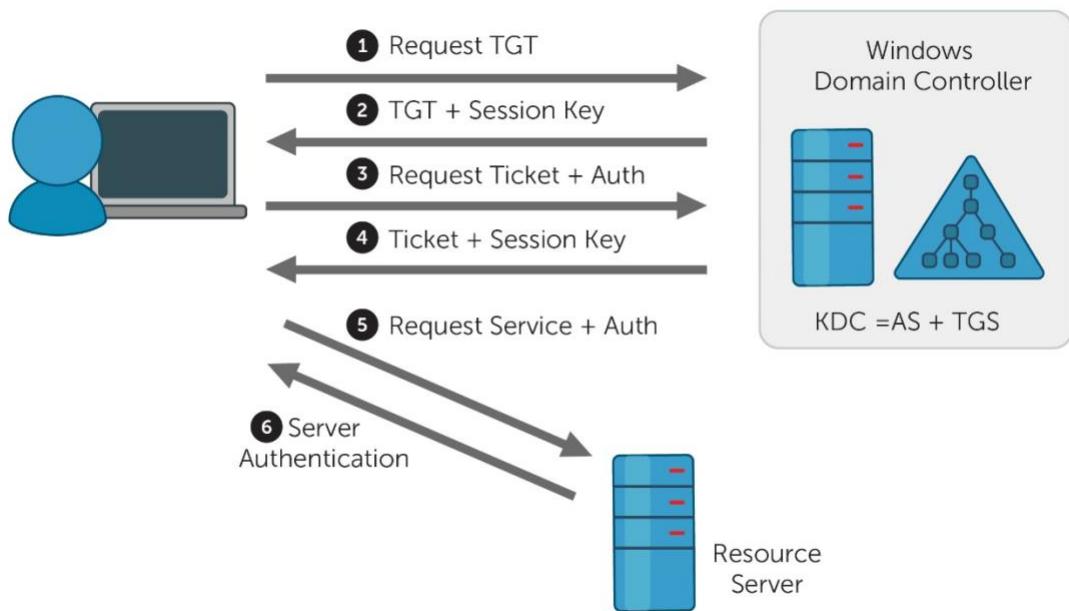
- Splits the password up. If it's over 7 characters, it is encoded in two sections.
- If one section is blank, the hash will be AAD3B435B51404EE
- Easy to break if password is 7 characters or under because you can split the hash
- SAM file presents as UserName:SID:LM_Hash:NTLM_Hash:::

Ntds.dit

Database file on a domain controller that stores passwords

- Located in %SystemRoot%\NTDS\Ntds.dit or
- Located in %SystemRoot%\System32\Ntds.dit
- Includes the entire Active Directory

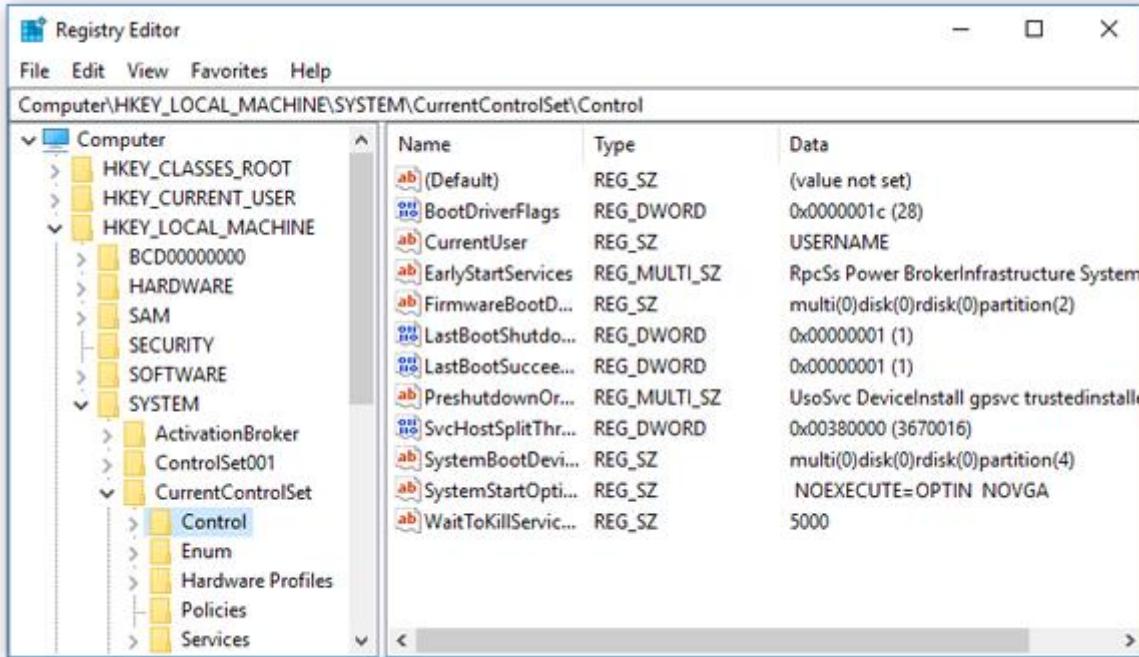
Kerberos for Active Directory Domain Services (AD DS)



- Steps of exchange
 1. Client asks **Key Distribution Center (KDC)** for a ticket. Sent in clear text.
 2. Server responds with **Ticket Granting Ticket (TGT)**. This is a secret key which is hashed by the password copy stored on the server.
 3. If client can decrypt it, the TGT is sent back to the server requesting a **Ticket Granting Service (TGS)** service ticket.
 4. Server sends TGS service ticket which client uses to access resources.
- 1. **Tools**
 - KerbSniff
 - KerbCrack
 - Both take a long time to crack

⚠️ Uses TCP/UDP Port 88

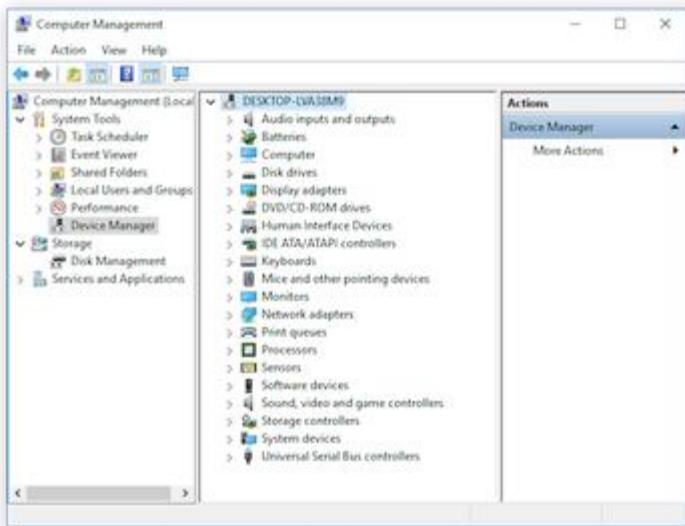
Registry



- Collection of all settings and configurations that make the system run
- Made up of keys and values
- Root level keys
 - **HKEY_LOCAL_MACHINE** (HKLM) - information on hardware and software
 - **HKEY_CLASSES_ROOT** (HKCR) - information on file associates and OLE classes
 - **HKEY_CURRENT_USER** (HKCU) - profile information for the current user including preferences
 - **HKEY_USERS** (HKU) - specific user configuration information for all currently active users
 - **HKEY_CURRENT_CONFIG** (HKCC) - pointer to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current
- Type of values
 - **REG_SZ** - character string
 - **REG_EXPAND_SZ** - expandable string value
 - **REG_BINARY** - a binary value
 - **REG_DWORD** - 32-bit unsigned integer
 - **REG_LINK** - symbolic link to another key
- Important Locations
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- Executables to edit
 - regedit.exe
 - regedt32.exe (preferred by Microsoft)

MMC



- Microsoft Management Console - used by Windows to administer system
- Has "snap-ins" that allow you to modify sets (such as Group Policy Editor)

Sigverif.exe



- File Signature Verification (Sigverif.exe) detects signed files and allows you to:
 - View the certificates of signed files to verify that the file has not been tampered with after being certified.

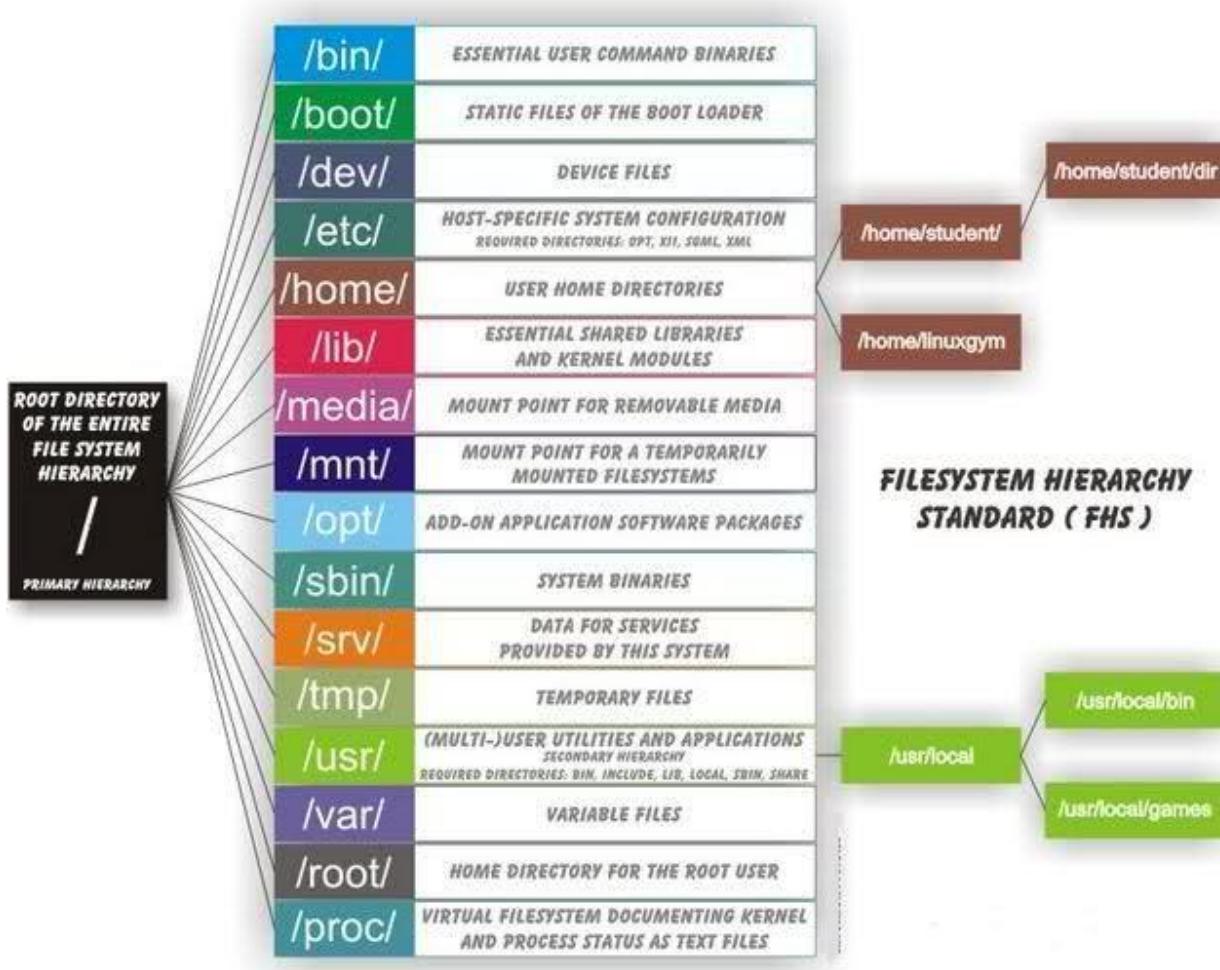


- Search for signed files.
- Search for unsigned files.

Linux Security Architecture

Linux Directory Structure

- Linux root is just a slash (/)
- Important locations
 - / - root directory
 - /bin - basic Linux commands
 - /dev - contains pointer locations to various storage and input/output systems
 - /etc - all administration files and passwords. Both password and shadow files are here
 - /home - holds the user home directories
 - /mnt - holds the access locations you've mounted
 - /sbin - system binaries folder which holds more administrative commands
 - /usr - holds almost all of the information, commands and files unique to the users



Linux Common Commands

Command	Description
adduser	Adds a user to the system
cat	Displays contents of file
cp	Copies
ifconfig	Displays network configuration information
kill	Kills a running process
ls	Displays the contents of a folder. -l option provides most information.
man	Displays the manual page for a command
passwd	Used to change password
ps	Process status. -ef option shows all processes
rm	Removes files. -r option recursively removes all directories and subdirectories
su	Allows you to perform functions as another user (super user)

- Adding an ampersand after a process name indicates it should run in the background.
- `pwd` - displays current directory
- `chmod` - changes the permissions of a folder or file
 - **Read is 4, write is 2 and execute is 1**
 -

Read Write Execute

r--	-w-	--x
4	2	1

- First number is user, second is group, third is others
- when you issue the `ls` command with `-la` flag on Linux, you can see the permissions. As you can see below the file have a permission for everyone (777), will be like this:
 - `rwxrwxrwx` ---> user
 - `rwxrwxrwx` ---> group
 - `rwxrwxrwx` ---> others
- Another example - **755** is everything for users, read/execute for group, and read/execute for others
 - `rwxr-xr-x` ---> user
 - `rwxr-xr-x` ---> group
 - `rwxr-xr-x` ---> others
- You also can set permissions like: `chmod g=rw` (set read/write for groups).
- **Root has UID and GID of 0** - you can see this information by issuing the command `id`.
 - `root@kali:~# id`
 - `uid=0(root) gid=0(root) groups=0(root)`
 -
- First user has UID and GID of 500 (Fedora and CentOS); in most Linux systems the **non-root/normal user are UID and GID of 1000**.
- `normal-user@kali:~# id`
 - `id`
 - `uid=1000(kali) gid=1000(kali)`
`groups=1000(kali),24(cdrom),25(floppy),27(sudo),29(audio),30(dip)`
`,44(video),46(plugdev),109(netdev),117(bluetooth),132(scanner)`
 -
- Passwords are stored in **/etc/shadow** for most current systems
- **/etc/passwd** stores passwords in hashes.
- `cat /etc/passwd`
 - `root:x:0:0:root:/root:/bin/bash`
 - `daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin`
 - `bin:x:2:2:bin:/bin:/usr/sbin/nologin`
 - `sys:x:3:3:sys:/dev:/usr/sbin/nologin`
 - `sync:x:4:65534:sync:/bin:/bin sync`
 - `(...)`
 -
- **/etc/shadow** stores passwords encrypted (hashed and salted) and is only accessible by root
- `sudo cat /etc/shadow`

```
o  root:!::18390:0:99999:7:::
o  daemon:*::18390:0:99999:7:::
o  bin:*::18390:0:99999:7:::
o  kali:$6$a/53BntOdPOaghAx$VCAdR3Af97cYTtWCtDp9iksacL3gj2Sgrb12EMix
   0iTuxc5jOQp1lbaRi.jNDsP2qjV3GvFAqd5Fu.8/7/P1.:18281:0:99999:7:::
o  (...)
```

Linux security

Linux is free and open source (source code can be reused and freely modified and redistributed both commercially and non-commercially)

Linux can be used in a wide verity of devices such as embedded device i.e., smartphones raspberry pi etc.

Benefits of using Linux

- It is very stable multi user, multi-tasking environment
- Standard platform (includes all tools and utilities typically associated with units)
- Flexibility and customizable (open source)
- Includes advanced graphical user interface (GNOME)
- Provides free general interests desktop application e.g., web browsers docx processors
- Can accommodate 100s of specialized applications; mars rover
- Freedom from malwares.

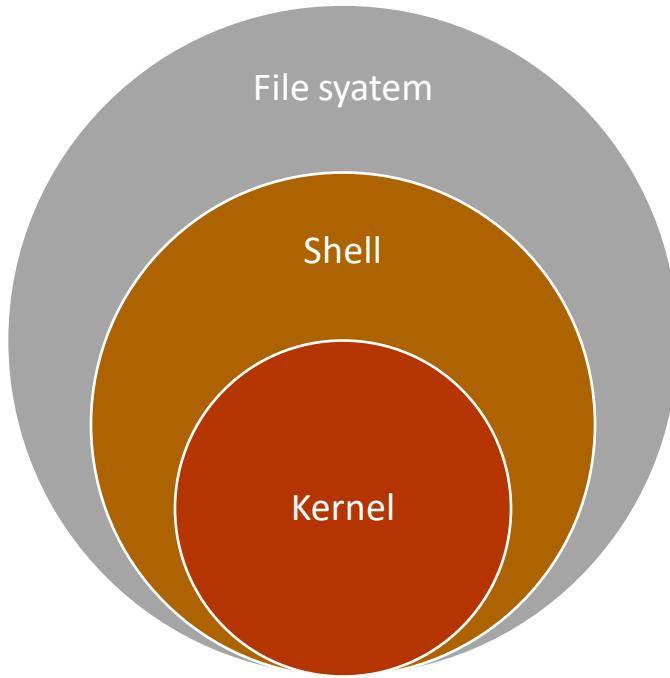
The GNU general public license allows anybody to;

- Use the software freely without any limitations
- Use the software with appropriately modifications free of charge as long as you do not distribute or sell the modified version

To ensure continued security one should do the following;

- Keep current with patches
- Monitor Log files (configuration files)
- Audit password strength (ripper)
- Check binary config files
- Regularly scan machine for rootkit and trojans
- Check for remote vulnerabilities

Linux structure



Kernel is the heart of the OS; it is the low-level core (interface between applications and hardware controls or functions and manage memory time clock management process communications and sets process priority)

Shell is a program provides interface between users and kernel it is a command interpreter

Types of shell

Sh – bourne shell

C shell –

K Sh Korn shell

Bash – bourne again shell

File system Linux treats everything as a file including hardware devices

It is arranged as a directory hierarchy the top-level directory is known a Root (top bottom)

Root kit versions

- LRK

- TORM
- Adore

Du command is mainly used to .. installed by rootkit

Ifconfig used to configure and display information about network interfaces

NXD is a supper sever designed to support servers that provide internet services.

KILL ALL it's a command used to stop all the services this command is trojaned in most root kits so administrators can not stop certain process that have been installed by the rootkit

Login it's a command that alters the log files such that the admin can't track any login services

Preventing root kit

- Use of firewalls
- Updating patches
- Use of IDS

Security features include firewall or networks

Know exactly what is running on all system

Grant access to users that are needed to perform their jobs

Use VPN and SSH (for secure communication >> data encryption in browsing.)

03) Data and information security

Data is a raw form of information

Data security is ensuring that data is kept safe from corruption and unsafe places

Unauthorized access of data may lead to numerous problems for the large cooperation even personal user

Overview Data and information security

1. data security
2. data availability
3. data backup and recovery
4. distributed systems
5. client server systems (user interface and management of database)

Data security management

Types of data security

➤ Encryption

Using an algorithm to transform normal text characters into an unreadable format, encryption keys scramble data so that only authorized users can read it. File and database encryption solutions serve as a final line of defense for sensitive volumes by obscuring their contents through encryption or tokenization. Most solutions also include security key management capabilities.

Data Erasure

More secure than standard data wiping, data erasure uses software to completely overwrite data on any storage device. It verifies that the data is unrecoverable.

Data Masking

By masking data, organizations can allow teams to develop applications or train people using real data. It masks personally identifiable information (PII) where necessary so that development can occur in environments that are compliant.

Data Resiliency

Resiliency is determined by how well a data center is able to endure or recover any type of failure – from hardware problems to power shortages and other disruptive events.

How data security and other security facets interact

Achieving enterprise-grade data security

The key to applying an effective data security strategy is adopting a risk-based approach to protecting data across the entire enterprise. Early in the strategy development process, taking business goals and regulatory requirements into account, stakeholders should identify one or two data sources containing the most sensitive information, and begin there. After establishing clear and tight policies to protect these limited sources, they can then extend these best practices across the rest of the enterprise's digital assets in a prioritized fashion. Implemented automated data monitoring and protection capabilities can make best practices far more readily scalable.

Data security and the cloud

Securing cloud-based infrastructures requires a different approach than the traditional model of situating defenses at the network's perimeter. It demands comprehensive cloud data discovery and classification tools, plus ongoing activity monitoring and risk management. Cloud monitoring tools can sit between a cloud provider's database-as-a-service (DBaaS) solution and monitor data in transit or redirect traffic to your existing security platform. This allows for policies to be applied uniformly no matter where the data resides.

Data security and BYOD

The use of personal computers, tablets, and mobile devices in enterprise computing environments is on the rise despite security leaders' well-founded concerns about the risks that this practice can pose. One recent survey found that 85% of companies allowed not only employees but also contractors, vendors, and suppliers to access enterprise resources from personal devices. One way of improving bring your own device (BYOD) security is to require employees who use personal devices to access corporate networks to install security software on those devices to enhance centralized control over and visibility into data access and movement. Another strategy is to build an enterprise-wide, security-first mindset, encouraging employees to utilize strong passwords, multi-factor authentication, regular software updates, and device backups, along with data encryption by teaching them the value of these actions.

Data security, privacy and protection solutions

Data security solutions

Protect data across multiple environments, meet privacy regulations and simplify operational complexity.

- **Explore data security solutions**

Data security services

Protect data against internal and external threats.

- **Explore data security services**

Homomorphic encryption

Unlock the value of sensitive data without decryption to preserve privacy.

- **Explore homomorphic encryption services**

Storage data backup and recovery

Go beyond data backup and recovery to unify workload protection and cyber resilience.

- **Explore data backup and recovery**

Data encryption solutions

Protect enterprise data and address regulatory compliance with data-centric security solutions.

- **Explore data encryption solutions**

Infrastructure security

Protect your data from vulnerabilities and cyberattacks on-premises and between clouds.

- **Explore infrastructure security solutions**

Data privacy

Strengthen data privacy protection with IBM data privacy solutions.

- **Explore data privacy solutions**

Ransomware protection

Protect your organization's data from ransomware threats.

- **Explore ransomware protection solutions**

Zero trust security

Protect critical data using zero trust security practices.

- **Explore zero trust security solutions**

Cloud computing

What is Cloud Computing?

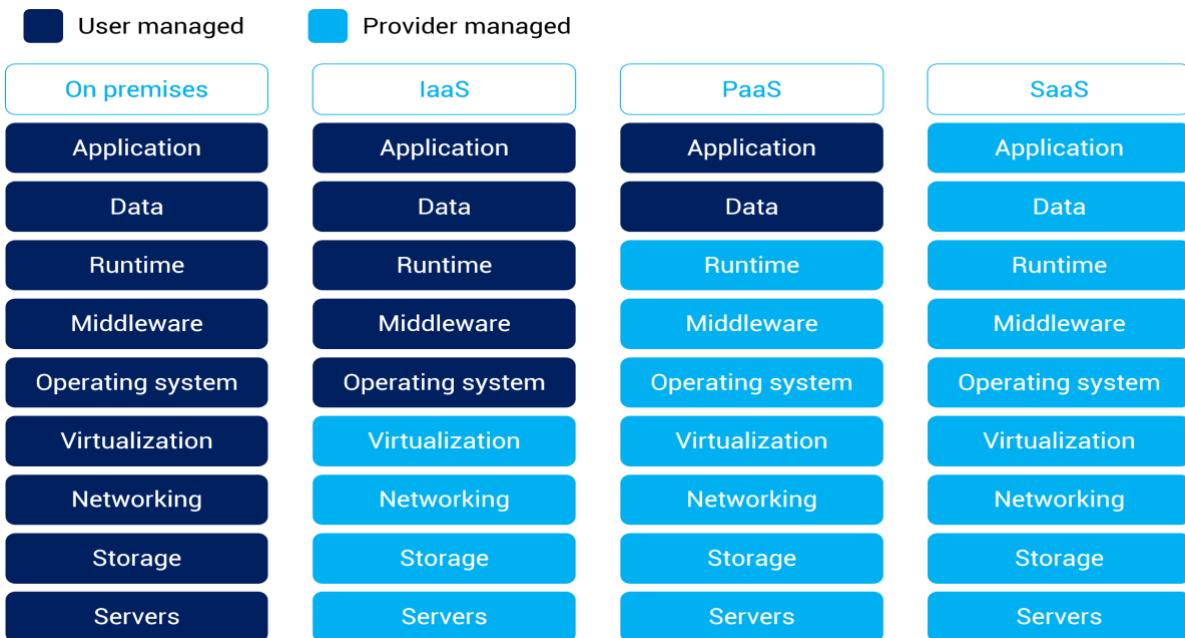
The cloud is a large group of interconnected computers. We usually use the symbol of cloud to denote the complicated networks in circuit. That is why the name cloud computing is given for these networks of computers. These computers may be personal or public. Cloud computing extends beyond a single company or enterprise. Access is via internet and it offers massive computing power and storage capability and enables wide scale group collaboration. Basically, it is a coming back to the centralized computing infrastructure which was popular in 1950s and 60s.

Cloud Computing Basics

- **Three Types of Service Models:**
 - **Infrastructure as a Service (IaaS)**
 - Provides virtualized computing resources
 - Third party hosts the servers with hypervisor running the VMs as guests
 - Subscribers usually pay on a per-use basis
 - e.g: AWS, Microsoft Azure, Digital Ocean, Google Cloud
 - **Platform as a Service (PaaS)**
 - Geared towards software development
 - Hardware and software hosted by provider
 - Provides ability to develop without having to worry about hardware or software
 - e.g.: Heroku, SalesForce
 - **Software as a Service (SaaS)**
 - Provider supplies on-demand applications to subscribers
 - Offloads the need for patch management, compatibility and version control
 - e.g: Microsoft Office 365, Dropbox storage, Google Docs.

Tech stack	Type
Software	SaaS
Apps	PaaS

OS	IaaS
Virtualization	managed by provider
Storage/Networking	managed by provider



Cloud Deployment Models

- **Private Cloud** - Cloud solely for use by one tenant; usually done in larger organizations.
- **Community Cloud** - Is made up of infrastructure from several different entities which may be cloud providers, business partners, and so on. (Members only type of thing)
- **Public Cloud** - Services provided over a network that is open for public to use; Amazon S3, Microsoft Azure - Open for business.
- **Hybrid Cloud** - A composition of two or more cloud deployment models.

NIST Cloud Architecture

The NIST cloud computing reference architecture (NIST SP 500-292) defines five major actors; Each actor is an entity (a person or an organization) that participates in a transaction or process and/or perform tasks in cloud computing.

- **Cloud Consumer** - A person or org. that maintains a business relationship with, and uses services from Cloud Providers; acquires and uses cloud products and services.
- **Cloud Provider** - A person, org. or entity responsible for making a service available; Purveyor of products and services.
- **Cloud Auditor** - Independent assessor of cloud service a security control.

- **Cloud Broker** - Manages use, performance and delivery of services as well as relationships between Cloud Providers to Cloud consumers.
- **Cloud Carrier** - Organization with responsibility of transferring data; Intermediary that provides connectivity and transport of Cloud services from Cloud providers to Cloud consumers. (e.g.: Telecom's)

 - **FedRAMP** - regulatory effort regarding cloud computing

 - **PCI DSS** - deals with debit and credit cards, but also has a cloud SIG

Five characteristics of cloud computing

The National Institute of Standards and Technology (NIST) defines cloud computing as it is known today through five particular characteristics.

1. **On-demand self-service**
2. **Broad network access**
3. **Multi-tenancy and resource pooling**
4. **Rapid elasticity and scalability**
5. **Measured service**

Threats:

- **Data Breach or Loss** - Biggest threat; includes malicious theft, erasure or modification
- **Shadow IT** - IT systems or solutions that are developed to handle an issue but aren't taken through proper approval chain
- **Abuse of Cloud Resources** - Another high threat (usually applies to IaaS and PaaS)
- **Insecure Interfaces and APIs** - Cloud services can't function without them, but need to make sure they are secure
- **Service Oriented Architecture** - API that makes it easier for application components to cooperate and exchange information
- **Insufficient due diligence** - Moving an application without knowing the security differences
- **Shared technology issues** - Multitenant environments that don't provide proper isolation
- **Unknown risk profiles** - Subscribers simply don't know what security provisions are made in the backgrounds
- **Wrapping Attack** - SOAP message intercepted and data in envelope is changed and sent/replayed
- **Session riding** - CSRF under a different name; deals with cloud services instead of traditional data centers
- **Others include malicious insiders, inadequate design and DDoS**
 - Other threats:
 - Loss/compromise of encryption keys
 - Isolation failure
 - Compliance risk

- VM vulnerabilities
- Vendor lock-on
- Jurisdictional issues based on changing geographic boundaries
- E-discovery/subpoena
- Cloud service termination/failure
- Improper/incomplete data handling & disposal
- Management network failure/interface compromise

Attacks:

1. Service hijacking via Social engineering & network sniffing
2. Session hijacking using XSS
3. DNS attacks
4. Side channel attacks - (e.g.: Using an existing VM on the same physical host to attack another)
5. Cross VM attacks
6. SQL injection
7. Cryptanalysis attacks
8. Wrapping attacks - performed during the translation of SOAP messages in the TLS layer; attackers duplicate the body of the message and send it to the targeted server impersonating the legitimate user.
9. DoS/DDoS attack
10. Man-in-the-Cloud attacks - abuse of cloud file synchronization services or tracking the user into installing malicious software that places the attacker's synchronization token for the service on their machine, allowing the attacker to steal the user's token and gain access to their files.

OWASP Top 10 Application Security Risks

1. **Injection** - Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
 - Input validation
 - Limit account privileges
2. **Broken Authentication** - Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
3. **Sensitive Data Exposure** - Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

4. **XML External Entities (XXE)** - Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
 - o If your application uses SAML for identify processing with federated security or Single Sing on (SSO). SAML uses XML.
 - o If applications accepts XML directly or XML uploads from untrusted sources, or inserts untrusted data into XML documents.
 - o Any of XML processors in the application or SOAP based web services that have (DTDs) enabled.
5. **Broken Access Control** - Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
6. **Security Misconfiguration** - is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
7. **Cross-Site Scripting XSS** - occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
 - o Reflected XSS
 - o Stored XSS
 - o DOM XSS
8. **Insecure Deserialization** - often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
9. **Using Components with Known Vulnerabilities** - Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
10. **Insufficient Logging & Monitoring** - Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Additional Attacks

1. **Directory Traversal (..)** - An attacker can get sensitive information like the contents of the /etc/passwd file that contains a list of users on the server; Log files, source code, access.log and so on

2. **Cross-site Request Forgery (CSRF)** - Forces an end user to execute unwanted actions on an app they're already authenticated on
 - o Inherits identity and privileges of victim to perform an undesired function on victim's behalf
 - o Captures the session and sends a request based off the logged in user's credentials
 - o Can be mitigated by sending **random challenge tokens**

Cloud Security Control Layers

Problem with cloud security is what you are allowed to test and what should you test; Another concern is with a hypervisor, if the hypervisor is compromised, all hosts on that hypervisor are as well.

1. **Applications** - SDCL (Software development cycle), WAF (web application firewall)
2. **Information** - DLP, encryption
3. **Management** - GRC, IAM , Patch & Configuration
4. **Network** - NIDS/NIPS, DNSSEC, QoS
5. **Trusted Computing Model** - attempts to resolve computer security problems through hardware enhancements
 - **Roots of Trust (RoT)** - set of functions within TCM that are always trusted by the OS
6. **Computer & Network Storage** - Encryption, Host-based firewall, HIDS/HIPS
7. **Physical** - Guards, Gates, Fences etc.

Tools

- **Cloud Inspect** - pen-testing application for AWS EC2 users
- **Cloud Passage Halo** - instant visibility and continuous protection for servers in any cloud
- **Dell Cloud Manager**
- **Qualys Cloud Suite**
- **Trend Micro's Instant-On Cloud Security**
- **Panda Cloud Office Protection**

Key Properties of Cloud Computing

The key properties of Cloud computing are

1. **User centric:** This means once a user is connected to cloud any data there, such as images, videos, applications, becomes his property. Not only the data but the devices connected also becomes his and he can share it with other users.
2. **Task Centric:** Cloud computing focus on what one need and how application can do it for us. Here documents are given more priority than the applications which create them.

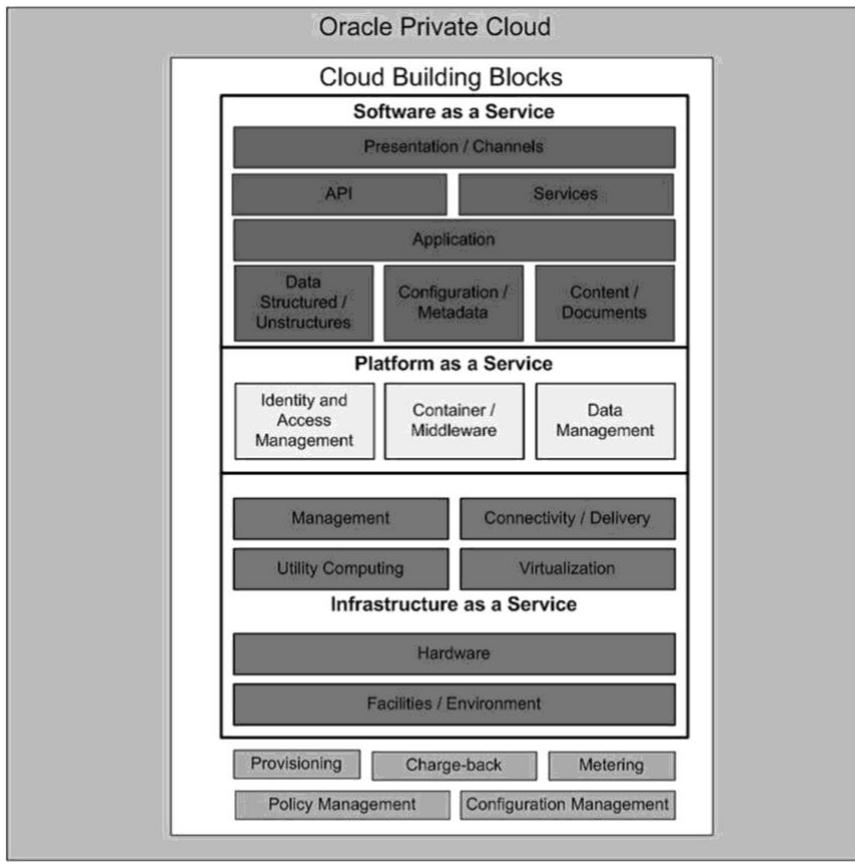
3. **Powerful:** Powerful in the sense that as there is large computers more computing power and mass data storage possible.
4. **Self-Healing:** Is called Self-healing because hot backups are available for every document in the cloud. Hence if one document crashes there will be its duplicate ready to run.
5. **Multi-tenancy & Intelligence:** Multi-tenancy refers to sharing of data and costs across a large pool of users. As various data are stored in cloud data mining and analysis are necessary for accessing information in an intelligent manner.
6. **Programmable:** Many processes in cloud computing shall be automated such as backing up crashed data with its duplicate. Hence programming is associated with cloud computing.
7. **Flexible:** Flexible as the users may be of different varieties and hence it has to match with their needs.

Understanding Cloud Computing

1. Understanding Cloud Architecture

Individual users connect to the cloud from their own personal computers or portable devices, over the Internet. To these individual users, the cloud is seen as a single application, device, or document. The hardware in the cloud is invisible.

Oracle Private Cloud



Copyright © 2009, Oracle Corporation. All Rights Reserved.

2. Understanding Cloud Storage

In Cloud computing data is stored on multiple third-party servers rather than on the dedicated servers in traditional network data storage.

3. Understanding Cloud Services

The wide range of applications and programs include Cloud Services. Any web-based service or application offered via cloud computing is called cloud services.

Benefits From Cloud Computing

1. Reduces Run time and Response time: As there is large computing capability run time and response time get reduced.
2. Minimize Infrastructure risk: As there is service providers to provide necessary infrastructure and services infrastructure risk get reduced. We need not purchase infrastructure.
3. Lower Cost of Entry: For new organizations the infra structure and services can be rented and this reduces their cost of entry into the market.

4. Increased Pace of innovation: As the new and small firms can compete with the leaders in the industry with the help of cloud computing, this increases the pace of innovation.

5. Cost Conscious users are satisfied: Most of the users are cost conscious. They are well satisfied by the services cloud computing provides.

Cloud Computing Services

1. Amazon Web Service

Amazon web services is the set of cloud computing services offered by Amazon. Different services provided by Amazon are

- a) Elastic Cloud Computing (EC2)**
- b) Simple Storage Service (S3)**
- c) Simple Queue Service (SQS)**
- d) Simple Database Service (SDS)**

2. Google App Engine

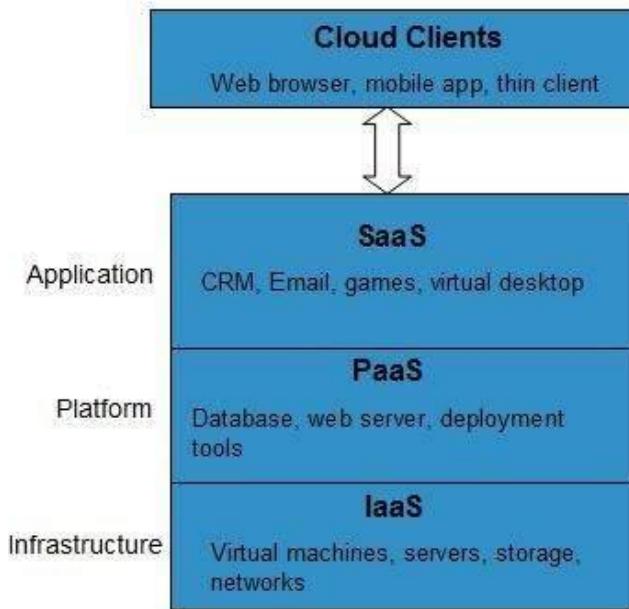
Google App Engine allows you to run your web Applications on Google's infrastructure.

The environment includes following features.

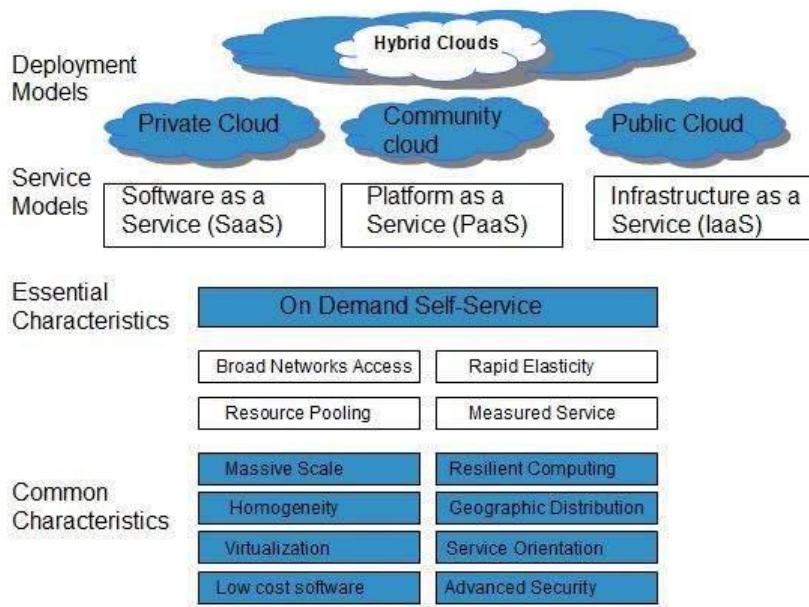
- dynamic web serving, with full support for common web technologies**
- persistent storage with queries, sorting and transactions**
- automatic scaling and load balancing**
- APIs for authenticating users and sending email using Google Accounts**
- a fully featured local development environment that simulates Google App Engine on your computer**

NIST Cloud Computing three service and Definition:

The National Institute of Standards and Technology (NIST) describes cloud computing as “a model” for on-demand network access to computing resources (e.g., networks, servers, storage, applications and services). Common Cloud Service Models are:



- **Cloud Software as a Service (SaaS):** The user has the possibility to use the service provider's applications over the network. These applications are accessed via different interfaces, thin client, Web browser, mobile devices...The customer manages and does not control the underlying cloud infrastructure including network, servers, operating systems, databases, storage, but can possibly benefit from access to restricted configurations, specific to user categories.
- **Cloud Platform as a Service (PaaS):** The consumer can deploy cloud infrastructure on its own applications. The user manages and does not control the underlying cloud infrastructure (network, servers, operating systems, databases, storage), but has control over the deployed applications and the ability to configure the environment of application hosting.
- **Cloud Infrastructure as a Service (IaaS):** The client can rent storage, processing power, network and other computing resources. The user manages and does not control the underlying cloud infrastructure but has control over databases, operating systems, and applications deployed.



The Benefits of Cloud Computing (Cloud Computing)

- Cost Reduction: Cloud computing is seen as an incremental investment; companies can save money in the long term by obtaining resources.
- Storage increase: instead of purchasing large amounts of storage before the need, organizations can increase storage incrementally, requesting additional disk space on the service provider when the need is recognized.
- Resource pooling: in the IT industry, this feature is also known as multi-tenancy, where many users / clients share a type and varied level of resources.
- Highly automated: As the software and hardware requirements are hosted on a cloud provider, IT departments sites no longer have to worry about keeping the things-to-date and available.
- Greater mobility: Once the information is stored in the cloud, access it is quite simple, just you have an Internet connection, regardless of where they are located.
- Change the IT focus: Once the responsibility of the computing environment has, essentially shifted to the cloud provider, IT departments can now focus more on the organization's needs and the development of strategic applications and tactics and not on operational needs of the day-to-day.
- Towards Green IT: By releasing the physical space, virtualization of applications and servers contributes to the reduction of equipment as well as the need for air conditioning, consequently, less energy waste.
- Keep updated things: Similar to change the IT focus, this benefit is because of the new demands of providers cloud services, ie, the focus of providers is to monitor and maintain the most recent tools and techniques for the contractor.

- Quick elasticity: this characteristic has to do with the fundamental aspects of Cloud flexibility and elasticity. For example, the web shops carry a standard number of transactions during the year, but it is necessary to increase near Christmas time. And of course, these stores do not want to pay for that capacity at peak during the rest of the year.
- Measurement service: which means services monitored, controlled and reported. This feature allows a model of pay-per-use service, or pay for use. It has similarities with the concept of telephone service packages where you pay a standard signature to basic levels, and paid extra for the additional service, without changing the contract.
- One can access applications as utilities, over the Internet.
- One can manipulate and configure the applications online at any time.
- It does not require to install a software to access or manipulate cloud application.
- Cloud Computing offers online development and deployment tools, programming runtime environment through **PaaS model**.
- Cloud resources are available over the network in a manner that provide platform independent access to any type of clients.
- Cloud Computing offers **on-demand self-service**. The resources can be used without interaction with cloud service provider.
- Cloud Computing is highly cost effective because it operates at high efficiency with optimum utilization. It just requires an Internet connection
- Cloud Computing offers load balancing that makes it more reliable.

The limitations of Cloud Computing (Cloud Computing)

The various problem areas for cloud computing environments are:

Security: As the data are no longer in their own organization, security becomes a major issue and questions must be answered, such as: Data is protected as adequate? There is a hacker-proof system? Can you meet the requirements regulations and government for privacy? How do you discover the leak information? Note also that corporate governance is always very concerned about the data that is stored outside the organization.

Location and Data Privacy: Where the data is stored? How data is stored? The provider has adequate security for data in places where they are stored?

Internet addiction: Since the cloud features are not available on the local network, you have to worry about the availability of the Internet. If you lose access to the Internet out, what happens to your cloud computing environment? If your service provider increasing period unavailability, what you do with your employees and customers? What do you do in case of increased latency or delays the answers?

Levels of availability and service: Most organizations are familiar with the agreements service levels. The service level agreement specifies the amount of service capacity that someone has to provide, along with

the penalties for not providing this level of service. How you can be sure that the cloud service provider has sufficient resources to maintain a service level agreement you signed with them?

Cryptography

Goals of cryptography

Nonrepudiation - Means by which a recipient can ensure the identity of the sender and neither party can deny sending.

Cryptography

Technical terms in crypto systems

- **Algorithm** is a set of mathematical rules used in encryption and decryption
- **Cryptography** is a science of secret writing that enables one to store and transmit data in a form that is available only to the intended individual
- **Crypto-system** is a hardware or a software that transform a message to cipher text and back to a plane text.
- **Crypt analysis** is the practice of obtaining plain text from cipher text without a key (cracking)
- **Cryptology** is the study of both cryptography and crypto analysis
- **Cipher text** is encrypted data (gibberish)
- **Plain text** is data in readable format.
- **Encipher** is the process of transforming data into unreadable format
- **Decipher** is the act of transforming data into a readable format
- **Key** is a secret sequence of bits and instruction that governs the act of encryption and decryption
- **Key clustering** is ana instance where deferent keys generate same plain text
- Key instance Possible values used to contest keys
- **Work factor** it is an estimated time effort and resources necessary to brake crypto-system

Types of cipher text

1. **Block cipher text** a block of message is encrypted at a time (DES data encryption standards that is 64 bits symmetric – the key is the same) when a block cipher is used for encryption and decryption purpose the message is divided into block of bits (64 bits) then put through submission transmission and other mathematical functions.

2. **Stream cipher text** is a cipher text in which every bit is encrypted at a time it is more secure than block type

Types of cryptography (algorithm)

1. Single key cryptography systems (symmetrical cryptograph) it uses a single key for both encryption and decryption
2. Public key cryptography systems (asymmetrical cryptography) it uses one key for encryption and another key for decryption
3. Hash functions

What is Cryptography?

Cryptography is the art and science of making a cryptosystem that is capable of providing information security.

Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

What is Cryptanalysis?

The art and science of breaking the cipher text is known as cryptanalysis.

Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

Note – Cryptography concerns with the design of cryptosystems, while cryptanalysis studies the breaking of cryptosystems.

Security Services of Cryptography

The primary objective of using cryptography is to provide the following four fundamental information security services. Let us now see the possible goals intended to be fulfilled by cryptography.

Confidentiality

Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as **privacy** or **secrecy**.

Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption.

Data Integrity

It is a security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidentally. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user.

Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

Authentication

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.

Authentication service has two variants –

- **Message authentication** identifies the originator of the message without any regard router or system that has sent the message.
- **Entity authentication** is assurance that data has been received from a specific entity, say a particular website.

Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

Non-repudiation

It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party.

Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

Where to Encrypt & Decrypt?

- **Data-in-Transit / Data-in motion:** Transport / Network
 - Not much protection as it travels
 - Many different switches, routers, devices
 - Network-based protection:
 - Firewall, IPS
 - Provide transport encryption:
 - TLS, IPsec
- **Data-at-Rest:** Resides in storage
 - Hard drive, SSD, flash drive, etc
 - Encrypt the data
 - Whole disk encryption
 - Database encryption
 - File or/ folder-level encryption

- Apply permissions
 - Access control lists
 - Only authorized users can access the data
- **Data-in-use / Data-in-process:** RAM & CPU
 - The data is in memory or CPU registers and cache
 - The data is almost always decrypted

Cryptography Primitives

Cryptography primitives are nothing but the tools and techniques in Cryptography that can be selectively used to provide a set of desired security services –

- Encryption
- Hash functions
- Message Authentication codes (MAC)
- Digital Signatures

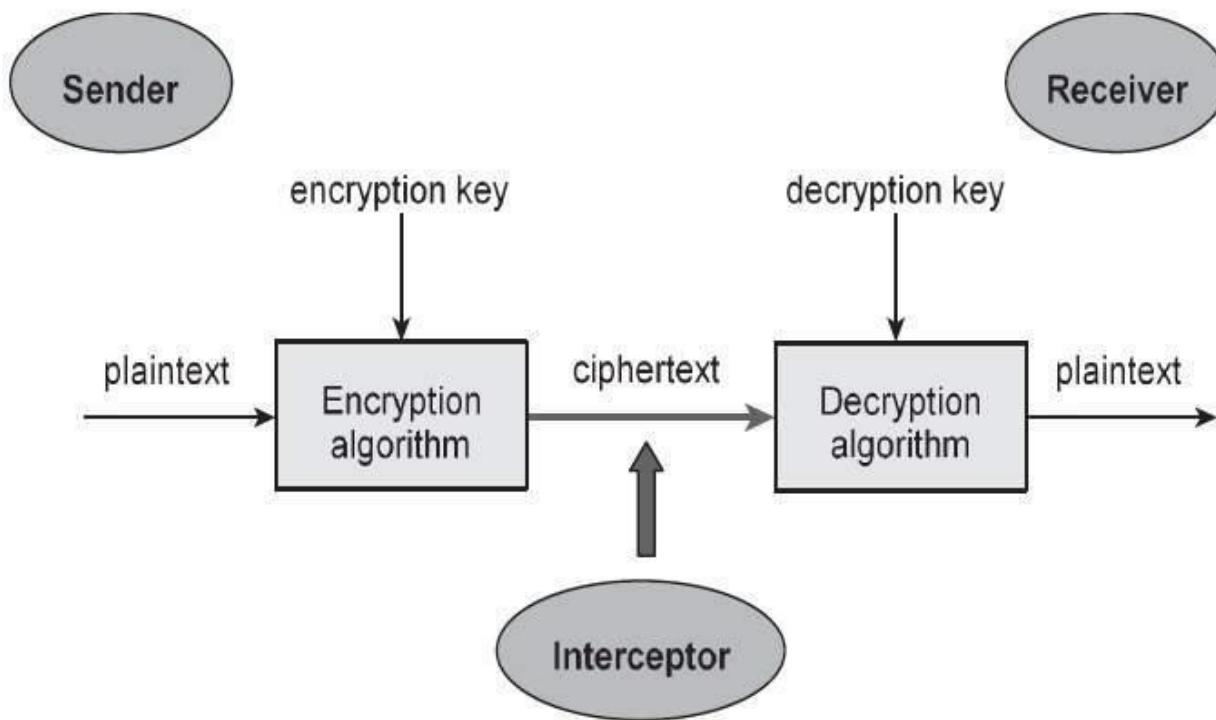
The following table shows the primitives that can achieve a particular security service on their own.

Primitives → Service	Encryption	Hash Function	MAC	Digital Signature
Confidentiality	Yes	No	No	No
Integrity	No	Sometimes	Yes	Yes
Authentication	No	No	Yes	Yes
Non Repudiation	No	No	Sometimes	Yes

Note – Cryptographic primitives are intricately related and they are often combined to achieve a set of desired security services from a cryptosystem.

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a **cipher system**.

Let us discuss a simple model of a cryptosystem that provides confidentiality to the information being transmitted. This basic model is depicted in the illustration below –



The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data.

The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

Encryption Algorithms

- **Algorithm** - step-by-step method of solving a problem
- **Two General Forms of Cryptography**
 - **Substitution** - bits are replaced by other bits
 - **Transposition** - doesn't replace; simply changes order
- **Encryption Algorithms** - mathematical formulas used to encrypt and decrypt data
- **Stream Cipher** - readable bits are encrypted one at a time in a continuous stream
 - Usually done by an XOR operation
 - Work at a high rate of speed
- **Block Cipher** - data bits are split up into blocks and fed into the cipher
 - Each block of data (usually 64 bits) encrypted with key and algorithm
 - Are simpler and slower than stream ciphers
- **XOR** - exclusive or; if inputs are the same (0,0 or 1,1), function returns 0; if inputs are not the same (0,1 or 1,0), function returns 1
- Key chosen for cipher must have a length larger than the data; if not, it is vulnerable to frequency attacks

Components of a Cryptosystem

The various components of a basic cryptosystem are as follows –

- **Plaintext.** It is the data to be protected during transmission.
- **Encryption Algorithm.** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
- **Ciphertext.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
- **Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- **Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a **key space**.

An **interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. He, however, must never know the decryption key.

Types of Cryptosystems

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system –

- Symmetric Key Encryption
- Asymmetric Key Encryption

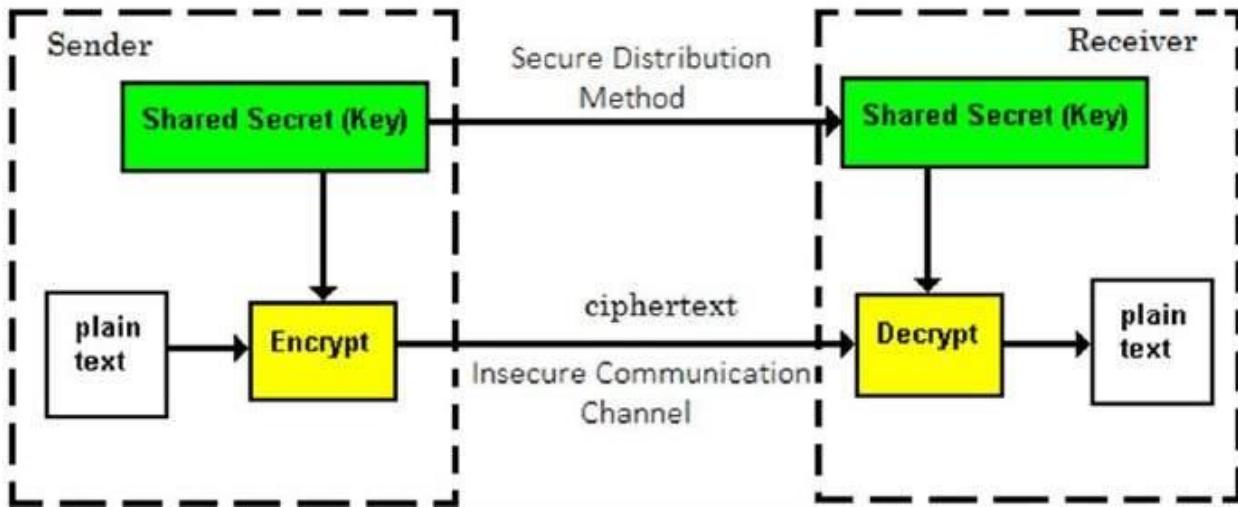
The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key.

Symmetric Key Encryption

The encryption process where **same keys are used for encrypting and decrypting** the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as **symmetric cryptography**. Symmetric cryptosystems are also sometimes referred to as **secret key cryptosystems**.

A few well-known examples of symmetric key encryption methods are – Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.



Prior to 1970, all cryptosystems employed symmetric key encryption. Even today, its relevance is very high and it is being used extensively in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain advantages over asymmetric key encryption.

The salient features of cryptosystem based on symmetric key encryption are –

- Persons using symmetric key encryption must share a common key prior to exchange of information.
- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of n people, to enable two-party communication between any two persons, the number of keys required for group is $n \times (n - 1)/2$.
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

Challenge of Symmetric Key Cryptosystem

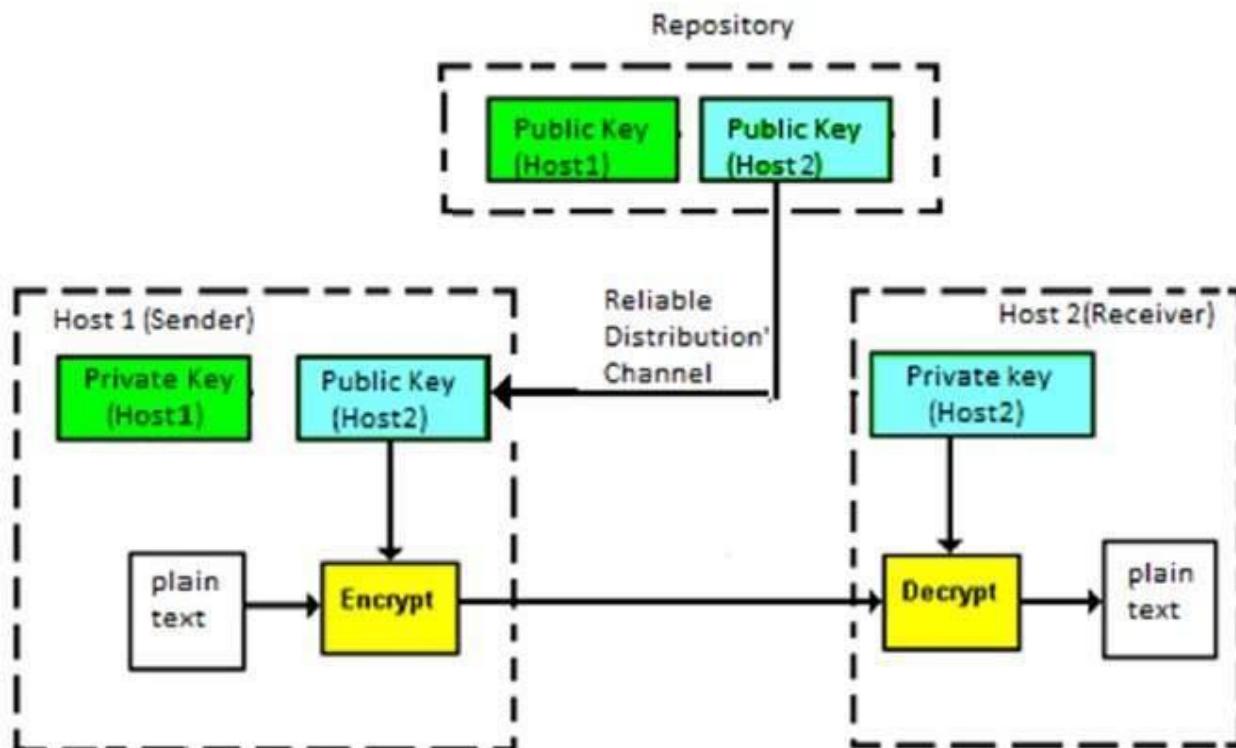
There are two restrictive challenges of employing symmetric key cryptography.

- **Key establishment** – Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.
- **Trust Issue** – Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver ‘trust’ each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

Asymmetric Key Encryption

The encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible. The process is depicted in the following illustration –



Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons. The salient features of this encryption scheme are as follows –

- Every user in this system needs to have a pair of dissimilar keys, **private key** and **public key**. These keys are mathematically related – when one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.
- It requires to put the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called **Public Key Encryption**.
- Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.

- When *Host1* needs to send data to *Host2*, he obtains the public key of *Host2* from repository, encrypts the data, and transmits.
- *Host2* uses his private key to extract the plaintext.
- Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.
- Processing power of computer system required to run asymmetric algorithm is higher.

Symmetric cryptosystems are a natural concept. In contrast, public-key cryptosystems are quite difficult to comprehend.

You may think, *how can the encryption key and the decryption key are ‘related’, and yet it is impossible to determine the decryption key from the encryption key?* The answer lies in the mathematical concepts. It is possible to design a cryptosystem whose keys have this property. The concept of public-key cryptography is relatively new. There are fewer public-key algorithms known than symmetric algorithms.

Challenge of Public Key Cryptosystem

Public-key cryptosystems have one significant challenge – the user needs to trust that the public key that he is using in communications with a person really is the public key of that person and has not been spoofed by a malicious third party.

This is usually accomplished through a Public Key Infrastructure (PKI) consisting a trusted third party. The third party securely manages and attests to the authenticity of public keys. When the third party is requested to provide the public key for any communicating person X, they are trusted to provide the correct public key.

The third party satisfies itself about user identity by the process of attestation, notarization, or some other process – that X is the one and only, or globally unique, X. The most common method of making the verified public keys available is to embed them in a certificate which is digitally signed by the trusted third party.

Relation between Encryption Schemes

A summary of basic key properties of two types of cryptosystems is given below –

	Symmetric Cryptosystems	Public Key Cryptosystems
Relation between Keys	Same	Different, but mathematically related
Encryption Key	Symmetric	Public
Decryption Key	Symmetric	Private

Due to the advantages and disadvantage of both the systems, symmetric key and public-key cryptosystems are often used together in the practical information security systems.

Kerckhoff's Principle for Cryptosystem

In the 19th century, a Dutch cryptographer A. Kerckhoff furnished the requirements of a good cryptosystem. Kerckhoff stated that a cryptographic system should be secure even if everything about the system, except the key, is public knowledge. The six design principles defined by Kerckhoff for cryptosystem are –

- The cryptosystem should be unbreakable practically, if not mathematically.
- Falling of the cryptosystem in the hands of an intruder should not lead to any compromise of the system, preventing any inconvenience to the user.
- The key should be easily communicable, memorable, and changeable.
- The ciphertext should be transmissible by telegraph, an unsecure channel.
- The encryption apparatus and documents should be portable and operable by a single person.
- Finally, it is necessary that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

The second rule is currently known as **Kerckhoff principle**. It is applied in virtually all the contemporary encryption algorithms such as DES, AES, etc. These public algorithms are considered to be thoroughly secure. The security of the encrypted message depends solely on the security of the secret encryption key.

Keeping the algorithms secret may act as a significant barrier to cryptanalysis. However, keeping the algorithms secret is possible only when they are used in a strictly limited circle.

In modern era, cryptography needs to cater to users who are connected to the Internet. In such cases, using a secret algorithm is not feasible, hence Kerckhoff principles became essential guidelines for designing algorithms in modern cryptography.

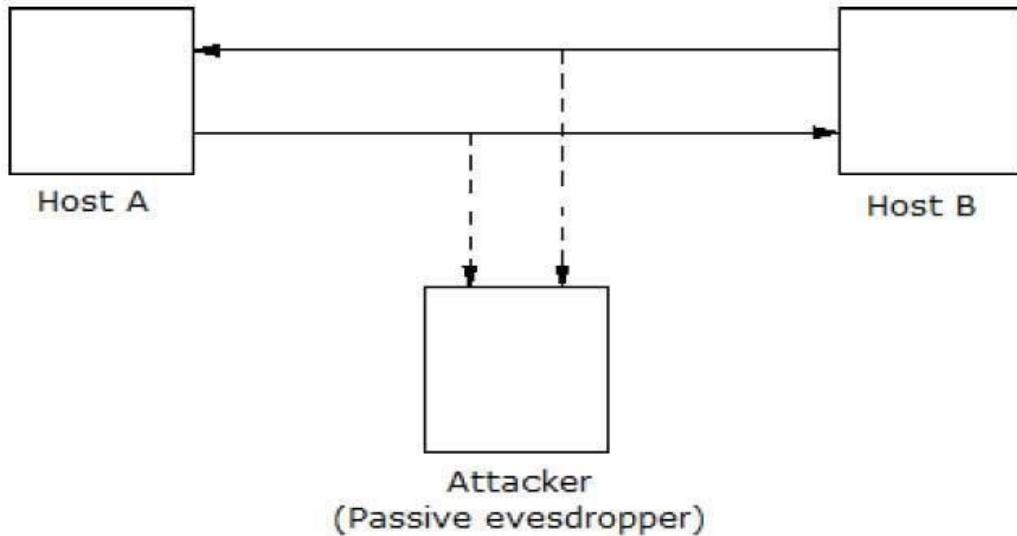
In the present era, not only business but almost all the aspects of human life are driven by information. Hence, it has become imperative to protect useful information from malicious activities such as attacks. Let us consider the types of attacks to which information is typically subjected to.

Attacks are typically categorized based on the action performed by the attacker. An attack, thus, can be **passive** or **active**.

Passive Attacks

The main goal of a passive attack is to obtain **unauthorized access to the information**. For example, actions such as intercepting and eavesdropping on the communication channel can be regarded as passive attack.

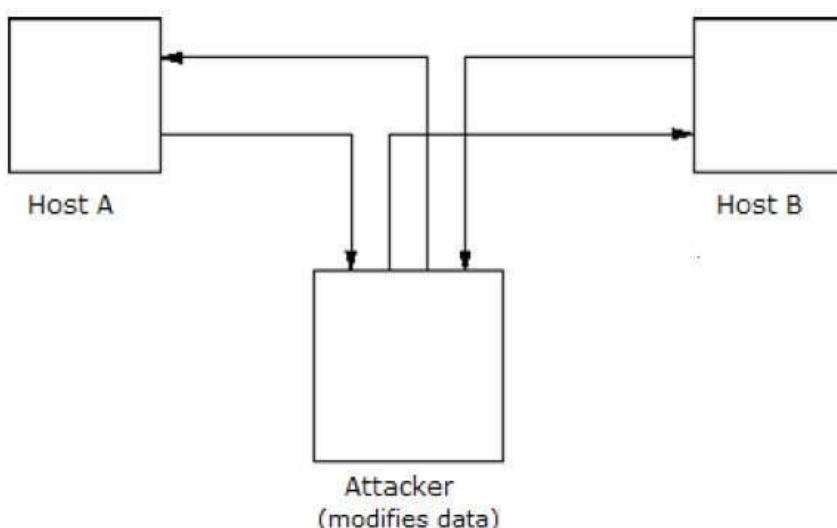
These actions are passive in nature, as they neither affect information nor disrupt the communication channel. A passive attack is often seen as *stealing* information. The only difference in stealing physical goods and stealing information is that theft of data still leaves the owner in possession of that data. Passive information attack is thus more dangerous than stealing of goods, as information theft may go unnoticed by the owner.



Active Attacks

An active attack involves changing the information in some way by conducting some process on the information. For example,

- Modifying the information in an unauthorized manner.
- Initiating unintended or unauthorized transmission of information.
- Alteration of authentication data such as originator name or timestamp associated with information
- Unauthorized deletion of data.
- Denial of access to information for legitimate users (denial of service).



Cryptography provides many tools and techniques for implementing cryptosystems capable of preventing most of the attacks described above.

Assumptions of Attacker

Let us see the prevailing environment around cryptosystems followed by the types of attacks employed to break these systems –

Environment around Cryptosystem

While considering possible attacks on the cryptosystem, it is necessary to know the cryptosystems environment. The attacker's assumptions and knowledge about the environment decides his capabilities.

In cryptography, the following three assumptions are made about the security environment and attacker's capabilities.

Details of the Encryption Scheme

The design of a cryptosystem is based on the following two cryptography algorithms –

- **Public Algorithms** – With this option, all the details of the algorithm are in the public domain, known to everyone.
- **Proprietary algorithms** – The details of the algorithm are only known by the system designers and users.

In case of proprietary algorithms, security is ensured through obscurity. Private algorithms may not be the strongest algorithms as they are developed in-house and may not be extensively investigated for weakness.

Secondly, they allow communication among closed group only. Hence they are not suitable for modern communication where people communicate with large number of known or unknown entities. Also, according to Kerckhoff's principle, the algorithm is preferred to be public with strength of encryption lying in the *key*.

Thus, the first assumption about security environment is that the **encryption algorithm is known to the attacker**.

Availability of Ciphertext

We know that once the plaintext is encrypted into ciphertext, it is put on unsecure public channel (say email) for transmission. Thus, the attacker can obviously assume that it has **access to the ciphertext generated by the cryptosystem**.

Availability of Plaintext and Ciphertext

This assumption is not as obvious as other. However, there may be situations where an attacker can have **access to plaintext and corresponding ciphertext**. Some such possible circumstances are –

- The attacker influences the sender to convert plaintext of his choice and obtains the ciphertext.

- The receiver may divulge the plaintext to the attacker inadvertently. The attacker has access to corresponding ciphertext gathered from open channel.
- In a public-key cryptosystem, the encryption key is in open domain and is known to any potential attacker. Using this key, he can generate pairs of corresponding plaintexts and ciphertexts.

Cryptographic Attacks

The basic intention of an attacker is to break a cryptosystem and to find the plaintext from the ciphertext. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain.

Hence, he applies maximum effort towards finding out the secret key used in the cryptosystem. Once the attacker is able to determine the key, the attacked system is considered as *broken* or *compromised*.

Based on the methodology used, attacks on cryptosystems are categorized as follows –

- **Ciphertext Only Attacks (COA)** – In this method, the attacker has access to a set of ciphertext(s). He does not have access to corresponding plaintext. COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext. Occasionally, the encryption key can be determined from this attack. Modern cryptosystems are guarded against ciphertext-only attacks.
- **Known Plaintext Attack (KPA)** – In this method, the attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext using this information. This may be done by determining the key or via some other method. The best example of this attack is *linear cryptanalysis* against block ciphers.
- **Chosen Plaintext Attack (CPA)** – In this method, the attacker has the text of his choice encrypted. So he has the ciphertext-plaintext pair of his choice. This simplifies his task of determining the encryption key. An example of this attack is *differential cryptanalysis* applied against block ciphers as well as hash functions. A popular public key cryptosystem, RSA is also vulnerable to chosen-plaintext attacks.
- **Dictionary Attack** – This attack has many variants, all of which involve compiling a ‘dictionary’. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.
- **Brute Force Attack (BFA)** – In this method, the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible keys is $2^8 = 256$. The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long.
- **Birthday Attack** – This attack is a variant of brute-force technique. It is used against the cryptographic hash function. When students in a class are asked about their birthdays, the answer is one of the possible 365 dates. Let us assume the first student's birthdate is 3rd Aug. Then to find the next student whose birthdate is 3rd Aug, we need to enquire $1.25^* \sqrt{365} \approx 25$ students.

Similarly, if the hash function produces 64 bit hash values, the possible hash values are 1.8×10^{19} . By repeatedly evaluating the function for different inputs, the same output is expected to be obtained after about 5.1×10^9 random inputs.

If the attacker is able to find two different inputs that give the same hash value, it is a **collision** and that hash function is said to be broken.

- **Man in Middle Attack (MIM)** – The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.
 - Host A wants to communicate to host B , hence requests public key of B .
 - An attacker intercepts this request and sends his public key instead.
 - Thus, whatever host A sends to host B , the attacker is able to read.
 - In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to B .
 - The attacker sends his public key as A 's public key so that B takes it as if it is taking it from A .
- **Side Channel Attack (SCA)** – This type of attack is not against any particular type of cryptosystem or algorithm. Instead, it is launched to exploit the weakness in physical implementation of the cryptosystem.
- **Timing Attacks** – They exploit the fact that different computations take different times to compute on processor. By measuring such timings, it is possible to know about a particular computation the processor is carrying out. For example, if the encryption takes a longer time, it indicates that the secret key is long.
- **Power Analysis Attacks** – These attacks are similar to timing attacks except that the amount of power consumption is used to obtain information about the nature of the underlying computations.
- **Fault analysis Attacks** – In these attacks, errors are induced in the cryptosystem and the attacker studies the resulting output for useful information.

Practicality of Attacks

The attacks on cryptosystems described here are highly academic, as majority of them come from the academic community. In fact, many academic attacks involve quite unrealistic assumptions about environment as well as the capabilities of the attacker. For example, in chosen-ciphertext attack, the attacker requires an impractical number of deliberately chosen plaintext-ciphertext pairs. It may not be practical altogether.

Nonetheless, the fact that any attack exists should be a cause of concern, particularly if the attack technique has the potential for improvement.

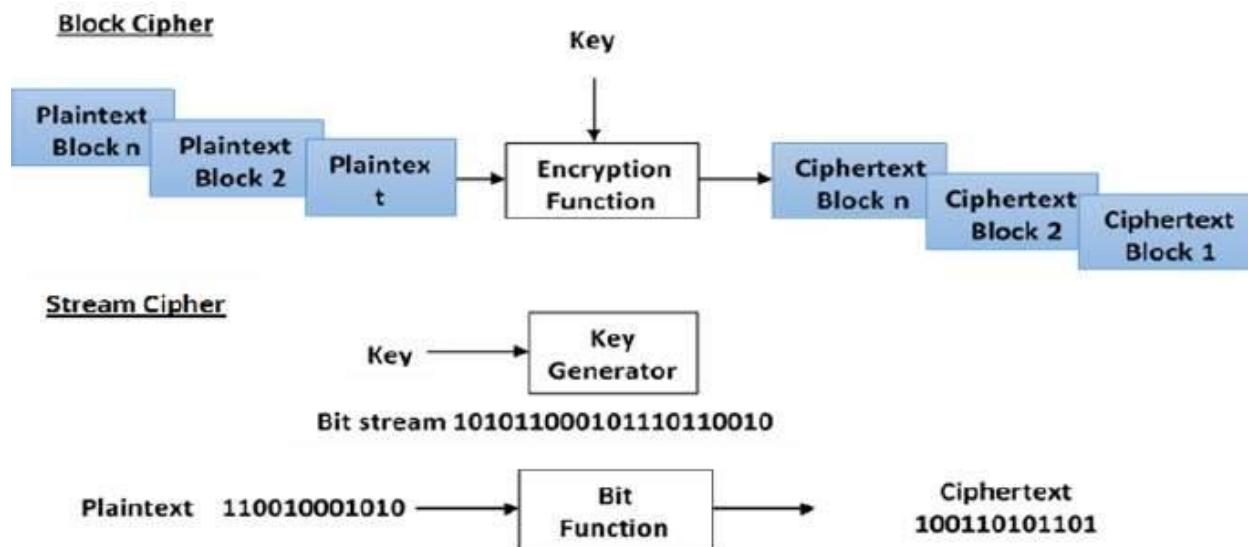
Digital data is represented in strings of binary digits (bits) unlike alphabets. Modern cryptosystems need to process these binary strings to convert them into another binary string. Based on how these binary strings are processed, a symmetric encryption schemes can be classified into –

Block Ciphers

In this scheme, the plain binary text is processed in blocks (groups) of bits at a time; i.e. a block of plaintext bits is selected, a series of operations is performed on this block to generate a block of ciphertext bits. The number of bits in a block is fixed. For example, the schemes DES and AES have block sizes of 64 and 128, respectively.

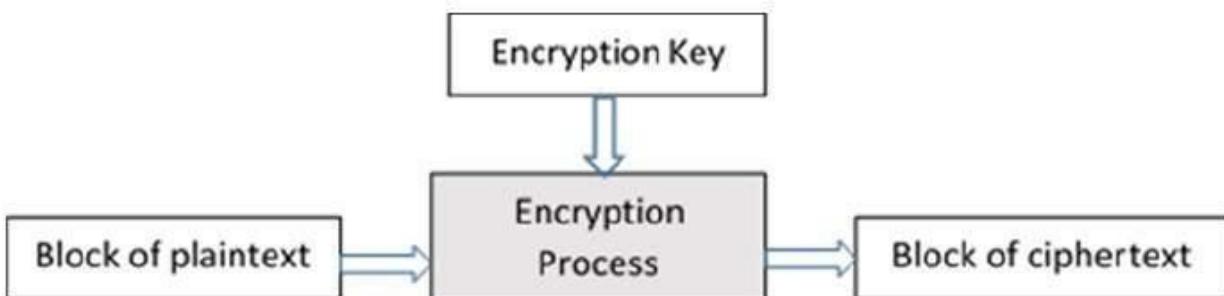
Stream Ciphers

In this scheme, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of ciphertext. Technically, stream ciphers are block ciphers with a block size of one bit.



Block cipher

The basic scheme of a block cipher is depicted as follows –



A block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size. The size of block is fixed in the given scheme. The choice of block size does not directly affect to the strength of encryption scheme. The strength of cipher depends up on the key length.

Block Size

Though any size of block is acceptable, following aspects are borne in mind while selecting a size of a block.

- **Avoid very small block size** – Say a block size is m bits. Then the possible plaintext bits combinations are then 2^m . If the attacker discovers the plain text blocks corresponding to some previously sent ciphertext blocks, then the attacker can launch a type of ‘dictionary attack’ by building up a dictionary of plaintext/ciphertext pairs sent using that encryption key. A larger block size makes attack harder as the dictionary needs to be larger.
- **Do not have very large block size** – With very large block size, the cipher becomes inefficient to operate. Such plaintexts will need to be padded before being encrypted.
- **Multiples of 8 bit** – A preferred block size is a multiple of 8 as it is easy for implementation as most computer processor handle data in multiple of 8 bits.

Padding in Block Cipher

Block ciphers process blocks of fixed sizes (say 64 bits). The length of plaintexts is mostly not a multiple of the block size. For example, a 150-bit plaintext provides two blocks of 64 bits each with third block of balance 22 bits. The last block of bits needs to be padded up with redundant information so that the length of the final block equal to block size of the scheme. In our example, the remaining 22 bits need to have additional 42 redundant bits added to provide a complete block. The process of adding bits to the last block is referred to as **padding**.

Too much padding makes the system inefficient. Also, padding may render the system insecure at times, if the padding is done with same bits always.

Block Cipher Schemes

There is a vast number of block cipher schemes that are in use. Many of them are publicly known. Most popular and prominent block ciphers are listed below.

- **Digital Encryption Standard (DES)** – The popular block cipher of the 1990s. It is now considered as a ‘broken’ block cipher, due primarily to its small key size.
- **Triple DES** – It is a variant scheme based on repeated DES applications. It is still a respected block cipher but inefficient compared to the new faster block ciphers available.
- **Advanced Encryption Standard (AES)** – It is a relatively new block cipher based on the encryption algorithm **Rijndael** that won the AES design competition.
- **IDEA** – It is a sufficiently strong block cipher with a block size of 64 and a key size of 128 bits. A number of applications use IDEA encryption, including early versions of Pretty Good Privacy (PGP) protocol. The use of IDEA scheme has a restricted adoption due to patent issues.

- **Twofish** – This scheme of block cipher uses block size of 128 bits and a key of variable length. It was one of the AES finalists. It is based on the earlier block cipher Blowfish with a block size of 64 bits.
- **Serpent** – A block cipher with a block size of 128 bits and key lengths of 128, 192, or 256 bits, which was also an AES competition finalist. It is a slower but has more secure design than other block cipher.

In the next sections, we will first discuss the model of block cipher followed by DES and AES, two of the most influential modern block ciphers.

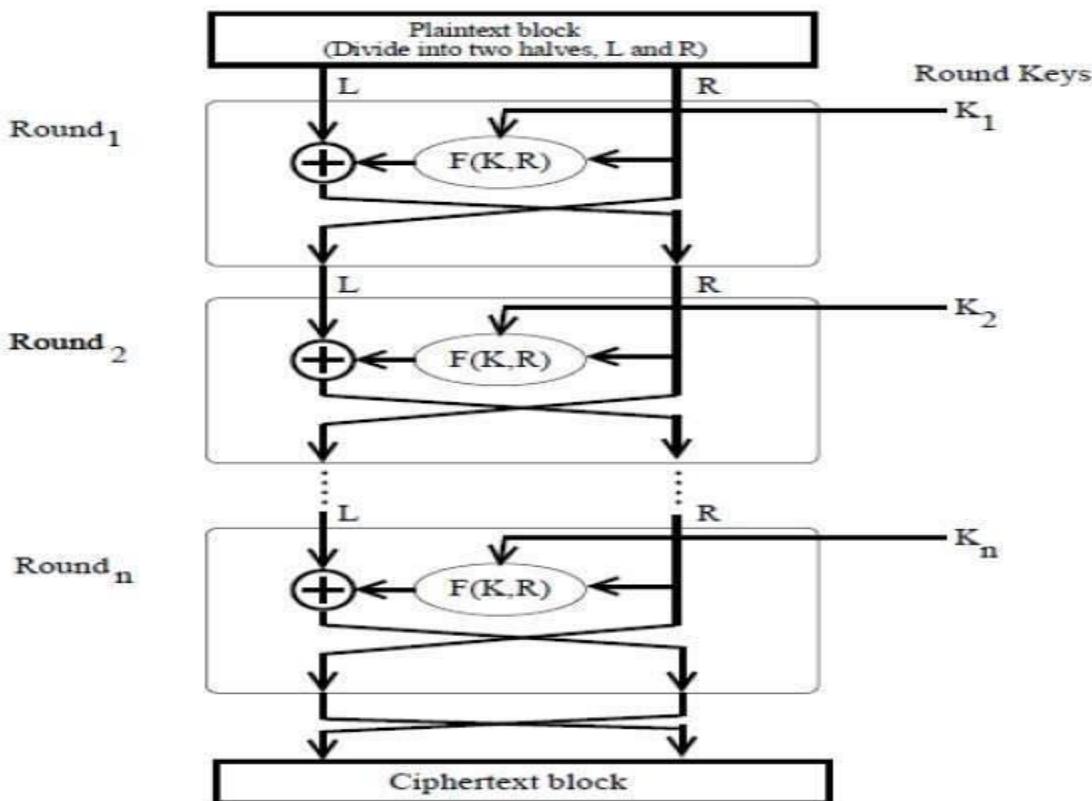
Feistel Cipher

Is not a specific scheme of block cipher. It is a design model from which many different block ciphers are derived. DES is just one example of a Feistel Cipher. A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.

Encryption Process

The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a “substitution” step followed by a permutation step.

Feistel Structure is shown in the following illustration –



- The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
- In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function ‘f’ that takes two input – the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.
- In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.
- The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
- Above substitution and permutation steps form a ‘round’. The number of rounds are specified by the algorithm design.
- Once the last round is completed then the two sub blocks, ‘R’ and ‘L’ are concatenated in this order to form the ciphertext block.

The difficult part of designing a Feistel Cipher is selection of round function ‘f’. In order to be unbreakable scheme, this function needs to have several important properties that are beyond the scope of our discussion.

Decryption Process

The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext block is fed into the start of the Feistel structure and then the process thereafter is exactly the same as described in the given illustration.

The process is said to be almost similar and not exactly same. In the case of decryption, the only difference is that the subkeys used in encryption are used in the reverse order.

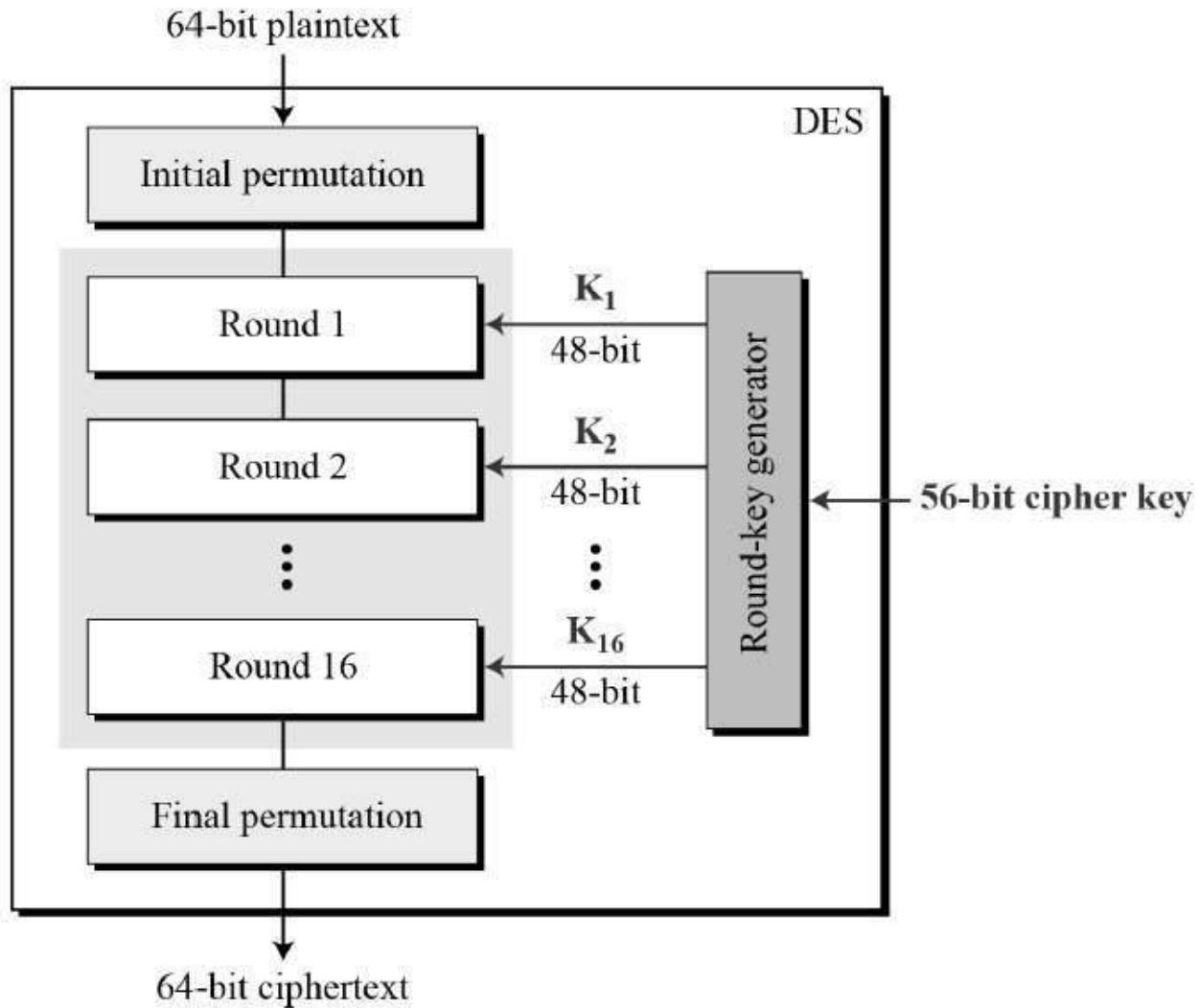
The final swapping of ‘L’ and ‘R’ in last step of the Feistel Cipher is essential. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.

Number of Rounds

The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes. Number of rounds in the systems thus depend upon efficiency–security tradeoff.

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration –

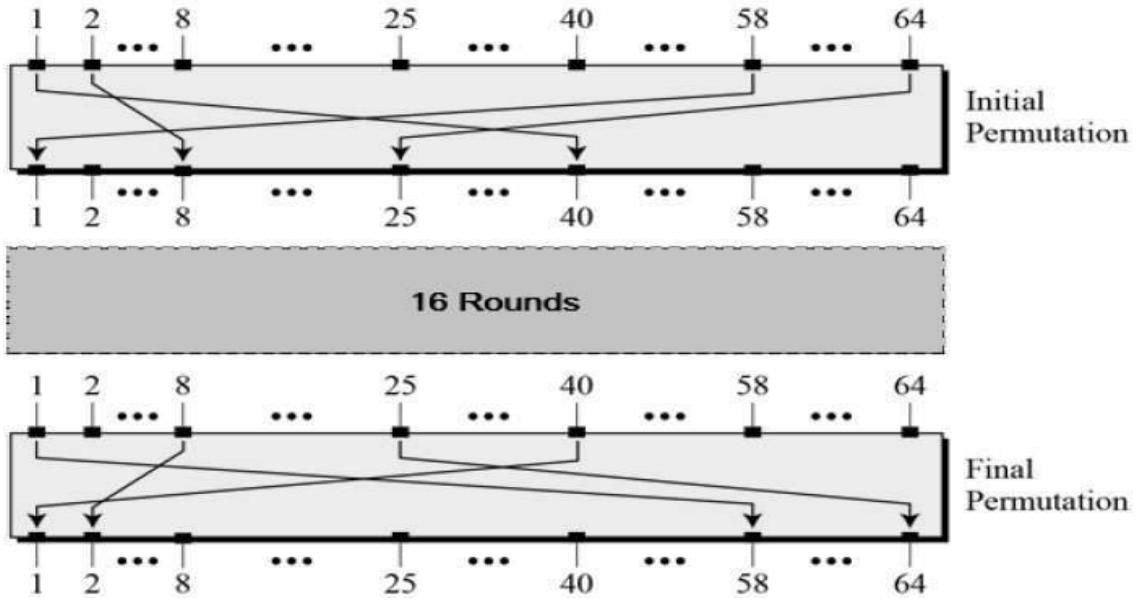


Since DES is based on the Feistel Cipher, all that is required to specify DES is –

- Round function
- Key schedule
- Any additional processing – Initial and final permutation

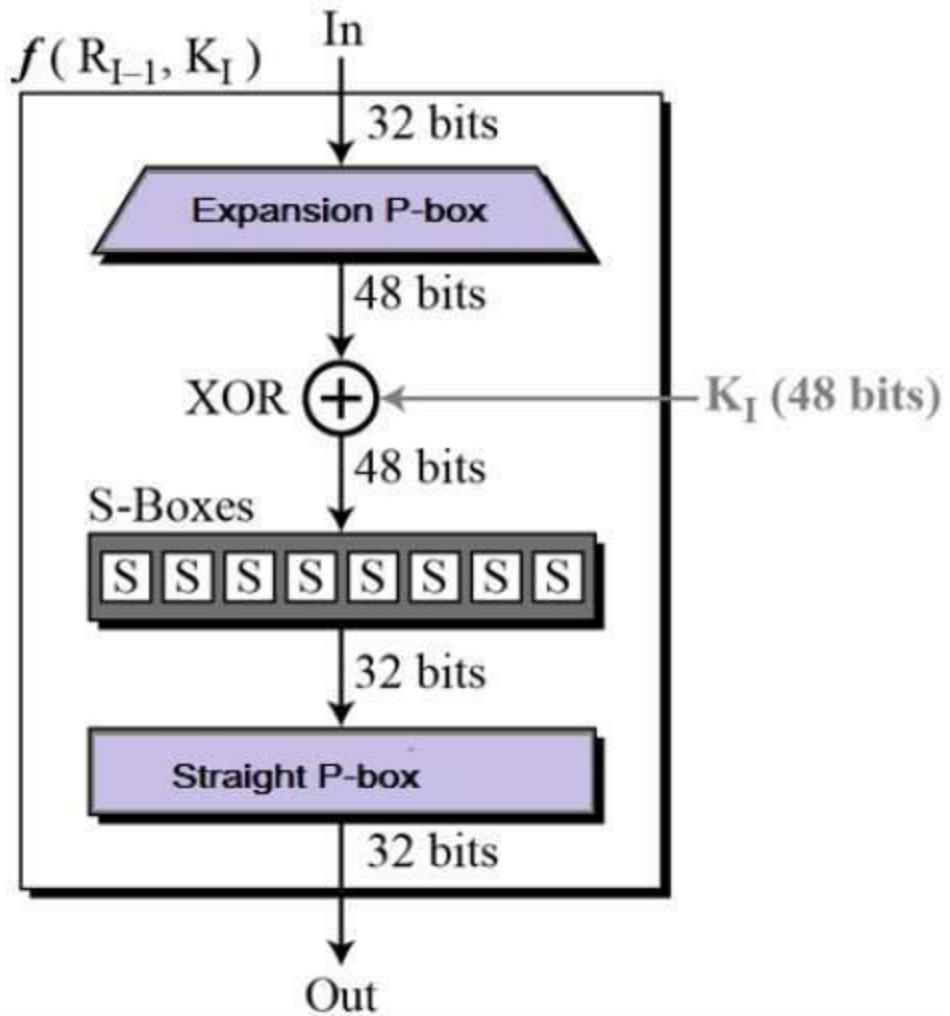
Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows

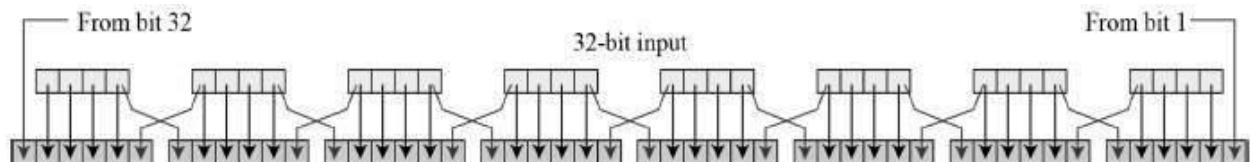


Round Function

The heart of this cipher is the DES function, f . The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



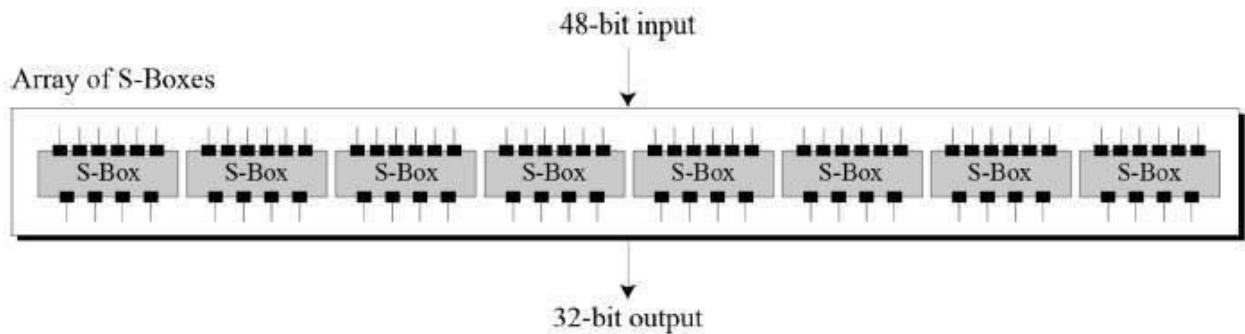
- **Expansion Permutation Box** – Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration –



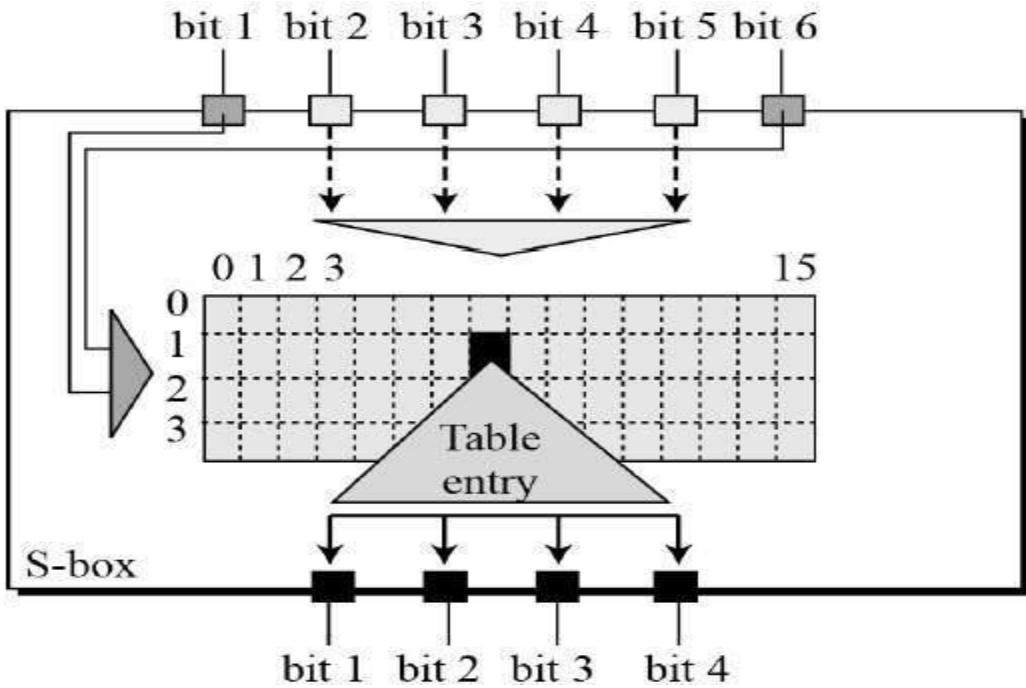
- The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown –

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

- **XOR (Whitener).** – After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.
- **Substitution Boxes.** – The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration –



- The S-box rule is illustrated below –

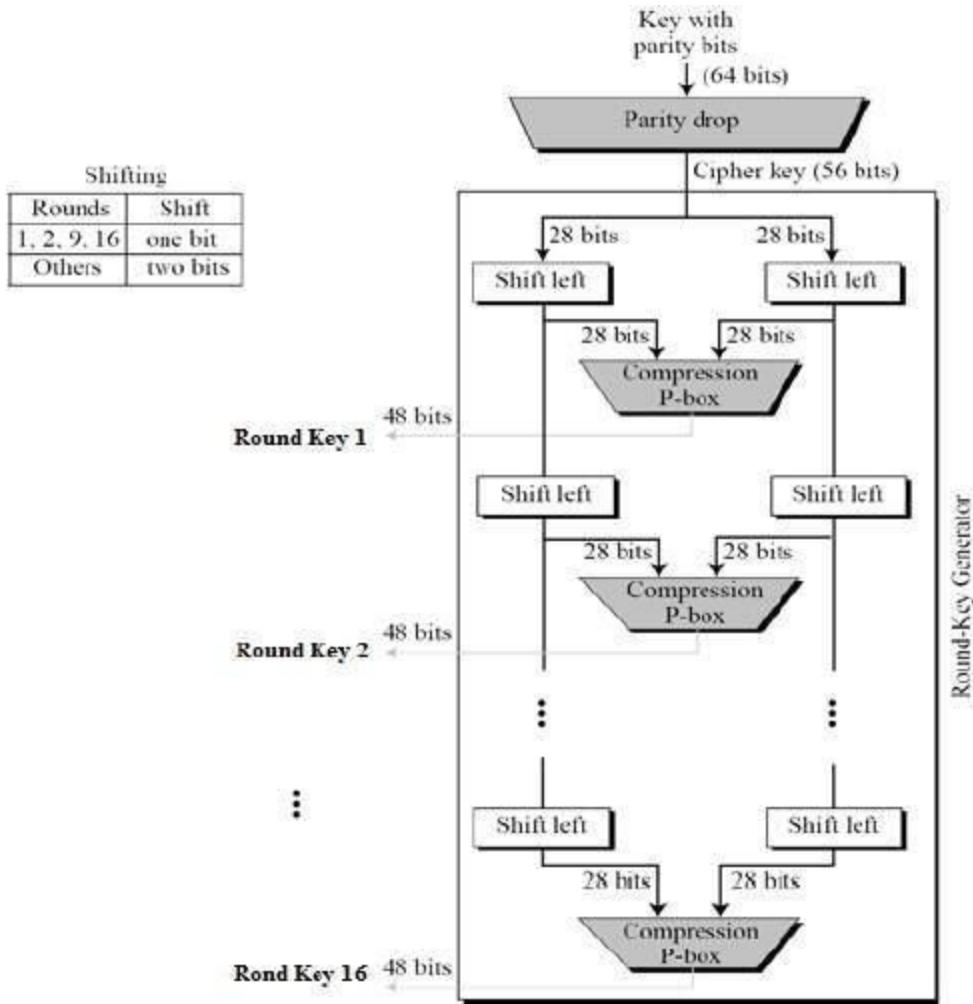


- There are a total of eight S-box tables. The output of all eight s-boxes is then combined into a 32-bit section.
- **Straight Permutation** – The 32-bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration –



The logic for Parity drops, shifting, and Compression P-box is given in the DES description.

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- **Avalanche effect** – A small change in plaintext results in the very great change in the ciphertext.
- **Completeness** – Each bit of ciphertext depends on many bits of plaintext.

During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well-designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

Triple DES

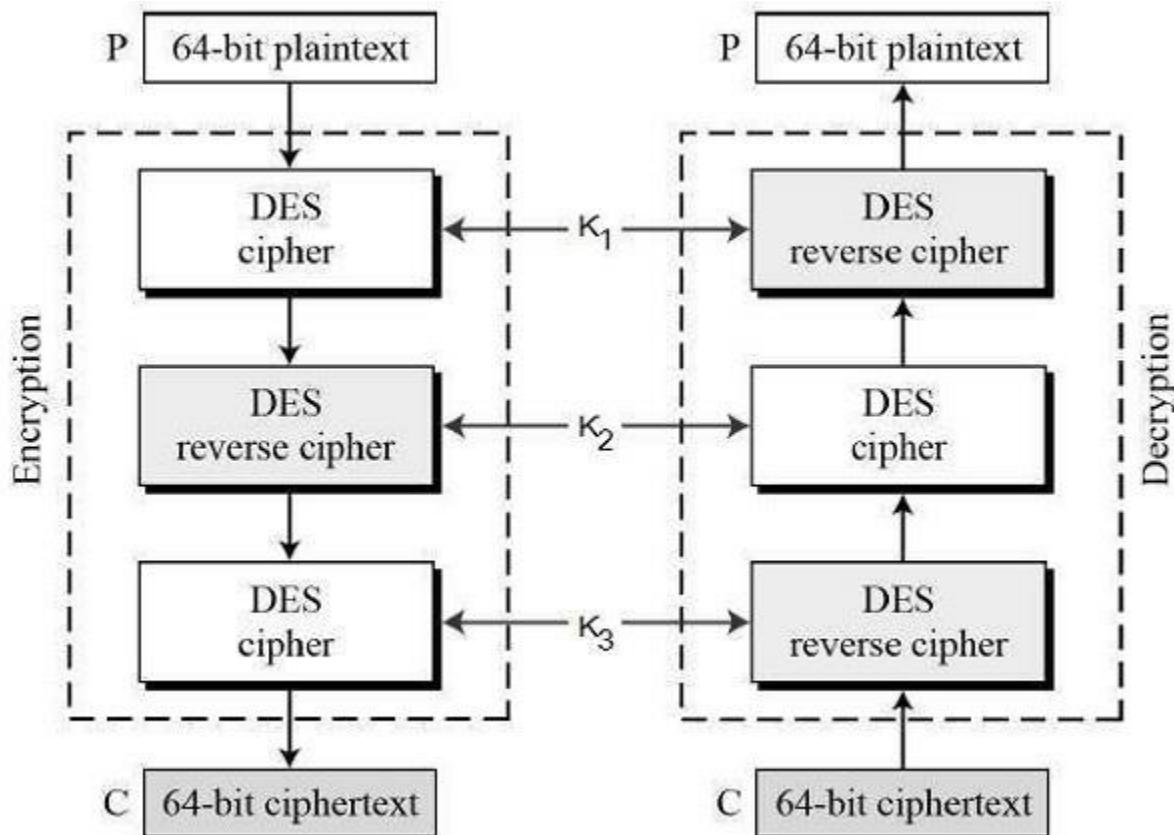
The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES. However, users did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures.

The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES (sometimes known as 3DES).

Incidentally, there are two variants of Triple DES known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES).

3-KEY Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K_1 , K_2 and K_3 . This means that the actual 3TDES key has length $3 \times 56 = 168$ bits. The encryption scheme is illustrated as follows –



The encryption-decryption process is as follows –

- Encrypt the plaintext blocks using single DES with key K_1 .
- Now decrypt the output of step 1 using single DES with key K_2 .
- Finally, encrypt the output of step 2 using single DES with key K_3 .
- The output of step 3 is the ciphertext.

- Decryption of a ciphertext is a reverse process. User first decrypt using K_3 , then encrypt with K_2 , and finally decrypt with K_1 .

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1 , K_2 , and K_3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that K_3 is replaced by K_1 . In other words, user encrypt plaintext blocks with key K_1 , then decrypt with key K_2 , and finally encrypt with K_1 again. Therefore, 2TDES has a key length of 112 bits.

Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

Advanced Encryption Standards (AES)

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

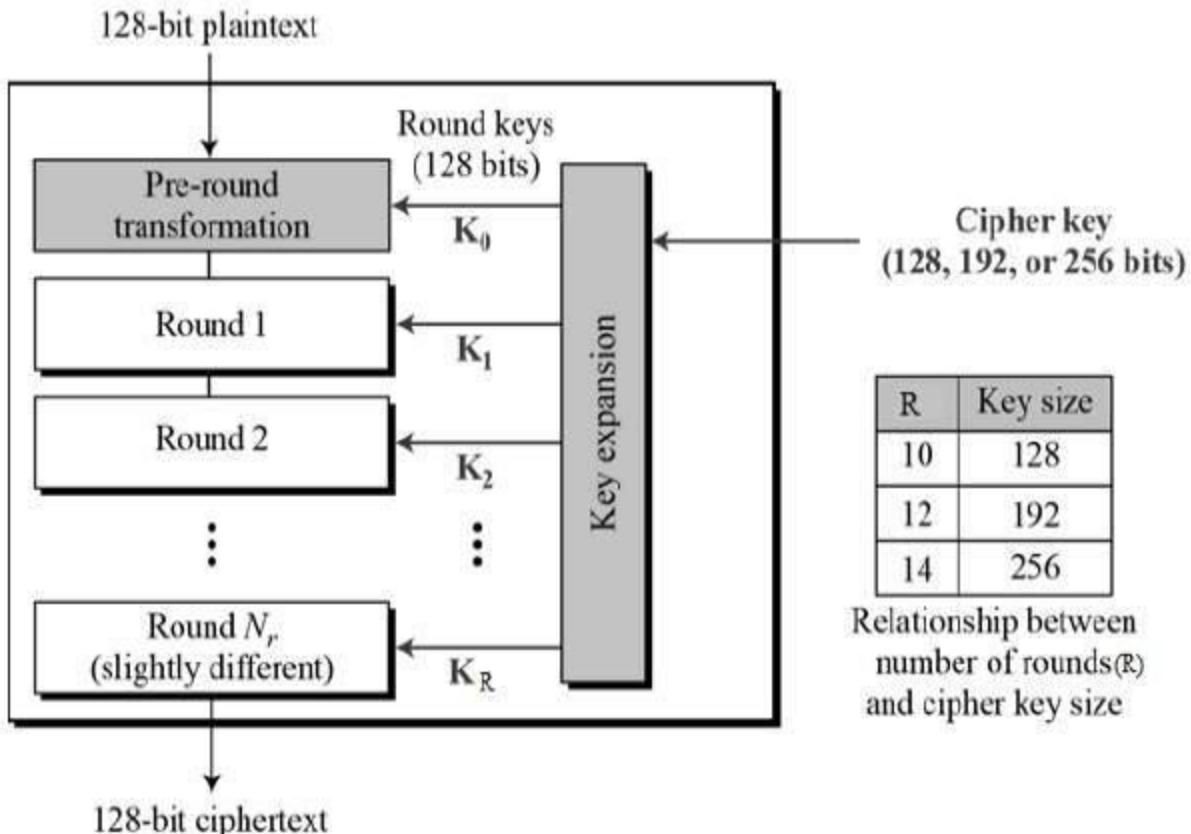
Operation of AES

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix –

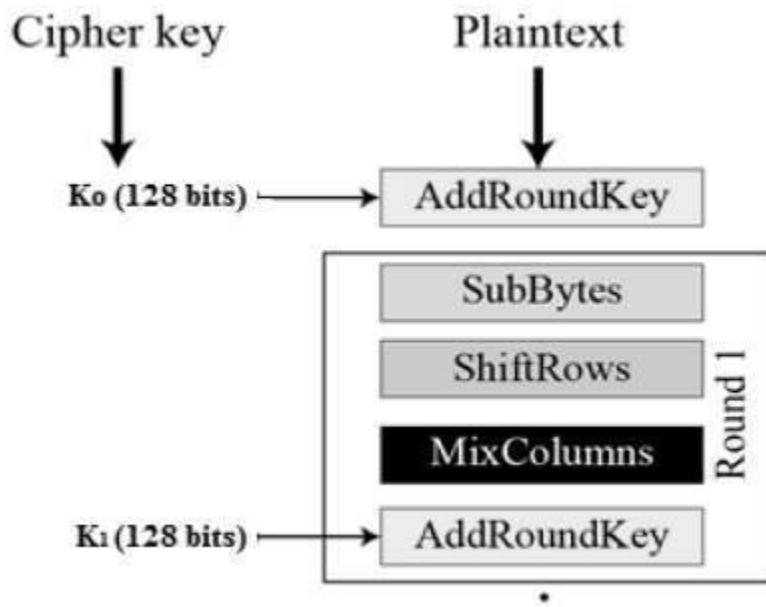
Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration –



Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four subprocesses. The first round process is depicted below –



Byte Substitution (Sub Bytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that ‘fall off’ are re-inserted on the right side of row. Shift is carried out as follows –

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order –

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of ‘future-proofing’ against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

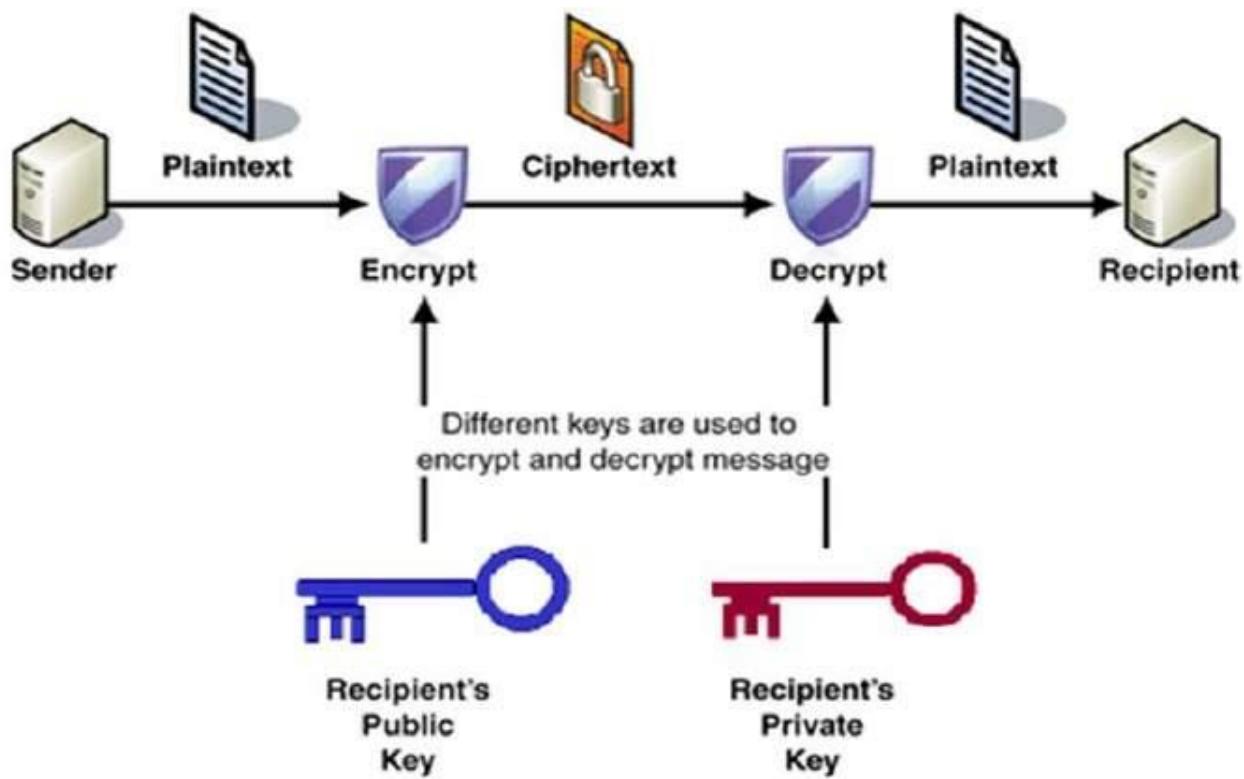
Public Key Cryptography

Unlike symmetric key cryptography, we do not find historical use of public-key cryptography. It is a relatively new concept.

Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.

The process of encryption and decryption is depicted in the following illustration –



The most important properties of public key encryption scheme are –

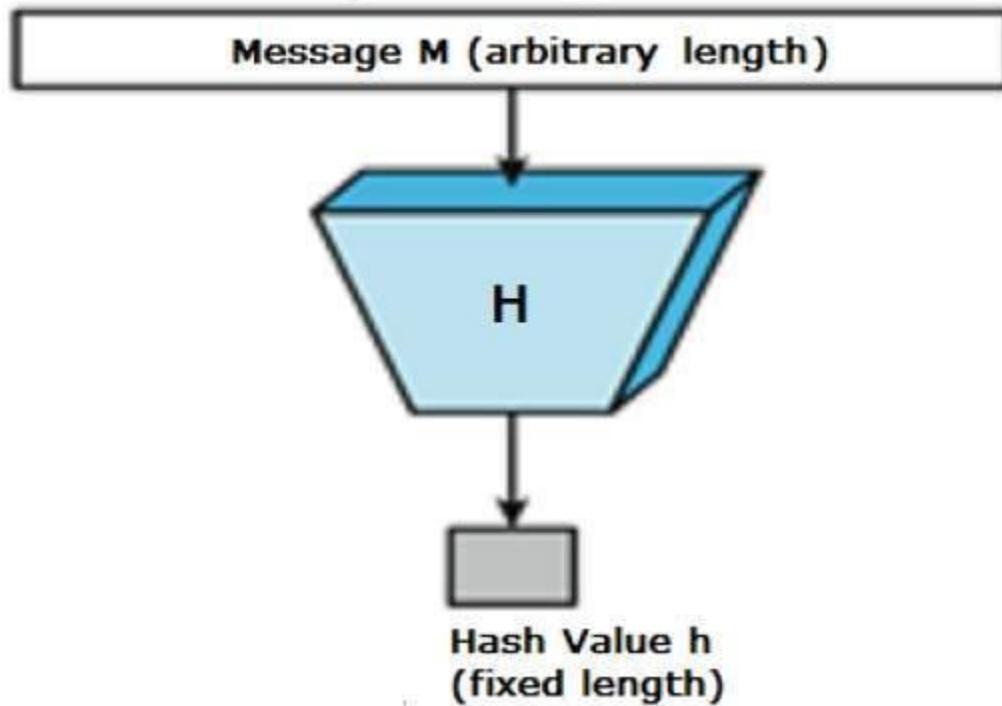
- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.

- Each receiver possesses a unique decryption key, generally referred to as his private key.
- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.
- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.
- Though private and public keys are related mathematically, it is not feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called **message digest** or simply **hash values**. The following picture illustrated hash function –



Features of Hash Functions

The typical features of hash functions are –

- **Fixed Length Output (Hash Value)**

- Hash function converts data of arbitrary length to a fixed length. This process is often referred to as **hashing the data**.
- In general, the hash is much smaller than the input data, hence hash functions are sometimes called **compression functions**.
- Since a hash is a smaller representation of a larger data, it is also referred to as a **digest**.
- Hash function with n bit output is referred to as an **n-bit hash function**. Popular hash functions generate values between 160 and 512 bits.
- **Efficiency of Operation**
 - Generally, for any hash function h with input x, computation of $h(x)$ is a fast operation.
 - Computationally hash functions are much faster than a symmetric encryption.

Properties of Hash Functions

In order to be an effective cryptographic tool, the hash function is desired to possess following properties

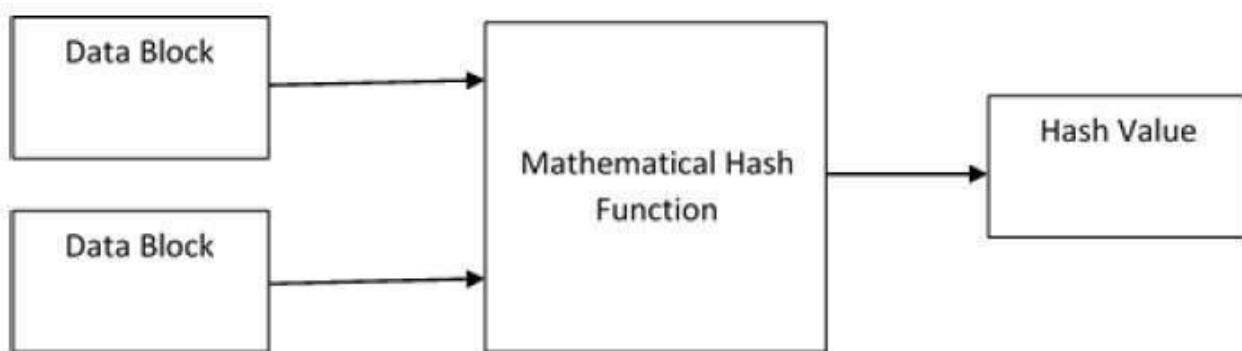
- **Pre-Image Resistance**
 - This property means that it should be computationally hard to reverse a hash function.
 - In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
 - This property protects against an attacker who only has a hash value and is trying to find the input.
- **Second Pre-Image Resistance**
 - This property means given an input and its hash, it should be hard to find a different input with the same hash.
 - In other words, if a hash function h for an input x produces hash value $h(x)$, then it should be difficult to find any other input value y such that $h(y) = h(x)$.
 - This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.
- **Collision Resistance**
 - This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.
 - In other words, for a hash function h, it is hard to find any two different inputs x and y such that $h(x) = h(y)$.

- Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find.
- This property makes it very difficult for an attacker to find two input values with the same hash.
- Also, if a hash function is collision-resistant **then it is second pre-image resistant**.

Design of Hashing Algorithms

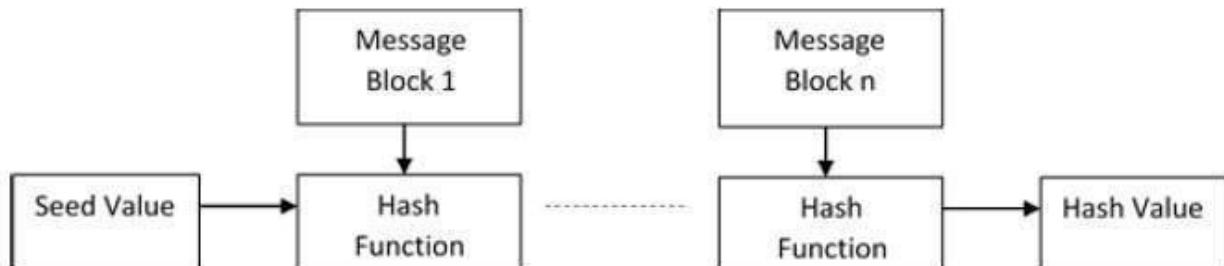
At the heart of a hashing is a mathematical function that operates on two fixed-size blocks of data to create a hash code. This hash function forms the part of the hashing algorithm.

The size of each data block varies depending on the algorithm. Typically the block sizes are from 128 bits to 512 bits. The following illustration demonstrates hash function –



Hashing algorithm involves rounds of above hash function like a block cipher. Each round takes an input of a fixed size, typically a combination of the most recent message block and the output of the last round.

This process is repeated for as many rounds as are required to hash the entire message. Schematic of hashing algorithm is depicted in the following illustration –



Since, the hash value of first message block becomes an input to the second hash operation, output of which alters the result of the third operation, and so on. This effect, known as an **avalanche** effect of hashing.

Avalanche effect results in substantially different hash values for two messages that differ by even a single bit of data.

Understand the difference between hash function and algorithm correctly. The hash function generates a hash code by operating on two blocks of fixed-length binary data.

Hashing algorithm is a process for using the hash function, specifying how the message will be broken up and how the results from previous message blocks are chained together.

Popular Hash Functions

Let us briefly see some popular hash functions –

Message Digest (MD)

MD5 was most popular and widely used hash function for quite some years.

- The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was adopted as Internet Standard RFC 1321. It is a 128-bit hash function.
- MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file. For example, file servers often provide a pre-computed MD5 checksum for the files, so that a user can compare the checksum of the downloaded file to it.
- In 2004, collisions were found in MD5. An analytical attack was reported to be successful only in an hour by using computer cluster. This collision attack resulted in compromised MD5 and hence it is no longer recommended for use.

Secure Hash Function (SHA)

Family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. Though from same family, there are structurally different.

- The original version is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology (NIST) in 1993. It had few weaknesses and did not become very popular. Later in 1995, SHA-1 was designed to correct alleged weaknesses of SHA-0.
- SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security.
- In 2005, a method was found for uncovering collisions for SHA-1 within practical time frame making long-term employability of SHA-1 doubtful.
- SHA-2 family has four further SHA variants, SHA-224, SHA-256, SHA-384, and SHA-512 depending up on number of bits in their hash value. No successful attacks have yet been reported on SHA-2 hash function.
- Though SHA-2 is a strong hash function. Though significantly different, its basic design is still follows design of SHA-1. Hence, NIST called for new competitive hash function designs.
- In October 2012, the NIST chose the Keccak algorithm as the new SHA-3 standard. Keccak offers many benefits, such as efficient performance and good resistance for attacks.

RIPEMD

The RIPEMD is an acronym for RACE Integrity Primitives Evaluation Message Digest. This set of hash functions was designed by open research community and generally known as a family of European hash functions.

- The set includes RIPEMD, RIPEMD-128, and RIPEMD-160. There also exist 256, and 320-bit versions of this algorithm.
- Original RIPEMD (128 bit) is based upon the design principles used in MD4 and found to provide questionable security. RIPEMD 128-bit version came as a quick fix replacement to overcome vulnerabilities on the original RIPEMD.
- RIPEMD-160 is an improved version and the most widely used version in the family. The 256 and 320-bit versions reduce the chance of accidental collision, but do not have higher levels of security as compared to RIPEMD-128 and RIPEMD-160 respectively.

Whirlpool

This is a 512-bit hash function.

- It is derived from the modified version of Advanced Encryption Standard (AES). One of the designer was Vincent Rijmen, a co-creator of the AES.
- Three versions of Whirlpool have been released; namely WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL.

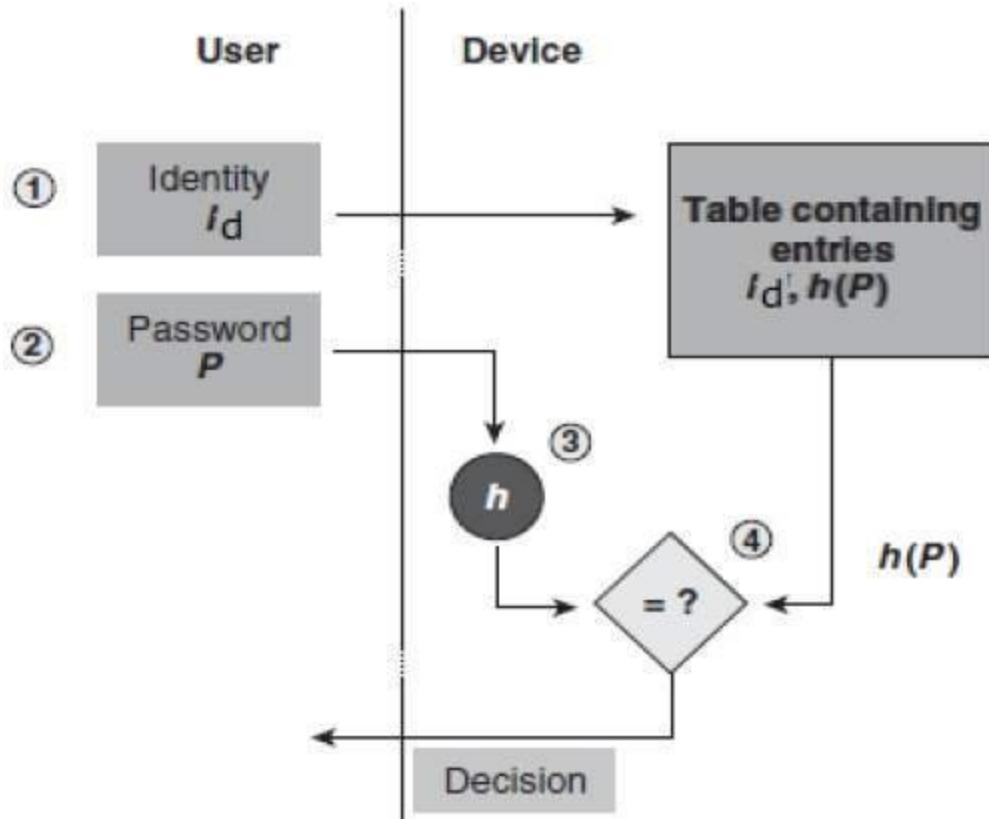
Applications of Hash Functions

There are two direct applications of hash function based on its cryptographic properties.

Password Storage

Hash functions provide protection to password storage.

- Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file.
- The Password file consists of a table of pairs which are in the form (user id, h(P)).
- The process of logon is depicted in the following illustration –

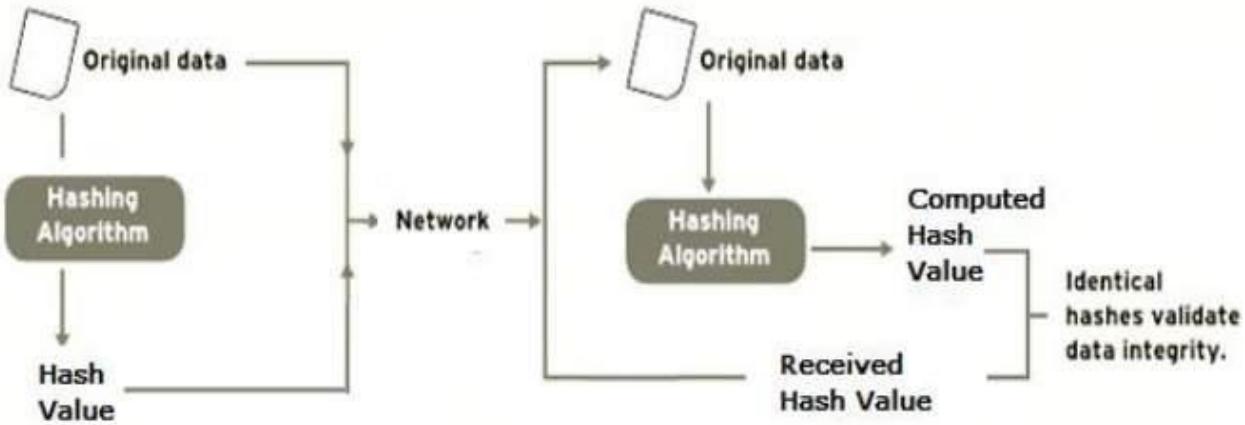


- An intruder can only see the hashes of passwords, even if he accessed the password. He can neither logon using hash nor can he derive the password from hash value since hash function possesses the property of pre-image resistance.

Data Integrity Check

Data integrity check is a most common application of the hash functions. It is used to generate the checksums on data files. This application provides assurance to the user about correctness of the data.

The process is depicted in the following illustration –



The integrity check helps the user to detect any changes made to original file. It however, does not provide any assurance about originality. The attacker, instead of modifying file data, can change the entire file and compute all together new hash and send to the receiver. This integrity check application is useful only if the user is sure about the originality of file

Cryptography – Benefits

Cryptography is an essential information security tool. It provides the four most basic services of information security –

- **Confidentiality** – Encryption technique can guard the information and communication from unauthorized revelation and access of information.
- **Authentication** – The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
- **Data Integrity** – The cryptographic hash functions are playing vital role in assuring the users about the data integrity.
- **Non-repudiation** – The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

All these fundamental services offered by cryptography has enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner.

Cryptography – Drawbacks

Apart from the four fundamental elements of information security, there are other issues that affect the effective use of information –

- A strongly encrypted, authentic, and digitally signed information can be **difficult to access even for a legitimate user** at a crucial time of decision-making. The network or the computer system can be attacked and rendered non-functional by an intruder.
- **High availability**, one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard against the threats such as denial of service or complete breakdown of information system.
- Another fundamental need of information security of **selective access control** also cannot be realized through the use of cryptography. Administrative controls and procedures are required to be exercised for the same.
- Cryptography does not guard against the vulnerabilities and **threats that emerge from the poor design of systems**, protocols, and procedures. These need to be fixed through proper design and setting up of a defensive infrastructure.
- Cryptography comes at cost. The cost is in terms of time and money –
 - Addition of cryptographic techniques in the information processing leads to delay.

- The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome financial budget.
- The security of cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

Future of Cryptography

Elliptic Curve Cryptography (ECC) has already been invented but its advantages and disadvantages are not yet fully understood. ECC allows to perform encryption and decryption in a drastically lesser time, thus allowing a higher amount of data to be passed with equal security. However, as other methods of encryption, ECC must also be tested and proven secure before it is accepted for governmental, commercial, and private use.

Quantum computation is the new phenomenon. While modern computers store data using a binary format called a "bit" in which a "1" or a "0" can be stored; a quantum computer stores data using a quantum superposition of multiple states. These multiple valued states are stored in "quantum bits" or "qubits". This allows the computation of numbers to be several orders of magnitude faster than traditional transistor processors.

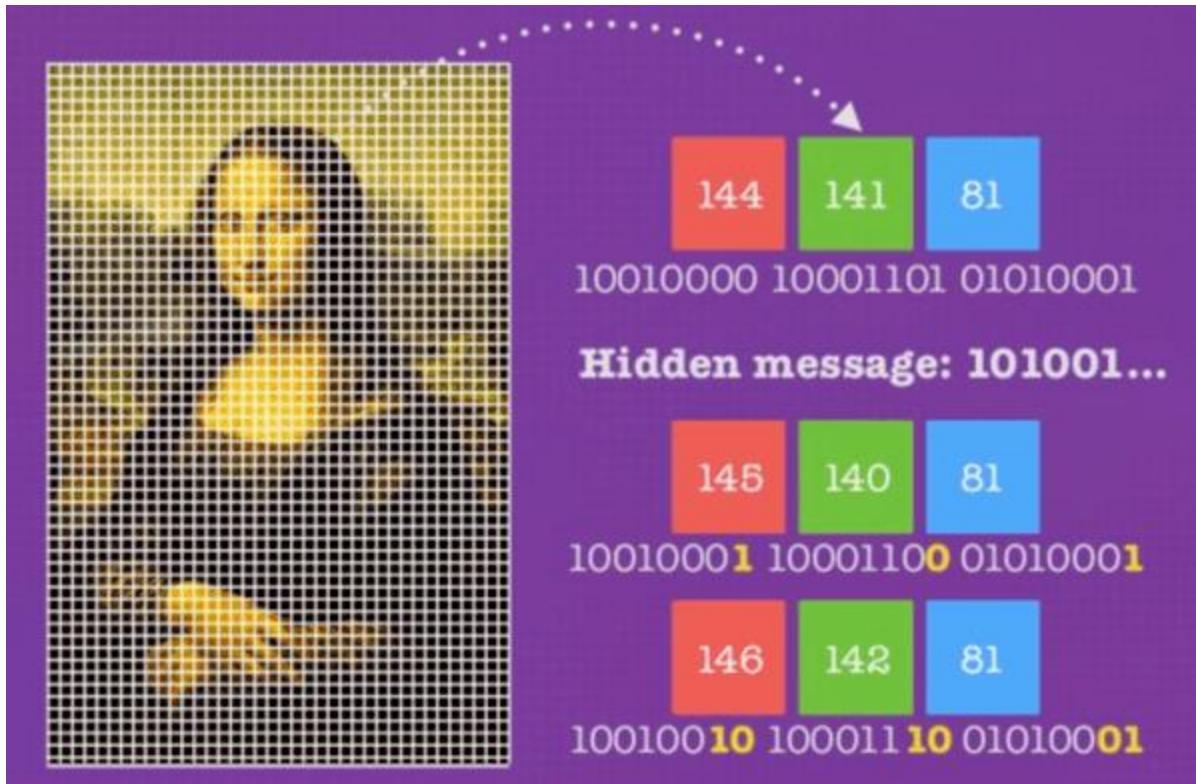
To comprehend the power of quantum computer, consider RSA-640, a number with 193 digits, which can be factored by eighty 2.2GHz computers over the span of 5 months, one quantum computer would factor in less than 17 seconds. Numbers that would typically take billions of years to compute could only take a matter of hours or even minutes with a fully developed quantum computer.

In view of these facts, modern cryptography will have to look for computationally harder problems or devise completely new techniques of archiving the goals presently served by modern cryptography.

Steganography

Steganography ("covered writing") is the science of hiding information "in plain sight". Unlike cryptography, the goal of steganography is to completely obscure the existence of information rather than conceal its content. Currently, the most common usage of steganography is to hide one computer file inside of another computer file.

Modern



The most common form of steganography used today hides files within image files on a computer. The hidden file is encoded in the least significant bits of the values encoding the color of each pixel of the image. Changing the least significant bits changes the appearance of the image very slightly, and is not perceptible to the naked eye. If the change is detectable at all, the colors will just look a little off as if the image was taken from a low-quality camera or in poor light. A similar process can be used to conceal data in sound files since the human ear is limited in its ability to differentiate different, similar frequencies (and in the range of frequencies it can detect).

Original image (top), followed by hiding a message using the least significant bits of the pixel values (1-bit and 2-bit)

Another modern steganographic scheme involves concealing pictures within a video file. The human eye and brain is capable of seeing up to one thousand frames per second. If a video is running at three thousand frames per second and every third frame is a hidden image, the hidden images would not be visible. However, an unlucky pause of the video or examination of the frames as images would reveal the hidden pictures.

Steganography Techniques

Depending on the nature of the cover object (actual object in which secret data is embedded), steganography can be divided into five types:

1. Text Steganography
2. Image Steganography
3. Video Steganography

4. Audio Steganography
5. Network Steganography

Let's explore each of them in detail.

Text Steganography

Text Steganography is hiding information inside the text files. It involves things like changing the format of existing text, changing words within a text, generating random character sequences or using context-free grammars to generate readable texts. Various techniques used to hide the data in the text are:

- Format Based Method
- Random and Statistical Generation
- Linguistic Method

Image Steganography

Hiding the data by taking the cover object as the image is known as image steganography. In digital steganography, images are widely used cover source because there are a huge number of bits present in the digital representation of an image. There are a lot of ways to hide information inside an image. Common approaches include:

- Least Significant Bit Insertion
- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Coding and Cosine Transformation

Audio Steganography

Cyber Security Training

In audio steganography, the secret message is embedded into an audio signal which alters the binary sequence of the corresponding audio file. Hiding secret messages in digital sound is a much more difficult process when compared to others, such as Image Steganography. Different methods of audio steganography include:

- Least Significant Bit Encoding
- Parity Encoding
- Phase Coding
- Spread Spectrum

This method hides the data in WAV, AU, and even MP3 sound files.

Video Steganography

In Video Steganography you can hide kind of data into digital video format. The advantage of this type is a large amount of data can be hidden inside and the fact that it is a moving stream of images and sounds. You can think of this as the combination of Image Steganography and Audio Steganography. Two main classes of Video Steganography include:

- Embedding data in uncompressed raw video and compressing it later
- Embedding data directly into the compressed data stream

Network Steganography (Protocol Steganography)

It is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, ICMP etc. You can use steganography in some covert channels that you can find in the OSI model. For Example, you can hide information in the header of a TCP/IP packet in some fields that are either optional.

In today's digitalized world, various software tools are available for Steganography. In the remainder of this Steganography Tutorial, we will explore some of the popular steganographic tools and their capabilities.

Steganography Tools

A variety of tools have been created to use steganography to hide files within other files on computers. Generally, steganography tools can be classified into image, audio, and/or network steganography tools.

In this section, we will explore some of the steganography tools from each of these categories and the different capabilities that they offer. This is by no means an exhaustive list of tools. Selections were made to give an idea of the available variety of capabilities.

Xiao Steganography

Xiao Steganography is a hybrid steganography tool that allows users to hide files within image (BMP) or audio (WAV) files. The tool also allows users to encrypt the hidden file with a variety of supported encryption algorithms (including RC4 and 3DES) and hashing algorithms (including SHA and MD5). The user provides a carrier file (the wrapper for the hidden file), the file to hide, a choice of encryption algorithm, and a secret key. To extract the hidden file, the user needs to provide the secret key.

SSuite Picsel

SSuite Picsel takes a different approach to image steganography. Rather than providing a single carrier image, the user provides a carrier image and a key image. The key image is used as a secret and is necessary to extract the hidden text file from the carrier image.

Steghide

Steghide is an open-source steganography tool that is capable of hiding data in image or audio files. It runs on the command line. One of the defining features of steghide is that it does not change the color-respective sample frequencies, making it immune to first-order statistical tests for color frequencies.

OpenPuff

OpenPuff is a "professional steganography tool" that allows users to conceal files in image, audio, video, or Flash files. It provides a wide array of features to protect hidden data from discovery.

Camouflage

Camouflage is unique among the tools that we have discussed here since it allows any file to be hidden within any other file. Camouflage provides encryption functionality to users and scrambles the contents of the hidden file before appending it to the original file.

Netcross

netcross is a steganography tool used for establishing covert IP channels across network perimeters with strong firewall rules. It uses DNS resolution requests and responses to carry data back and forth across the firewall.

Using Steganography to Deliver Attacks

Today, attackers use **PowerShell** and **BASH** scripts to automate attacks. So are pen testers. For example, attackers have been embedding actual scripts within macro-enabled Excel and Word documents. Once a victim opens the Excel or Word doc, they activate the embedded, secret script.

The attacker doesn't need to trick the user into using applications such as Steghide. In this case, the hacker – or pen tester – is “living off the land.” The attacker is using a steganographic application to take advantage of common Windows applications and features such as Excel and PowerShell. All the victim needs to do is read the doc, and an unfortunate series of events begins to occur.

1. First, the victim clicks on an Excel document that an attacker has modified using steganography.
2. That click unleashes a hidden PowerShell script.
3. This script then installs an installer app into the Windows computer. This installer app moves quickly and is so subtle that typical antivirus applications don't notice it.
4. This downloader then goes out to the internet and grabs updated versions of **malware** such as URL Zone (or more recent tools) that then compromise the victim's computer.

Over the years, attackers have used the procedure above to deliver **ransomware** such as Snatch. Hackers have installed sophisticated malware that is capable of keylogging, enlisting computers into **DDoS botnets**, or installing trojans, such as the latest variants of **Rovnix** and **Pillowmint**. The list goes on.

Detecting Steganography

Security analysts work to identify the tactics, techniques and procedures (TTPs) of attackers and pen testers. Over the years, they have identified typical signatures that steganographic applications use. This is why antivirus applications, for example, can identify typical moves made by steganographic applications.

Therefore, pen testers and attackers morph and modify their procedures to thwart detection. And so, the “cat and mouse” game continues: attackers constantly modify tools and techniques, and security analysts constantly look for new signatures and methods.

How is Steganography different from Cryptography?

At their core, both of them have almost the same goal, which is protecting a message or information from the third parties. However, they use a totally different mechanism to protect the information.

Cryptography changes the information to ciphertext which cannot be understood without a decryption key. So, if someone were to intercept this encrypted message, they could easily see that some form of **encryption** had been applied. On the other hand, steganography does not change the format of the information but it conceals the existence of the message.

	STEGANOGRAPHY	CRYPTOGRAPHY
Definition	It is a technique to hide the existence of communication	It's a technique to convert data into an incomprehensible form
Purpose	Keep communication secure	Provide data protection
Data Visibility	Never	Always
Data Structure	Doesn't alter the overall structure of data	Alters the overall structure of data
Key	Optional, but offers more security if used	Necessary requirement
Failure	Once the presence of a secret message is discovered, anyone can use the secret data	If you possess the decryption key, then you can figure out original message from the ciphertext

So, in other words, steganography is more discreet than cryptography when we want to send confidential information. The downside being, the hidden message is easier to extract if the presence of secret is discovered. For the remainder of this steganography tutorial, we will learn about different steganography techniques and tools.

04) UNDERSTANDING NETWORK TYPES AND ITS SECURITY

Computer network is an interconnection of computers that use interconnection for the purpose of sharing resources

Application of networks

- Access to remote location
- Sharing of data hardware and software
- Person to person communication
- Electronic commerce

Type of network

- LAN (local area network)
- MAN (metropolitan area network is a computer network that connects computers in an metropolis area or cities of towns)
- WAN (wide area network it telecommunication network that extends over a large geographical area it covers states/ provinces/ continents/ entire world) it's a networks that connects world wide
- PAN (personal area network is a computer that connects personal items like speakers BT)
- SAN (storage area network)

Network topology

Topology this is the way computers are connected to each other (network architecture)

The configuration, or topology, of a network is key to determining its performance. Network topology is the way a network is arranged, including the physical or logical description of how links and nodes are set up to relate to each other. There are numerous ways a network can be arranged, all with different pros and cons, and some are more useful in certain circumstances than others. Admins have a range of options when it comes to choosing a network topology, and this decision must account for the size and scale of their business, its goals, and budget. Several tasks go into effective network topology management, including configuration management, visual mapping, and general performance monitoring. The key is to understand your objectives and requirements to create and manage the network topology in the right way for your business.

What Is Network Topology?

Network topology refers to how various nodes, devices, and connections on your network are physically or logically arranged in relation to each other. Think of your network as a city, and the topology as the



road map. Just as there are many ways to arrange and maintain a city—such as making sure the avenues and boulevards can facilitate passage between the parts of town getting the most traffic—there are several ways to arrange a network. Each has advantages and disadvantages and depending on the needs of your company, certain arrangements can give you a greater degree of connectivity and security.

There are two approaches to network topology: physical and logical. Physical network topology, as the name suggests, refers to the physical connections and interconnections between nodes and the network—the wires, cables, and so forth. Logical network topology is a little more abstract and strategic, referring to the conceptual understanding of how and why the network is arranged the way it is, and how data moves through it.

Why Is Network Topology Important?

The layout of your network is important for several reasons. Above all, it plays an essential role in how and how well your network functions. Choosing the right topology for your company's operational model can increase performance while making it easier to locate faults, troubleshoot errors, and more effectively allocate resources across the network to ensure optimal network health. A streamlined and properly managed network topology can increase energy and data efficiency, which can in turn help to reduce operational and maintenance costs.

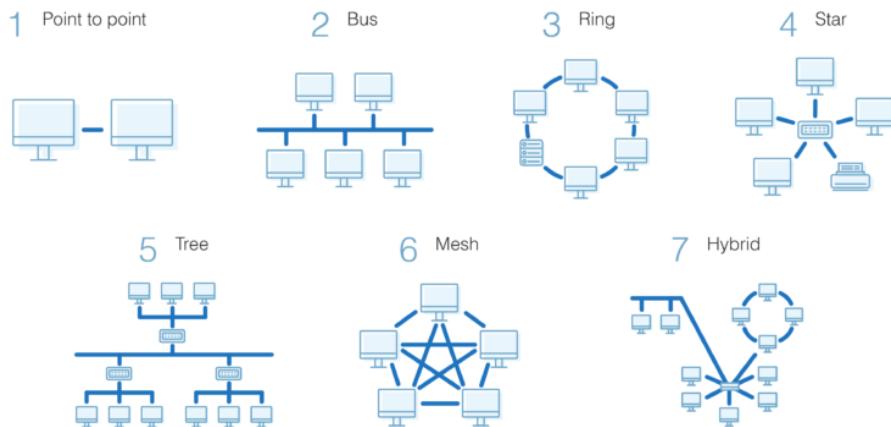
The design and structure of a network are usually shown and manipulated in a software-created network topology diagram. These diagrams are essential for a few reasons, but especially for how they can provide visual representations of both physical and logical layouts, allowing administrators to see the connections between devices when troubleshooting.

The way a network is arranged can make or break network functionality, connectivity, and protection from downtime. The question of, "What is network topology?" can be answered with an explanation of the two categories in the network topology.

1. **Physical** – The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged. Setup, maintenance, and provisioning tasks require insight into the physical network.
2. **Logical** – The logical network topology is a higher-level *idea* of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network. Logical network topology includes any virtual and cloud resources.

Effective network management and monitoring require a strong grasp of both the physical and logical topology of a network to ensure your network is efficient and healthy.

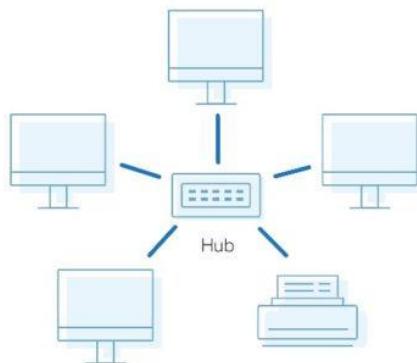
Network Topology Types



What Is Star Topology?

A star topology, the most common network topology, is laid out so every node in the network is directly connected to one central hub via coaxial, twisted-pair, or fiber-optic cable. Acting as a server, this central node manages data transmission—as information sent from any node on the network has to pass through the central one to reach its destination—and functions as a repeater, which helps **prevent data loss**.

Star Topology



Advantages of Star Topology

Star topologies are common since they allow you to conveniently manage your entire network from a single location. Because each of the nodes is independently connected to the central hub, should one go down, the rest of the network will continue functioning unaffected, making the star topology a stable and secure network layout.

Additionally, devices can be added, removed, and modified without taking the entire network offline.

On the physical side of things, the structure of the star topology uses relatively little cabling to fully connect the network, which allows for both straightforward setup and management over time as the network expands or contracts. The simplicity of the network design makes life easier for administrators, too, because it's easy to identify where errors or performance issues are occurring.

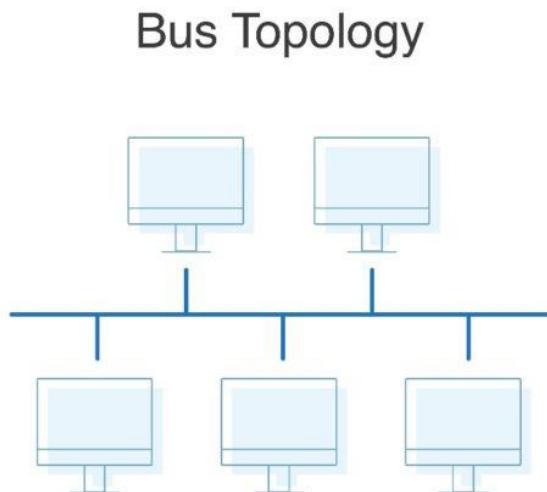
Disadvantages of Star Topology

On the flipside, if the central hub goes down, the rest of the network can't function. But if the central hub is properly managed and kept in good health, administrators shouldn't have too many issues.

The overall bandwidth and performance of the network are also limited by the central node's configurations and technical specifications, making star topologies expensive to set up and operate.

What Is Bus Topology?

A bus topology orients all the devices on a network along a single cable running in a single direction from one end of the network to the other—which is why it's sometimes called a “line topology” or “backbone topology.” Data flow on the network also follows the route of the cable, moving in one direction.



Advantages of Bus Topology

Bus topologies are a good, cost-effective choice for smaller networks because the layout is simple, allowing all devices to be connected via a single coaxial or RJ45 cable. If needed, more nodes can be easily added to the network by joining additional cables.

Disadvantages of Bus Topology

However, because bus topologies use a single cable to transmit data, they're somewhat vulnerable. If the cable experiences a failure, the whole network goes down, which can be time-consuming and expensive to restore, which can be less of an issue with smaller networks.

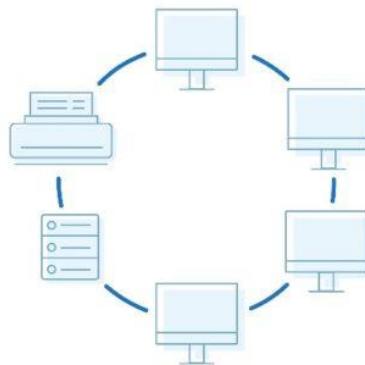
Bus topologies are best suited for small networks because there's only so much bandwidth, and every additional node will slow transmission speeds.

Furthermore, data is "half-duplex," which means it can't be sent in two opposite directions at the same time, so this layout is not the ideal choice for networks with huge amounts of traffic.

What Is Ring Topology? Single vs. Dual

Ring topology is where nodes are arranged in a circle (or ring). The data can travel through the ring network in either one direction or both directions, with each device having exactly two neighbors.

Ring Topology



Pros of Ring Topology

Since each device is only connected to the ones on either side, when data is transmitted, the packets also travel along the circle, moving through each of the intermediate nodes until they arrive at their destination. If a large network is arranged in a ring topology, repeaters can be used to ensure packets arrive correctly and without data loss.

Only one station on the network is permitted to send data at a time, which greatly reduces the risk of packet collisions, making ring topologies efficient at transmitting data without errors.

By and large, ring topologies are cost-effective and inexpensive to install, and the intricate point-to-point connectivity of the nodes makes it relatively easy to identify issues or misconfigurations on the network.

Cons of Ring Topology

Even though it's popular, a ring topology is still vulnerable to failure without proper network management. Since the flow of data transmission moves unidirectionally between nodes along each ring, if one node goes down, it can take the entire network with it. That's why it's imperative for each of the nodes to be monitored and kept in good health. Nevertheless, even if you're vigilant and attentive to node performance, your network can still be taken down by a transmission line failure.

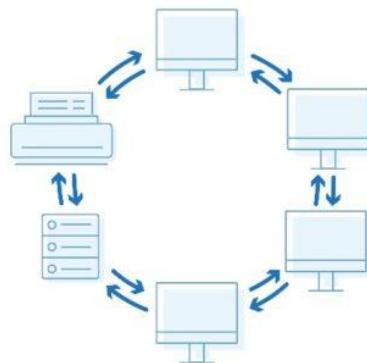
The question of scalability should also be taken into consideration. In a ring topology, all the devices on the network share bandwidth, so the addition of more devices can contribute to overall communication delays. Network administrators need to be mindful of the devices added to the topology to avoid overburdening the network's resources and capacity.

Additionally, the entire network must be taken offline to reconfigure, add, or remove nodes. And while that's not the end of the world, scheduling downtime for the network can be inconvenient and costly.

What Is Dual-Ring Topology?

A network with ring topology is half-duplex, meaning data can only move in one direction at a time. Ring topologies can be made full-duplex by adding a second connection between network nodes, creating a dual ring topology.

Dual Ring Topology



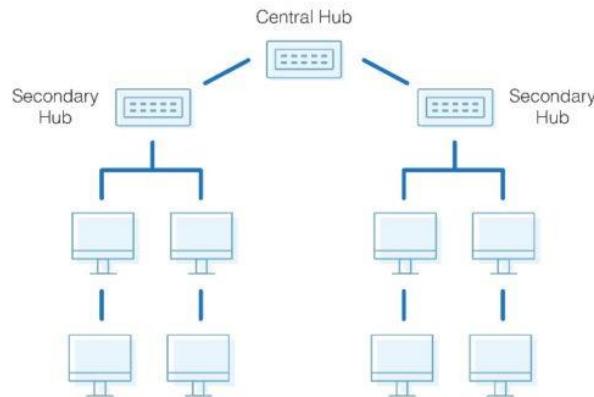
Advantages of Dual-Ring Topology

The primary advantage of dual ring topology is its efficiency: because each node has two connections on either side, information can be sent both clockwise and counterclockwise along the network. The secondary ring included in a dual-ring topology setup can act as a redundant layer and backup, which helps solve for many of the disadvantages of traditional ring topology. Dual ring topologies offer a little extra security, too: if one ring fails within a node, the other ring is still able to send data.

What Is Tree Topology?

The tree topology structure gets its name from how the central node functions as a sort of trunk for the network, with nodes extending outward in a branch-like fashion. However, where each node in a star topology is directly connected to the central hub, a tree topology has a parent-child hierarchy to how the nodes are connected. Those connected to the central hub are connected linearly to other nodes, so two connected nodes only share one mutual connection. Because the tree topology structure is both extremely flexible and scalable, it's often used for wide area networks to support many spread-out devices.

Tree Topology



Pros of Tree Topology

Combining elements of the star and bus topologies allows for the easy addition of nodes and network expansion. Troubleshooting errors on the network is also a straightforward process, as each of the branches can be individually assessed for performance issues.

Cons of Tree Topology

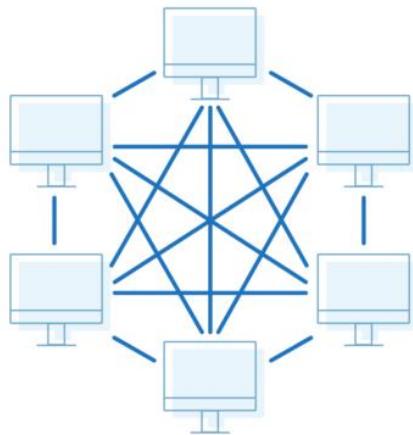
As with the star topology, the entire network depends on the health of the root node in a tree topology structure. Should the central hub fail, the various node branches will become disconnected, though connectivity within—but not between—branch systems will remain.

Because of the hierarchical complexity and linear structure of the network layout, adding more nodes to a tree topology can quickly make proper management an unwieldy, not to mention costly, experience. Tree topologies are expensive because of the sheer amount of cabling required to connect each device to the next within the hierarchical layout.

What Is Mesh Topology?

A mesh topology is an intricate and elaborate structure of point-to-point connections where the nodes are interconnected. Mesh networks can be full or partial mesh. Partial mesh topologies are mostly interconnected, with a few nodes with only two or three connections, while full-mesh topologies are—surprise!—fully interconnected.

Mesh Topology



The web-like structure of mesh topologies offers two different methods of data transmission: routing and flooding. When data is routed, the nodes use logic to determine the shortest distance from the source to destination, and when data is flooded, the information is sent to all nodes within the network without the need for routing logic.

Advantages of Mesh Topology

Mesh topologies are reliable and stable, and the complex degree of interconnectivity between nodes makes the network resistant to failure. For instance, no single device going down can bring the network offline.

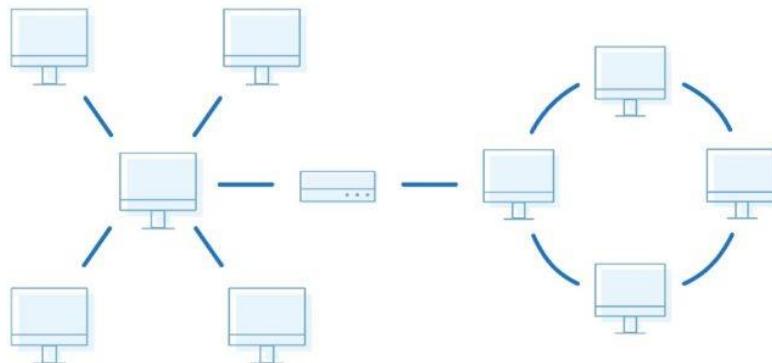
Disadvantages of Mesh Topology

Mesh topologies are incredibly labor-intensive. Each interconnection between nodes requires a cable and configuration once deployed, so it can also be time-consuming to set up. As with other topology structures, the cost of cabling adds up fast, and to say mesh networks require a lot of cabling is an understatement.

What Is Hybrid Topology?

Hybrid topologies combine two or more different topology structures—the tree topology is a good example, integrating the bus and star layouts. Hybrid structures are most commonly found in larger companies where individual departments have personalized network topologies adapted to suit their needs and network usage.

Hybrid Topology



Advantages of Hybrid Topology

The main advantage of hybrid structures is the degree of flexibility they provide, as there are few limitations on the network structure itself that a hybrid setup can't accommodate.

Disadvantages of Hybrid Topology

However, each type of network topology comes with its own disadvantages, and as a network grows in complexity, so too does the experience and know-how required on the part of the admins to keep everything functioning optimally. There's also the monetary cost to consider when creating a hybrid network topology.

Which Topology Is Best for Your Network?



No network topology is perfect, or even inherently better than the others, so determining the right structure for your business will depend on the needs and size of your network. Here are the key elements to consider:

- Length of cable needed
- Cable type
- Cost
- Scalability

Cable Length

Generally, the more cable involved in network topology, the more work it'll require to set up. The bus and star topologies are on the simpler side of things, both being fairly lightweight, while mesh networks are much more cable- and labor-intensive.

Cable Type

The second point to consider is the type of cable you'll install. Coaxial and twisted-pair cables both use insulated copper or copper-based wiring, while fiber-optic cables are made from thin and pliable plastic or glass tubes. Twisted-pair cables are cost-effective but have less bandwidth than coaxial cables. Fiber-optic cables are high performing and can transmit data far faster than twisted-pair or coaxial cables, but they also tend to be far more expensive to install, because they require additional components like optical receivers. So, as with your choice of network topology, the wiring you select depends on the needs of your network, including which applications you'll be running, the transmission distance, and desired performance.

Cost

As I've mentioned, the installation cost is important to account for, as the more complex network topologies will require more time and funding to set up. This can be compounded if you're combining different elements, such as connecting a more complex network structure via more expensive cables (though using fiber-optic cables in a mesh network is overdoing it, if you ask me, because of how interconnected the topology is). Determining the right topology for your needs, then, is a matter of striking the right balance between installation and operating costs and the level of performance you require from the network.

Scalability

The last element to consider is scalability. If you anticipate your company and network expanding—or if you'd like it to be able to—it'll save you time and hassle down the line to use an easily modifiable network topology. Star topologies are so common because they allow you to add, remove, and alter nodes with minimal disruption to the rest of the network. Ring networks, on the other hand, have to be taken entirely offline for any changes to be made to any of the nodes.

How to Map Network Topology

When you're starting to design a network, topology diagrams come in handy. They allow you to see how the information will move across the network, which, in turn, allows you to predict potential choke points. Visual representation makes it easier to create a streamlined and efficient network design, while also acting as a good reference point if you find yourself needing to troubleshoot errors.



A topology diagram is also essential for having a comprehensive understanding of your network's functionality. In addition to assisting with the troubleshooting process, the bird's-eye view provided by a topology diagram can help you visually identify the pieces of the infrastructure your network is lacking, or which nodes need monitoring, upgrading, or replacing.

The good news is you don't have to do it manually: you can easily create a map of your network.

What is Network Security?

The process of taking precautions to protect the underlying networking infrastructure from unauthorized access, misuse, failure, alteration, destruction, or inappropriate disclosure is known as network security. It's a set of rules designed to protect integrity, accessibility and confidentiality within a network. To secure their networks from possible security threats, network administrators must take preventative steps. Registered users have access to networks, while malicious actors are prevented from executing threats and exploits.

Digitization is currently changing our world, resulting in improvements to virtually all of our everyday activities. If companies want to provide the services that their staff and customers expect, they must secure their networks. It finally safeguards the company's credibility. With the number of hackers growing and getting smarter daily, the need for network security tools is becoming increasingly important.

Network security is a technique that ensures the security of an organization's assets, including all network traffic. It covers both software and hardware components. Efficient network protection monitors network access by detecting and preventing a wide variety of threats from spreading or accessing the network.

The internet has unquestionably become an important part of our everyday lives. Security is required for computer networks used in daily transactions and communication within the government, individuals, and businesses. But are you certain that your network is safe?

Many people try to damage our Internet-connected devices, infringe on our privacy, and make Internet services unusable. Network security has become a key concern in cybersecurity due to the frequency and variety of current attacks and the possibility of new and potentially disruptive attacks in the future. Computers, users, and programs may execute their authorized critical functions safely by implementing network security measures.

How can we ensure network security?

When it comes to network security in an enterprise, there are several levels to remember. Attacks can occur at any layer of the network security layers model, so your network security hardware, software, and policies must be configured to cover all of them.

Physical, technical, and administrative controls are the most common forms of network security controls. The various types of network security and how each control works are described briefly below.

Physical Network Security



Physical security is essential for safeguarding confidential data and information. New network security risks have arisen as a result of the ever-changing work environment and employee activity. Physical safety can appear to be a no-brainer. New types of attacks, unauthorized access, and computer hardware theft, on the other hand, are all too common. As a result of this threat, devices have become more compact and easier to steal.

Although most cybersecurity solutions focus on anti-malware software, firewall settings, and other data protection measures, the physical security of IT resources is equally essential. The majority of these devices undoubtedly contain valuable organizational data that a disgruntled employee may hack. Furthermore, most users are reckless with security, posing a greater threat to network security.

Staying proactive in risk management, computer, and network protection, and keeping your employees safe through security awareness training, especially on layered security, is the best approach.

Technical Network Security

The confidentiality of data on the network, whether inbound or outbound, is protected by technical network security. It is essential to protect data and systems from unauthorized access as well as malicious activities by employees.

Administrative Network Security

Administrative network security controls are organizational-level security policies that govern user actions, such as how users are authenticated, their level of access, and how IT staff members execute infrastructure changes.

What are the different types of Network Security?

Access Control

Network access control is a method of improving a private organizational network's security by limiting network resources to endpoint devices that meet its security policy. Two main components make up a standard network access control scheme:

Restricted Access and Network Boundary Security

Restricted access: User authentication and authorization control, responsible for defining and authenticating various users to the network system, are used to access network devices. The process of granting or refusing special access permissions to a protected resource is known as authorization.

Network Boundary Protection regulates logical communication into and out of networks. Multiple firewalls, for example, may be used to avoid unauthorized access to network infrastructure. Besides, intrusion detection and prevention tools can be used to protect against Internet-based attacks.

Application Security

Application security is the method of identifying, restoring, and improving the security of software. Most of this occurs during the development process, but it also involves tools and approaches for protecting applications after they have been deployed. As hackers increasingly target applications with their attacks, it's becoming more relevant.

The protection of applications is attracting a lot of publicity. There are hundreds of resources available to protect different aspects of your application's portfolio, ranging from locking down coding changes to assessing inadvertent coding risks, evaluating encryption options, and auditing permissions and access rights. There are advanced resources for web applications, smartphone apps, network-based apps, and firewalls.

Firewalls Security

A firewall is a network security system that monitors incoming and outgoing network traffic, allowing or disallowing data packets based on security rules. It aims to create a firewall between your internal network and incoming traffic from external sources (such as the internet) to prevent malicious traffic such as viruses and hackers from entering. The primary goal of a firewall is to allow non-threatening traffic while keeping dangerous traffic out.

Virtual Private Networks (VPN)

A virtual private network (VPN) is an encrypted connection between a computer and a network over the internet. The encrypted link helps in the secure transmission of sensitive data. It defends against unwanted eavesdropping on the traffic and allows the user to operate remotely. The encryption is carried out in real-time. In corporate settings, VPN technology, is commonly used. VPN can hide IP addresses and physical location while encrypting data when online. VPN uses existing one network infrastructure; it creates tunnelling protocols to provide security authentication and integrity to users.

Benefits of VPN

- It allows extended geographical connection
- It is cost effective

Advantages of VPN

- Secure your network
- Hide private information
- Prevent data and bandwidth throttling

Wireless networks

Computer networks that are not connected by cables are called wireless networks. They generally use radio waves for communication between the network nodes. They allow devices to be connected to the network while roaming around within the network coverage.



Types of Wireless Networks

- Wireless LANs – Connects two or more network devices using wireless distribution techniques.
- Wireless MANs – Connects two or more wireless LANs spreading over a metropolitan area.
- Wireless WANs – Connects large areas comprising LANs, MANs and personal networks.

Advantages of Wireless Networks

- It provides clutter-free desks due to the absence of wires and cables.
- It increases the mobility of network devices connected to the system since the devices need not be connected to each other.
- Accessing network devices from any location within the network coverage or Wi-Fi hotspot becomes convenient since laying out cables is not needed.
- Installation and setup of wireless networks are easier.

- New devices can be easily connected to the existing setup since they needn't be wired to the present equipment. Also, the number of equipment that can be added or removed to the system can vary considerably since they are not limited by the cable capacity. This makes wireless networks very scalable.
- Wireless networks require very limited or no wires. Thus, it reduces the equipment and setup costs.

Examples of wireless networks

- Mobile phone networks
- Wireless sensor networks
- Satellite communication networks
- Terrestrial microwave networks

Wireless Security

Wireless network protection is mainly concerned with preventing unauthorized and malicious access to a wireless network. Wireless network protection is typically provided by wireless devices (typically a wireless router/switch) that encrypt and protect all wireless communication by default. Even if the security of the wireless network is broken, the hacker would be unable to see the quality of the traffic/packets in transit. Furthermore, wireless intrusion detection and prevention systems secure a wireless network by alerting the network administrator in the event of a security breach.

Wired Equivalent Policy (WEP) and Wireless Protected Access (WPA) are two common algorithms and standards for ensuring wireless network security (WPA).

What are the risks to your wireless network?

Whether it's a home or business network, the risks to an unsecured wireless network are the same. Some of the risks include:

Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer in range of your access point can use your connection. The typical indoor broadcast range of an access point is 150–300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment or condominium, failure to secure your wireless network could open your internet connection to many unintended users. These users may be able to conduct illegal activity, monitor and capture your web traffic, or steal personal files.

Wardriving

Wardriving is a specific kind of piggybacking. The broadcast range of a wireless access point can make internet connections available outside your home, even as far away as your street. Savvy computer users know this, and some have made a hobby out of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks. This practice is known as “wardriving.”

Evil Twin Attacks (cloning a system and increasing the signal strength for clients to use it as it is the first priority than the original authentic system)

In an evil twin attack, an adversary gathers information about a public network access point, then sets up their system to impersonate it. The adversary uses a broadcast signal stronger than the one generated by the legitimate access point; then, unsuspecting users connect using the stronger signal. Because the victim is connecting to the internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, and other personal information. Always confirm the name and password of a public Wi-Fi hotspot prior to use. This will ensure you are connecting to a trusted access point.

Wireless Sniffing

Many public access points are not secured and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted "in the clear," malicious actors could use sniffing tools to obtain sensitive information such as passwords or credit card numbers. Ensure that all the access points you connect to use at least WPA2 encryption.

Unauthorized Computer Access

An unsecured public wireless network combined with unsecured file sharing could allow a malicious user to access any directories and files you have unintentionally made available for sharing. Ensure that when you connect your devices to public networks, you deny sharing files and folders. Only allow sharing on recognized home networks and only while it is necessary to share items. When not needed, ensure that file sharing is disabled. This will help prevent an unknown attacker from accessing your device's files.

Shoulder Surfing (eavesdropping)

In public areas malicious actors can simply glance over your shoulder as you type. By simply watching you, they can steal sensitive or personal information. Screen protectors that prevent shoulder-surfers from seeing your device screen can be purchased for little money. For smaller devices, such as phones, be cognizant of your surroundings while viewing sensitive information or entering passwords.

Theft of Mobile Devices

Not all attackers rely on gaining access to your data via wireless means. By physically stealing your device, attackers could have unrestricted access to all of its data, as well as any connected cloud accounts. Taking measures to protect your devices from loss or theft is important, but should the worst happen, a little preparation may protect the data inside. Most mobile devices, including laptop computers, now have the ability to fully encrypt their stored data—making devices useless to attackers who cannot provide the proper password or personal identification number (PIN). In addition to encrypting device content, it is also advisable to configure your device's applications to request login information before allowing access to any cloud-based information. Last, individually encrypt or password-protect files that contain personal or sensitive information. This will afford yet another layer of protection in the event an attacker is able to gain access to your device.

What can you do to minimize the risks to your wireless network?

- Change default passwords. Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily available to obtain online, and so provide only marginal protection. Changing default

passwords makes it harder for attackers to access a device. Use and periodic changing of complex passwords is your first line of defense in protecting your device. (See Choosing and Protecting Passwords.)

- Restrict access. Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses. Consult your user documentation for specific information about enabling these features. You can also utilize the “guest” account, which is a widely used feature on many wireless routers. This feature allows you to grant wireless access to guests on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials.
- Encrypt the data on your network. Encrypting your wireless data prevents anyone who might be able to access your network from viewing it. There are several encryption protocols available to provide this protection. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information being transmitted between wireless routers and wireless devices. WPA3 is currently the strongest encryption. WPA and WPA2 are still available; however, it is advisable to use equipment that specifically supports WPA3, as using the other protocols could leave your network open to exploitation.
- Protect your Service Set Identifier (SSID) (is a sequence of characters that uniquely names the network i.e., network name. each set of wireless devices communicating directly with each other is called a basic service set BSS; several BSS can be joined to form a logical WLAN segment known as extended service set ESS. SSID is given 1-32 bytes) ←*short notes* || prevent outsiders from easily accessing your network, avoid publicizing your SSID. All Wi-Fi routers allow users to protect their device’s SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer’s default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.
- Install a firewall. Consider installing a firewall directly on your wireless devices (a host-based firewall), as well as on your home network (a router- or modem-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer (see Understanding Firewalls for Home and Small Office Use).
- Maintain antivirus software. Install antivirus software and keep your virus definitions up to date. Many antivirus programs also have additional features that detect or protect against spyware and adware (see Protecting Against Malicious Code and What Is Cybersecurity?).
- Use file sharing with caution. File sharing between devices should be disabled when not needed. You should always choose to only allow file sharing over home or work networks, never on public networks. You may want to consider creating a dedicated directory for file sharing and restrict access to all other directories. In addition, you should password protect anything you share. Never open an entire hard drive for file sharing (see Choosing and Protecting Passwords).
- Keep your access point software patched and up to date. The manufacturer of your wireless access point will periodically release updates to and patches for a device’s software and firmware. Be sure to check the manufacturer’s website regularly for any updates or patches for your device.
- Check your internet provider’s or router manufacturer’s wireless security options. Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network. Check the customer support area of their websites for specific suggestions or instructions.
- Connect using a Virtual Private Network (VPN). Many companies and organizations have a VPN. VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

Wireless LAN security

Is a network that allows device to connect and communicate wirelessly (without use of cables)

Standards of WLAN (802.11)

- 802.11a
- 802.11b
- 802.11g
- 802.11n

802.11b

Supports bandwidth up to 11Mbps, provides better servers for home market

PRO low cost (cheap), signal range is good and not easily obstructed

CONs slowest maximum speed, interference on the unregulated frequency.

802.11a

Due to interference 802.11a was developed for business networks. Supports bandwidth up to 54Mbps.
Signals are regulated

PROs fast max speed compared to 802.11b, regulated frequencies from other devices

CONs high cost shorter range signal (more easily obstructed)

802.11g

Attempts to combine the best of both (802.11a and 802.11b). supports up to 54Mbps max bandwidth and a great signal. It is backward compatible with (802.11a/b)

PROs fast max speed, signal range is good and not easily obstructed.

CONs More costly than (802.11a/b), appliances may interfere on the unregulated signal frequency.

802.11n

It was designed to improve on 802.11g in the amount of bandwidth supported by utilizing multiple signals and antennas. Supports data rates of 100Mbps.

PROs fastest max speed and best signal range, more resistant to signal interference from external appliances

CONs costs more than the others.

WLAN components

Wireless client receiver: used to connect a client device i.e., computers, laptops through Access Points.

Access Points: they provide the wireless clients with a point of access into a network. They support three mode of APs **root mode, repeater and bridge mode.**

Antenna: used to reinforce signal strength in wireless transmission in data and VoIP's

Types of antennas

- **Parabolic (dish)** are the most directional antennas and deliver the highest gains. They are tightly focused on a designed direction which makes them ideal for point-to-point connection. A correctly aligned pair of antennas can extent the range of wireless network to 20 miles.
- **Home directional antennas:** radiates the signal outward equally in all direction, they are used to access large area where the access receiver is unknown. CONs of directional is that picks a lot of noise
- **Reflector's antennas** (sectorized) have similar shape of home directional but have reflectors behind the poles that directs the transmitted signal in a certain direction.
- **Yagi antennas** consists of multiple elements that are all aligned to guide incoming waves from a particular direction to the receiving dipole of the antenna.

Types of WLANs

A WLAN is comprised of NIC access point (APs) and network management.

- **Peer to peer WLANs** P2P network allows wireless devices to wirelessly communicate with the other.
 - i. To establish p2p Wlan we require wireless adapters
 - ii. How many Pcs are needed?
 - iii. Equip each Pc with wireless adapter
 - iv. Configure each adapter NIC in all Pcs
- Setting up a WLAN
 - i. Site survey; a site survey is done to explore the environment
 - ii. Access point; it is connected through a single cable which allows it to access information while the end devices access wirelessly within the network
 - iii. Managing the WLAN; the network manager can use web-based management tools to manage the access points from anywhere on the and configure monitor or do any changes
 - iv. extending WLANs; in areas where 2 WLANs are to be connected, the directional antennas are supposed to be used to link the network.

WLAN performance can be affected by distance & obstacles; to position an optimal network connection follow the guideline bellow



- i. don't settle premature on a location for a wireless access-point
- ii. install the wireless access-point or router in a central position.
- iii. Avoid physical obstruction whenever possible.
- iv. Avoid reflective surfaces
- v. Install access-point or a router 1 meter away from other both electoral devices and appliances to avoid the interference.

- **Infrastructure WLANs**

Intrusion Prevention System

An intrusion prevention system (IPS) is a form of network security that detects and prevents threats that have been detected. Intrusion detection systems keep an eye on the network at all times, searching for potential malicious events and recording data about them. The IPS notifies system administrators about these incidents and takes preventative steps, including closing access points and configuring firewalls to prevent potential attacks.

IPS solutions may also be used to define corporate security practices, discouraging staff and network visitors from breaching the law. With so many access points on a standard business network, you'll need a way to keep an eye out for signs of possible breaches, injuries, or attacks. Network attacks are becoming more complex, and even the most robust security strategies are being penetrated.

WIPS configuration consist of several components of;

- Antennas (wireless scanning of radio spectrum and are usually installed in secured places)
- Server (analyses packets)
- Console (provides user primary users in to the system admittatur and reporting)

Network management and control

FTP services



FTP (File Transfer Protocol) is used to communicate and transfer files between computers on a **TCP/IP** (Transmission Control Protocol/Internet Protocol) network, aka the internet. Users, who have been granted access, can receive and transfer files in the File Transfer Protocol server (also known as FTP host/site).

As a website developer, FTP is used to make changes to a website. Given the large number of files that need to be handled, it is more comfortable and secure to manage them using FTP.

In this article, we will learn all the basics about FTP and how to use the protocol.

How does FTP work?

FTP connection needs two parties to establish and communicate on the network. To do that, users need to have permission by providing credentials to the FTP server. Some public FTP servers may not require credentials to access their files. The practice is common in a so-called anonymous FTP.

There are two distinct communication channels while establishing an FTP connection. The first one is called the command channel where it initiates the instruction and response. The other one is called a data channel, where the distribution of data happens.

To get or transfer a file, an authorized user will use the protocol to request on creating changes in the server. In return, the server will grant that access. This session is known as the active connection mode.

The distribution in active mode might face a problem if a firewall is protecting the user's machine. The firewall usually does not allow any unauthorized sessions from an external party.

The **passive** mode is used if that issue occurs. In this mode, the user establishes both command and the data channel. This mode then asks the server to **listen** rather than to attempt to create a connection back to the user.

How to use FTP

There are three approaches on how to establish an FTP connection. A very simple method is using a command-line FTP, such as using Command prompt for Windows or Terminal in Mac/Linux. Developers still use it today for transferring files using FTP.

A user also can use a web browser to communicate with the FTP server. A web browser is more convenient when users want to access large directories in the server. Yet, it's often less reliable and slower than using a dedicated FTP program.

Today, the most common practice to use FTP, especially for a web developer, is by using an FTP client.



An FTP client provides more freedom compared to the command line and web browser. It is also easier to manage and more powerful compared to the other methods.

There are also more features available whilst using such a client. For example, it allows users to transfer a large file and use the synchronizing utility.

How to Connect to Hostinger FTP

There are many FTP clients to choose from. From free open-source applications to premium options. For the purpose of this article, we will use FileZilla, an open-source and popular FTP client.

We will need an FTP server first, and we can set one up using our Hostinger account.

1. Login to your Hostinger account and navigate to the **FTP accounts** section
2. Create a new FTP account by filling out a new username and password

 **Create a New FTP Account**

Directory	/home/u251975009/domains/hostinger-dev-21.xyz	/public_html
Username*	Username	
Password*	8 characters min.	 
✓ Create		

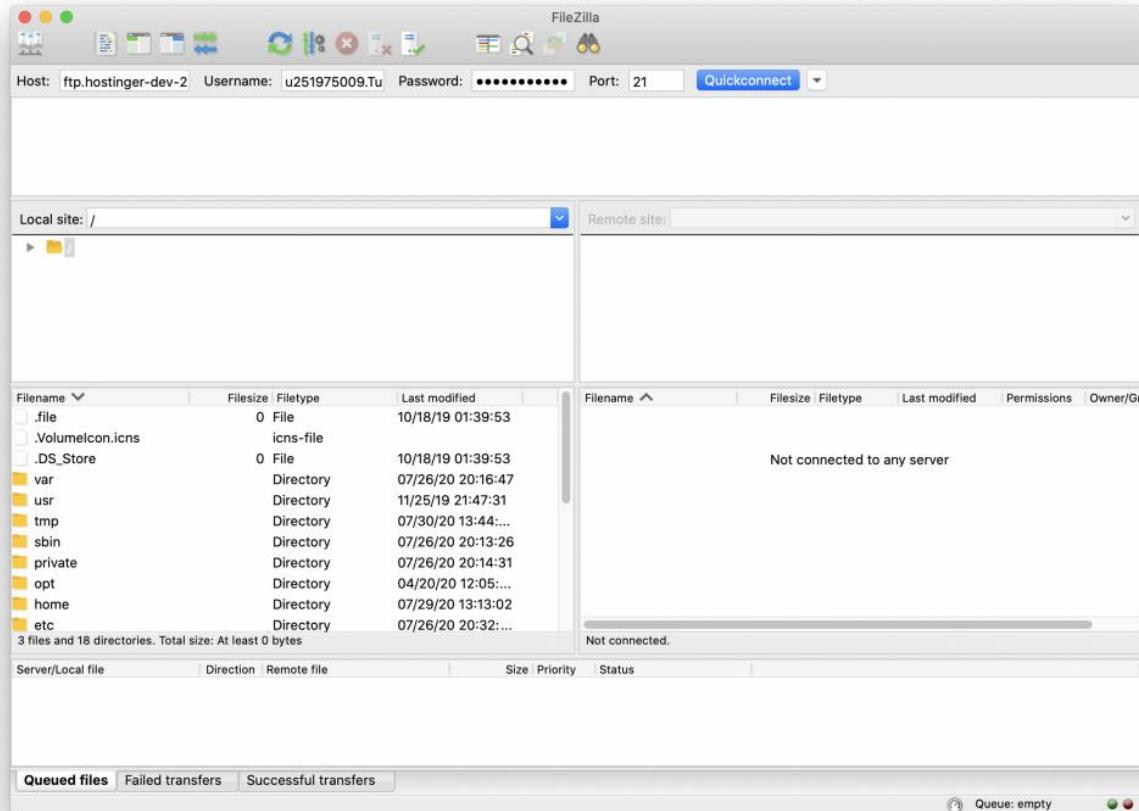
3. You will see new FTP servers (Hostname) under the list of active FTP accounts

 **List of Active FTP Accounts**

Hostname *	Directory	Username	Actions
ftp.hostinger-dev-21.xyz	/home/u251975009/domains/hostinger-dev-21.xyz/public_html	u251975009.Tutorial	



4. In FileZilla, insert the hostname, username, and password and hit the **Quickconnect** button. You can also fill the port number. Otherwise, port 21 is used by default.



5. The status window will tell you if you are logged in to the FTP server. As you can see in the **Remote Site** window, these are the files that the server has.

Conclusion

So there you have it, you can send and receive files from an FTP server. As a web developer, you will need to use FTP with an FTP client to access the website that you are managing. Furthermore, it is easier to create and remove directories and read a large number of files on the server.

We hope this article helps you to understand FTP as well as the different methods and programs used.

API

Application Programming Interface (API)

Application programming interfaces, or APIs, simplify software development and innovation by enabling applications to exchange data and functionality easily and securely.

What is an application programming interface (API)?

An application programming interface, or API, enables companies to open up their applications' data and functionality to external third-party developers, business partners, and internal departments within their companies. This allows services and products to communicate with each other and leverage each other's data and functionality through a documented interface. Developers don't need to know how an API is implemented; they simply use the interface to communicate with other products and services. API use has surged over the past decade, to the degree that many of the most popular web applications today would not be possible without APIs.

How an API works

An API is a set of defined rules that explain how computers or applications communicate with one another. APIs sit between an application and the web server, acting as an intermediary layer that processes data transfer between systems.

Here's how an API works:

1. **A client application initiates an API call** to retrieve information—also known as a *request*. This request is processed from an application to the web server via the API's Uniform Resource Identifier (URI) and includes a request verb, headers, and sometimes, a request body.
2. **After receiving a valid request**, the API makes a call to the external program or web server.
3. **The server sends a response** to the API with the requested information.
4. **The API transfers the data** to the initial requesting application.

While the data transfer will differ depending on the web service being used, this process of requests and response all happens through an API. Whereas a user interface is designed for use by humans, APIs are designed for use by a computer or application.

APIs offer security by design because their position as middleman facilitates the abstraction of functionality between two systems—the API endpoint decouples the consuming application from the infrastructure providing the service. API calls usually include authorization credentials to reduce the risk of attacks on the server, and an API gateway can limit access to minimize

security threats. Also, during the exchange, HTTP headers, cookies, or query string parameters provide additional security layers to the data.

For example, consider an API offered by a payment processing service. Customers can enter their card details on the frontend of an application for an ecommerce store. The payment processor doesn't require access to the user's bank account; the API creates a unique token for this transaction and includes it in the API call to the server. This ensures a higher level of security against potential hacking threats.

Why we need APIs

Whether you're managing existing tools or designing new ones, you can use an application programming interface to simplify the process. Some of the main benefits of APIs include the following:

- **Improved collaboration:** The average enterprise uses almost 1,200 cloud applications (link resides outside of IBM), many of which are disconnected. APIs enable integration so that these platforms and apps can seamlessly communicate with one another. Through this integration, companies can automate workflows and improve workplace collaboration. Without APIs, many enterprises would lack connectivity and would suffer from informational silos that compromise productivity and performance.
- **Easier innovation:** APIs offer flexibility, allowing companies to make connections with new business partners, offer new services to their existing market, and, ultimately, access new markets that can generate massive returns and drive digital transformation. For example, the company Stripe began as an API with just seven lines of code. The company has since partnered with many of the biggest enterprises in the world, diversified to offer loans and corporate cards, and was recently valued at USD 36 billion (link resides outside of IBM).
- **Data monetization:** Many companies choose to offer APIs for free, at least initially, so that they can build an audience of developers around their brand and forge relationships with potential business partners. However, if the API grants access to valuable digital assets, you can monetize it by selling access (this is referred to as the API economy). When AccuWeather (link resides outside of IBM) launched its self-service developer portal to sell a wide range of API packages, it took just 10 months to attract 24,000 developers, selling 11,000 API keys and building a thriving community in the process.
- **Added security:** As noted above, APIs create an added layer of protection between your data and a server. Developers can further strengthen API security by using tokens, signatures, and Transport Layer Security (TLS) encryption; by implementing API gateways to manage and authenticate traffic; and by practicing effective API management.

Common API examples

Because APIs allow companies to open up access to their resources while maintaining security and control, they have become a valuable aspect of modern business. Here are some popular examples of application programming interfaces you may encounter:

- **Universal logins:** A popular API example is the function that enables people to log in to websites by using their Facebook, Twitter, or Google profile login details. This convenient feature allows any website to leverage an API from one of the more popular services to quickly authenticate the



user, saving them the time and hassle of setting up a new profile for every website service or new membership.

- **Third-party payment processing:** For example, the now-ubiquitous "Pay with PayPal" function you see on ecommerce websites works through an API. This allows people to pay for products online without exposing any sensitive data or granting access to unauthorized individuals.
- **Travel booking comparisons:** Travel booking sites aggregate thousands of flights, showcasing the cheapest options for every date and destination. This service is made possible through APIs that provide application users with access to the latest information about availability from hotels and airlines. With an autonomous exchange of data and requests, APIs dramatically reduce the time and effort involved in checking for available flights or accommodation.
- **Google Maps:** One of the most common examples of a good API is the Google Maps service. In addition to the core APIs that display static or interactive maps, the app utilizes other APIs and features to provide users with directions or points of interest. Through geolocation and multiple data layers, you can communicate with the Maps API when plotting travel routes or tracking items on the move, such as a delivery vehicle.
- **Twitter:** Each Tweet contains descriptive core attributes, including an author, a unique ID, a message, a timestamp when it was posted, and geolocation metadata. Twitter makes public Tweets and replies available to developers and allows developers to post Tweets via the company's API.

Types of APIs

Nowadays, most application programming interfaces are web APIs that expose an application's data and functionality over the internet. Here are the four main types of web API:

- **Open APIs** are open source application programming interfaces you can access with the HTTP protocol. Also known as public APIs, they have defined API endpoints and request and response formats.
- **Partner APIs** are application programming interfaces exposed to or by strategic business partners. Typically, developers can access these APIs in self-service mode through a public API developer portal. Still, they will need to complete an onboarding process and get login credentials to access partner APIs.
- **Internal APIs** are application programming interfaces that remain hidden from external users. These private APIs aren't available for users outside of the company and are instead intended to improve productivity and communication across different internal development teams.
- **Composite APIs** combine multiple data or service APIs. These services allow developers to access several endpoints in a single call. Composite APIs are useful in microservices architecture where performing a single task may require information from several sources.

Types of API protocols

As the use of web APIs has increased, certain protocols have been developed to provide users with a set of defined rules that specifies the accepted data types and commands. In effect, these API protocols facilitate standardized information exchange:

- **SOAP** (Simple Object Access Protocol) is an API protocol built with XML, enabling users to send and receive data through SMTP and HTTP. With SOAP APIs, it is easier to share

information between apps or software components that are running in different environments or written in different languages.

- **XML-RPC** is a protocol that relies on a specific format of XML to transfer data, whereas SOAP uses a proprietary XML format. XML-RPC is older than SOAP, but much simpler, and relatively lightweight in that it uses minimum bandwidth.
- **JSON-RPC** is a protocol similar to XML-RPC, as they are both remote procedure calls (RPCs), but this one uses JSON instead of XML format to transfer data. Both protocols are simple. While calls may contain multiple parameters, they only expect one result.
- **REST** (Representational State Transfer) is a set of web API architecture principles, which means there are no official standards (unlike those with a protocol). To be a REST API (also known as a RESTful API), the interface must adhere to certain architectural constraints. It's possible to build RESTful APIs with SOAP protocols, but the two standards are usually viewed as competing specifications.

APIs, web services, and microservices

A web service is a software component that can be accessed via a web address. Therefore, by definition, web services require a network. As a web service exposes an application's data and functionality, in effect, every web service is an API. However, not every API is a web service.

Traditionally, API referred to an interface connected to an application that may have been created with any of the low-level programming languages, such as Javascript. The modern API adheres to REST principles and the JSON format and is typically built for HTTP, resulting in developer-friendly interfaces that are easily accessible and widely understood by applications written in Java, Ruby, Python, and many other languages.

When using APIs, there are two common architectural approaches—service-oriented architecture (SOA) and microservices architecture.

- **SOA** is a software design style where the features are split up and made available as separate services within a network. Typically, SOA is implemented with web services, making the functional building blocks accessible through standard communication protocols. Developers can build these services from scratch, but they usually create them by exposing functions from legacy systems as service interfaces.
- **Microservices architecture** is an alternative architectural style that divides an application into smaller, independent components. Applying the application as a collection of separate services makes it easier to test, maintain, and scale. This methodology has risen to prominence throughout the cloud computing age, enabling developers to work on one component independent of the others.

While SOA was a vital evolutionary step in application development, microservices architecture is built to scale, providing developers and enterprises with the agility and flexibility they need to create, modify, test, and deploy applications at a granular level, with shorter iteration cycles and more efficient use of cloud computing resources.

Proxy

What is a proxy?

As the need for internet access at the workplace grows, web proxies come from a need to secure an organization's internal network from external threats. Broadly speaking, a web proxy, also referred to as a proxy or proxy server, is a way to filter the connection between your computer and the internet.

Let's break it down.

Say you want to check your Facebook profile to see how many likes that picture of your dog received. You open up a web browser and type in "www.facebook.com".

Without a web proxy, your computer would simply connect directly to the internet to access the website and display it for you.

With a proxy, your computer will connect to a separate server, the proxy, that sits between the computer and the internet. The web proxy acts like airport security and is in charge of screening what websites are allowed access or not.

What is and is not allowed is determined by your organization's IT policy. If social media sites are restricted, then, unfortunately, that means you'll have to wait until you get home to check your Facebook.



Why do you need web proxy?

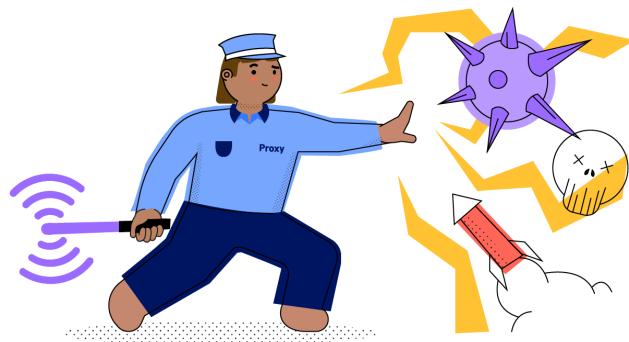
There are two overall reasons why larger organizations use web proxies in their network security setup: to protect their private data and to improve the performance of their internal network.

Insure your assets against threats

The top reason why a web proxy is needed on a network is that it protects a company's data assets by limiting websites that potentially contain malicious code.

And not just data assets, but physical assets too when you consider the possible costs of replacing an organization's hardware when a virus renders it unusable.

Enterprise companies might have confidential proprietary information, their employees' private data, as well as their customers' personal information sitting on their local network. With all this valuable data to protect, it doesn't seem so excessive to monitor internet usage.



Improve network performance

Depending on the type of proxy you use and how it is set up, it is possible that using a proxy can improve performance by caching web pages.

For example, let's say you recently visited airtame.com. The proxy can save a temporary copy of the webpage which it stores locally so that when your colleague visits airtame.com later that day, the proxy can serve up that copy instead of having to retrieve the original from the internet.

This is most useful for frequently visited websites, for instance, if you often refer to your company's website. It's saving you the loading time of the page every time you visit.

Every organization's network is different and can have different needs. Luckily, there are several ways to incorporate a web proxy, or even a set of web proxies, into any network setup, which makes it a flexible solution.

Proxy in action

Not every company makes use of web proxies. The majority of web proxy users are enterprise-level companies or educational institutions that need a manageable way of monitoring the large volume of internet users on their network.

Enterprise companies and educational institutions use proxies to keep their network safe, but they go about it in slightly different ways.

Enterprise

For larger corporations, corporate espionage is not just the stuff of James Bond films. It is a real threat that makes it necessary for companies to monitor the traffic coming in and out of their network. These companies use proxies to filter everything – websites, emails, and any applications that access internet.

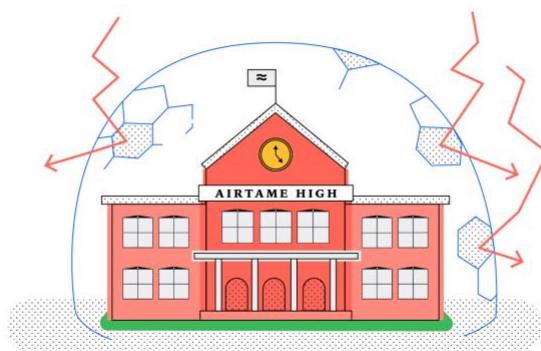
Of course, sometimes a web proxy also protects us from ourselves. Checking social media may seem harmless, but let's admit that it is a productivity threat. In this case, companies use proxies to set time limits for social media use during business hours.

At schools and universities

For schools and universities, it is important to use a web proxy that blocks access to adult content. In this case, purchasing a quality service that keeps an up-to-date database of known adult content sites is key.

In certain instances, it is necessary to block access to radically political websites or sites that promote hate speech, both to ensure a safe environment for students, as well as make sure students cite quality source material in their research.

Another reason schools and universities invest in a good database is to monitor sites known to carry malicious code. Even if a malicious website attempts to hide behind a normal website and redirect you to a site running malware, the web proxy flags this as abnormal behavior and blocks access.



Using Airtame with a web proxy setup

Our latest product update introduces web proxy support. This means that, if your organization uses a web proxy setup, you can now configure Airtame to access the proxy and thereby reach the internet.

[quote: “Web proxy support is a big step forward for Airtame and our enterprise customers, where security and wireless screen sharing go hand-in-hand.” – Simon Hangaard, Head of Product Management at Airtame]

Airtame requires internet access in order to receive important product updates and to make use of certain tools. For example, you can register your Airtame devices to Airtame Cloud, our web-based device management tool that, among other things, lets you remotely monitor devices.

Another useful Airtame feature that requires internet is our Home screen, which lets you display web-based dashboards or even slideshows.

Network classes

A B and C Classes of Networks

Internet addresses are allocated by the InterNIC (<http://www.internic.net>), the organization that administers the Internet. These IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E exist, but are not generally used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of Class A, B, and C Internet addresses, each with an example address:

- Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.
- Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.
- Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

In some scenarios, the default subnet mask values do not fit the needs of the organization, because of the physical topology of the network, or because the numbers of networks (or hosts) do not fit within the default subnet mask restrictions. The next section explains how networks can be divided using subnet masks.

Class A Network (/ 8 Prefixes)



This network is 8-bit network prefix. Its highest bit is set to 0, and contains a 7-bit network number and a **24-bit host number**.

A maximum of **126, which is $(2^7 - 2)$, networks can be defined**; two is subtracted because all an (0 and 1) subnet cannot be used in certain routers using RIP-1 Protocol. Each network supports a maximum of 16,777,214 ($2^{24} - 2$) hosts per network. You must subtract two because the base network represents host “0”, and the last host on the network is actually used for 1s (“broadcast”) and may not be assigned to any host.

The class **A** network address block contains 2^{31} power (2,147,483,648) individual addresses. The IPv4 address space contains a maximum of 2^{32} power (4,294,967,296) addresses, which mean that a class **A** network address space is 50% of the total IPv4 unicast, address space.

Class B Networks (/16 Prefixes)

This network is a 16-bit network prefix; its highest bit order is set to **1-0**. It is a 14-bit network number with a 16-bit host number.

This class defines $16,384 (2^{14})$ /16 networks, and supports a maximum of 65,534 ($2^{16} - 2$) hosts per network. Class B /16 block address is $(1,073,741,824) = 2^{30}$; therefore, it represent 25% of the total IPV4.

Class C Networks (/24 Prefixes)

This is a 24-bit network prefix; it has a 3 bit set to the highest order **1-1-0**. It is a 21-bit network number with 8-bit host number.

This class defines a maximum of $2,097,152 (2^{21})$ /24 networks. And each network supports up to 254 ($2^8 - 2$) hosts. The entire class C network represents 2^{29} (536,870,912) addresses; therefore, it is only 12.5 % of the total IPv4.

Other Networks

There are two other networks that are not commonly used, class D and Class E. Class D has its highest bit order set to **1-1-1-0** it is used to support multicasting. Class E has its highest bit order set to **1-1-1-1** which is reserved for experimental use.

Router security

Wireless internet or Wi-Fi access has become a necessity in the home and workplace, but it can also open a door to risks from hackers, scammers, and identity thieves. Whether in your home or office, an unsecured Wi-Fi router running on the default manufacturer settings could be a liability when it comes to hackers and Wi-Fi squatters accessing your private information and burdening your broadband.

If your Wi-Fi network isn't secured properly — a public IP address, no unique Wi-Fi password — you could be letting anyone with a wireless-enabled device gain access. You might not be worried about someone using your wireless connection, but the real risk is exposing sensitive information you send and receive — your emails, banking information, and maybe even your smart home's daily schedule — to cybercriminals.

A router is a key component for transferring data to one network to another network. Router look like a small device and nowadays mainly router used for distribution internet. Router work on 3 layer concept and they need software also for rotate data or information on other end. The main purpose of router is breaking a big network into small networks router is also use for connecting 2 or more network of different address on same point or end. Router divide a big network domain into many parts equally. The main reason of dividing big domain into many sub domain or subnet is for better quality and for more user can use that network. Here we talking about public networks like WIFI etc. Internet providing companies work on same pattern to maintain quality of internet and for gaining more users. With the help of this method that called 3 layer method internet provider divide 1 big data in many users otherwise they need more networks.



For dividing one network into many subs network need a full roadmap. And roadmap required software because without software network can't access on another end network. Router work as a main infrastructure in routing network and information or WIFI signals

Function of Router:

- Main function of router is spread the WIFI signals or other kind of information to one network to another network.
- Divided big domain data into many sub nets or sub networks for maintain the quality.
- WIFI routers connect one or more big data network in same point or end.
- Router work on 3-layer concept. 3 layer is a whole path or process.
- If the address of both network or sub net Is same than signals not move to another point because they need two different addresses for working perfectly.

What is Routing Protocols?

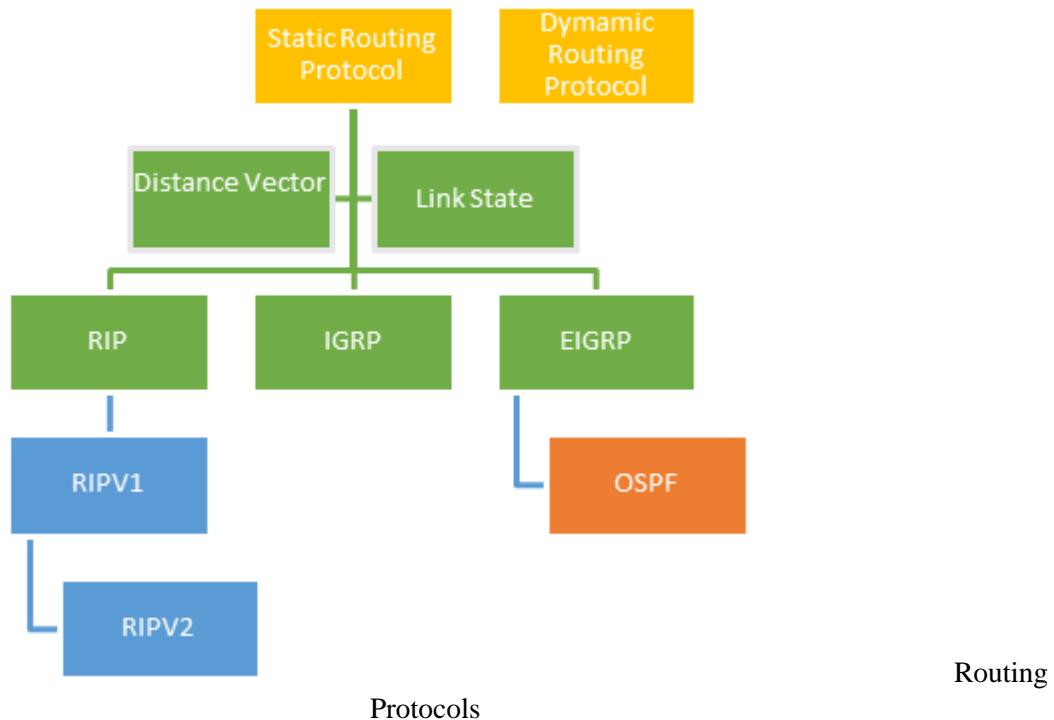
Routing Protocols are the set of defined rules used by the routers to communicate between source & destination. They do not move the information to the source to a destination, but only update the routing table that contains the information.

Network Router protocols helps you to specify way routers communicate with each other. It allows the network to select routes between any two nodes on a computer network.

Types of Routing Protocols

There are mainly two types of Network Routing Protocols

- Static
- Dynamic



Static Routing Protocols

Static routing protocols are used when an administrator manually assigns the path from source to the destination network. It offers more security to the network.

Advantages

- No overhead on router CPU.



- No unused bandwidth between links.
- Only the administrator is able to add routes

Disadvantages

- The administrator must know how each router is connected.
- Not an ideal option for large networks as it is time intensive.
- Whenever link fails all the network goes down which is not feasible in small networks.

Dynamic Routing Protocols

Dynamic routing protocols are another important type of routing protocol. It helps routers to add information to their routing tables from connected routers automatically. These types of protocols also send out topology updates whenever the network changes' topological structure.

Advantage:

- Easier to configure even on larger networks.
- It will be dynamically able to choose a different route in case if a link goes down.
- It helps you to do load balancing between multiple links.

Disadvantage:

- Updates are shared between routers, so it consumes bandwidth.
- Routing protocols put an additional load on router CPU or RAM.

Distance Vector Routing Protocol (DVR)

Distance Vector Protocols advertise their routing table to every directly connected neighbor at specific time intervals using lots of bandwidths and slow converge.

In the Distance Vector routing protocol, when a route becomes unavailable, all routing tables need to be updated with new information.

Advantages:

- Updates of the network are exchanged periodically, and it is always broadcast.
- This protocol always trusts route on routing information received from neighbor routers.

Disadvantages:

- As the routing information are exchanged periodically, unnecessary traffic is generated, which consumes available bandwidth.

Internet Routing Protocols:



The following are types of protocols which help data packets find their way across the Internet:

Routing Information Protocol (RIP)

RIP is used in both LAN and WAN Networks. It also runs on the Application layer of the OSI model. The full form of RIP is the Routing Information Protocol. Two versions of RIP are

1. RIPv1
2. RIPv2

The original version or RIPv1 helps you determine network paths based on the IP destination and the hop count journey. RIPv1 also interacts with the network by broadcasting its IP table to all routers connected with the network.

RIPv2 is a little more sophisticated as it sends its routing table on to a multicast address.

Interior Gateway Protocol (IGP)

IGRP is a subtype of the distance-vector interior gateway protocol developed by CISCO. It is introduced to overcome RIP limitations. The metrics used are load, bandwidth, delay, MTU, and reliability. It is widely used by routers to exchange routing data within an autonomous system.

This type of routing protocol is the best for larger network size as it broadcasts after every 90 seconds, and it has a maximum hop count of 255. It helps you to sustain larger networks compared to RIP. IGRP is also widely used as it is resistant to routing loop because it updates itself automatically when route changes occur within the specific network. It is also given an option to load balance traffic across equal or unequal metric cost paths.

Link State Routing Protocol

Link State Protocols take a unique approach to search the best routing path. In this protocol, the route is calculated based on the speed of the path to the destination and the cost of resources.

Routing protocol tables:

Link state routing protocol maintains below given three tables:

- **Neighbor table:** This table contains information about the neighbors of the router only. For example, adjacency has been formed.
- **Topology table:** This table stores information about the whole topology. For example, it contains both the best and backup routes to a particular advertised network.
- **Routing table:** This type of table contains all the best routes to the advertised network.

Advantages:



- This protocol maintains separate tables for both the best route and the backup routes, so it has more knowledge of the inter-network than any other distance vector routing protocol.
- Concept of triggered updates are used, so it does not consume any unnecessary bandwidth.
- Partial updates will be triggered when there is a topology change, so it does not need to update where the whole routing table is exchanged.

Exterior Gateway Protocol (EGP)

EGP is a protocol used to exchange data between gateway hosts that are neighbors with each other within autonomous systems. This routing protocol offers a forum for routers to share information across different domains. The full form for EGP is the Exterior Gateway Protocol. EGP protocol includes known routers, network addresses, route costs, or neighboring devices.

Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a hybrid routing protocol that provides routing protocols, distance vector, and link-state routing protocols. The full form routing protocol EIGRP is Enhanced Interior Gateway Routing Protocol. It will route the same protocols that IGRP routes using the same composite metrics as IGRP, which helps the network select the best path destination.

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) protocol is a link-state IGP tailor-made for IP networks using the Shortest Path First (SPF) method.

OSPF routing allows you to maintain databases detailing information about the surrounding topology of the network. It also uses the Dijkstra algorithm (Shortest path algorithm) to recalculate network paths when its topology changes. This protocol is also very secure, as it can authenticate protocol changes to keep data secure.

Here are some main differences between these Distance Vector and Link State routing protocols:

Distance Vector	Link State
Distance Vector protocol sends the entire routing table.	Link State protocol sends only link-state information.
It is susceptible to routing loops.	It is less susceptible to routing loops.
Updates are sometimes sent using broadcast.	Uses only multicast method for routing updates.
It is simple to configure.	It is hard to configure this routing protocol.
Does not know network topology.	Know the entire topology.

Distance Vector	Link State
Example RIP, IGRP.	Examples: OSPF IS-IS.

Intermediate System-to-Intermediate System (IS-IS)

ISIS CISCO routing protocol is used on the Internet to send IP routing information. It consists of a range of components, including end systems, intermediate systems, areas, and domains.

The full form of ISIS is Intermediate System-to-Intermediate System. Under the IS-IS protocol, routers are organized into groups called areas. Multiple areas are grouped to make form a domain.

Border Gateway Protocol (BGP)

BGP is the last routing protocol of the Internet, which is classified as a DPVP (distance path vector protocol). The full form of BGP is the Border Gateway Protocol.

This type of routing protocol sends updated router table data when changes are made. Therefore, there is no auto-discovery of topology changes, which means that the user needs to configure BGP manually.

What is the purpose of Routing Protocols?

Routing protocols are required for the following reasons:

- Allows optimal path selection
- Offers loop-free routing
- Fast convergence
- Minimize update traffic
- Easy to configure
- Adapts to changes
- Scales to a large size
- Compatible with existing hosts and routers
- Supports variable length

Classful Vs. Classless Routing Protocols

Here are some main differences between these routing protocols:

Classful Routing Protocols	Classless Routing Protocols
Classful routing protocols never send subnet mask detail during routing updates.	Classless routing protocols can send IP subnet mask information while doing routing updates.
RIPv1 and IGRP are classful protocols. These two are classful protocols as they do not include subnet mask information.	RIPv2, OSPF, EIGRP, and IS-IS are all types of class routing protocols which has subnet mask information within updates.

Summary:

Features	RIP V1	RIP V2	IGRP	OSPF	EIGRP
Classful/Classless	Classful	Classless	Classful	Classless	Classless
Metric	Hop	Hop	Composite Bandwidth, Delay.	Bandwidth	Composite, Bandwidth, Delay.
Periodic	30 seconds	30 seconds	90 seconds	None	30 seconds
Advertising Address	255.255.255.255	223.0.0.9	255.255.255.255	224.0.0.5 224.0.0.6	224.0.0.10
Category	Distance Vector	Distance Vector	Distance Vector	Link State	Hybrid
Default Distance	120	120	200	110	170

Types of routers

Core router

Core routers are generally used by service providers (i.e. AT&T, Verizon, Vodafone) or cloud providers (i.e. Google, Amazon, Microsoft). They provide maximum bandwidth to connect additional routers or switches. Most small businesses will not need core routers. But very large enterprises that have many employees working in various buildings or locations may use core routers as part of their network architecture.

Edge router

An edge router, also called a gateway router or just "gateway" for short, is a network's outermost point of connection with external networks, including the Internet.

Edge routers are optimized for bandwidth and designed to connect to other routers to distribute data to end users. Edge routers don't usually offer Wi-Fi or the ability to manage local networks fully. They typically have only Ethernet ports—an input to connect to the Internet and several outputs to connect additional routers.

Edge router and modem are somewhat interchangeable terms, though the latter term is no longer commonly used by manufacturers or IT professionals when referencing edge routers.

Distribution router

A distribution router, or interior router, receives data from the edge router (or gateway) via a wired connection and sends it on to end users, typically via Wi-Fi, though the router usually also includes physical (Ethernet) connections for connecting users or additional routers.

Wireless router

Wireless routers, or residential gateways, combine the functions of edge routers and distribution routers. These are commonplace routers for home networks and Internet access.

Most service providers provide full-featured wireless routers as standard equipment. But even if you have the option to use an ISP's wireless router in your small business, you may want to use a business-level router to take advantage of better wireless performance, more connectivity controls, and security.

Virtual router

Virtual routers are pieces of software that allow some router functions to be virtualized in the cloud and delivered as a service. These routers are ideal for large businesses with complex network needs. They offer flexibility, easy scalability, and a lower entry cost. Another benefit of virtual routers is reduced management of local network hardware.

How to choose small business routers

Connectivity

Pay close attention to the numbers and types of ports (such as phone, Ethernet, cable, and USB) to make sure you can connect the necessary devices. Remember that unused ports are fine to have, as they allow you to expand the network when needed.

Bandwidth



Sufficient bandwidth is important for user experience. It ensures maximum performance for multiple users: the more users, the greater the bandwidth needed. You can grow your business's network by adding additional routers or hubs if necessary, but insufficient bandwidth anywhere in the network can cause bottlenecks.

Wireless capability

Wi-Fi is a given, but there are different standards. The latest, [Wi-Fi 6](#) (802.11ax), can deliver much higher transmission speeds, especially when multiple access points (such as devices or additional routers) are connected at once. Wi-Fi 6 routers are backwards-compatible with old Wi-Fi standards.

Simplified setup and management

Most routers provide a browser-based interface that connects directly to your router to perform setup and admin. However, many manufacturers now offer mobile apps that are specially designed for their devices and provide more intuitive interfaces and easier setup.

Security

Your router should at least offer WPA or WPA 2 password protection. Some routers also have firewall software, which continuously scans incoming data for potential malware and viruses. Another important tool is MAC (Media Access Control) address filtering, which uses device-specific IDs to screen users and build a whitelist or blacklist for network access.

Flexibility

Consider routers that have at least one power over ethernet (PoE) port. PoE provides both data and electricity power supply to external devices such as wireless access points, VoIP phones, IP and cameras. PoE eliminates cabling and provides additional flexibility to your networks.

Automatic updates

Routers contain software that requires updates to maintain performance and security. Many manufacturers update software automatically, which is preferable because it happens in the background without any action on your part.

User changeable configurations

This feature allows you to manage network traffic, guest networks, parental controls, and security settings. The process is easier to handle if the router's configuration can be managed from an app as opposed to a browser interface.

Guest networks



Guest networks are an important layer of extra security for when guests visiting the business need Wi-Fi access. A guest network will limit access to the business's devices and files, while still offering connectivity to visitors.

Quality of service (QoS) controls

Combined with tools to look at usage across all users, this feature allows you to limit network use to up- or downstream transmissions, control for certain types of use (video streaming, for example), and specify bandwidth for different users. This feature helps you improve security as well as network monitoring.

Mesh networks

If you've had experience with Wi-Fi extenders, you may have found that they can do as much harm as good. They create multiple networks that don't communicate with each other, as well as device incompatibilities that can cause bandwidth bottlenecks.

A better solution is a mesh network, which allows you to place multiple Wi-Fi transmitters across your office, all on one network. Unlike extenders, which you can use with any wireless router, mesh networks require a router with this capability built-in.

Basic router security

Every router should have a strong password to help keep out the bad guys. Some new routers come with default passwords, but you should change these during setup. Creating a new, complex, unique password for your wireless router is easy. It should only take a couple of minutes. Specific instructions vary from one router to another, but the basic idea is this:

1. All wireless routers have a numerical address. If you've lost the instructions, you can probably find yours by searching online for your router's model number.
2. In Security Settings, create a name for the router, and a password, and then select a type of encryption, like WAP2. Do not name your router something that can easily be associated with you, such as your last name.
3. Make sure you choose a complex password that you can remember, but one that's not easy to guess.
4. Don't forget to save the updated information when prompted. Your router is now secured against roaming cybercriminals.

Different types of encryptions

Depending on your router, you might have options for different kinds of encryption. The most common router encryption types are WEP, WPA and WPA2. Commercial routers from brands like Netgear, Linksys, and ASUS often include:



- Wired Equivalent Privacy (WEP): This is the oldest and most popular form of router encryption available. However, it is the least secure of all encryption protocols. It uses radio-waves that are easy to crack. For every data packet that is transmitted it uses the same encryption key. With the help of automated software, this information can easily be analyzed.
- Wi-Fi Protected Access (WPA): The Wi-Fi Alliance came up with WPA to offer an encryption protocol without the shortcomings of WEP. It scrambles the encryption key thereby getting rid of the problems caused by hackers cracking the radio-waves. This is also a less secure form of encryption, partly because of legacy hardware and firmware that still used WEP as their main protocol. However, it is a significant improvement over WEP.
- Wi-Fi Protected Access 2 (WPA2): This encryption type is currently the most secure and most recent form of encryption available. You should always select WPA2 if it is available. It not only scrambles the encryption key but is also does not allow the use of Temporal Key Integrity Protocol or TKIP which is known to be less secure than AES.
- Advanced Encryption Standard: When possible, you'll want to use AES on top of WPA2 or WPA. This is the same type of encryption used by the federal government to secure classified information. Routers made after 2006 should have the option to enable this on top of WPA2.

How to set up Wi-Fi router securely: The specifics

Manufacturers know how important it is to make their products user-friendly. Most routers come with instructions that are easy to set up and configure. Apps are replacing bulky user manuals and web interfaces that walk users through the set-up process. While using apps has made setting up routers easier for customers, the router may not be completely secure. Here are a few things to consider before setting up the router.

- **Update your router with new firmware and keep it up to date**

Updating your router's firmware is an important security measure to help protect your router against the latest threats. Most modern routers allow you to enable notifications to prompt you when the manufacturer makes patches and updates to the router's firmware available. Some manufacturers may even push the update automatically to your hardware, so you don't have to do anything. However, there are some routers that have updates within the settings option. In this case, the user has to make sure that the firmware is manually updated regularly.

- **Change your login credentials and router password**

Traditional routers come with a default password created by the manufacturer. While it may look complex and resistant to hacking, there is a good chance most models of the same router share the same password. These passwords are often easy to trace or find on the internet.

Make sure you change the password of your router during setup. Choose a complex alphanumerical password with multiple characters. If possible, change the username of your network, too. After all, it makes up half of the log-in credentials.

- **Always use WPA2 to secure your wireless network**



Wi-Fi Protected Access 2, better known as WPA2, is a commonly used network security technology used on wireless routers.

It is one of the most secure encryption options available in the market since 2006. WPA2 scrambles the traffic going in and out of the router. That means even if someone is within range and can see traffic, all they see is the encrypted version.

- **Disable WPS**

Wi-Fi Protected Setup (WPS) was created with the intention of making the user experience easier and quicker when connecting new devices to the network. It works on the idea that you press a button on the router and a button on the device. This makes both devices' pair automatically. The user has the option to use a personal identification number, or PIN, to setup the device to create a connection. This eliminates the use of the 16-character WPA password that most routers use. However, because of the PIN, WPS earned a bad reputation for being insecure. The PIN is an eight-digit number that can easily be hacked by repeatedly using various combinations of the usernames and passwords. This is carried out with the help of software. This kind of an attack is called a brute force attack. Most routers allow users to disable WPS. Even if the PIN option appears to be disabled, it is wise to disable WPS. In recent years, it was discovered that many routers from reputed manufacturers allowed PIN-based authentication even when it appeared to be disabled.

- **Schedule your wireless network's online schedule**

If you don't use internet-connected devices like smart coffee makers and smart refrigerators, then scheduling your wireless network's online schedule may work for you. It helps to disable the internet when it is not in use. A disabled network won't show up in hacker's list.

- **Get rid of any risky or unverified services**

It would be wise to disable remote access to your router when you are actively connected to it.

Take UPnP, for example. Universal Plug and Play or UPnP is an easy way to allow devices to find other devices on your network. It can also alter the router to allow devices from other networks to access your device. However, it has helped hackers to introduce malware and viruses by making them bypass the firewall. Mirai Botnet is an example of one such attack.

- **Setup a guest network for smart home devices**

A guest network has its advantages. It not only provides your guests with a unique SSID and password, but it also restricts outsiders from accessing your primary network where your connected devices work.

Once you have set up a guest network, you will not have to share your primary network password with your guests. They will be unable to access your Internet of Things-enabled devices or infect your network and devices with malware or viruses that may be on their devices.



- Change the default SSID; Changing the SSID name secures the network since it is in default.
- Reduce or eliminate the use of DHCP on routers
- Turn off ping response.

Other router security helpers

Aside from your router settings and making sure to use your Wi-Fi network's security features, there are some other options, like using a virtual private network, in addition to device security and identity theft.

Use a virtual private network or VPN

A virtual private network (VPN) encrypts connections between devices, creating online privacy and anonymity. A VPN can mask your internet protocol (IP) address so your online actions are virtually untraceable. VPN services establish secure and encrypted connections to provide greater privacy of the data you send and receive, even on secured Wi-Fi hotspots.

Always use a firewall

A firewall monitors incoming and outgoing network traffic and allows or blocks specific traffic. It is an important security feature to look for when selecting a router. For the online safety of your network and devices, it's smart to never disable a firewall.

Install and use a strong antivirus and security software

Setting up security for your wireless network doesn't take much time at all and will do much to help protect you against hackers. Cybercriminals work tirelessly to gain access to your personal and financial information. A small investment in security software could go a long way.

Even if you don't have neighbors you want to prevent from borrowing your Wi-Fi, you'll be protecting yourself from more dangerous snoops. Especially now that so many homes are connected and various devices are using Wi-Fi, you'll be wise to protect all of the information those devices contain. Don't take chances. Just a few minutes of selecting the right home Wi-Fi router settings can mean all the difference to your connected world.

NAPT Services

ADSL details (asymmetric digital subscriber line; Is a data communication technology that enable faster data transmission over copper telephone lines than a conventional voice band modem can provide. A splitter or micro filter allows a single telephone connection to be used for both ADSL services and voice calls the same time.)

Router trouble shooting

Steps to troubleshoot

DOS/DDOS

What is a denial-of-service attack?

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

What are DOS and DDOS?

Denial of Service, or DOS, is a threat where large amounts of traffic requests are directed towards a server or website (usually more than it can handle) to disrupt the service and alter its availability for a long amount of time. During a DOS attack, the server may experience a lag of usage or a complete blackout of all its services until normalcy is restored.

Distributed Denial of Service, or DDOS, happens when a series of different flooding requests are sent to a website to disrupt its service or provide the visitors a terrible user experience. DDOS often occurs from more than one source, and the service is heavily targeted to provide a

How DoS attacks work

Let's look at how DoS attacks are performed and the techniques used. We will look at five common types of attacks.

Ping of Death

The ping command is usually used to test the availability of a network resource. It works by sending small data packets to the network resource. The ping of death takes advantage of this and sends data packets above the maximum limit (65,536 bytes) that TCP/IP allows. TCP/IP fragmentation breaks the packets into small chunks that are sent to the server. Since the sent data packages are larger than what the server can handle, the server can freeze, reboot, or crash.

Smurf

This type of attack uses large amounts of Internet Control Message Protocol (ICMP) ping traffic target at an Internet Broadcast Address. The reply IP address is spoofed to that of the intended victim. All the replies are sent to the victim instead of the IP used for the pings. Since a single

Internet Broadcast Address can support a maximum of 255 hosts, a smurf attack amplifies a single ping 255 times. The effect of this is slowing down the network to a point where it is impossible to use it.

Buffer overflow

A buffer is a temporal storage location in RAM that is used to hold data so that the CPU can manipulate it before writing it back to the disc. Buffers have a size limit. This type of attack loads the buffer with more data than it can hold. This causes the buffer to overflow and corrupt the data it holds. An example of a buffer overflow is sending emails with file names that have 256 characters.

Teardrop

This type of attack uses larger data packets. TCP/IP breaks them into fragments that are assembled on the receiving host. The attacker manipulates the packets as they are sent so that they overlap each other. This can cause the intended victim to crash as it tries to re-assemble the packets.

SYN attack

SYN is a short form for Synchronize. This type of attack takes advantage of the three-way handshake to establish communication using TCP. SYN attack works by flooding the victim with incomplete SYN messages. This causes the victim machine to allocate memory resources that are never used and deny access to legitimate users.

DoS attack tools

The following are some of the tools that can be used to perform DoS attacks.

- **Nemesy**— this tool can be used to generate random packets. It works on windows. This tool can be downloaded from <http://packetstormsecurity.com/files/25599/nemesy13.zip.html>. Due to the nature of the program, if you have an antivirus, it will most likely be detected as a virus.
- **Land and LaTierra**— this tool can be used for IP spoofing and opening TCP connections
- **Blast**— this tool can be downloaded from <http://www.opencomm.co.uk/products/blast/features.php>
- **Panther**— this tool can be used to flood a victim's network with UDP packets.
- **Botnets**— these are multitudes of compromised computers on the Internet that can be used to perform a distributed denial of service attack.

DoS Protection: Prevent an attack

An organization can adopt the following policy to protect itself against Denial of Service attacks.

- Attacks such as SYN flooding take advantage of bugs in the operating system. **Installing security patches** can help reduce the chances of such attacks.

- **Intrusion detection systems** can also be used to identify and even stop illegal activities
- **Firewalls** can be used to stop simple DoS attacks by blocking all traffic coming from an attacker by identifying his IP.
- **Routers** can be configured via the Access Control List to limit access to the network and drop suspected illegal traffic.

Hacking Activity: Ping of Death

We will assume you are using Windows for this exercise. We will also assume that you have at least two computers that are on the same network. DOS attacks are illegal on networks that you are not authorized to do so. This is why you will need to setup your own network for this exercise.

Open the command prompt on the target computer

Enter the command ipconfig. You will get results similar to the ones shown below

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\DAEMON>ipconfig

Windows IP Configuration

Mobile Broadband adapter Mobile Broadband Connection 3:

Connection-specific DNS Suffix . :
IPv4 Address . . . . . : 10.128.131.108
Subnet Mask . . . . . : 255.255.255.248
Default Gateway . . . . . : 10.128.131.105

```

For this example, we are using Mobile Broadband connection details. Take note of the IP address. Note: for this example to be more effective, and you must use a LAN network.

Switch to the computer that you want to use for the attack and open the command prompt

We will ping our victim computer with infinite data packets of 65500

Enter the following command

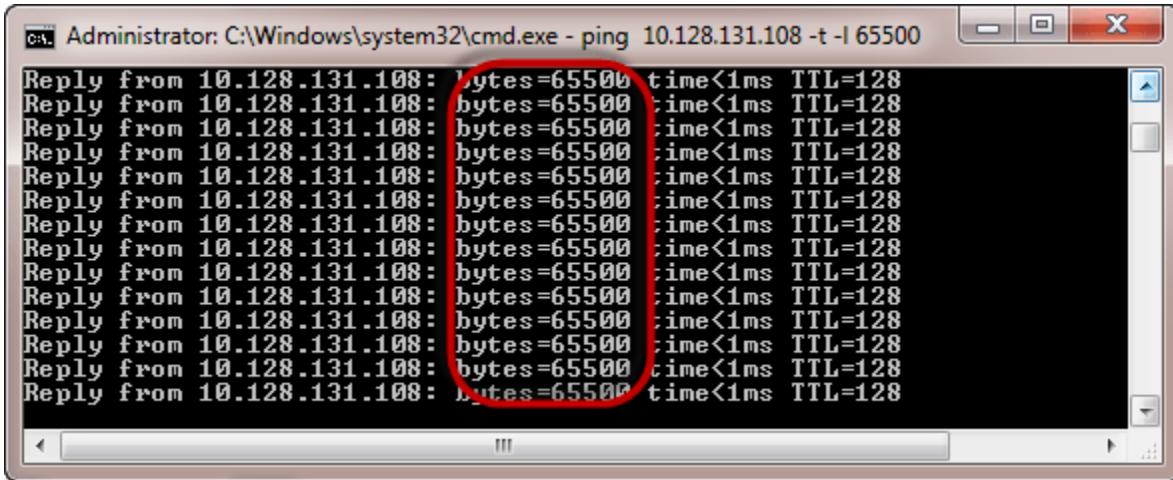
ping 10.128.131.108 -t |65500

HERE,

- “ping” sends the data packets to the victim
- “10.128.131.108” is the IP address of the victim
- “-t” means the data packets should be sent until the program is stopped

- “-l” specifies the data load to be sent to the victim

You will get results similar to the ones shown below



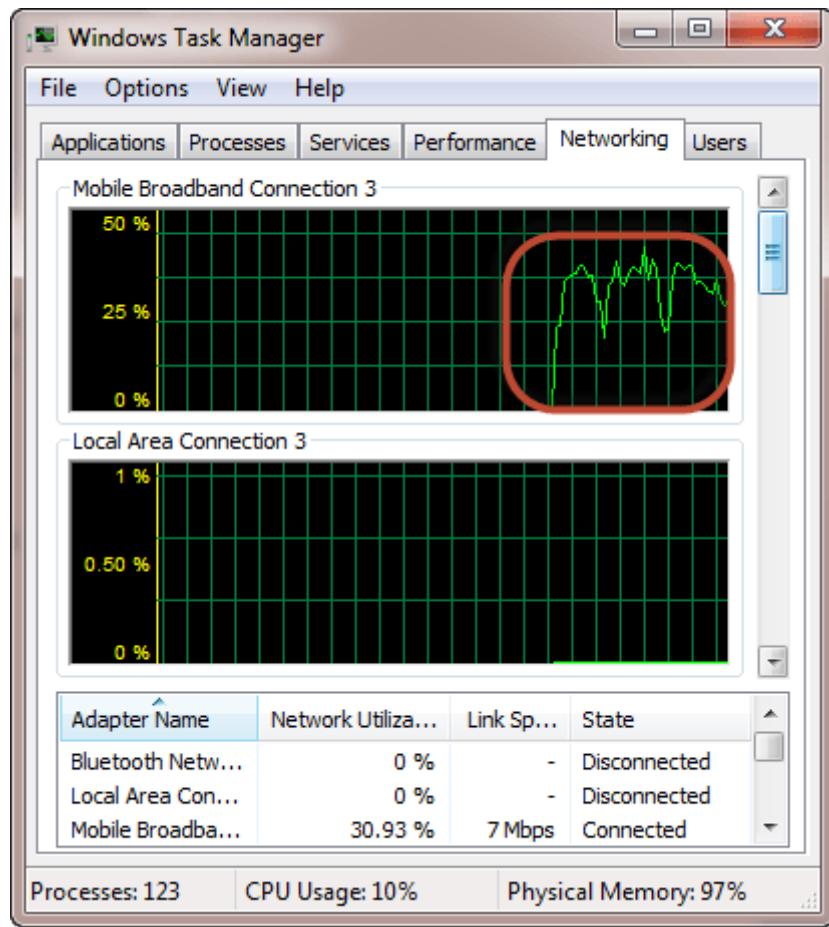
```
Administrator: C:\Windows\system32\cmd.exe - ping 10.128.131.108 -t -l 65500
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
```

Flooding the target computer with data packets doesn't have much effect on the victim. In order for the attack to be more effective, you should attack the target computer with pings from more than one computer.

The above attack can be used to attacker routers, web servers etc.

If you want to see the effects of the attack on the target computer, you can open the task manager and view the network activities.

- Right click on the taskbar
- Select start task manager
- Click on the network tab
- You will get results similar to the following



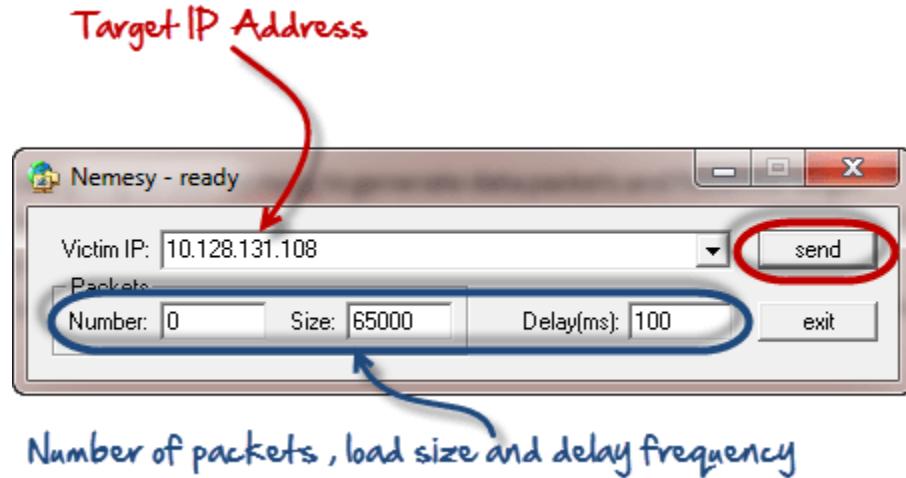
If the attack is successful, you should be able to see increased network activities.

Hacking Activity: Launch a DOS attack

In this practical scenario, we are going to use Nemesy to generate data packets and flood the target computer, router or server.

As stated above, Nemesy will be detected as an illegal program by your anti-virus. You will have to disable the anti-virus for this exercise.

- Download Nemesy from <http://packetstormsecurity.com/files/25599/nemesy13.zip.html>
- Unzip it and run the program Nemesy.exe
- You will get the following interface



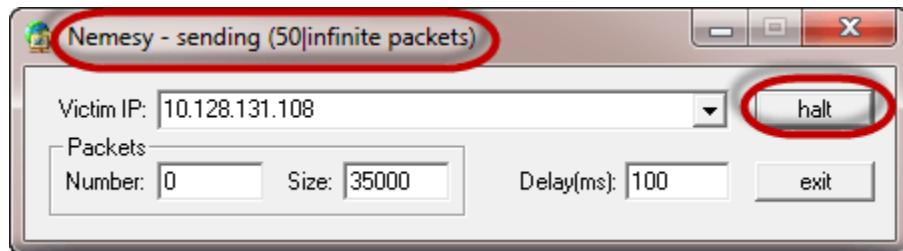
Enter the target IP address, in this example; we have used the target IP we used in the above example.

HERE,

- **0 as the number of packets means infinity.** You can set it to the desired number if you do not want to send, infinity data packets
- The **size field specifies the data bytes to be sent** and the delay **specifies the time interval** in milliseconds.

Click on send button

You should be able to see the following results



The title bar will show you the number of packets sent

Click on halt button to stop the program from sending data packets.

You can monitor the task manager of the target computer to see the network activities.

Summary

- A denial-of-service attack's intent is to deny legitimate users access to a resource such as a network, server etc.

- There are two types of attacks, denial of service and distributed denial of service.
- A denial-of-service attack can be carried out using SYN Flooding, Ping of Death, Teardrop, Smurf or buffer overflow
- Security patches for operating systems, router configuration, firewalls and intrusion detection systems can be used to protect against denial-of-service attacks

catastrophic effect.

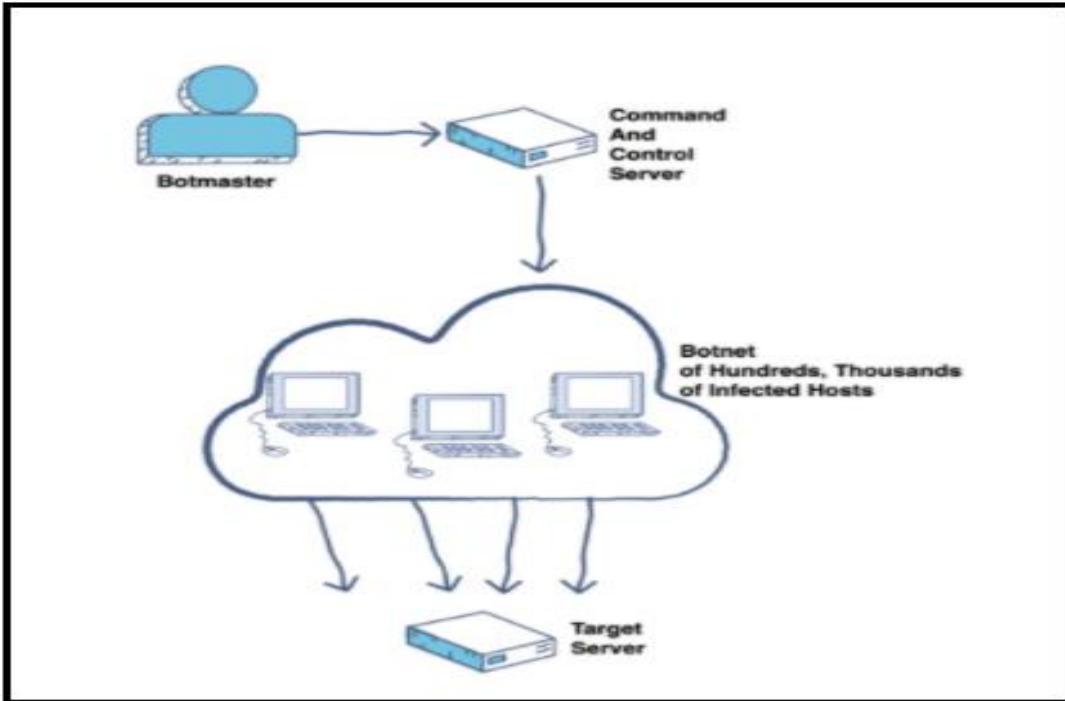


Image Source:- ICM

Differences between DOS and DDOS?

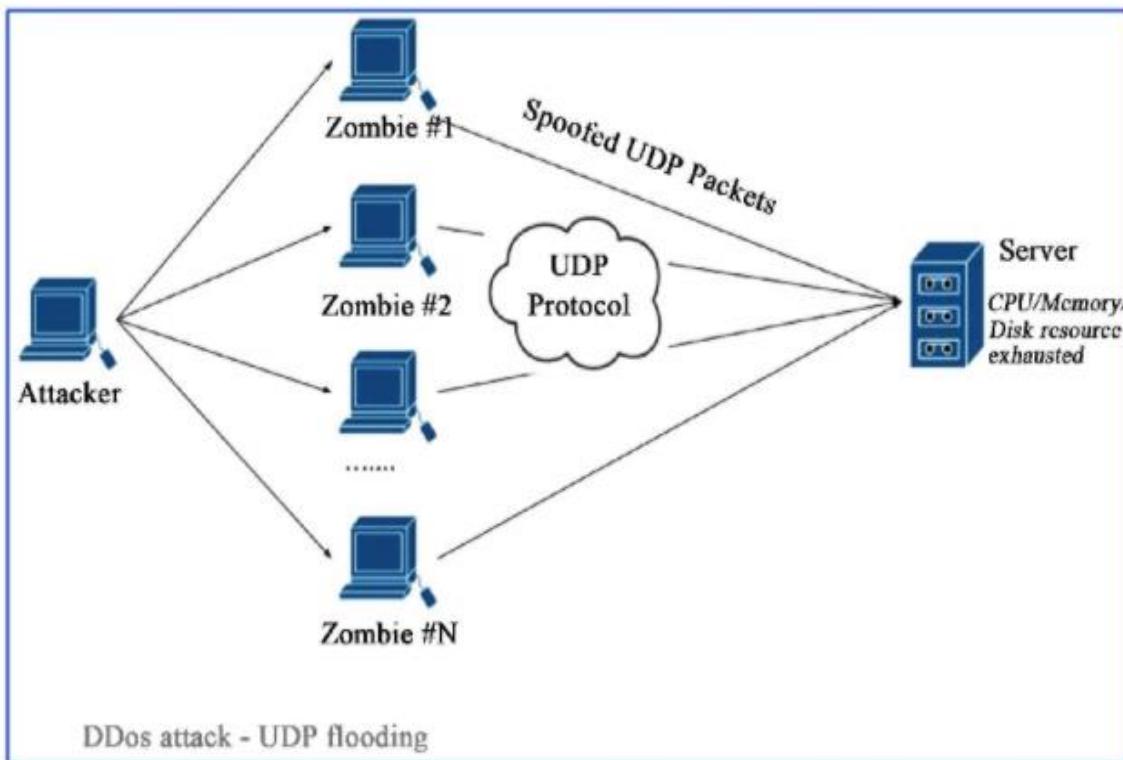
Both DOS and DDOS attacks are commonly performed by people to perturb users, and it is not an intrusion of computer systems. Common DOS attacks are performed via simple search requests, hyperlinks, or Wi-Fi systems, whereas DDOS attacks can occur via web pages or emails. DDOS attacks are extremely difficult to control because millions of sources, called Botnets, are used to perform this attack. The flooding requests of DOS attacks are usually less than DDOS, so it is comparatively easy to control or prevent. Botnets usually consist of devices, such as security cameras, that are rented or bought to deliver DDOS attacks. The victims' devices may be severely affected by malware, leading to a failure of the system for a long period.

A DOS attack is relatively easier to perform, where the source stays single, whereas DDOS attacks are a complicated process and require a higher level of expertise. Various defense systems and security protocols are targeted to make the targets dysfunctional, paralyzing millions of victims in seconds.

Types of DDOS attacks

Distributed Denial of Service or DDOS is commonly performed through these following methods:

- **UDP Flood:** - A UDP flood DDOS attack targets a user with User Datagram Protocol (UDP) Packets. The attack aims to flood the random ports on the remote host and send for an application listening. By the time the host discovers that there are no application requests, the server is disrupted, sending back an “unreachable packet.” The entire network consumes all the limit requests and exceeds its limit.



- **Ping Flood:** - In this attack, ICMP floods the host with ICMP requests, and without waiting for the replies, it continuously sends the requests. When the count exceeds the limit, the server fails and reaches a “Hang mode” for a while.

What is a distributed denial-of-service attack?

A distributed denial-of-service (DDoS) attack occurs when multiple machines are operating together to attack one target. DDoS attackers often leverage the use of a botnet—a group of hijacked internet-connected devices to carry out large scale attacks. Attackers take advantage of security vulnerabilities or device weaknesses to control numerous devices using command and control software. Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack.

Botnets—made up of compromised devices—may also be rented out to other potential attackers. Often the botnet is made available to “attack-for-hire” services, which allow unskilled users to launch DDoS attacks.

DDoS allows for exponentially more requests to be sent to the target, therefore increasing the attack power. It also increases the difficulty of attribution, as the true source of the attack is harder to identify.

DDoS attacks have increased in magnitude as more and more devices come online through the Internet of Things (IoT) (see Securing the Internet of Things). IoT devices often use default passwords and do not have sound security postures, making them vulnerable to compromise and exploitation. Infection of IoT devices often goes unnoticed by users, and an attacker could easily compromise hundreds of thousands of these devices to conduct a high-scale attack without the device owners’ knowledge.

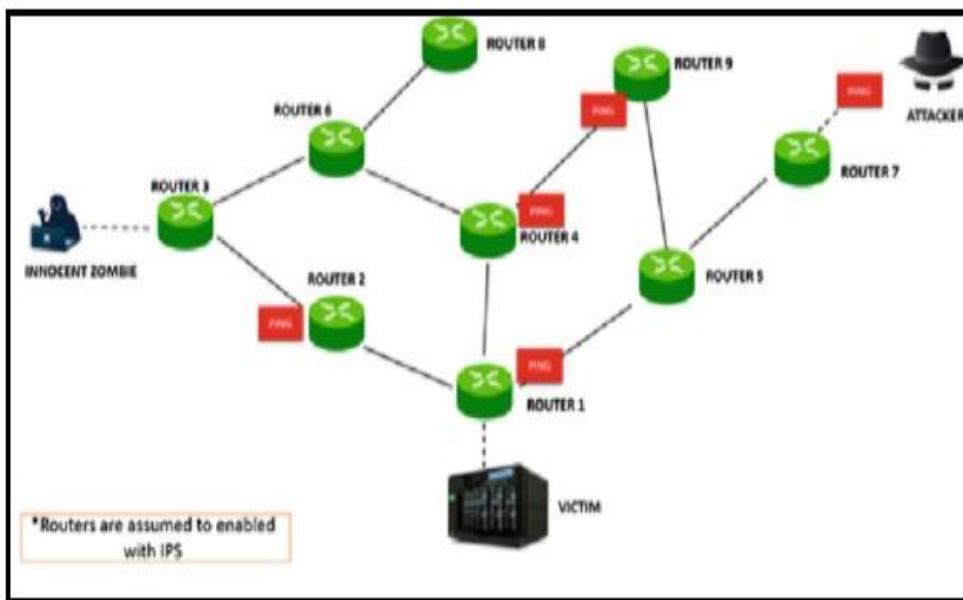


Image Source:-

- **SYN Flood:** - This is an acute DDoS attack where the attackers send unlimited SYN requests from spoofed IP addresses and then ignore the ACK response. When the host cannot receive the ACK response, it continues to wait for the acknowledgment, rendering the service unavailable to the users. The SYN flood exploits the three-way handshake connection sequence of the TCP-IP model, where the SYN request has to be acknowledged with an ACK response.

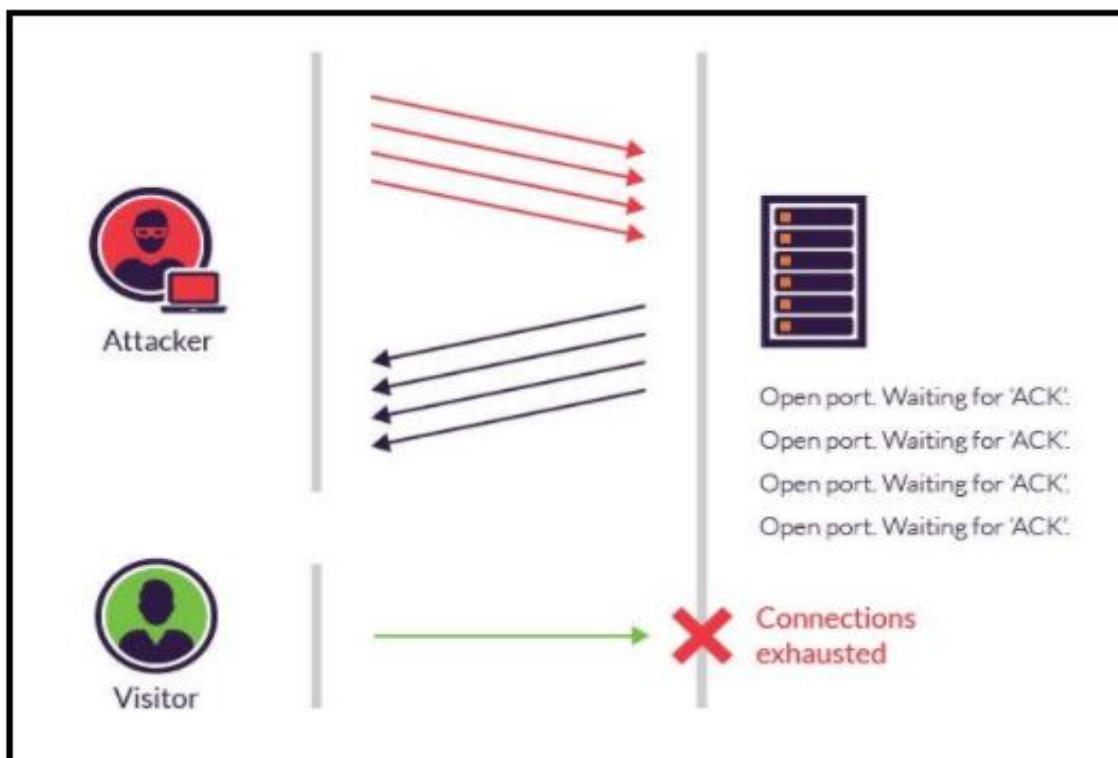
What is common denial-of-service attacks?

There are many different methods for carrying out a DoS attack. The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DoS attack,

the attacker sends several requests to the target server, overloading it with traffic. These service requests are illegitimate and have fabricated return addresses, which mislead the server when it tries to authenticate the requestor. As the junk requests are processed constantly, the server is overwhelmed, which causes a DoS condition to legitimate requestors.

- In a **Smurf Attack**, the attacker sends Internet Control Message Protocol broadcast packets to a number of hosts with a spoofed source Internet Protocol (IP) address that belongs to the target machine. The recipients of these spoofed packets will then respond, and the targeted host will be flooded with those responses.
- A **SYN flood** occurs when an attacker sends a request to connect to the target server but does not complete the connection through what is known as a three-way handshake—a method used in a Transmission Control Protocol (TCP)/IP network to create a connection between a local host/client and server. The incomplete handshake leaves the connected port in an occupied status and unavailable for further requests. An attacker will continue to send requests, saturating all open ports, so that legitimate users cannot connect.

Individual networks may be affected by DoS attacks without being directly targeted. If the network's internet service provider (ISP) or cloud service provider has been targeted and attacked, the network will also experience a loss of service.



What is Denial of Service (SUMMARY)

Denial of Service (DoS): is an attack that occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.

There are 3 ways to perform a DoS attack; Normal, Reflection and Pulsing (Intermittent attack).

3 outputs can happen:

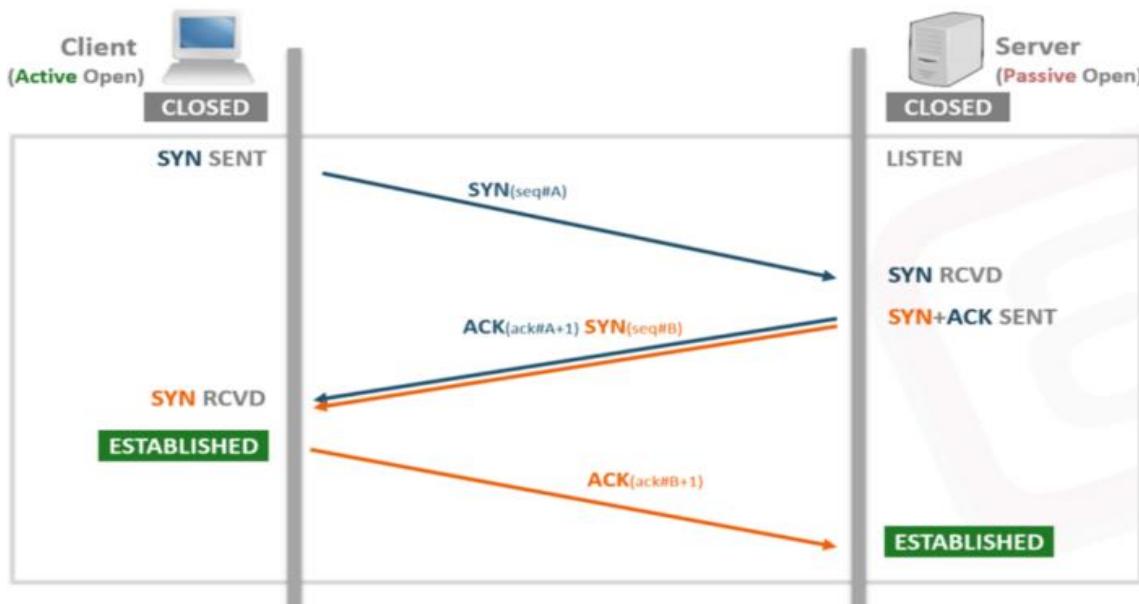
- Choking access to the service — the path is congested that the legitimate request can't go through.
- Disabling the service typically by sending a malformed packet.
- Downgrading service performance by exhausting host resources.

3 techniques are used to achieve DoS:

- Network-based attacks: TCP SYN flood, Smurf (ICMP) flood, UDP flood, ARP flood, DNS reflection...
- Wireless attacks: De-authentication, routing congesting...
- Application attacks: HTTP services, FTP services, SIP services...

Infrastructure Denial of Service

TCP SYN flood is the most common form of DoS. **TCP 3-way handshake : SYN — SYN-ACK — ACK**. A TCP SYN flood happens when the TCP handshake doesn't complete properly.



TCP 3-way Handshake

HPing3 is command tool in Kali Linux used to perform a DoS attack.

A reflection attack happens when a source sends the packet to an intermediate system and that system responds not to the source but to the target. This happens when the attacker spoofs the IP address of the target before sending packets, so when the intermediate system replies it replies to the spoofed IP address hence attacking the target.

Hyenae is a highly flexible platform independent network packet generator. It allows you to reproduce several MITM, DoS and DDoS attack scenarios.

Smurf (ICMP) flooding attack is a form of reflection attack, it targets the broadcast address on the reflector system hence using all the responding machines on that system.

LOIC is used to generate a massive amount of network traffic. It floods the target with TCP, UDP or HTTP packets. Single attacker is not sufficient, it requires a botnet. It has plugins like DOS attack plugin which scan the target to find an open port and flood it with SYN packets. Or it can be used to perform ARP poisoning.

An amplification attack takes place when we send packets to a server then we get a much larger packets back in reply.

NTP is a protocol designed to synchronize the clocks of computers over a network.

Memcached software is a free and open-source distributed memory object caching system intended for use in speeding up dynamic web applications by alleviating database load.

An attacker can use Memcached to store a large packet and restore it in a DoS attack. They can also use it in ransomware & amplification DoS attacks.

Wireless Denial of Service

Attacking a Wireless host is basically performing a de-authentication attack were denying legitimate users from authenticating to the host. **Aireplay** is a tool that can be used for this type of attacks.

Application Denial of Service

Websites are often a target for a Dos attack. **GoldenEye** is a tool used to perform such attacks, basically it creates a lot of open sockets in the target system consuming all available sockets. This type of attack is called HTTP flooding or webserver DoS attack.

SwitchBlade is an open-source tool provided by OWASP used by penetration testers to test Webapps.

BlackEnergy started as a web-based distributed DDoS tool. But it got some updates and it is now known as BlackEnergy2 which supports a wide range of attacks.

BlackEnergy is a sophisticated Botnet, it actively hides from malware detection systems using encryption, it injects code into system processes and can handle multiple IP addresses per host.

How is works:

It allocates virtual memory, copies the decryptor code to memory and gives it control. It creates a decryptor driver with a random name and DDoS extension in System32/Drivers. A service is also created for the driver. The driver has a 16-byte key that is used to create another key used to decrypt the injection archive using RC4. Then the driver locates svchost.exe and allocates memory in its address space and injects the malicious code. The DLL, injected into svchost.exe contain two addresses for its command-and-control server (in case one of them is down). It sends an HTTP request to the command-and-control server, which responds with an encrypted XML configuration file. This contains instructions on the targets for the DDoS and the attack modules to use. then the attack starts.

BlackEnergy can run multiple attacks with different commands like:

- icmp: ICMP ping flood.
- syn: TCP SYN flood.
- udp: UDP traffic flood.
- http: HTTP GET request flooder.
- data: binary packet flooder.
- dns: DNS request flooder.

FTP service is also a possible target for a DoS attack.

RangeAmp attacks on the CDN: The attack uses HTTP to amplify web traffic and bring down Content Delivery Networks using a flaw in the HTTP range request.

SIP Service attacks

VOIP services use a SIP proxy server to send data packets. **SIP is Session Initiation Protocol.**

to establish a SIP session there is a handshake to be performed. When the SIP proxy server receives a SIP invite, it looks for the number in its registry. If the number does exist the server passes the invite request. If the two numbers communicate, the acknowledgments are made.

Flooding a SIP server happens by flooding with a huge number of invite requests.



Ransomware

An example of ransomware is AIDS Ransomware: it was on a diskette (back in 1989), it executed, hid directories and encrypted files then asked for payments to be sent to a PO box in Panama.

Ransomware uses cryptography to encrypt the files and victims usually chose to pay as it is easier than pursuit and prosecution.

Crypto locker: is a malware threat. It is a Trojan horse that infects your computer and then searches for files to encrypt. This includes anything on your hard drives and all connected media. Crypto locker ransomware is distributed via botnets, drops with a randomly generated name, inserts startup command into registry (to insure it will restart after a reboot). If the operation is successful, it will generate a public key and bitcoin address, a wallpaper is generated with information how to pay the ransom. Victims are given a deadline to pay the ransom, otherwise their files will be deleted.

Another example of Ransomware is **Petya**. It encrypts the master file table on the victim's Windows system; therefore, they cannot access any of their files. First thing, it changes the master boot record to disable booting in safe mode. It then encrypts the master file and renders all files on the system inaccessible. A solution was found for this malware and the key to decrypt the file can be extracted.

Mitigation Techniques

There are two approaches to achieve mitigation: Mitigation by design and Operational mitigation:

Mitigation by design:

- Priority-based servicing
- Egress filtering
- Ingress filtering

Operational mitigation:

- IP address verification
- Rate limiting
- ACLs
- Detecting known malicious threats and dropping them.
- Defecting traffic anomalies.

Examples of commercial Anti-Dos services:

- CloudFlare
- Akamai
- Project Shield

PeerShark is a tool used to detect P2P attacks and Botnets.

IoT has brought a wide range of problematic settings which makes the security difficult like:

- Communication protocols and mobility.
- Shared or default passwords.
- Physically unprotected.
- Unreliable authentication.
- Insecure access protocols.
- Lack of firmware updates.

Conclusion

As we've seen, Cybersecurity is critical to implement in every IT system, irrespective of the purpose of the usage. A Cyberattacks impact is as devastating as a terrorist attack on a country, and it can threaten all important data and sources. The loss of such confidentiality can result in any business, or even country, whose security has been compromised. The mitigation of DOS and DDOS attacks have been performed by various Cloud Service providers, such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP). Security has always been a major issue in IT systems, and confidentiality should be protected by all means.

Spoofing

What is spoofing?

"I am serious. And don't call me Shirley."

Yes, it's the famous line from the endlessly quotable 1980 film, *Airplane*. Films like *Airplane*, *Spaceballs*, and *The Naked Gun*, and songs from "Weird Al" Yankovic, and Flight of the Conchords are all spoofs. Spoofs imitate other movies, artists, and genres for comedic effect, and we love them for it. But there's another kind of spoof, and it's designed to hurt us, rather than entertain us.

Spoofing definition



Spoofing, as it pertains to cybersecurity, is when someone or something pretends to be something else in an attempt to gain our confidence, get access to our systems, steal data, steal money, or spread malware. Spoofing attacks come in many forms, primarily:

- Email spoofing
- Website and/or URL spoofing
- Caller ID spoofing
- Text message spoofing
- GPS spoofing
- Man-in-the-middle attacks
- Extension spoofing
- IP spoofing
- Facial spoofing

So how do the cybercriminals fool us? Often times, merely invoking the name of a big, trusted organization is enough to get us to give up information or take some kind of action. For example, a spoofed email from PayPal or Amazon might inquire about purchases you never made. Concerned about your account, you might be motivated to click the included link.

From that malicious link, scammers will send you to a malware download or a faked login page—complete with a familiar logo and spoofed URL—for the purpose of harvesting your username and password.

There are many more ways a spoofing attack can play out. In all of them, fraudsters rely on the naiveté of their victims. If you never doubt the legitimacy of a website and never suspect an email of being faked, then you're likely to become a victim of a spoofing attack at some point.

To that end, this article is all about spoofing. We'll educate you on the types of spoofs, how spoofing works, how to discern legitimate emails and websites from fake ones, and how to avoid becoming a target for fraudsters.

Now, let's get serious about spoofing.

“Spoofing, as it pertains to cybersecurity, is when someone or something pretends to be something else in an attempt to gain our confidence, get access to our systems, steal data, steal money, or spread malware.”

Types of spoofing

Email spoofing

Email spoofing. Strictly speaking, email spoofing is the act of sending emails with false sender addresses, usually as part of a phishing attack designed to steal your information, infect your computer with malware or just ask for money. Typical payloads for malicious emails include

ransomware, adware, cryptojackers, Trojans (like Emotet), or malware that enslaves your computer in a botnet (see DDoS).

But a spoofed email address isn't always enough to fool the average person. Imagine getting a phishing email with what looks like a Facebook address in the sender field, but the body of the email is written in basic text, no design or HTML to speak of—not even a logo. That's not something we're accustomed to receiving from Facebook, and it should raise some red flags. Accordingly, phishing emails will typically include a combination of deceptive features:

- False sender address designed to look like it's from someone you know and trust—possibly a friend, coworker, family member, or company you do business with. In a recent twist, a bug in Gmail allows scammers to send emails with no sender address—at least not one your average user can see. It takes some technical know-how to see the malicious string of code used to make the "From" field appear blank.
- In the case of a company or organization, the email may include familiar branding; e.g. logo, colors, font, call to action button, etc.
- Spear phishing attacks target an individual or small group within a company and will include personalized language and address the recipient by name.
- Typos—lots of them. Try as they might to fool us, email scammers don't spend much time proofreading their own work. Email spoofs often have typos—or worse. If the email looks like someone translated the text through Google Translate, chances are it was. Be wary of unusual sentence constructions. Here's an example: "Greetings sir. If you please, make certain this data is well and good." Bizarre sentences like that should give you a reason to be suspicious unless big tech companies are hiring time travelling writers from the Victorian era.

Email spoofing plays a critical role in sextortion scams. These scams trick us into thinking our webcams (which have been around for 25 years, can you believe it?) have been hijacked with spyware and used to record us watching porn. These spoofed emails will say something like "I've been watching you watch porn," which is an incredibly weird thing to say. Who's the real creep in this scenario? The scammers then demand some amount of Bitcoin or else they will send the video to all your contacts. To create the impression of legitimacy the emails will also include an outdated password from some previous data breach. The spoof comes into play when the scammers disguise the email sender field to look as if it's being sent from your supposedly breached email account. Rest assured, chances are no one is actually watching you.

Website spoofing

Website spoofing is all about making a malicious website look like a legitimate one. The spoofed site will look like the login page for a website you frequent—down to the branding, user interface, and even a spoofed domain name that looks the same at first glance. Cybercriminals use spoofed websites to capture your username and password (aka login spoofing) or drop malware onto your computer (a drive-by download). A spoofed website will generally be used in conjunction with an email spoof, in which the email will link to the website.

It's also worth noting that a spoofed website isn't the same as a hacked website. In the case of a website hacking, the real website has been compromised and taken over by cybercriminals—no spoofing or faking involved. Likewise, malvertising is its own brand of malware. In this case,

cybercriminals have taken advantage of legitimate advertising channels to display malicious ads on trusted websites. These ads secretly load malware onto the victim's computer.

Website Spoofing

Applications such as the Social Engineering Toolkit (SET), shown below, exist to create convincing websites. Many times, these websites have seemingly legitimate names that are often convincing variations of legitimate sites.



Figure 3: The Social Engineering Toolkit (SET)

For example, an attacker may send a text or email directing the victim to reset a password at www.comptial.com, instead of the legitimate website www.comptia.org.

It is even possible to obtain encryption certificates for spoofed websites. This can make the ruse even more convincing to a distracted user.

Caller ID spoofing

Caller ID spoofing happens when scammers fool your caller ID by making the call appear to be coming from somewhere it isn't. Scammers have learned that you're more likely to answer the phone if the caller ID shows an area code the same or near your own. In some cases, scammers will even spoof the first few digits of your phone number in addition to the area code to create the impression that the call is originating from your neighborhood (aka neighbor spoofing). As it happens, [Malwarebytes for Android](#) and [Malwarebytes for iOS](#) block incoming scam calls, making caller ID spoofing a thing of the past.

Text message spoofing

Text message spoofing or SMS spoofing is sending a text message with someone else's phone number or sender ID. If you've ever sent a text message from your laptop, you've spoofed your own phone number in order to send the text, because the text did not actually originate from your phone. Companies frequently spoof their own numbers, for the purposes of marketing and convenience to the consumer, by replacing the long number with a short and easy to remember alphanumeric sender ID. Scammers do the same thing—hide their true identity behind an alphanumeric sender ID, often posing as a legitimate company or organization. The spoofed texts will often include links to [SMS phishing sites \(smishing\)](#) or malware downloads.

Text message scammers are now taking advantage of the healthy job market by posing as staffing agencies, sending victims to-good-to-be-true job offers. [In one example](#), a work from home position at Amazon included a "Brand new Toyota Corolla." First of all, why does one need a company car if they're working from home? Second, is a Toyota "Corrola" a generic version of the Toyota Corolla? Nice try, scammers.

GPS spoofing

GPS spoofing occurs when you trick your device's GPS into thinking you're in one location, when you're actually in another location. Why on Earth would anyone want to GPS spoof? Two words: Pokémon GO. Using GPS spoofing, Pokémon GO cheaters are able to make the popular mobile game think they're in proximity to an in-game gym and take over that gym (winning in-game currency). In fact, the cheaters are actually in a completely different location—or country. Similarly, videos can be found on YouTube showing Pokémon GO players catching various Pokémon without ever leaving their house. While GPS spoofing may seem like child's play, there are other more nefarious implications to consider. By some accounts, [Russia is already using GPS spoofing](#) to misdirect naval vessels as a trial run for future cyberwarfare attacks on United States aerial drones. Hitting closer to home, hackers could even spoof the GPS in your car and send you to the wrong destination, or worse, [send you into oncoming traffic](#).

Man-in-the-middle (MitM) attack

Man-in-the-middle (MitM) attack. You like that free Wi-Fi at your local coffee shop? Have you considered what would happen if a cybercriminal hacked the Wi-Fi or created another fraudulent Wi-Fi network in the same location? In either case, you have a perfect setup for a



man-in-the-middle attack, so named because cybercriminals are able to intercept web traffic between two parties. The spoof comes into play when the criminals alter the communication between the parties to reroute funds or solicit sensitive personal information like credit card numbers or logins.

Side note: While MitM attacks usually intercept data in the Wi-Fi network, another form of MitM attack intercepts the data in the browser. This is called a man in the browser (MitB) attack.

Extension spoofing

Extension spoofing occurs when cybercriminals need to disguise executable malware files. One common extension spoofing trick criminals like to use is to name the file something along the lines of "filename.txt.exe". The criminals know file extensions are hidden by default in Windows so to the average Windows user this executable file will appear as "filename.txt".

IP spoofing

IP spoofing is used when someone wants to hide or disguise the location from which they're sending or requesting data online. As it applies to cyberthreats, IP address spoofing is used in distributed denial of service attacks (DDoS) to prevent malicious traffic from being filtered out and to hide the attacker's location.

It is relatively easy to create – or spoof – any element of a traditional IP address. As a result, it is possible for attackers to thwart detection and trick people or machines into revealing information or unwittingly engaging in attacks.

For example, check out the following command created on a Linux system:

```
james@stangernet1:~/Desktop$ hping3 -a 10.18.21.24 192.168.55.56 -S -q -p 80 --flood[DM4]
```

Basically, this command is telling a Linux system to send a flood of TCP SYN packets to a victim computer with the IP address of 192.168.55.56. This is an example of how a Denial of Service (DoS) attack is conducted. Similarly, when multiple systems work together to target one system, that's known as a Distributed Denial of Service (DDoS) attack.

Going back to the above example, the command also tells the Linux system to spoof the source IP address of all of the packets. This flood of packets will have the fake source IP address of 10.18.21.24.26.

The diagram below shows the results from the above command.



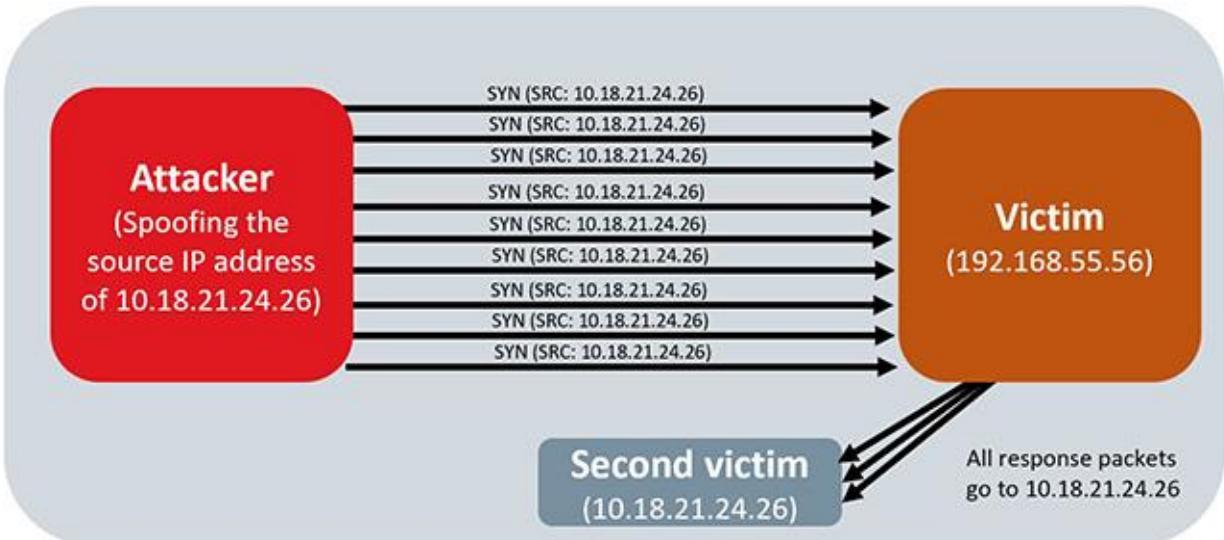


Figure 4: Diagram of a DoS attack

In this attack, a flood of partial TCP synchronization commands with a spoofed source address (10.18.21.24.26) have been sent. The victim computer receives this flood of packets, and then responds to what it thinks is the correct IP address.

But because the source address is a fake, the victim system can't respond properly. Instead, the victim will dutifully process all of these thousands of fake TCP packets again and again. Eventually the victim system will become overwhelmed and will no longer be able to work.

Plus, any responses from the victim will go to a third IP address. That third IP address might be real or fake. If the third IP address is real, then that system could become an additional victim.

How to Identify and Protect Against Spoofing Attacks

The primary way spoofers hack organizations is by tricking employees. Thankfully, most organizations have active cybersecurity programs to avoid these things.

The IT industry has created many solutions to combat malware and spoofing – and it's always creating new ones. For example, the IPv6 specification includes effective authentication and encryption mechanisms.

The IT industry continues to adopt two-factor authentication (2FA), which is where you combine the use of biometric information (e.g., facial recognition, fingerprints) with passwords or a physical token. The use of 2FA can help reduce facial recognition system hacks, as well as phishing.

The best way to protect yourself against phishing and caller ID spoofing is to educate yourself about how to identify fake emails and websites and how to respond to unsolicited offers and demands. This is why smart organizations have regular end user training campaigns.

IT professionals can use sophisticated intrusion detection applications and security information and event management (SIEM) tools. Many times, IT pros use IP tracking services, such as [IP Tracker](#), [IP2Location](#) and [InfoSniper](#) to track packets.

The screenshot shows a web page titled "Trace IP With IP Tracker". It has two main sections: "Find IP Address - What Is My IP Location?" and "Geolocation Show on Map".

Find IP Address - What Is My IP Location?

- My IP: 68.233.228.235
[My Public IP] [IP Lookup - IP Blacklist Check](#)
- Reverse DNS: 235.228.233.68.in-addr.ARPA
- Host Address: server.ip-tracker.org
[Domain To Location - Domain Country - Domain To IP](#)
- Nameservers: cleo.ns.cloudflare.com >> 173.245.59.89
melinda.ns.cloudflare.com >> 173.245.58.198
- Remote Port: 52345
- Proxy Checker Header: Not Detected
- Browser Referer: Direct
- Computer System: Windows NT 10.0 (Windows 10.0)
User Agent: Chrome 83.0.4103.61
Main Version Number: 83.0;
Layout Engine: Blink;
Engine Version: 537.36
- Browser Type: en-US,en;q=0.9
- Tracked Location for: 68.233.228.235**
- Continent: North America (NA)
- Country: United States (US)
- Capital: Washington
- State: Florida
- City: Tampa
- Postal: 33614
- Area: 813
- Metro: 539
- ISP: NOC4Hosts

Figure 5: The IP Tracker website

But, the primary way IT pros can guard against spoofing is to carefully learn all the details about the underlying network protocols and best practices necessary to run a network. This means that you should learn about the TCP/IP family of protocols, which include the Transmission Control Protocol (TCP), the Internet Protocol (IP), the User Datagram Protocol (UDP) and many others.

Facial spoofing

Facial spoofing. The latest form of spoof might be the most personal, because of the implications it carries for the future of technology and our personal lives. As it stands, facial ID technology is fairly limited. We use our faces to unlock our mobile devices and laptops, and not much else. Soon enough though, we might find ourselves making payments and signing documents with our faces. Imagine the ramifications when you can open up a line of credit with your face. Scary stuff. Researchers have demonstrated how 3D facial models built from your pictures on social media can already be used to hack into a device locked via facial ID. Taking things a step further, the Malwarebytes Labs blog reported on deepfake technology being used to create fake news videos and fake sex tapes, featuring the voices and likenesses of politicians and celebrities, respectively.

How does spoofing work?

Okay, so we've explored the various forms of spoofing and glossed over the mechanics of each. In the case of email spoofing, however, there's a bit more worth going over. There are a few ways cybercriminals are able to hide their true identity in an email spoof. The most foolproof option is to hack an unsecure mail server. In this case the email is, from a technical standpoint, coming from the purported sender.

The low-tech option is to simply put whatever address in the "From" field. The only problem is if the victim replies or the email cannot be sent for some reason, the response will go to whoever is listed in the "From" field—not the attacker. This technique is commonly used by spammers to use legitimate emails to get past spam filters. If you've ever received responses to emails you've never sent this is one possible reason why, other than your email account being hacked. This is called backscatter or collateral spam.

Another common way attackers spoof emails is by registering a domain name similar to the one they're trying to spoof in what's called a homograph attack or visual spoofing. For example, "rnalwarebytes.com". Note the use of the number "1" instead of the letter "l". Also note the use of the letters "r" and "n" used to fake the letter "m". This has the added benefit of giving the attacker a domain they can use for a creating a spoofed website.

Whatever the spoof may be, it's not always enough to just throw a fake website or email out into the world and hope for the best. Successful spoofing requires a combination of the spoof itself and social engineering. Social engineering refers to the methods cybercriminals use to trick us into giving up personal information, clicking a malicious link, or opening a malware-laden attachment. There are many plays in the social engineering playbook. Cybercriminals are counting on the vulnerabilities we all carry as human beings, such as fear, naiveté, greed, and vanity, to convince us to do something we really shouldn't be doing. In the case of a sextortion scam, for instance, you might send the scammer Bitcoin because you fear your proverbial dirty laundry being aired out for everyone to see.

Human vulnerabilities aren't always bad either. Curiosity and empathy are generally good qualities to have, but criminals love to target people who exhibit them. Case in point, the



stranded grandchildren scam, in which a loved one is allegedly in jail or in the hospital in a foreign country and needs money fast. An email or text might read, "Grandpa Joe, I've been arrested for smuggling drugs in [insert name of country]. Please send funds, oh and btw, don't tell mom and dad. You're the best [three happy face winking emojis]!" Here the scammers are counting on the grandparent's general lack of knowledge about where his grandson is at any given time.

"Successful spoofing requires a combination of the spoof itself and social engineering. Social engineering refers to the methods cybercriminals use to trick us into giving up personal information, clicking a malicious link, or opening a malware-laden attachment."

How do I detect spoofing?

Here are the signs you're being spoofed. If you see these indicators, hit delete, click the back button, close out your browser, do not pass go.

Website spoofing

- No lock symbol or green bar. All secure, reputable websites need to have an SSL certificate, which means a third-party certification authority has verified that the web address actually belongs to the organization being verified. One thing to keep in mind. While a site may have a padlock, that doesn't mean it's the real deal. Just remember, nothing is 100 percent safe on the Internet.
- The website is not using file encryption. HTTP, or Hypertext Transfer Protocol, is as old as the Internet and it refers to the rules used when sharing files across the web. Legitimate websites will almost always use HTTPS, the encrypted version of HTTP, when transferring data back and forth. If you're on a login page and you see "http" as opposed to "https" in your browser's address bar, you should be suspicious.
- Use a password manager. A password manager like 1Password will autofill your login credentials for any legitimate website you save in your password vault. However, if you navigate to a spoofed website your password manager will not recognize the site and not fill in the username and password fields for you—a good sign you're being spoofed.

Email spoofing

- Doublecheck the sender's address. As mentioned, scammers will register fake domains that look very similar to legitimate ones.
- Google the contents of the email. A quick search might be able to show you if a known phishing email is making its way around the web.
- Embedded links have unusual URLs. You can check URLs before clicking by hovering over them with your cursor.
- Typos, bad grammar, and unusual syntax. Scammers don't proofread their work.
- The contents of the email are too good to be true.
- There are attachments. Be wary of attachments—particularly when coming from an unknown sender.

Caller ID spoofing

- Caller ID is easily spoofed. It's a sad state of affairs when our landlines have become a hotbed of scam calls. It's especially troubling when you consider that the majority of people who still have landlines are the elderly—the group most susceptible to scam calls. Let calls to the landline from unknown callers go to voicemail or the answering machine.

How can I protect against spoofing?

First and foremost, you should learn how to spot a spoofing attack. In case you skipped over the "How do I detect spoofing?" section you should go back and read it now.

Turn on your spam filter. This will stop the majority of spoofed emails from ever making it to your inbox.

Don't click on links or open attachments in emails if the email is coming from an unknown sender. If there's a chance the email is legitimate, contact the sender through some other channel and confirm the contents of the email.

Log in through a separate tab or window. If you get a suspicious email or text message, requesting that you log in to your account and take some kind of action, e.g., verify your information, don't click the provided link. Instead, open another tab or window and navigate to the site directly. Alternatively, log in through the dedicated app on your phone or tablet.

Pick up the phone. If you've received a suspicious email, supposedly from someone you know, don't be afraid to call or text the sender and confirm that they, indeed, sent the email. This advice is especially true if the sender makes an out-of-character request like, "Hey, will you please buy 100 iTunes gift cards and email me the card numbers? Thanks, Your Boss."

Show file extensions in Windows. Windows does not show file extensions by default, but you can change that setting by clicking the "View" tab in File Explorer, then checking the box to show file extensions. While this won't stop cybercriminals from spoofing file extensions, at least you'll be able to see the spoofed extensions and avoid opening those malicious files.

Invest in a good cybersecurity program. In the event that you click on a bad link or attachment, don't worry, a good cybersecurity program will be able to alert you to the threat, stop the download and prevent malware from getting a foothold on your system or network. Malwarebytes, for example, has cybersecurity products for Windows, Mac, and Chromebook. Business users, we've got you covered too.

Malwarebytes for iOS and Malwarebytes for Android will block calls and text messages from known scam numbers. This is a great fix for parents and grandparents still relying on an old landline. Cut the cord and set them up with a basic smartphone with Malwarebytes already installed.

Networking summary

Short Summary.

- A computer network is a group of two or more interconnected computer systems
- Computer networks help you to connect with multiple computers together to send and receive information
- Switches work as a controller which connects computers, printers, and other hardware devices
- Routers help you to connect with multiple networks. It enables you to share a single internet connection and saves money
- Servers are computers that hold shared programs, files, and the network operating system
- Clients are computer device which accesses and uses the network and shares network resources
- Hub is a device that splits a network connection into multiple computers.
- Access points allow devices to connect to the wireless network without cables
- Network Interface card sends, receives data and controls data flow between the computer and the network
- A protocol is the set of defined rules which allows two entities to communicate across the network
- Hostname, IP Address, DNS Server, and host are important unique identifiers of computer networks.
- ARP stands for Address Resolution Protocol
- RAR Reverse Address Resolution Protocol gives an IP address of the device with given a physical address as input.
- Computer network helps you to share expensive software's and database among network participants
- The biggest drawback of installing computer network is that its initial investment for hardware and software can be costly for initial set-up
- Types of connections in computer networks can be categorized according to their size as well as their purpose
- PAN is a computer network which generally consists of a computer, mobile, or personal digital assistant
- LAN (local area network) is a group of computer and peripheral devices which are connected in a limited area
- WAN (Wide Area Network) is another important computer network that is spread across a large geographical area
- A metropolitan area network or MAN is consisting of a computer network across an entire city, college campus, or a small region
- WLAN is a wireless local area network that helps you to link single or multiple devices using. It uses wireless communication within a limited area like home, school, or office building.
- SAN is a storage area network is a type of network which allows consolidated, block-level data storage
- System area network offers high-speed connection in server-to-server applications, storage area networks, and processor-to-processor applications

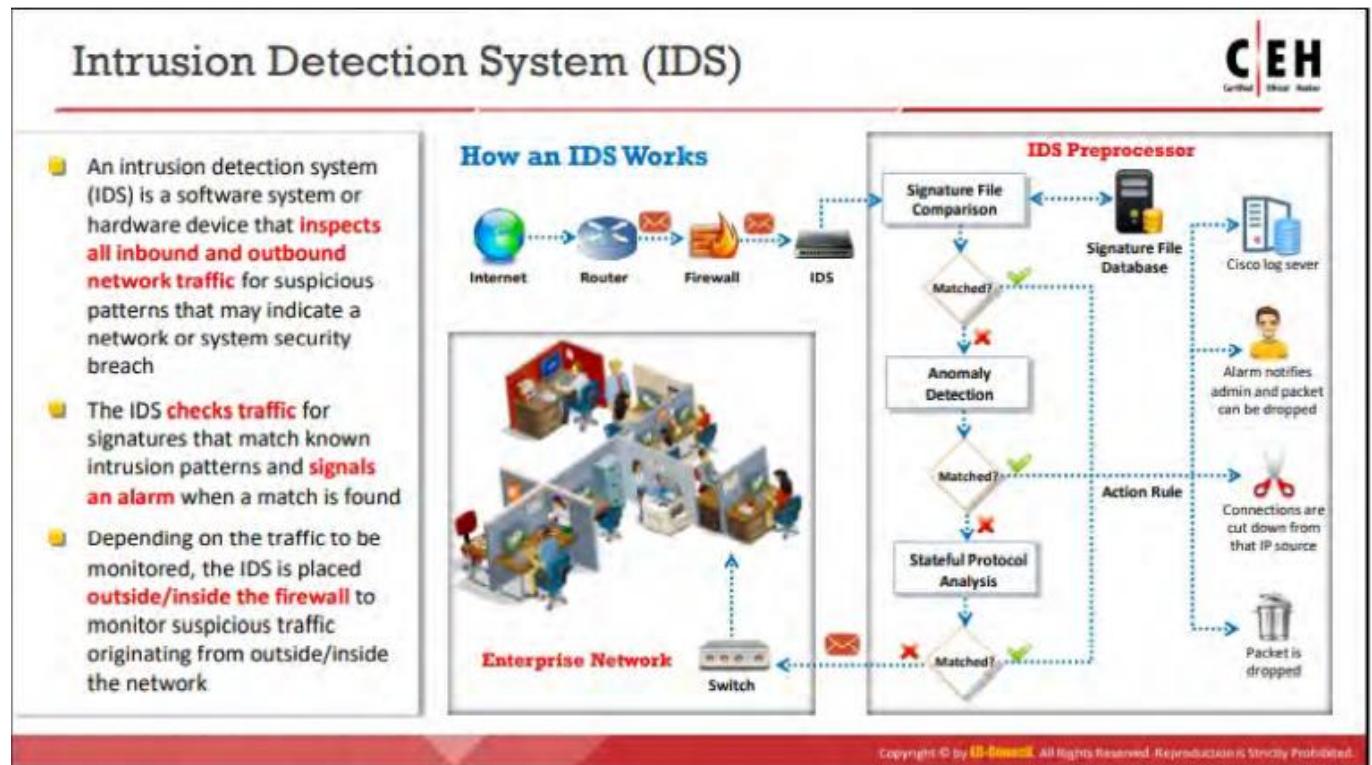
- POLAN is a networking technology which helps you to integrate into structured cabling
- Home network (HAN) is always built using two or more interconnected computers to form a local area network (LAN) within the home
- Enterprise private network (EPN) networks are built and owned by businesses that want to securely connect various locations
- Campus area network (CAN) is made up of an interconnection of LANs in a specific geographical area
- A VPN is a private network which uses a public network to connect remote sites or users together
- The OSI Model is a logical and conceptual model that defines network communication which is used by systems open to interconnection and communication with other systems
- In OSI model, layer should only be created where the definite levels of abstraction are needed.
- OSI layer helps you to understand communication over a network
- In 1984, the OSI architecture was formally adopted by ISO as an international standard
- The full form of TCP/IP model explained as Transmission Control Protocol/ Internet Protocol.
- TCP supports flexible architecture
- Four TCP/IP model layers are 1) Application Layer 2) Transport Layer 3) Internet Layer 4) Network Interface
- Application layer interacts with an application program, which is the highest level of OSI model.
- Internet layer is a second layer of the TCP/IP model. It is also known as a network layer.
- Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system.
- Network Interface Layer is this layer of the four-layer TCP/IP model. This layer is also called a network access layer.
- OSI model is developed by ISO (International Standard Organization) whereas TCP/IP model is developed by ARPANET (Advanced Research Project Agency Network).
- An Internet Protocol address that is also known as an IP address is a numerical label.
- HTTP is a foundation of the World Wide Web.
- SMTP stands for Simple mail transfer protocol which supports the e-mail is known as a simple mail transfer
- SNMP stands for Simple Network Management Protocol.
- DNS stands for Domain Name System.
- TELNET stands for Terminal Network. It establishes the connection between the local and remote computer
- FTP stands for File Transfer Protocol. It is a mostly used standard protocol for transmitting the files from one machine to another.
- The biggest benefit of TCP/IP model is that it helps you to establish/set up a connection between different types of computers.
- TCP/IP is a complicated model to set up and manage.
- TCP 3-way handshake or three-way handshake or TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between server and client.
- Syn use to initiate and establish a connection
- ACK helps to confirm to the other side that it has received the SYN.

- SYN-ACK is a SYN message from local device and ACK of the earlier packet.
- FIN is used for terminating a connection.
- TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server
- In the first step, the client establishes a connection with a server
- In this second step, the server responds to the client request with SYN-ACK signal set
- In this final step, the client acknowledges the response of the Server
- TCP automatically terminates the connection between two separate endpoints.
- VLAN is defined as a custom network which is created from one or more local area networks.
- VLAN in networking are identified by a number.
- A Valid range is 1-4094. On a VLAN switch, you assign ports with the proper VLAN number.
- Virtual LANs offer structure for making groups of devices, even if their networks are different.
- The main difference between LAN and VLAN is that In LAN, the network packet is advertised to each and every device Whereas in VLAN, the network packet is sent to only a specific broadcast domain.
- The primary advantage of VLAN is that it reduces the size of broadcast domains.
- The drawback of VLAN is that an injected packet may lead to a cyber-attack.
- VLAN is used when you have 200+ devices on your LAN.

05) Evading IDS, IPS, Firewall and Honeypots

Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system.



Intrusion Detection Systems (IDS) use known signatures to detect intrusions and protect your system. IDS systems require regular signature updates to be capable to identify and protect against the latest attacks.

It can be used in two areas:

- **Network based devices.** (Network deployment with this type IDS scans all traffic looking for anomalous patterns in the traffic behavior anti-virus.)

- **Host based systems.** (IDS applications runs on a local hosts by examining application specific logs looking for anomalies in log patterns, most are installed in a work station or server)

IDS send alerts when an intrusion is detected to the administrators for them to take action.

An Intrusion Prevention System (IPS) is an IDS that can block intrusion on its own. In enterprises, IPS is first executed in monitoring mode to learn normal traffic then the prevention stage is activated to protect the system.

Anomaly Detection System (ADS) is a device used to detect malicious behavior. They build a model of normal data flows then they detect what they considered an anomaly comparing to what they learned.

One of the most common problems with IDS is their false-positive, when they detect legitimate activity as an intrusion or their false-negative where they neglect an intrusion which compromises the system.

To protect against malicious websites there are 2 techniques:

- **Blacklisting:** prohibiting access to black listed websites it only protects against known malicious websites.
- **Whitelisting:** allowing access to only known websites and blocking the rest this is a much more effective technique.

Snort is an IDS built on top of TCP dump, includes packet analytics and detection rules and has plugin capability for pre- and post-analysis.

Security Onion is another example of IDS that provides a comprehensive intrusion detection, network security monitoring, and log management solution.

Reputation is another technique in combating malicious activities. It's a logical extension of threat intelligence in which the collective intelligence is able to provide a reputational feed to devices to complement the signature-based ID as feeds. Reputation-based intrusion detection is a powerful feature that can help prevent threats from malware and zero-day attacks by sharing collective intelligence.

Einstein was developed by the US Computer Emergency Readiness Team as an intrusion detection system for monitoring the network gateways of government departments and agencies for unauthorized traffic. But it failed because of its low detection rate.

Types of intrusion detection systems

Intrusion detection systems come in different variations and can detect suspicious activity using different methods and capabilities. Usually, the different flavors of IDSs can be classified by five types:

Network intrusion detection system (NIDS)

A network intrusion detection system (NIDS) is set up across the network, on tactical points, where it monitors inbound and outbound traffic to and from all devices on a network. It examines traffic and matches it with indicators of known attacks. When anomalous activity is detected, an alert is generated for the incident to be examined further. Uses SYN, FIN, NULL, XMAS and ODDBALL

Host intrusion detection system (HIDS)

A host intrusion detection system (HIDS) runs on all of a network's hosts and devices that have access to the internet as well as the internal network. It monitors the operations of individual hosts and tracks the status of all files on an endpoint and detects any activity, such as deletion or modification of system files. An HIDS also scans all data packets that are sent to or from an endpoint, meaning it can detect suspicious activity that originates inside an organization, an important capability to aid in the prevention of insider threats.

Protocol-based intrusion detection system (PIDS)

A protocol-based intrusion detection system (PIDS) is typically deployed on a web server and is used to monitor and analyze communication between devices on a network and online resources, as it scans data transmitted over HTTP/HTTPS.

Application protocol-based intrusion detection system (APIDS)

An application protocol-based intrusion detection system (APIDS) monitors the communication between users and applications. It monitors the packets transmitted over application-specific protocols and identifies instructions, tracing it to individual users.

Hybrid intrusion detection system

A hybrid intrusion detection system is defined exactly as its name implies: it's a combination of two or more types of IDSs. In the hybrid type, the capabilities of two systems—host- and network-based IDSs for example—are combined, rendering it more effective than any single type of IDS.

Intrusion detection systems are also categorized as active or passive:

- **An active IDS** is also known as an intrusion detection and prevention system (IDPS). Not only is it configured to monitor traffic and detect anomalous behavior, it is also automated to block any suspected attacks with blocking IPs or by restricting access to sensitive resources without any need for admin involvement.
- **A passive IDS** only monitors and analyzes network traffic and alerts an admin to a potential attack. It doesn't have the ability to perform any blocking or preventative activity on its own.

General Indications of Intrusions



Intrusion attempts on networks, systems, or file systems can be identified by following some general indicators:

File System Intrusions

By observing system files, the presence of an intrusion can be identified. System files record the activities of the system. Any modification or deletion of the file attributes or the file itself is a sign that the system has been a target of an attack:

- If you find new, unknown files/programs on your system, then there is a possibility that the system has been intruded into. The system can be compromised to the extent that it can, in turn, compromise other network systems.
- When an intruder gains access to a system, he or she tries to escalate privileges to gain administrative access. When the intruder obtains administrator privileges, he/she could change file permissions, for example, from read-only to write.
- Unexplained modifications in file size are also an indication of an attack. Make sure you analyze all your system files.
- The presence of rogue suid and sgid files on your Linux system that do not match your master list of suid and sgid files could indicate an attack.
- You can identify unfamiliar file names in directories, including executable files with strange extensions and double extensions.
- Missing files are also a sign of a probable intrusion/attack.

Network Intrusions

Similarly, general indications of network intrusions include:

- A sudden increase in bandwidth consumption
- Repeated probes of the available services on your machines
- Connection requests from IPs other than those in the network range, which imply that an unauthenticated user (intruder) is attempting to connect to the network
- Repeated login attempts from remote hosts
- A sudden influx of log data, which could indicate attempts at DoS attacks, bandwidth consumption, and DDoS attacks

System Intrusions

Similarly, general indications of system intrusions include:

- Sudden changes in logs such as short or incomplete logs
- Unusually slow system performance
- Missing logs or logs with incorrect permissions or ownership
- Modifications to system software and configuration files
- Unusual graphic displays or text messages
- Gaps in system accounting
- System crashes or reboots
- Unfamiliar processes
- Change in signatures

Evasion Techniques

Evading IDS

Techniques

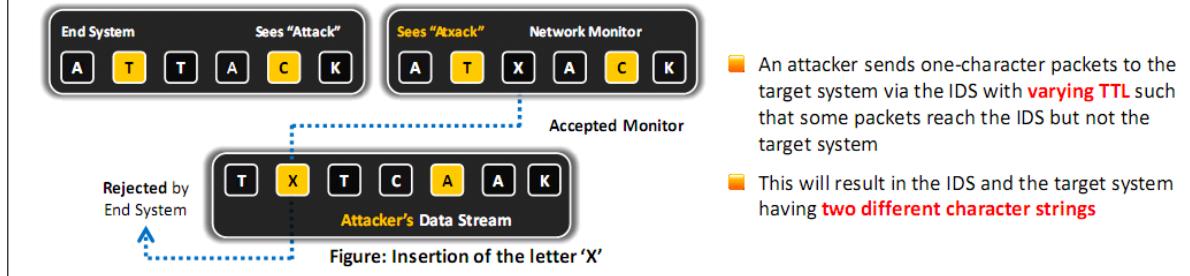
IDS Evasion Techniques		
1 Insertion Attack	7 Unicode Evasion	13 Polymorphic Shellcode
2 Evasion	8 Fragmentation Attack	14 ASCII Shellcode
3 Denial-of-Service Attack	9 Overlapping Fragments	15 Application-Layer Attacks
4 Obfuscating	10 Time-To-Live Attacks	16 Desynchronization
5 False Positive Generation	11 Invalid RST Packets	17 Encryption
6 Session Splicing	12 Urgency Flag	18 Flooding

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Insertion Attack

- Attacker confuses the IDS by forcing it to read invalid packets
- An IDS blindly believes and accepts a packet that an end system rejects and the attacker exploits this condition and inserts data into the IDS
- Occurs when NIDS is less strict in processing packets than the internal network
- The attacker obscures extra traffic and IDS concludes the traffic is harmless
- The IDS gets more packets than the destination

- IDS and the end system construct two different strings



Evasion

- End System Accepts a packet that an IDS rejects
- Using this technique an attacker exploits the host computer without the IDS ever realizing it
- Attacker sends portions of the request in packet that the IDS mistakenly rejects allowing the removal of parts of the stream from the IDS
- The IDS gets fewer packets than the destination

DoS

- IDSs use a centralized server for logging alerts
- If attackers know the IP address of the centralized server, they can perform a DoS or other hack to slow down or crash the server
- As result attacker intrusion attempts will not be logged

Obfuscation

- Encode the attack packet payload
- Attackers manipulate the path referenced in the signature to fool the HIDS
- Attackers can encode attack patterns in Unicode to bypass IDS filtering but be understood by an iis webserver
- Polymorphic code is another means to circumvent signature-based IDS by creating unique attack patterns
- Use encrypted protocols such as https so the IDS can't read the packet

False Positive Generation

- Craft malicious packets just to generate alerts
- These packets generate a large number of false positive alerts
- False positives are used to hide the real attack traffic
- Makes it difficult to differentiate the attack traffic with the false positives

Session Splicing

- Attacker splits the attack traffic into many packets
- It is effective against IDS that do not reconstruct packets before checking them against intrusion signatures
- If attackers are aware of delay in packet reassembly at the IDS, they can add delay between packet transmissions to bypass the reassembly

- IDS stops reassembly if they do not receive packets within a certain time
- IDS will stop working if the target host keeps session active for a time longer than the IDS reassembly time
- Any attack attempt after a successful splicing attack will not be logged by the IDS

Unicode Evasion

- Unicode is a character coding system to support worldwide interchange processing and display of the written texts
- In the Unicode space all the code points are treated differently but it is possible that there could be multiple representations of a single character
- Because of this complexity some IDS handle Unicode improperly
- Attacker convert attack string into Unicode to avoid IDS

Fragmentation Attack

- Can be used when fragmentation timeouts vary between IDS and host
- If a fragment reassembly timeout is 10 sec at the IDS and 20 sec at the target system attackers will send the second fragment after 15 secs
- IDS will drop the fragment as the second fragment is received but the target will reassemble the fragment
- When and IDS timeout exceeds the Victims timeout multiple fragments can be sent at different times so that the IDS receives some packets and the target receives other

Overlapping Fragments

- Generates a series of tiny fragments with overlapping TCP sequence numbers

Time to live

- Attacker needs to have prior knowledge of the topology
- This information can be obtained using tools such as traceroute
- IDS will receive both fragments target receives first fragment only

Invalid RST packet

- Attacker send RST packet to the IDS with an Invalid checksum
- IDS stops processing the packet thinking the TCP communication session has ended
- The target checks the RST packet checksum and drops it because it is invalid

Urgency Flag

- IDS do not consider the urgent pointer
- This results in the IDS and the target systems having different sets of packets

Polymorphic Shellcode

- Signature based NIDS identifies an attack by matching attack signatures with incoming and outgoing data

- Signatures are based off of commonly used string in shell code
- Polymorphic shellcode includes multiple signatures making it difficult to detect the signature
- Encode the payload using some technique and then place a decoder before the payload
- Shellcode is completely rewritten each time it is sent evading detection
- This technique also evades the commonly used shellcode strings

ASCII Shellcode

- ASCII Shellcode can be used to evade IDS because the pattern matching does not work with the ASCII values
- Scope of ASCII shellcode is limited as all assembly instructions cannot be converted to ASCII values directly
- Can be overcome by using other sets of instructions for converting ASCII values properly

Application Layer Attacks

- Uses compression to hide malicious code
- Signature IDS cannot detect signature in compressed files
- Enables an attacker to exploit the vulnerabilities in compressed data

Desynchronization

- **Pre-Connection SYN**
 - Initial SYN packet is sent before the real connection
 - If the SYN packet is received after the TCP control block is opened the IDS resets the appropriate sequence number to match that of the newly received SYN packet
 - Attackers send fake SYN packets with a completely invalid sequence number to desync the IDS
 - Stops the IDS from monitoring all legit traffic
- **Post Connection SYN**
 - Attempts to desync the IDS from the actual sequence numbers that the kernel is honoring
 - Send a post connection SYN packet in the data stream which have divergent sequence numbers
 - Target ignores the SYN packet as it references an already established connection
 - The point of the attack is to get the IDS to resync its notion of the sequence numbers to the new SYN packet
 - Causes the IDS to ignore legitimate part of the original stream
 - Once the IDS resyncs a RST packet is sent to close down the connection

Encryption

- Encrypted sessions with the victim can't be read by the IDS

Flooding

- Attacker sends loads of unnecessary traffic to produce noise

As a pentester you need to test these evasion tools and see how effective is an organization's system to protect against intrusion.

When creating a payload, we need to make sure that it isn't detected as malicious by the target's firewall or IDS system. There are many possible ways to obfuscate the payload, one of them using msfvenom.

Obfuscated malware needs to be in readable form still to be able to execute. One of the ways to insure that is not detected by IDS is to inject it in benign files.

Malware packers obfuscate the malicious code by compressing, masking using XOR or encrypting it. They may also include anti-sandboxing code.

The Andromeda Gamarue Custom Packer is a custom packer used to ensure that the attacks have its own fingerprint and cannot be based on previous attacks.

Fileless attacks means that the malware is not written to disk but rather executed directly in memory and evade being detected.

Malware can be hidden in an alternate data stream to evade detection. Alternate data streams can be used to hide executable files.

Analyzing malware can be dangerous to live production systems. It is advisable to use virtual environment or sandboxes while doing so.

What is not an IDS

- Vulnerability assessment tools
- Cryptographic systems e.g., VPN, SSL and radius

Intrusion protection systems (IPS)

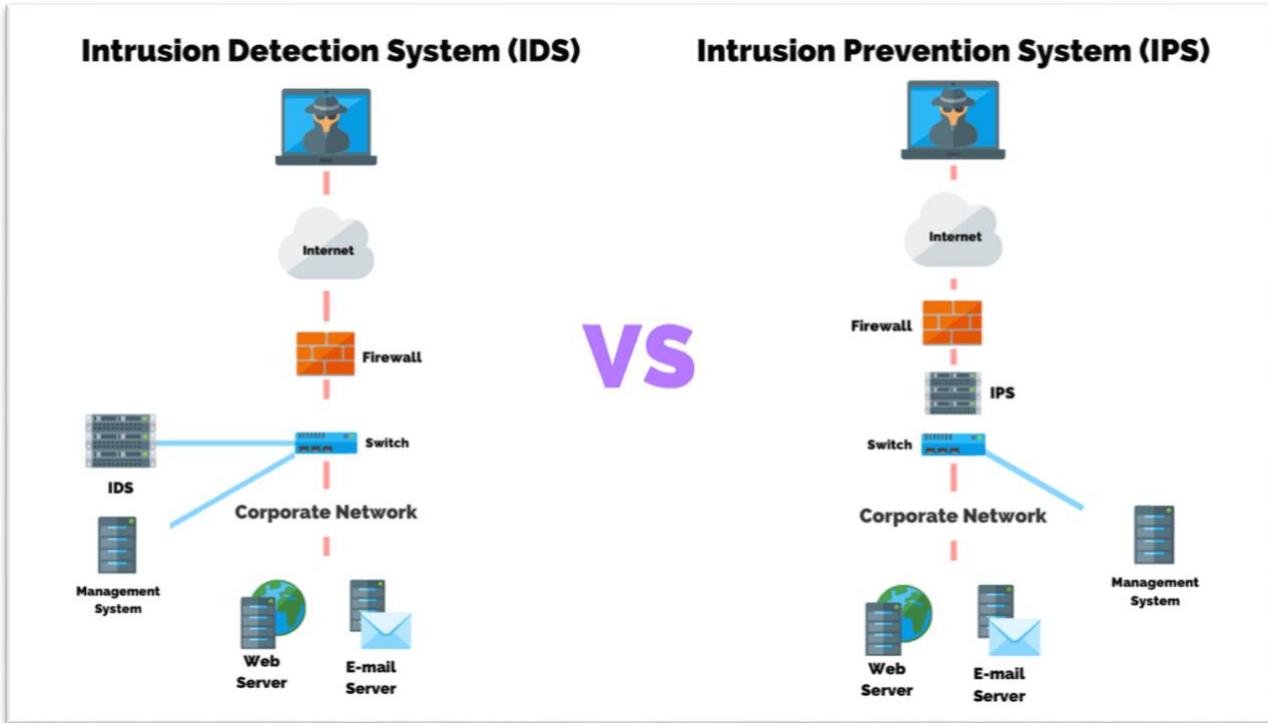
IPS and IDS - What is the Difference?

When looking into IPS solutions, you may also come across intrusion detection systems (IDS). Before we look into how intrusion prevention systems work, let's take a look at the difference between IPS and IDS.

The main difference between IPS and IDS **is the action they take when a potential incident has been detected.**

Intrusion Prevention System (IPS) - ACTIVE monitoring of activity looking for anomalies and alerting/notifying AND **taking action when they are found.**

Intrusion Detection System (IDS) - PASSIVE monitoring of activity looking for anomalies and alerting/notifying when they are found.



- Intrusion prevention systems control the access to an IT network and protect it from abuse and attack. These systems are designed to monitor intrusion data and take the necessary action to prevent an attack from developing.
- Intrusion detection systems are not designed to block attacks and will simply monitor the network and send alerts to systems administrators if a potential threat is detected.

How Do Intrusion Prevention Systems Work?

Intrusion prevention systems work by scanning all network traffic. There are a number of different threats that an IPS is designed to prevent, including:

- Denial of Service (DoS) attack
- Distributed Denial of Service (DDoS) attack
- Various types of exploits
- Worms
- Viruses

The IPS performs real-time packet inspection, deeply inspecting every packet that travels across the network. If any malicious or suspicious packets are detected, the IPS will carry out one of the following actions:

- Terminate the TCP session that has been exploited and block the offending source IP address or user account from accessing any application, target hosts or other network resources unethically.
- Reprogram or reconfigure the firewall to prevent a similar attack occurring in the future.

- Remove or replace any malicious content that remains on the network following an attack. This is done by repackaging payloads, removing header information and removing any infected attachments from file or email servers.

Types of Prevention

An intrusion prevention system is typically configured to use a number of different approaches to protect the network from unauthorized access. These include:

- **Signature-Based** - The signature-based approach uses predefined signatures of well-known network threats. When an attack is initiated that matches one of these signatures or patterns, the system takes necessary action.
- **Anomaly-Based** - The anomaly-based approach monitors for any abnormal or unexpected behavior on the network. If an anomaly is detected, the system blocks access to the target host immediately.
- **Policy-Based** - This approach requires administrators to configure security policies according to organizational security policies and the network infrastructure. When an activity occurs that violates a security policy, an alert is triggered and sent to the system administrators.

The IPS often sits directly behind the firewall and provides a complementary layer of analysis that negatively selects for dangerous content. Unlike its predecessor the Intrusion Detection System (IDS)—which is a passive system that scans traffic and reports back on threats—the IPS is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network. Specifically, these actions include:

- Sending an alarm to the administrator (as would be seen in an IDS)
- Dropping the malicious packets
- Blocking traffic from the source address
- Resetting the connection

As an inline security component, the IPS must work efficiently to avoid degrading network performance. It must also work fast because exploits can happen in near real-time. The IPS must also detect and respond accurately, so as to eliminate threats and false positives (legitimate packets misread as threats).

Detection

The IPS has a number of detection methods for finding exploits, but signature-based detection and statistical anomaly-based detection are the two dominant mechanisms.

Signature-based detection is based on a dictionary of uniquely identifiable patterns (or signatures) in the code of each exploit. As an exploit is discovered, its signature is recorded and stored in a continuously growing dictionary of signatures. Signature detection for IPS breaks down into two types:

1. **Exploit-facing signatures** identify individual exploits by triggering on the unique patterns of a particular exploit attempt. The IPS can identify specific exploits by finding a match with an exploit-facing signature in the traffic stream
2. **Vulnerability-facing signatures** are broader signatures that target the underlying vulnerability in the system that is being targeted. These signatures allow networks to be protected from variants of an exploit that may not have been directly observed in the wild, but also raise the risk of false positives.

Statistical anomaly detection takes samples of network traffic at random and compares them to a pre-calculated baseline performance level. When the sample of network traffic activity is outside the parameters of baseline performance, the IPS takes action to handle the situation.

Firewalls

Firewalls are often seen as NAC devices. Use of rule sets to filter traffic can implement security policy.

Firewalls types:

- **Stateful (Dynamic Packet Filtering)** - Layer 3 + 4 (Network + Transport layer)
- **Stateless (Static Packet Filtering)** - Layer 3 (Network)
- **Deep Packet Inspection** - Layer 7 (Application Layer)
- **Proxy Firewall** - Mediates communications between untrusted and trusted end-points (server/hosts/clients). A proxy firewall is a network security system that protects network resources by filtering messages at the Application Layer 7. A proxy firewall may also be called an application firewall or gateway firewall

Proxy Types:

- **Circuit-level proxy** - Firewall that works on **Layer 5 (Session layer)**; They monitor TCP handshaking between packets to determine whether a requested session is legitimate.
- **Application-level proxy** - Any service or server that acts as a proxy for client computer requests at the application's protocols.

⚠ An application-level proxy is one that knows about the particular application it is providing proxy services for; it understands and interprets the commands in the application protocol. A circuit-level proxy is one that creates a circuit between the client and the server without interpreting the application protocol.

- **Multi-homed Firewall (dual-homed)** - Firewall that has two or more interfaces; One interface is connected to the untrusted network and another interface is connected to the trusted network. A DMZ can be added to a multi-homed firewall just by adding a third interface.

- **Bastion hosts** - Endpoint that is exposed to the internet but has been hardened to withstand attacks; Hosts on the screened subnet designed to protect internal resources.
- **Screened host** - Endpoint that is protected by a firewall.
- **Packet-filtering** - Firewalls that only looked at headers

⚠ Only uses rules that **implicitly denies** traffic unless it is allowed.

⚠ Oftentimes uses **network address translation** (NAT) which can apply a one-to-one or one-to-many relationship between external and internal IP addresses.

⚠ **Private zone** - hosts internal hosts that only respond to requests from within that zone

Evading Firewalls

1 Firewalling	6 Using IP Address in Place of URL	11 SSH Tunneling
2 Banner Grabbing	7 Using Proxy Server	12 Through External Systems
3 IP Address Spoofing	8 ICMP Tunneling	13 Through MITM Attack
4 Source Routing	9 ACK Tunneling	14 Through Content
5 Tiny Fragments	10 HTTP Tunneling	15 Through XSS Attack

Firewall Identification

- **Port Scanning**
 - Identifies open ports and services running
 - Open ports can be further probed to identify the version of services
 - Some firewall will uniquely identify themselves with how they respond to simple port scans
- **Firewalking**
 - Uses TTL values to determine gateway ACL filters and map networks by analyzing ip packet responses
 - Attacker sends TCP or UDP packet to the targeted firewall with a TTL set to one hop greater than the firewall
 - If the packet makes it through the firewall a TTL exceeded in transit will be returned
- **Banner Grabbing**

- Banners announce the service that is running on the port
- Banner grabbing is a fingerprint method
- Main services that send out banners are FTP telnet and web servers

IP Address Spoofing

- IP Address spoofing is a hijack technique in which an attacker masquerades as a trusted host to conceal his identity spoof web sites hijack browsers or gain unauthorized access to a network
- Attackers modify the addressing information in the IP packet header and the source address bits field in order to bypass the firewall

Source Routing

- Allows the sender of a packer to specify the route the packet takes through the network
- As the packet travels through the nodes in the network each router examines the destination IP address and chooses the next hop to direct the packet to the destination
- In source routing the sender makes some of these decisions
- Allows the attacker to avoid going through the firewall

Tiny Fragments

- Attacker creates tiny packet fragments forcing some of the TCP packet header information into the next fragment
- IDS filter rules that specify patterns will not match with the fragmented packets due to broken header information
- The attack will succeed if the filtering router examines only the first fragment and allows other fragments to pass through
- This attack is used to avoid user defined filtering rules and works when the firewall checks only for the tcp header information

Bypass Blocked Sites using IP address in Place of URL

- This method involves typing the IP address directly in browsers address bar in place of typing the blocked website domain name

Bypass blocked sites using anonymous website surfing

- Uses VPN or proxy to encrypt traffic

Bypassing firewall through ICMP tunneling method

- Allows tunneling a backdoor shell in the data portion of ICMP echo packets
- The payload portion of an ICMP packet is not examined by many firewalls

Bypassing firewall through ACK tunneling Method

- Tunneling a backdoor application with TCP packets with ACK bit set
- ACK bit is used to acknowledge receipt of a packet

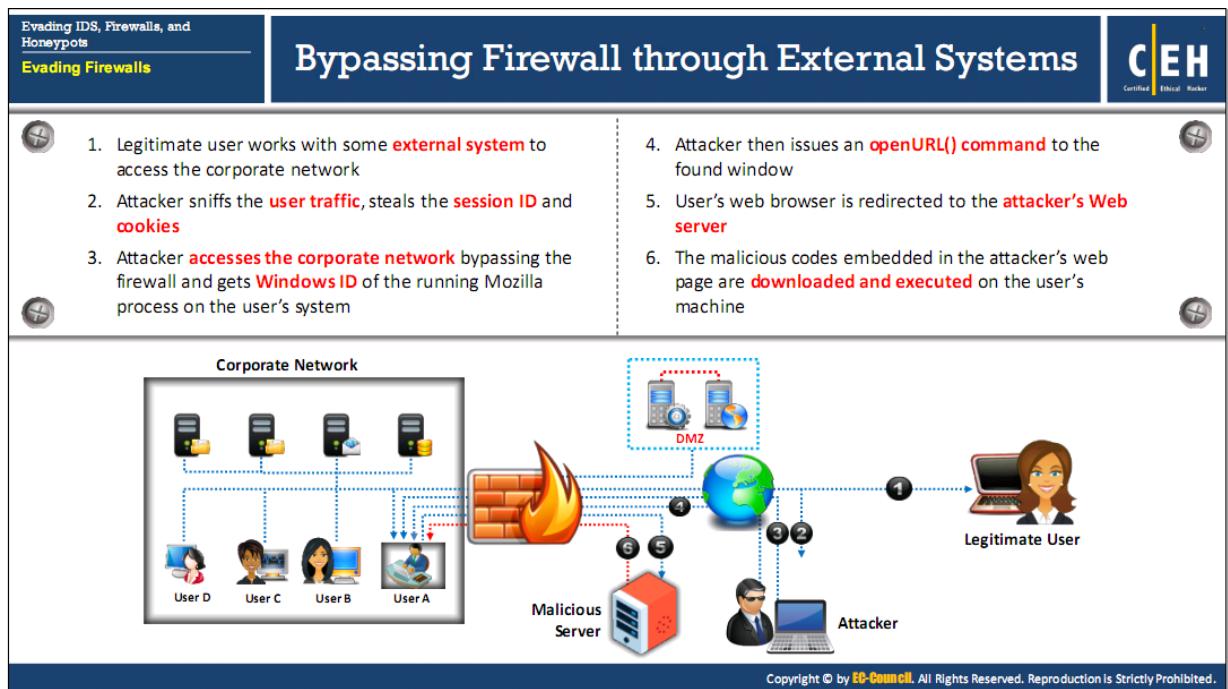
Bypassing Firewall through HTTP tunneling Method

- HTTP tunneling allow attackers to tunnel data through HTTP packets
- HTTP tunneling allow sending traffic for other services like FTP over HTTP or HTTPS

Bypassing firewall through SSH tunneling

- Attackers use openssh to encrypt and tunnel all the traffic from a local machine to a remote machine to avoid detection by perimeter security controls

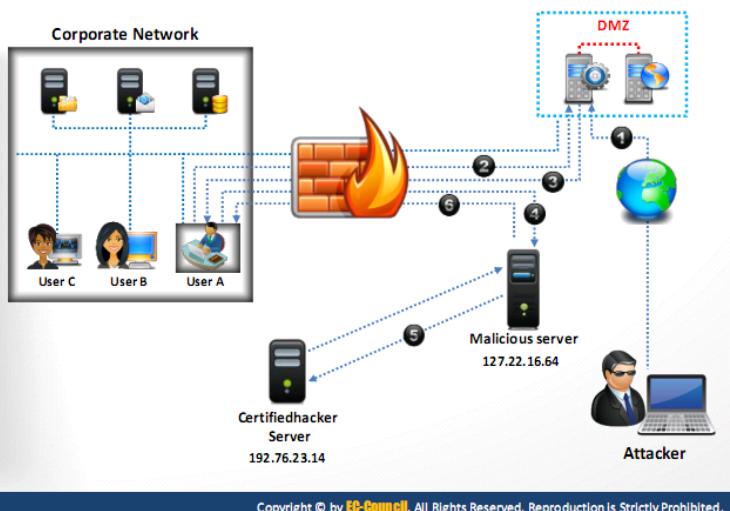
Bypassing firewall through external systems



Bypassing firewall through MITM attack

- Attackers make use of the DNS server and routing techniques to bypass restrictions

1. Attacker performs **DNS server poisoning**
2. User A requests for www.certifiedhacker.com to the **corporate DNS server**
3. Corporate DNS server sends the **IP address (127.22.16.64) of the attacker**
4. User A accesses the **attacker's malicious server**
5. Attacker connects with the **real host and tunnels the user's HHTP traffic**
6. The malicious codes embedded in the attacker's web page are **downloaded and executed** on the user's machine



Bypassing through content

- Attacker sends the content containing malicious code to the user and tricks him/her to open it so that the malicious code can be executed

Bypassing Web application firewall (WAF) using XSS attack

- XSS attack exploits vulnerabilities that occur while processing input parameters of the end users and the server responses in a web application

Using ASCII values to bypass WAF

- After replacing XSS payload with its equivalent ASCII values

```
<scirpt>String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83, 34, 41)</script>
```

Using Hex Encoding to bypass WAF

- After encoding the XSS payload,

```
%3C%73%63%69%72%70%74%3E%6C%65%72%74%28%22%58%53%53%22%29%3C%2F%73%63%72%69%70%74%3E
```

Using Obfuscation to bypass WAF

- After encoding the XSS payload,

```
<sCriPT>aLeRT ("XSS")</sCriPT>
```

- Attackers inject malicious HTML code in the victim's website to bypass the WAF

IDS/Firewall Evading Tools

Traffic IQ Professional

- Enables security professionals to audit and validate the behavior of security devices by generating the standard application traffic or attack traffic between two virtual machines

Colasoft Packet builder

- Network packet crafter
- Used to build all types of custom networks

Honeypots

Honeypots are decoy systems or servers deployed alongside production systems within your network. When deployed as enticing targets for attackers, honeypots can add security monitoring opportunities for blue teams and misdirect the adversary from their true target.

- **Honeynet** - Two or more honeypots on a network form a honeynet. Honeynets and honeypots are usually implemented as parts of larger Network Intrusion Detection Systems.
- A **Honeyfarm** is a centralized collection of honeypots and analysis tools.

Types of Honeypots:

1. **Low-interaction** ---> Simulates/imitate services and systems that frequently attract criminal attention. They offer a method for collecting data from blind attacks such as botnets and worm's malware.
 2. **High interaction** ---> Simulates all services and applications and is designed to be completely compromised
 3. **Production** ---> Serve as decoy systems inside fully operating networks and servers, often as part of an intrusion detection system (IDS). They deflect criminal attention from the real system while analyzing malicious activity to help mitigate vulnerabilities.
 4. **Research** ---> Used for educational purposes and security enhancement. They contain trackable data that you can trace when stolen to analyze the attack.
- **Honeypot Tools:**
 - Specter
 - Honeyd
 - KFSensor (Honeypot IDS)

Detecting Honeypots

- Attacker can determine the presence of honeypots by probing the services running on a system
- Attackers craft malicious probe packets to scan for services such as HTTPS SMTSP and IMAPS
- Ports that show a particular service running but deny a three way handshake connection indicated the presence of a honeypot

Detecting and Defeating Honeypots

- **Detecting presence of Layer 7 Tar Pits**
 - Look at the latency of the response from the service
- **Detecting presence of layer 4 tar pits**
 - Analyze the TCP window size where tar pits continuously acknowledge incoming packets even though the TCP window size is reduced to zero
- **Detecting presence of layer 2 tar pits**
 - Look for the response with unique MAC address which act as kind of black hole
 - Need to be on the same layer 2 network
- **Detecting Honeypots running on VMWare**
 - Look at the IEE standards for the current range of MAC addresses assigned to VMWare Inc
- **Detecting presence of Honeyd Honeypot**
 - Perform time-based TCP finger printing methods
- **Detecting presence of user mode linux honeypot**
 - Analyze the files such as /proc/mounts /proc/interrupts and /proc/cmdline
- **Detecting presence of Sebek based honeypots**
 - Sebek logs everything that is accessed via read() before transferring to the network causing congesting effect Analyze congestion in the network layer
- **Detecting presence of snort inline honeypot**
 - Analyze outgoing packets by capturing Snort inline modified packet through another host system and identifying the packet modification
- **Detecting presence of fake AP**
 - Fake access points only send beacon frames but do not generate any fake traffic on the access points and an attacker can monitor the network traffic and easily notice the presence of fake AP
- **Detecting presence of bait and switch honeypots**
 - Look at specific TCP/IP parameters like round trip time, TTL, and the TCP timestamp

Send Safe Honeypot Hunter

- Tool designed for checking lists of HTTPS and SOCKS proxies for Honey pots

IDS Firewall Evasion Countermeasures

How to defend Against IDS Evasion

- Shutdown switch ports
- Perform in depth analysis of ambiguous network traffic
- Use TCP FIN or RST packet to terminate malicious TCP sessions
- Look for code other than 0x90 to defend against polymorphic shellcode
- Train users to identify attack patterns and regularly update/ patch
- Deploy IDS after a thorough analysis of network topology nature of network traffic and the number of host to monitor
- Use a traffic normalizer to remove potential ambiguity from packet stream before it reaches IDS
- Ensure IDS normalize fragmented packets and allows those packets to be reassembled In the proper order
- Define DNS server for client resolver in routers or similar network devices
- Harden the security of all communication devices such as modems, routers, switches, etc

- Block ICMP TTL expired packets
- Update antivirus signature regularly
- Use a traffic normalization solution at the IDS to prevent the system against evasion
- Store the attack information for future analysis

How to defend against firewall evasion

1	Configuration of the firewall should be done in such a way that the IP address of an intruder should be filtered out	8	Run regular risk queries to identify vulnerable firewall rules
2	Set the firewall ruleset to deny all traffic and enable only the services required	9	Monitor user access to firewalls and control who can modify the firewall configuration
3	If possible, create a unique user ID to run the firewall services. Rather than running the services using the administrator or root IDs	10	Specify the source and destination IP addresses as well as the ports
4	Configure a remote syslog server and apply strict measures to protect it from malicious users	11	Notify the security policy administrator on firewall changes and document them
5	Monitor firewall logs at regular intervals and investigate all suspicious log entries found	12	Control physical access to the firewall
6	By default, disable all FTP connections to or from the network	13	Take regular backups of the firewall ruleset and configuration files
7	Catalog and review all inbound and outbound traffic allowed through the firewall	14	Schedule regular firewall security audits

Firewall Penetration Testing

Firewall IDS Penetration Testing

- Helps evaluate ingress and egress traffic filtering capabilities

Sniffing and Evasion (SUMMARY)

Basic Knowledge

- Sniffing is capturing packets as they pass on the wire to review for interesting information
- **MAC** (Media Access Control) - physical or burned-in address - assigned to NIC for communications at the Data Link layer
 - 48 bits long
 - Displayed as 12 hex characters separated by colons
 - First half of address is the **organizationally unique identifier** - identifies manufacturer
 - Second half ensures no two cards on a subnet will have the same address
- NICs normally only process signals meant for it
- **Promiscuous mode** - NIC must be in this setting to look at all frames passing on the wire
- **CSMA/CD** - Carrier Sense Multiple Access/Collision Detection - used over Ethernet to decide who can talk
- **Collision Domains**

- Traffic from your NIC (regardless of mode) can only be seen within the same collision domain
- Hubs by default have one collision domain
- Switches have a collision domain for each port

Protocols Susceptible

- SMTP is sent in plain text and is viewable over the wire. SMTP v3 limits the information you can get, but you can still see it.
- FTP sends user ID and password in clear text
- TFTP passes everything in clear text
- IMAP, POP3, NNTP and HTTP all send over clear text data
- TCP shows sequence numbers (usable in session hijacking)
- TCP and UCP show open ports
- IP shows source and destination addresses

ARP

- Stands for Address Resolution Protocol
- Resolves IP address to a MAC address
- Packets are ARP_REQUEST and ARP_REPLY
- Each computer maintains its own ARP cache, which can be poisoned
- **Commands**
 - **arp -a** - displays current ARP cache
 - **arp -d *** - clears ARP cache
- Works on a broadcast basis - both requests and replies are broadcast to everyone
- **Gratuitous ARP** - special packet to update ARP cache even without a request
 - This is used to poison cache on other machines

IPv6

- Uses 128-bit address
- Has eight groups of four hexadecimal digits
- Sections with all 0s can be shortened to nothing (just has start and end colons)
- Double colon can only be used once
- Loopback address is ::1

IPv6 Address Type	Description
Unicast	Addressed and intended for one host interface
Multicast	Addressed for multiple host interfaces
Anycast	Large number of hosts can receive; nearest host opens
IPv6 Scopes	Description
Link local	Applies only to hosts on the same subnet (Address block fe80::/10)

IPv6 Scopes	Description
Site local	Applies to hosts within the same organization (Address block FEC0::/10)
Global	Includes everything

- Scope applies for multicast and anycast
- Traditional network scanning is **computationally less feasible**

Wiretapping

- **Lawful interception** - legally intercepting communications between two parties
- **Active** - interjecting something into the communication
- **Passive** - only monitors and records the data
- **PRISM** - system used by NSA to wiretap external data coming into US

Active and Passive Sniffing

- **Passive sniffing** - watching network traffic without interaction; only works for same collision domain
- **Active sniffing** - uses methods to make a switch send traffic to you even though it isn't destined for your machine
- **Span port** - switch configuration that makes the switch send a copy of all frames from other ports to a specific port
 - Not all switches have the ability to do this
 - Modern switches sometimes don't allow span ports to send data - you can only listen
- **Network tap** - special port on a switch that allows the connected device to see all traffic
- **Port mirroring** - another word for span port

MAC Flooding

- Switches either flood or forward data
- If a switch doesn't know what MAC address is on a port, it will flood the data until it finds out
- **CAM Table** - the table on a switch that stores which MAC address is on which port
 - If table is empty or full, everything is sent to all ports
- This works by sending so many MAC addresses to the CAM table that it can't keep up
- **Tools**
 - Etherflood
 - Macof
- **Switch port stealing** - tries to update information regarding a specific port in a race condition
- MAC Flooding will often destroy the switch before you get anything useful, doesn't last long and it will get you noticed. Also, most modern switches protect against this.

ARP Poisoning

- Also called ARP spoofing or gratuitous ARP
- This can trigger alerts because of the constant need to keep updating the ARP cache of machines
- Changes the cache of machines so that packets are sent to you instead of the intended target

- **Countermeasures**
 - Dynamic ARP Inspection using DHCP snooping
 - XArp can also watch for this
 - Default gateway MAC can also be added permanently into each machine's cache
- **Tools**
 - Cain and Abel
 - WinArpAttacker
 - Ufasoft
 - dsniff

DHCP Starvation

- Attempt to exhaust all available addresses from the server
- Attacker sends so many requests that the address space allocated is exhausted
- DHCPv4 packets - DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK
- DHCPv6 packets - Solicit, Advertise, Request (Confirm/Renew), Reply
- **DHCP Steps**
 1. Client sends DHCPDISCOVER
 2. Server responds with DHCPOFFER
 3. Client sends request for IP with DHCPREQUEST
 4. Server sends address and config via DHCPACK
- **Tools**
 1. Yersinia
 2. DHCPstarv
- Mitigation is to configure DHCP snooping
- **Rogue DHCP Server** - setup to offer addresses instead of real server. Can be combined with starvation to real server.

Spoofing

- **MAC Spoofing** - changes your MAC address. Benefit is CAM table uses most recent address.
- Port security can slow this down, but doesn't always stop it
- MAC Spoofing makes the switch send all packets to your address instead of the intended one until the CAM table is updated with the real address again
- **IRDP Spoofing** - hacker sends ICMP Router Discovery Protocol messages advertising a malicious gateway
- **DNS Poisoning** - changes where machines get their DNS info from, allowing attacker to redirect to malicious websites

Sniffing Tools

- **Wireshark**
 - Previously known as Ethereal
 - Can be used to follow streams of data
 - Can also filter the packets so you can find a specific type or specific source address
 - **Example filters**
 - ! (arp or icmp or dns) - filters out the "noise" from ARP, DNS and ICMP requests
 - http.request - displays HTTP GET requests

- tcp contains string - displays TCP segments that contain the word "string"
 - ip.addr==172.17.15.12 && tcp.port==23 - displays telnet packets containing that IP
 - tcp.flags==0x16 - filters TCP requests with ACK flag set
- **tcpdump**
 - Recent version is WinDump (for Windows)
 - **Syntax**
 - tcpdump flag(s) interface
 - tcpdump -i eth1 - puts the interface in listening mode
- **tcptrace**
 - Analyzes files produced by packet capture programs such as Wireshark, tcpdump and Etherpeek
- **Other Tools**
 - **Ettercap** - also can be used for MITM attacks, ARP poisoning. Has active and passive sniffing.
 - **Capsa Network Analyzer**
 - **Snort** - usually discussed as an Intrusion Detection application
 - **Sniff-O-Matic**
 - **EtherPeek**
 - **WinDump**
 - **WinSniffer**

Devices To Evade

- **Intrusion Detection System (IDS)** - hardware or software devices that examine streams of packets for malicious behavior
 - **Signature based** - compares packets against a list of known traffic patterns
 - **Anomaly based** - makes decisions on alerts based on learned behavior and "normal" patterns
 - **False negative** - case where traffic was malicious, but the IDS did not pick it up
 - **HIDS** (Host-based intrusion detection system) - IDS that is host-based
 - **NIDS** (Network-based intrusion detection system) - IDS that scans network traffic
- **Snort** - a widely deployed IDS that is open source
 - Includes a sniffer, traffic logger and a protocol analyzer
 - Runs in three different modes
 - **Sniffer** - watches packets in real time
 - **Packet logger** - saves packets to disk for review at a later time
 - **NIDS** - analyzes network traffic against various rule sets
 - Configuration is in /etc/snort on Linux and c:\snort\etc in Windows
 - **Rule syntax**
 - alert tcp !HOME_NET any -> \$HOME_NET 31337 (msg : "BACKDOOR ATTEMPT-Backorifice")
 - This alerts about traffic coming not from an external network to the internal one on port 31337
 - **Example output**
 - 10/19-14:48:38.543734 0:48:542:2A:67 -> 0:10:B5:3C:34:C4 type:0x800 len:0x5EA **xxx -> xxx TCP TTL:64 TOS:0x0 ID:18112 IpLen:20 DgmLen:1500 DF**
 - Important info is bolded
- **Firewall**

- An appliance within a network that protects internal resources from unauthorized access
- Only uses rules that **implicitly denies** traffic unless it is allowed
- Oftentimes uses **network address translation** (NAT) which can apply a one-to-one or one-to-many relationship between external and internal IP addresses
- **Screened subnet** - hosts all public-facing servers and services
- **Bastion hosts** - hosts on the screened subnet designed to protect internal resources
- **Private zone** - hosts internal hosts that only respond to requests from within that zone
- **Multi-homed** - firewall that has two or more interfaces
- **Packet-filtering** - firewalls that only looked at headers
- **Stateful inspection** - firewalls that track the entire status of a connection
- **Circuit-level gateway** - firewall that works on Layer 5 (Session layer)
- **Application-level gateway** - firewall that works like a proxy, allowing specific services in and out

Evasion Techniques

- **Slow down** - faster scanning such as using nmap's -T5 switch will get you caught. Pros use -T1 switch to get better results
- **Flood the network** - trigger alerts that aren't your intended attack so that you confuse firewalls/IDS and network admins
- **Fragmentation** - splits up packets so that the IDS can't detect the real intent
- **Unicode encoding** - works with web requests - using Unicode characters instead of ascii can sometimes get past
- **Tools**
 - **Nessus** - also a vulnerability scanner
 - **ADMmutate** - creates scripts not recognizable by signature files
 - **NIDSbench** - older tool for fragmenting bits
 - **Inundator** - flooding tool

Firewall Evasion

- ICMP Type 3 Code 13 will show that traffic is being blocked by firewall
- ICMP Type 3 Code 3 tells you the client itself has the port closed
- Firewall type can be discerned by banner grabbing
- **Firewalking** - going through every port on a firewall to determine what is open
- **Tools**
 - CovertTCP
 - ICMP Shell
 - 007 Shell
- The best way around a firewall will always be a compromised internal machine

Honeypots

- A system setup as a decoy to entice attackers
- Should not include too many open services or look too easy to attack
- **High interaction** - simulates all services and applications and is designed to be completely compromised
- **Low interaction** - simulates a number of services and cannot be completely compromised
- **Examples**

- Specter
- Honeyd
- KFSensor

06) Attacking a System

Goals:

1. **Gaining Access** - Uses information gathered to exploit the system
 - o **Password Attacks:**
 - Non-electronic attacks
 - Active online attacks
 - Passive online attacks
 - Offline attacks
2. **Escalating Privileges** - Granting the account you've hacked admin or pivoting to an admin account
3. **Executing Applications** - Putting back doors into the system so that you can maintain access
4. **Hiding Files** - Making sure the files you leave behind are not discoverable
5. **Covering Tracks** - Cleaning up everything else (log files, etc.)
 - o clearev - Meterpreter shell command to clear log files (issued inside Metasploit Framework)
 - o Clear MRU list in Windows
 - o In Linux, append a dot in front of a file to hide it

Password Attacks

⚡ Check out the practical labs on [Dumping and Cracking SAM hashes \[1\]](#), [Rainbow Tables Basics \[2\]](#) and [LLMNR/NBT-NS \[3\]](#).

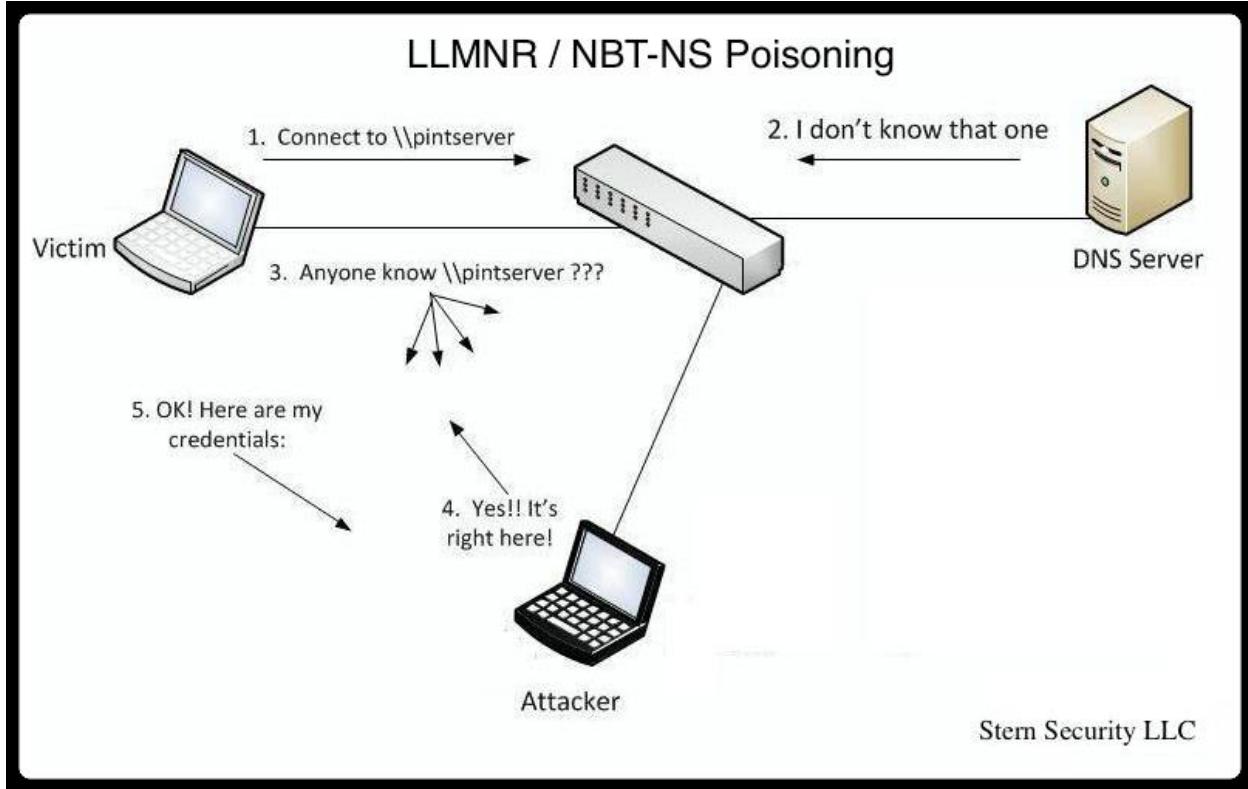
Non-electronic - non-technical attacks.

- Social engineering attacks - most effective.
- Shoulder surfing
- Dumpster diving
- Snooping around
- Guessing

Active online - done by directly communicating with the victim's machine.

- Includes **Dictionary** and **Brute-force attacks**, **hash injections**, **phishing**, **Trojans**, **spyware**, **keyloggers** and **password guessing**
- [**LLMNR / NBT-NS Poisoning**](#) - attack based off Windows technologies that caches DNS locally. Responding to these poisons the local cache. If an NTLM v2 hash is sent over, it can be sniffed out and then cracked.
 - o ⚡ [LLMNR/NBT-NS practical lab](#)
 - o **LLMNR uses UDP 5355**
 - o **NBT-NS uses UDP 137**

- Responder is the tool to sniff the access logs from LLMNR / NBT-NS



- **Keylogging** - process of using a hardware device or software application to capture keystrokes of a user
- Active online attacks are easier to detect and take a longer time
- **Tools for Active Online Attack:**
 - Medusa
 - Hydra
 - NBNSpoof
 - Pupy
 - Metasploit
 - Responder - **LLMNR and NBT-NS responder**, it will answer to *specific* NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool will only answers to File Server Service request, which is for **SMB**.
- Can combine "net" commands with a tool such as **NetBIOS Auditing tool** or **Legion** to automate the testing of user IDs and passwords
 - **Tools for NetBIOS attack:**
 - Hydra
 - Metasploit

Passive online - Sniffing the wire in hopes of intercepting a password in clear text or attempting a replay attack or man-in-the-middle attack

- **Tools for Passive Online Attack:**
 - Cain and Abel - Can poison ARP and then monitor the victim's traffic; Also used for cracking hash passwords (LM, NTLM), sniff network packets for password, sniff out for local stored passwords, etc.
 - Ettercap - MITM tool for LAN's, DNS Spoofing; Help against SSL encryption; Intercept the traffic on a network segment, capture passwords, and conduct an active eavesdropping against a number of common protocols.
 - KerbCrack - built-in sniffer and password cracker looking for port 88 Kerberos traffic
 - ScoopLM - specifically looks for Windows authentication traffic on the wire and has a password cracker

⚠ Services/Protocols that uses Clear text:

Service Port

FTP 20/21

TELNET 23

SMTP 25

HTTP 80

POP3 110

IMAPv4 143

NetBIOS 139,445

SNMP 161,162

SQLnet 1521

Offline - when the hacker steals a copy of the password file (Plaintext or Hash) and does the cracking on a separate system.

- **Dictionary Attack** - uses a word list to attack the password. Fastest method of attacking
 - **Wordlists** - A wordlist or a password dictionary is a collection of passwords stored in plain text. It's basically a text file with a bunch of passwords in it. One popular example of wordlist is the [rockyou.txt](#) containing 14,341,564 unique passwords.
 - You also can generate your own wordlist with given parameters like length, combining letters and numbers, profiling etc.
 - Tools for generate Wordlists:
 - CeWL
 - crunch
- **Brute force attack** - Tries every combination of characters to crack a password
 - Can be faster if you know parameters (such as at least 7 characters, should have a special character, etc.)
- **Hybrid attack** - Takes a dictionary attack and replaces characters (such as a 0 for an o) or adding numbers to the end

- **Rainbow tables** - Uses pre-hashed passwords to compare against a password hash. Is faster because the hashes are already computed.
- **Tools for cracking password files (CLI):**
 - John the Ripper - Works on Unix, Windows and Kerberos; Compatible with MySQL, LDAP and MD4.
 - [Hashcat](#) - Advanced password recovery tool; Provides several options like hash modes OS's, documents, password managers... (MD5, SHA-family, RIPE-MD, NTLM, LM, BitLocker, OSX, MD5 salted or iterated, and the list goes on).

```
hashcat (v6.2.1) starting...

CUDA API (CUDA 11.3)
=====
* Device #1: NVIDIA GeForce RTX 2080 Ti, 10137/11264 MB, 68MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Early-Skip
* Not-Iterated
* Prepended-Salt
* Single-Hash
* Single-Salt
* Brute-Force
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1100 MB

e983672a03adcc9767b24584338eb378:00:hashcat

Session.....: hashcat
Status.....: Cracked
Hash.Name....: SolarWinds Serv-U
Hash.Target....: e983672a03adcc9767b24584338eb378:00
Time.Started....: Sun May 23 11:43:13 2021 (1 sec)
Time.Estimated....: Sun May 23 11:43:14 2021 (0 secs)
Guess.Mask.....: ?a?a?a?a?a?at [7]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 24620.9 MH/s (32.19ms) @ Accel:32 Loops:1024 Thr:1024 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 31606272000/735091890625 (4.30%)
Rejected.....: 0/31606272000 (0.00%)
Restore.Point....: 0/857375 (0.00%)
Restore.Sub.#1....: Salt:0 Amplifier:35840-36864 Iteration:0-1024
Candidates.#1....: 4{,erat -> cyr ~}t
Hardware.Mon.#1...: Temp: 62c Fan: 31% Util:100% Core:1920MHz Mem:7000MHz Bus:16

Started: Sun May 23 11:43:12 2021
Stopped: Sun May 23 11:43:15 2021
```

- **Tools for cracking password files (GUI):**
 - Cain & Abel - Windows software; Cracks hash passwords (LM, NTLM), sniff network packets for password, sniff out for local stored passwords, etc.
 - L0phcrack - Paid software; Extract and crack hashes; Uses brute force or dictionary attack;
 - Ophcrack - Free open-source; Cracks Windows log-in passwords by using LM hashes through rainbow tables.
 - Rainbowcrack - Rainbow tables generator for password cracking
 - Legion - Legion automates the password guessing in NetBIOS sessions. Legion scans multiple IP address ranges for Windows shares and also offers a manual dictionary attack tool.
 - KerbCrack - Crack Kerberos passwords.
 - Mimikatz - Steal credentials and escalate privileges (Windows NTLM hashes and Kerberos tickets(Golden Ticket Attack); 'Pass-the-hash' and 'Pass-the-ticker').
 - fgdump - Dump SAM databases on Windows machines.
 - Pwdump⁷ - Dump SAM databases on Windows machines.
- **CHNTPW** - chntpw is a software utility for **resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8, 8.1 and 10**. It does this by editing the SAM database where Windows stores password hashes.
 - **Physical access** to victim's computer
 - Startup on BIOS and allow boot to CD or USB
 - Modify the SAM user account information through the CHNTPW

⚠ rtgen, winrtgen - Tools for generate your own rainbow tables.

⚠ SAM (Security Account Manager) is a database file **present in Windows machines that stores user accounts and security descriptors for users on a local computer**. It stores users passwords in a hashed format (in LM hash and NTLM hash). Because a hash function is one-way, this provides some measure of security for the storage of the passwords.

⚠ /etc/shadow is where **hashed password data** is stored in **Linux systems** (only users with high privileges can access).

⚠ Password attack countermeasures:

- **Length of passwords** is good against **brute-force attacks**.
- **Password complexity** is good against **dictionary attacks**.

Authentication

- **Three Different Types**
 - **Something You Are** - Uses biometrics to validate identity (retina, fingerprint, etc.)
 - Downside is there can be lots of false negatives

- **False acceptance rate (FAR) - Type II** - Likelihood that an unauthorized user will be accepted (This would be bad)
 - **False injection rate (FRR) - Type I** - Likelihood that an authorized user will be rejected
 - **Crossover error rate (CER)** - Combination of the two; the lower the CER, the better the system
 - **Active** - requires interaction (retina scan or fingerprint scanner)
 - **Passive** - Requires no interaction (iris scan)
- **Something You Have** - Usually consists of a token of some kind (swipe badge, ATM card, etc.)
 - This type usually requires something alongside it (such as a PIN for an ATM card)
 - Some tokens are single-factor (such as a plug-and-play authentication)
- **Something You Know** - Better known as a password
 - Most systems use this because it is universal and well-known
- **Two-Factor** - When you have two types of authentication such as something you know (password) and something you have (access card)
- **Strength of passwords** - Determined by length and complexity
 - ECC says that both should be combined for the best outcome
 - Complexity is defined by number of character sets used (lower case, upper case, numbers, symbols, etc.)
- **Default passwords** - always should be changed and never left what they came with. Databases such as cirt.net, default-password.info and open-sez.me all have databases of these

Malwares

⚡ This chapter has [practical labs](#)

- What is Malware?

Any software intentionally designed to cause damage to a computer, server or computer network. The code is described as computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware, among other terms. Malware has a malicious intent, acting against the interest of the computer user.

Types of Viruses and Worms



- **How it works?**
 1. Infection Phase - a virus planted on a target system and replicates itself and attaches to one or more executable files
 2. Attack phase - the infected file is executed accidentally by the user, or in some way is deployed and activated

- **Virus** - Designed to spread from host to host and has the ability to replicate itself. They cannot reproduce/spread without help. They operate by inserting or attaching itself to a legitimate program or document in order to execute its code.
- **Macro Virus** - Written in a macro language (e.g.: VBA) and that is platform independent.
- **Compression Viruses** - Another type of virus that appends itself to executables on the system and compresses them by user's permissions.
- **Stealth Virus** - Hides the modifications it has made; Trick antivirus software; intercepting its requests to the OS and provides false and bogus information.
- **Polymorphic Virus** - Produces varied but operational copies of itself. A polymorphic virus may have no parts that remain identical between infections, making it very hard to detect using signatures.
- **Multipart Virus** - Attempts to infect both boot sector and files; generally, refers to viruses with multiple infection methods
- **Self-garbling (metamorphic) virus** - Rewrites itself every time it infects a new file.
- **Other Virus Types**
 - **Boot Sector Virus** - known as system virus; moves boot sector to another location and then inserts its code into the original location
 - **Shell Virus** - wraps around an application's code, inserting itself before the application's
 - **Cluster Virus** - modifies directory table entries so every time a file or folder is opened, the virus runs
 - **Encryption Virus** - uses encryption to hide the code from antivirus
 - **Cavity Virus** - overwrite portions of host files as to not increase the actual size of the file; uses null content sections
 - **Sparse Infector Virus** - only infects occasionally (e.g., every 10th time)
 - **File Extension Virus** - changes the file extensions of files to take advantage of most people having them turned off (readme.txt.vbs shows as readme.txt)
- **Virus Makers**
 - Sonic Bat
 - PoisonVirus Maker
 - Sam's Virus Generator
 - JPS Virus Maker
- **Worm** - self-replicating malware that sends itself to other computers without human intervention
 - Usually doesn't infect files - just resides in active memory
 - Often used in botnets
- **Ghost Eye Worm** - hacking tool that uses random messaging on Facebook and other sites to perform a host of malicious efforts.
- **Logic Bomb** - Executes a program when a certain event happens or a date and time arrives.
- **Rootkit** - Set of malicious tools that are loaded on a compromised system through stealthy techniques; Very hard to detect;
- **Ransomware** - malicious software designed to deny access to a computer until a price is paid; usually spread through email

- **WannaCry** - famous ransomware; within 24 hours had 230,000 victims; exploited unpatched SMB vulnerability
 - **Other Examples**
 - Cryptorbit
 - CryptoLocker
 - CryptoDefense
 - police-themed
- **Trojan horse** - A program that is disguised as another legitimate program with the goal of carrying out malicious activities in the background without user's knowledge.
 - **RAT - Remote Access Trojans** - Malicious programs that run on systems and allow intruders to access and use a system remotely.
- **Immunizer** - Attaches code to a file or application, which would fool a virus into 'thinking' it was already infected. (e.g.: like human vaccine).
- **Behavior blocking** - Allowing the suspicious code to execute within the OS and watches its interactions looking for suspicious activities.

 - Viruses needs help/interaction to propagate; Worms self propagates

Major characteristics of viruses:

1. Infecting other files
2. Alteration of data
3. Transforms itself
4. Corruption of files and data
5. Encrypts itself
6. Self-replication

Stages of Virus Lifecycle:

1. Design
2. Replication
3. Launch
4. Detection
5. Incorporation - A.V. figures out the virus pattern & builds signatures to identify and eliminate the virus
6. Execution of the damage routine - A.V. to the rescue

Malware Basics

- **How is malware distributed?**
 - SEO manipulation
 - Social Engineering / Click-jacking
 - Phishing
 - Malvertising
 - Compromising legitimate sites

- Drive-by downloads
 - Spam
- **Malware** - software designed to harm or secretly access a computer system without informed consent
 - Most is downloaded from the Internet with or without the user's knowledge
- **Overt Channels** - legitimate communication channels used by programs
- **Covert Channels** - used to transport data in unintended ways
- **Wrappers** - programs that allow you to bind an executable to an innocent file

Basic components of Malware

1. **Crypters** - use a combination of encryption and code manipulation to render malware undetectable to security programs; protects from being scanned or found during analysis.
2. **Downloader** - Used to download additional malware.
3. **Dropper** - Used to install additional malware into the target system.
4. **Exploit** - Malicious code used to execute on a specific vulnerability.
5. **Injector** - Used to expose vulnerable processes in the target system to the exploit.
6. **Obfuscator** - Used to conceal the true purpose of the malware.
7. **Packers** - Used to bundle all of the malware files together into a single executable.
8. **Payload** - Used to take over the target machine.
9. **Malicious Code** - Used to define the abilities of the malware.

Exploit Kits - help deliver exploits and payloads

- Infinity
- Bleeding Life
- Crimepack
- Blackhole Exploit Kit

Trojans

- Software that appears to perform a desirable function but instead performs malicious activity
 - To hackers, it is a method to gain and maintain access to a system
 - Trojans are means of delivery whereas a backdoor provides the open access
 - Trojans are typically spread through **Social Engineering**.
- **Types of Trojans:**
 - **Defacement trojan**
 - **Proxy server trojan**
 - **Botnet trojan**
 - Chewbacca
 - Skynet
 - **Remote access trojans**
 - RAT

- MoSucker
 - Optix Pro
 - Blackhole
- **E-banking trojans**
 - Zeus
 - Spyeye
- **IoT Trojans**
- **Security Software Disable Trojans**
- **Command Shell Trojan** - Provides a backdoor to connect to through command-line access
 - Netcat
- **Covert Channel Tunneling Trojan (CCTT)** - a RAT trojan; creates data transfer channels in previously authorized data streams

Infection Process:

1. Creation of a Trojan using Trojan Construction Kit
2. Create a Dropper
 - Used to install additional malware into the target system.
3. Create a Wrapper
 - Wrappers - programs that allow you to bind an executable to an innocent file
4. Propagate the Trojan
5. Execute the Dropper

Trojan Port Numbers:

Trojan Name	TCP Port
Death	2
Senna Spy	20
Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	21
Shaft	22
Executor	80
Hackers Paradise	31,456
TCP Wrappers	421
Ini-Killer	555
Doom, Santaz Back	666
Silencer, WebEx	1001
DolyTrojan	1011
RAT	1095-98
SubSeven	1243
Shiva-Burka	1600
Trojan Cow	2001



Trojan Name	TCP Port
Deep Throat	6670-71
Tini	7777
Dumaru.Y	10000
SubSeven 1.0-1.8, MyDoom.B	10080
VooDoo Doll, NetBus 1.x, GabanBus, Pie Bill Gates, X-Bill	12345
Whack a Mole	12361-3
NetBus	17300
Back Orifice	31337,8
SubSeven, PhatBot, AgoBot, Gaobot	65506

⚠ - Its not necessary to know every possible trojan port in the history for the CEH exam, it's good for understanding.

Trojan Countermeasures

1. Avoid clicking on unusual or suspect email attachments
2. Block unused ports
3. Monitor network traffic
4. Avoid downloading from untrusted sources
5. Install & updated anti-virus software
6. Scan removable media before use
7. Validate file integrity of all externally sourced software
8. Enable auditing
9. Configure Host-Based firewalls
10. Use IDS

Techniques

- **netstat -an** - shows open ports in numerical order
- **netstat -b** - displays all active connections and the processes using them
- **Process Explorer** - Microsoft tool that shows you everything about running processes
- **Registry Monitoring Tools**
 - SysAnalyzer
 - Tiny Watcher
 - Active Registry Monitor
 - Regshot
- **Msconfig** - Windows program that shows all programs set to start on startup
- **Tripwire** - integrity verifier that can act as a HIDS in protection against trojans
- **SIGVERIF** - build into Windows to verify the integrity of the system
 - Log file can be found at `c:\windows\system32\sigverif.txt`
 - Look for drivers that are not signed

Malware Analysis

Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor.

Types of Malware analysis:

1. **Static (Code Analysis)** - performed by fragmenting the binary file into individual elements that can be analyzed without executing them.
 - o File fingerprinting
 - o Local & online scanning of elements to see if they match known malware profiles
 - o String searching
 - o Identifying packers/obfuscators used
 - o Identifying the PE's (portable executable) information
 - o Identify dependencies
 - o Malware disassembly
 2. **Dynamic (Behavioral Analysis)** - performed by executing the malware to see what effect it has on the system.
 - o System baselining
 - o Host integrity monitoring
- **Tools for Disassembling | Debugging | Reverse Engineering:**
 - o IDA Pro
 - o OllyDbg
 - o Ghidra by NSA
 - **Sheepdip** - Dedicated computer which is used to test files on removable media for viruses before they are allowed to be used with other computers.

Steps

1. Make sure you have a good test bed
 - o Use a VM with NIC in host-only mode and no open shares
 2. Analyze the malware on the isolated VM in a static state
 - o Tools - binText and UPX help with looking at binary
 3. Run the malware and check out processes
 - o Use Process Monitor, etc. to look at processes
 - o Use NetResident, TCPview or even Wireshark to look at network activity
 4. Check and see what files were added, changed, or deleted
 - o Tools - IDA Pro, VirusTotal, Anubis, Threat Analyzer
- **Preventing Malware**
 - o Make sure you know what is going on in your system
 - o Have a good antivirus that is up to date
 - Airgapped - isolated on network

Rootkits

- Software put in place by attacker to obscure system compromise
- Hides processes and files
- Also allows for future access
- **Examples**
 - Horsepill - Linus kernel rootkit inside initrd
 - Grayfish - Windows rootkit that injects in boot record
 - Firefef - multi-component family of malware
 - Azazel
 - Avatar
 - Necurs
 - ZeroAccess
- **Hypervisor level** - rootkits that modify the boot sequence of a host system to load a VM as the host OS
- **Hardware** - hide malware in devices or firmware
- **Boot loader level** - replace boot loader with one controlled by hacker
- **Application level** - directed to replace valid application files with Trojans
- **Kernel level** - attack boot sectors and kernel level replacing kernel code with back-door code; most dangerous
- **Library level** - use system-level calls to hide themselves
- One way to detect rootkits is to map all the files on a system and then boot a system from a clean CD version and compare the two file systems

Ways of Spread

Drive-by download: The unintended download of computer software from a website via the Internet. User's get infected by the download that happens without the knowledge, or without the understanding of the consequences.

Homogeneity: A setup where all the systems are running on the same operating system and connected to the same network.

Vulnerability: A security defect in software that can be attacked by malware.

Backdoor: An opening or break left in the operating systems, hardware, network or cybersecurity by design.

Types of Malware Attacks

0-Day: A zero-day vulnerability is an undisclosed flaw that hackers can exploit. It's called 0-day because it is not publicly reported or announced before becoming active.

Exploit: A threat made real via a successful attack on an existing vulnerability.

Privilege escalation: Another type of malware attacks is privilege escalation. A situation where the attacker gets escalated access to the restricted data.

Evasion: Evasion is another type of malware attack. The techniques malware maker design to avoid detection and analysis of their malware by security systems.

Blended threat: A malware package that combines the characteristics of multiple kinds of the malicious program like Trojans, viruses worms, seeking to exploit more than one system vulnerability.

Other Important Terms

Botnet: A number of Internet-connected devices that are running one or more bots. Botnets are used to perform distributed denial of service attacks, send spam, and steal data.

Containment: The process of stopping the spread of malware, and preventing further damage to hosts.

Endpoint: A security approach to the protection of computer networks that are remotely bridged to client devices.

Payload: The part of the malware program that actually does the damage.

Privilege: In computing, privilege means access to modify a system.

Signature: Signs that are specific to either a certain type of behavior or a specific item of malware.

Threat: In computing security, a computer or network is deemed under threat when it harbors persistent software vulnerabilities, thereby increasing the possibility or certainty of a malicious attack

Track: Evidence of an intrusion into a system or a network.

Zombie: The operating systems connected to the Internet that has been compromised by a hacker, computer virus. It can be used to perform malicious tasks.

Different Types of Malwares



Running into the word that starts with mal is a literal sign that something is bad. In general, most experts view the term malware as a contraction of two words — malicious software.

So much so that viruses are now just the tip of the iceberg.

Recent study data say that the majority of the malicious programs out there in the wild today are Trojans and computer worms, with viruses having declined in numbers. A 2011 study had Trojan horses amount to 69.99% of all malware tracked, while viruses only made up 16.82%. This is a number that has clearly gone up.

A more recent study in 2017 found that malware aimed at mobile devices like smartphones and tablets is increasing at an alarming rate, and even coming pre-installed on devices.

But what are the various types of malware, and how exactly are they classified?

Let's see how attackers install and deploy these malware types.

1. Viruses

The primary characteristic that a piece of software must possess to qualify as a virus is an urge to reproduce that is programmed into it. This mechanism means that this type of malware will distribute copies of itself, using any means to spread.

They hide within computer files, and the computer must run that file (execute that code, in other words) for a virus to do its dirty functions.

- Boot sector viruses
- file infecting viruses
- polymorphic viruses
- stealth viruses
- multi-partite viruses

1a. System or boot infectors

A virus can infect a system as a resident virus by installing itself as part of the operating system.

2a. File infectors

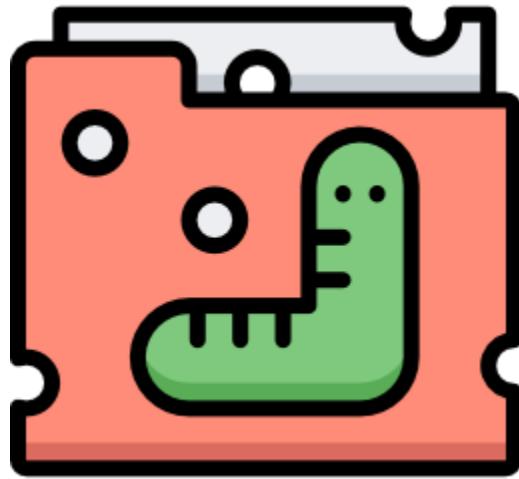
Many viruses sneak up into ordinary executable files like .EXE and .COM in order to up their chances of being run by a user. Programs including batch files and script files like .BAT, .JS, .VB, and .SCR extension is susceptible.

3a. Macro viruses

These kinds of viruses are the ones that run inside specific application files that allow macro programs in order to extend the capabilities of a given software.

Some infamous examples of viruses over the years are the Concept virus, the Chernobyl virus (also known as CIH), the Anna Kournikova virus, Brain and RavMonE.exe.

2. Worms



The second of the two kinds of infectious malware. A worm is a standalone software that replicates without targeting and infecting specific files that are already present on a computer. They usually target the operating system files and work until the drive they are in becomes empty.

Basically, whereas viruses add themselves inside existing files, worms carry themselves in their own containers.

Computer worms usually show up via email and instant messages. They use a computer network to spread.

3. Trojan Horses



A Trojan is a malicious program that misrepresents itself to appear as a legitimate program. The term is derived from the [Ancient Greek story](#) of the wooden horse that was used to invade the city of Troy by stealth — these are just as deadly on computers.

Trojan horse payload is usually a backdoor that allows attackers to gain access to the infected computer. Trojans also give cybercriminals access to the personal information of a user like IP addresses, passwords and banking details.

Trojan horse is now considered to be the most dangerous of all malicious program, particularly the ones that are designed to gain access and steal sensitive information from the victim's computer.

4. Rootkits



A [rootkit](#) is a collection of software specifically designed to permit malicious program that gathers sensitive information, into your system.

These software work like a back door for different types of malware to enter and gain access, and are now being used extensively by hackers to infect systems.

The root access in other words.

Detecting and removing a rootkit is difficult — more so in cases where the rootkit resides inside the kernel of an operating system. Reinstalling the operating systems is often the only solution to protect your PC.

Example – The first malicious rootkit to gain notoriety on Windows was NTRootkit in 1999, but the most popular is the [Sony BMG copy protection rootkit scandal](#).

5. Ransomware

The most devastating type of malicious programs, by some counts. Definitely one of the most advanced and constantly on the rise these days. [Ransomware](#) blocks access to the data of a victim, threatening to either publish it or delete it until a ransom is paid. Worse yet, there is no guarantee that paying a ransom will return access to the data, or prevent it from deletion. Usually, ransomware uses phishing to spread.

This manner of [digital extortion](#) has been in play since the late 80s, it returned to prominence in late 2013 with the advent of digital currency that is used to collect the ransom money.

6. Keyloggers



Software that records all the data that is typed using a keyboard. [Keyloggers](#) usually are not capable of recording information that is entered using virtual keyboards and other input devices, but physical keyboards are at risk with this type of malware.

Keyloggers store the gathered data and send it to the attacker, who can then extract sensitive data like username and passwords as well as credit card details.

7. Grayware

Grayware is a recently coined term that came into use around 2004. It is used to describe unwanted applications and files that though are not classified as a malicious program, can worsen the performance of computers and lead to security risks.

Grayware alludes to both adware and spyware. Almost all commercially available security software can detect these potentially unwanted programs.

7a. Adware



Although ad-supported software is now much more common types and known as adware in some circles, the word has been linked to malicious program for quite some time. While adware can refer to any program that is supported by advertising, malicious adware usually shows advertisements in the form of popups and windows.

It is perhaps the most lucrative and least harmful malware, designed with the specific purpose of displaying advertisements on your computer.

Botnet

Is a group of computers connected for malicious purpose? Botnet affect the victim machine by slowing it down through a DDOS and DOS

7b. Spyware



[Spyware](#), as the name gives away, is software that constantly spies on you. Its main purpose is to keep track of your Internet activity in order to send adware. Spyware is also used to gather sensitive information about an organization without their knowledge, and send that data to another entity, without consent of the victim.

What can Hackers do with Malware?

Hackers can gain full access to your computer using the malicious program. They can steal your sensitive files like images and personal videos. They can deploy keyloggers that could steal your confidential information like bank login details and credit card information. Or simply hackers could use your PC to deploy an attack.

What is the Most Dangerous Malware?

All malicious program is created to harm the users. While some of them are just to annoy users and track their activity, others could cause significant damage. Some of the most dangerous malware are Ransomware, Rootkits, and Trojan horse.

Is a Virus a Type of Malware?

Yes, malware is a malicious program. Every software that is created with malicious intent is malware. Viruses are designed to delete and corrupt the user's data. Thus they are malicious.

How is Malware Spread?

The malicious program uses various means to spread. Some of the major methods are drive-by download, homogeneity, vulnerability, and backdoor.

What makes machines vulnerable?

- Use of the same OS
- Software bugs
- Human error
- Misconfiguration
- Over privileged users
- Un-updated systems

How to prevent machine vulnerability

Antimalware strategies

- Website security scan
- Eliminating over privileged code

Attacking methodologies

1. **Peer to peer;** connects to a server the users Gnutella, an open-source file sharing technology and file sharing protocol. An attack that initiates the process by serving as a peer in a p2p network and sending commands to the victim which they can pass them to others.
2. **Botnets (zombies)** hackers can install bots in multiple computers via such methods; email attachments. Can also set up botnet machines connected remotely.
3. **Hybrid threats** hackers can write worms to create hybrid threats
4. **Spam** this it the sending of unsolicited emails and also hide the sender's identity

SQL Injection

SQL Injection is considered as one of the most common attacks as it can bring serious and harmful consequences to your system and sensitive data.

WHAT IS AN SQL INJECTION

How To Prevent From SQL Injection Attacks



© www.SoftwareTestingHelp.com

What is SQL Injection?

Some of the user inputs might be used in framing SQL Statements which are then executed by the application on the database. It is NOT possible for an application to handle the inputs given by the user properly.

If this is the case, a malicious user could provide unexpected inputs to the application that are then used to frame and execute SQL statements on the database. This is called SQL Injection. The consequences of such an action could be alarming.

As the name itself implies, the purpose of the SQL Injection attack is to inject the malicious SQL code.

Each and every field of a website is like a gate to the database. In the login form, the user enters the login data, in the search field the user enters a search text, and in the data saving form the user enters data to be saved. All the indicated data goes to the database.

Instead of correct data, if any malicious code is entered, then there is a possibility for some serious damage to happen to the database and the whole system.

SQL Injection is performed with the SQL programming language. SQL (Structured Query Language) is used for managing the data held in the database. Therefore during this attack, this programming language code is being used as a malicious injection.

This is one of the most popular attacks, as databases are used for almost all technologies.

Most of the applications use some type of database. An application under test might have a user interface that accepts user input that is used to perform the following tasks:

#1) Show the relevant stored data to the user e.g., the application checks the credentials of the user using the login information entered by the user and exposes only the relevant functionality and data to the user.

#2) Save the data entered by the user to the database e.g. once the user fills up a form and submits it, the application proceeds to save the data to the database; this data is then made available to the user in the same session as well as in the subsequent sessions.

Recommended Tools

#1) Acunetix



Acunetix is a web application security scanner with the capabilities for managing the security of all web assets. It can detect over 7000 vulnerabilities including SQL injection. It uses advanced macro recording technology that enables you to scan complex multi-level forms as well as password-protected areas of the site.

There will be no lengthy setup or onboarding time. The tool is intuitive and easy to use. Scanning will be performed at lightning-fast speed. It helps with automating the security through features like scheduling & prioritizing the scans, automatic scanning of new builds, etc

#2) Netsparker



Netsparker offers the SQL Injection Vulnerability Scanner that has features of automatic detection of all variants of the injection vulnerability like blind, out-of-bound, in-band, etc.

It uses the Proof-Based Scanning™ Technology. It offers functionalities for penetration testing, remote file inclusions, checking the web servers for misconfigurations, cross-site scripting, etc. Netsparker can be seamlessly integrated with your current systems.

Risks of SQL Injection



Nowadays, a database is being used for almost all the systems and websites, as data should be stored somewhere.

As sensitive data is being stored in the database, there are more risks involved in the system's security. If any personal website or blog's data would be stolen, then there won't be much damage when compared to the data that would be stolen from the banking system.

The main purpose of this attack is to hack the system's database, therefore this attack's consequences can really be harmful.

The following things might result from SQL Injection

- Hacking other person's account.
- Stealing and copying website's or system's sensitive data.
- Changing the system's sensitive data.
- Deleting system's sensitive data.
- The user can log in to the application as another user, even as an administrator.
- Users can view private information belonging to other users e.g., details of the other users' profiles, transaction details, etc.
- The user could change application configuration information and the data of the other users.
- The user could modify the structure of the database; even delete tables in the application database.
- The user can take control of the database server and execute commands on it at will.

The above-listed risks can really be considered serious, as restoring a database or its data can cost a lot. It can cost your company a reputation and money to restore lost data and systems.

Therefore it is highly recommended to protect your system against this type of attack and consider Security Testing as a good investment in your product's and company's reputation.

As a tester, I would like to comment, that testing against possible attacks is a good practice even if [Security Testing](#) was not planned. This way you can protect and test the product against unexpected cases and malicious users.

The Essence of this Attack

As mentioned earlier, the essence of this attack is to hack the database with malicious purpose.

In order to perform this Security Testing, initially, you need to find the vulnerable system parts and then send malicious SQL code through them to the database. If this attack is possible for a system, then appropriate malicious SQL code will be sent and harmful actions may be performed in the database.

Each and every field of a website is like a gate to the database. Any data or input that we usually enter into any field of the system or website goes to the database query. Therefore, instead of correct data, if we type any malicious code, then it may be executed in the database query and bring harmful consequences.



In order to perform this attack, we have to change the act and purpose of the appropriate database query. One possible method to perform it is to make the query always true and insert your malicious code after that. Changing the database query to always true can be performed with simple code like ‘ or 1=1;—.



Testers should keep in mind, that while checking if changing the query to always true can be performed or not, different quotes should be tried – single and double. Therefore, if we have tried code like ‘ or 1=1;—, we should also try the code with double quotes “ or 1=1;—.



For example, let's consider that we have a query, that is searching for the entered word in the database table:

```
select * from notes nt where nt.subject = 'search_word';
```

Therefore instead of the search word, if we enter a SQL Injection query ‘ or 1=1;—, then the query will always become true.

```
select * from notes nt where nt.subject = ' ' or 1=1;—
```

In this case, the parameter “subject“ is closed with the quote and then we have code or 1=1, which makes a query always true. With the sign “—“ we comment on the rest of the query code, which will not be executed. It is one of the most popular and easiest ways to start controlling the query.

Few other codes may also be used to make the query always true, like:

- ‘ or ‘abc’=‘abc’;—
- ‘ or ‘ ‘=‘ ‘;—

The most important part here is that after the comma sign we can enter any malicious code that we would like to be executed.

For Example, it may be ‘ or 1=1; drop table notes; —

```
' or 1=1; drop table notes; --
```

If this injection is possible, then any other malicious code may be written. In this case, it will only depend on the malicious user's knowledge and intention. How to Check SQL Injection?

Checking for this vulnerability can be performed very easily. Sometimes it is enough to type ‘ or “ sign in the tested fields. If it returns any unexpected or extraordinary message, then we can be sure that SQL Injection is possible for that field.

For Example, if you get an error message like ‘Internal Server Error‘ as a search result, then we can be sure that this attack is possible in that part of the system.

Other results that may notify a possible attack include:

- Blank page loaded.
- No error or success messages – functionality and page do not react to the input.
- Success message for malicious code.

Let's look around at how this works in practice.

For Example, Let's test if an appropriate login window is vulnerable for SQL Injection. **In the email address or password field, just type sign in as shown below.**



If such input returns result like error message ‘Internal Server Error‘ or any other listed inappropriate result, then we can almost be sure that this attack is possible for that field.

Internal Server Error

A very tricky **SQL Injection code** may also be tried. I would like to mention, that in my career I have not encountered any cases when there was an ‘Internal Server Error’ message as a result of the sign, but at times the fields did not react to more complicated SQL code.

Therefore, checking for SQL Injections with a single quote ‘ is quite a trustworthy way to check if this attack is possible or not.

If the single quote does not return any inappropriate results, then we can try to enter double quotes and check the results.



Also, SQL code for changing the query to always true can be considered as a way to check if this attack is possible or not. It closes the parameter and changes the query to ‘true’. Therefore if not being validated, such input can also return any unexpected result and inform the same, that this attack is possible in this case.



Checking for possible SQL attacks can also be performed from the website’s link. Suppose we have a website’s link as <http://www.testing.com/books=1>. In this case ‘books‘ is a parameter and ‘1‘ is its value. If in the provided link we would write ‘ sign instead of 1, then we would check for possible injections.

Therefore link [http://www.testing.com/books=](http://www.testing.com/books=') will be like a test if the SQL attack is possible for the website <http://www.testing.com> or not.



In this case, if link [http://www.testing.com/books=](http://www.testing.com/books=') returns an error message like ‘Internal Server Error‘ or a blank page or any other unexpected error message, then also we can be sure that SQL Injection is possible for that website. Later, we can try to send more tricky SQL code through the website’s link.

To check if this attack is possible through the website’s link or not, code like ‘ or 1=1;– can also be sent.



As an experienced software tester, I would like to remind, that not only the unexpected error message can be considered as a SQL Injection vulnerability, but many testers check for possible attacks only in accordance with error messages.

However, it should be remembered that no validation error message or successful message for malicious code can also be a sign that this attack could be possible.

Security Testing of Web Applications Against SQL Injection

Security testing of web applications explained with simple examples:

Since the consequences of allowing this vulnerability technique could be severe, it follows that this attack should be tested during the security testing of an application. Now with an overview of this technique, let us understand a few practical examples of SQL injection.

Important: This SQL Injection Test should be tested only in the test environment.

If the application has a login page, it is possible that the application uses dynamic SQL such as the statement below. This statement is expected to return at least a single row with the user details from the Users table as the result set when there is a row with the username and password entered in the SQL statement.

```
SELECT * FROM Users WHERE User_Name = '' & strUserName & " AND Password = '' & strPassword & "';"
```

If the tester would enter John as the strUserName (in the textbox for username) and Smith as strPassword (in the textbox for password), then the above SQL statement would become:

```
SELECT * FROM Users WHERE User_Name = 'John' AND Password = 'Smith';
```

If the tester would enter John'-- as strUserName and no strPassword, then the SQL statement would become:

```
SELECT * FROM Users WHERE User_Name = 'John'-- AND Password = 'Smith';
```

Note that the part of the SQL statement after John is turned into a comment. If there are any users with the username of John in the Users table, the application will allow the tester to log in as the user John. The tester can now view the private information of the user John.

What if the tester does not know the name of any existing user of the application? In this case, the tester can try common usernames like admin, administrator, and sysadmin.

If none of these users exists in the database, then the tester could enter John' or 'x'='x as strUserName and Smith' or 'x'='x as strPassword. This would cause the SQL statement to become like the one below.

```
SELECT * FROM Users WHERE User_Name = 'John' or 'x'='x' AND Password = 'Smith' or 'x'='x';
```

Since 'x'='x' condition is always true, the result set would consist of all the rows in the Users table. The application will allow the tester to log in as the first user in the Users table.

Important: The tester should request the database administrator or the developer to copy the table in question before attempting the following attacks.

If the tester would enter John'; DROP table users_details;—as strUserName and anything as strPassword, then the SQL statement would be like the one below.

```
SELECT * FROM Users WHERE User_Name = 'John'; DROP table users_details; -- AND Password = 'Smith';
```

This statement could cause the table “users_details” to be permanently deleted from the database.

Though the above examples deal with using the SQL injection technique only in the login page, the tester should test this technique on all the pages of the application that accept user input in textual format e.g. search pages, feedback pages, etc.

SQL injection might be possible in applications that use SSL. Even a firewall might not be able to protect the application against this technique.

I have tried to explain this attack technique in a simple form. I would like to re-iterate that this attack should be tested only in a test environment and not in the development environment, production environment or any other environment.

Instead of manually testing whether the application is vulnerable to SQL attack or not, one could use a [Web Vulnerability Scanner](#) that checks for this vulnerability.

Vulnerable Parts of this Attack

Before starting the testing process, every sincere tester should more or less know which parts would be most vulnerable to this attack.

It is also a good practice to plan which field of the system is to be tested exactly and in what order. In my testing career, I have learned that it is not a good idea to test fields against SQL attacks randomly as some fields can be missed.

As this attack is being performed in the database, all data entry system parts, input fields, and website links are vulnerable.

Vulnerable parts include:

- Login fields
- Search fields
- Comment fields
- Any other data entry and saving fields
- Website links

It is important to note that while testing against this attack, it is not enough to check only one or a few fields. It is quite common, that one field may be protected against SQL Injection, but then another does not. Therefore it is important not to forget to test all the website's fields.

Automating SQL Injection Tests

As some tested systems or websites can be quite complicated and contain sensitive data, testing manually can be really difficult and it takes a lot of time too. Therefore testing against this attack with special tools can really be helpful at times.

One such SQL Injection tool is [SOAP UI](#). If we have automated regression tests at the API level, then we can also switch checks against this attack using this tool. The SOAP UI tool already has code templates to check against this attack. These templates can also be supplemented by your own written code. It is quite a reliable tool.

However, a test should already be automated at the API level, which is not that easy. Another possible way to test automatically is by using various browser plugins.

It is worth mentioning, that even if automated tools save your time, they are not always considered to be very reliable. If you are testing a banking system or any website with very sensitive data, it is highly recommended to test it manually. You can see the exact results and analyze them. Also, in this case, we can be sure that nothing was skipped.

Comparison with Other Attacks

SQL Injection can be considered as one of the most serious attacks, as it influences the database and can cause serious damage to your data and the whole system.

For sure it can have more serious consequences than a Javascript Injection or HTML Injection, as both of them are performed on the client-side. For comparison, with this attack, you can have access to the whole database.

In order to test against this attack, you should have quite a good knowledge of SQL programming language and in general, you should know how database queries are working. Also while performing this injection attack, you should be more careful and observant, as any inaccuracy can be left as SQL vulnerabilities.

Conclusion

We hope you would have got a clear idea of what a SQL Injection is and how we should prevent these attacks.

However, it is highly recommended to test against this type of attack every time a system or website with a database is being tested. Any left database or system vulnerabilities can cost the company's reputation as well as a lot of resources to restore the whole system.

As testing against this injection helps to find the most important security vulnerabilities, it is also recommended to invest your knowledge along with testing tools. If Security Testing is planned, then testing against SQL Injection should be planned as one of the first testing parts.

Cross-site Scripting (XSS)

In this section, we'll explain what cross-site scripting is, describe the different varieties of cross-site scripting vulnerabilities, and spell out how to find and prevent cross-site scripting.

What is cross-site scripting (XSS)?

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

How does XSS work?

Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript to users. When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the application.



Labs

If you're already familiar with the basic concepts behind XSS vulnerabilities and just want to practice exploiting them on some realistic, deliberately vulnerable targets, you can access all of the labs in this topic from the link below.

[View all XSS labs](#)

XSS proof of concept

You can confirm most kinds of XSS vulnerability by injecting a payload that causes your own browser to execute some arbitrary JavaScript. It's long been common practice to use the `alert()` function for this purpose because it's short, harmless, and pretty hard to miss when it's successfully called. In fact, you solve the majority of our XSS labs by invoking `alert()` in a simulated victim's browser.

Unfortunately, there's a slight hitch if you use Chrome. From version 92 onward (July 20th, 2021), cross-origin iframes are prevented from calling `alert()`. As these are used to construct some of the more advanced XSS attacks, you'll sometimes need to use an alternative PoC payload. In this scenario, we recommend the `print()` function. If you're interested in learning more about this change and why we like `print()`, [check out our blog post](#) on the subject.

As the simulated victim in our labs uses Chrome, we've amended the affected labs so that they can also be solved using `print()`. We've indicated this in the instructions wherever relevant.

What are the types of XSS attacks?

There are three main types of XSS attacks. These are:

- [Reflected XSS](#), where the malicious script comes from the current HTTP request.
- [Stored XSS](#), where the malicious script comes from the website's database.
- [DOM-based XSS](#), where the vulnerability exists in client-side code rather than server-side code.

Reflected cross-site scripting

Reflected XSS is the simplest variety of cross-site scripting. It arises when an application receives data in an HTTP request and includes that data within the immediate response in an unsafe way.

Here is a simple example of a reflected XSS vulnerability:

`https://insecure-website.com/status?message>All+is+well. <p>Status: All is well.</p>`

The application doesn't perform any other processing of the data, so an attacker can easily construct an attack like this:



`https://insecure-website.com/status?message=<script>/*+Bad+stuff+here...+*</script> <p>Status: <script>/* Bad stuff here... *</script></p>`

If the user visits the URL constructed by the attacker, then the attacker's script executes in the user's browser, in the context of that user's session with the application. At that point, the script can carry out any action, and retrieve any data, to which the user has access.

Reflected XSS

In this section, we'll explain reflected cross-site scripting, describe the impact of reflected XSS attacks, and spell out how to find reflected XSS vulnerabilities.

What is reflected cross-site scripting?

Reflected cross-site scripting (or XSS) arises when an application receives data in an HTTP request and includes that data within the immediate response in an unsafe way.

Suppose a website has a search function which receives the user-supplied search term in a URL parameter:

`https://insecure-website.com/search?term=gif`

The application echoes the supplied search term in the response to this URL:

`<p>You searched for: gift</p>`

Assuming the application doesn't perform any other processing of the data, an attacker can construct an attack like this:

`https://insecure-website.com/search?term=<script>/*+Bad+stuff+here...+*</script>`

This URL results in the following response:

`<p>You searched for: <script>/* Bad stuff here... *</script></p>`

If another user of the application requests the attacker's URL, then the script supplied by the attacker will execute in the victim user's browser, in the context of their session with the application.

Impact of reflected XSS attacks

If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user. Amongst other things, the attacker can:

- Perform any action within the application that the user can perform.



- View any information that the user is able to view.
- Modify any information that the user is able to modify.
- Initiate interactions with other application users, including malicious attacks, that will appear to originate from the initial victim user.

There are various means by which an attacker might induce a victim user to make a request that they control, to deliver a reflected XSS attack. These include placing links on a website controlled by the attacker, or on another website that allows content to be generated, or by sending a link in an email, tweet or other message. The attack could be targeted directly against a known user, or could be an indiscriminate attack against any users of the application:

The need for an external delivery mechanism for the attack means that the impact of reflected XSS is generally less severe than [stored XSS](#), where a self-contained attack can be delivered within the vulnerable application itself.

Reflected XSS in different contexts

There are many different varieties of reflected cross-site scripting. The location of the reflected data within the application's response determines what type of payload is required to exploit it and might also affect the impact of the vulnerability.

In addition, if the application performs any validation or other processing on the submitted data before it is reflected, this will generally affect what kind of XSS payload is needed.

How to find and test for reflected XSS vulnerabilities

The vast majority of reflected cross-site scripting vulnerabilities can be found quickly and reliably using Burp Suite's [web vulnerability scanner](#).

Testing for reflected XSS vulnerabilities manually involves the following steps:

- **Test every entry point.** Test separately every entry point for data within the application's HTTP requests. This includes parameters or other data within the URL query string and message body, and the URL file path. It also includes HTTP headers, although XSS-like behavior that can only be triggered via certain HTTP headers may not be exploitable in practice.
- **Submit random alphanumeric values.** For each entry point, submit a unique random value and determine whether the value is reflected in the response. The value should be designed to survive most input validation, so needs to be fairly short and contain only alphanumeric characters. But it needs to be long enough to make accidental matches within the response highly unlikely. A random alphanumeric value of around 8 characters is normally ideal. You can use Burp Intruder's number payloads [https://portswigger.net/burp/documentation/desktop/tools/intruder/payloads/types#numbers] with randomly generated hex values to generate suitable random values. And you can use Burp Intruder's [grep payloads option](#) to automatically flag responses that contain the submitted value.
- **Determine the reflection context.** For each location within the response where the random value is reflected, determine its context. This might be in text between HTML tags, within a tag attribute which might be quoted, within a JavaScript string, etc.

- **Test a candidate payload.** Based on the context of the reflection, test an initial candidate XSS payload that will trigger JavaScript execution if it is reflected unmodified within the response. The easiest way to test payloads is to send the request to [Burp Repeater](#), modify the request to insert the candidate payload, issue the request, and then review the response to see if the payload worked. An efficient way to work is to leave the original random value in the request and place the candidate XSS payload before or after it. Then set the random value as the search term in Burp Repeater's response view. Burp will highlight each location where the search term appears, letting you quickly locate the reflection.
- **Test alternative payloads.** If the candidate XSS payload was modified by the application, or blocked altogether, then you will need to test alternative payloads and techniques that might deliver a working XSS attack based on the context of the reflection and the type of input validation that is being performed. For more details, see [cross-site scripting contexts](#)
- **Test the attack in a browser.** Finally, if you succeed in finding a payload that appears to work within Burp Repeater, transfer the attack to a real browser (by pasting the URL into the address bar, or by modifying the request in [Burp Proxy's intercept view](#), and see if the injected JavaScript is indeed executed. Often, it is best to execute some simple JavaScript like `alert(document.domain)` which will trigger a visible popup within the browser if the attack succeeds.

Common questions about reflected cross-site scripting

What is the difference between reflected XSS and stored XSS? Reflected XSS arises when an application takes some input from an HTTP request and embeds that input into the immediate response in an unsafe way. With stored XSS, the application instead stores the input and embeds it into a later response in an unsafe way.

What is the difference between reflected XSS and self-XSS? Self-XSS involves similar application behavior to regular reflected XSS, however it cannot be triggered in normal ways via a crafted URL or a cross-domain request. Instead, the vulnerability is only triggered if the victim themselves submits the XSS payload from their browser. Delivering a self-XSS attack normally involves socially engineering the victim to paste some attacker-supplied input into their browser. As such, it is normally considered to be a lame, low-impact issue.

Stored XSS

In this section, we'll explain stored cross-site scripting, describe the impact of stored XSS attacks, and spell out how to find stored XSS vulnerabilities.

What is stored cross-site scripting?

Stored cross-site scripting (also known as second-order or persistent XSS) arises when an application receives data from an untrusted source and includes that data within its later HTTP responses in an unsafe way.

Suppose a website allows users to submit comments on blog posts, which are displayed to other users. Users submit comments using an HTTP request like the following:

```
POST /post/comment HTTP/1.1 Host: vulnerable-website.com Content-Length: 100
postId=3&comment=This+post+was+extremely+helpful.&name=Carlos+Montoya&email=carlos%40normal-
user.net
```

After this comment has been submitted, any user who visits the blog post will receive the following within the application's response:

```
<p>This post was extremely helpful.</p>
```

Assuming the application doesn't perform any other processing of the data, an attacker can submit a malicious comment like this:

```
<script>/* Bad stuff here... */</script>
```

Within the attacker's request, this comment would be URL-encoded as:

```
comment=%3Cscript%3E%2F*%2BBad%2Bstuff%2Bhere...%2B*%2F%3C%2Fscript%3E
```

Any user who visits the blog post will now receive the following within the application's response:

```
<p><script>/* Bad stuff here... */</script></p>
```

The script supplied by the attacker will then execute in the victim user's browser, in the context of their session with the application.

Impact of stored XSS attacks

If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user. The attacker can carry out any of the actions that are applicable to the impact of [reflected XSS vulnerabilities](#).

In terms of exploitability, the key difference between reflected and stored XSS is that a stored XSS vulnerability enables attacks that are self-contained within the application itself. The attacker does not need to find an external way of inducing other users to make a particular request containing their exploit. Rather, the attacker places their exploit into the application itself and simply waits for users to encounter it.

The self-contained nature of stored cross-site scripting exploits is particularly relevant in situations where an XSS vulnerability only affects users who are currently logged in to the application. If the XSS is reflected, then the attack must be fortuitously timed: a user who is induced to make the attacker's request at a time when they are not logged in will not be compromised. In contrast, if the XSS is stored, then the user is guaranteed to be logged in at the time they encounter the exploit.

Stored XSS in different contexts



There are many different varieties of stored cross-site scripting. The location of the stored data within the application's response determines what type of payload is required to exploit it and might also affect the impact of the vulnerability.

In addition, if the application performs any validation or other processing on the data before it is stored, or at the point when the stored data is incorporated into responses, this will generally affect what kind of XSS payload is needed.

How to find and test for stored XSS vulnerabilities

Many stored XSS vulnerabilities can be found using Burp Suite's [web vulnerability scanner](#).

Testing for stored XSS vulnerabilities manually can be challenging. You need to test all relevant "entry points" via which attacker-controllable data can enter the application's processing, and all "exit points" at which that data might appear in the application's responses.

Entry points into the application's processing include:

- Parameters or other data within the URL query string and message body.
- The URL file path.
- HTTP request headers that might not be exploitable in relation to [reflected XSS](#).
- Any out-of-band routes via which an attacker can deliver data into the application. The routes that exist depend entirely on the functionality implemented by the application: a webmail application will process data received in emails; an application displaying a Twitter feed might process data contained in third-party tweets; and a news aggregator will include data originating on other web sites.

The exit points for stored XSS attacks are all possible HTTP responses that are returned to any kind of application user in any situation.

The first step in testing for stored XSS vulnerabilities is to locate the links between entry and exit points, whereby data submitted to an entry point is emitted from an exit point. The reasons why this can be challenging are that:

- Data submitted to any entry point could in principle be emitted from any exit point. For example, user-supplied display names could appear within an obscure audit log that is only visible to some application users.
- Data that is currently stored by the application is often vulnerable to being overwritten due to other actions performed within the application. For example, a search function might display a list of recent searches, which are quickly replaced as users perform other searches.

To comprehensively identify links between entry and exit points would involve testing each permutation separately, submitting a specific value into the entry point, navigating directly to the exit point, and determining whether the value appears there. However, this approach is not practical in an application with more than a few pages.

Instead, a more realistic approach is to work systematically through the data entry points, submitting a specific value into each one, and monitoring the application's responses to detect cases where the submitted value appears. Particular attention can be paid to relevant application functions, such as comments on blog posts. When the submitted value is observed in a response, you need to determine whether the data is indeed being stored across different requests, as opposed to being simply reflected in the immediate response.

When you have identified links between entry and exit points in the application's processing, each link needs to be specifically tested to detect if a stored XSS vulnerability is present. This involves determining the context within the response where the stored data appears and testing suitable candidate XSS payloads that are applicable to that context. At this point, the testing methodology is broadly the same as for finding reflected XSS vulnerabilities.

DOM-based XSS

In this section, we'll describe DOM-based [cross-site scripting](#) (DOM XSS), explain how to find DOM XSS vulnerabilities, and talk about how to exploit DOM XSS with different sources and sinks.

What is DOM-based cross-site scripting?

DOM-based XSS vulnerabilities usually arise when JavaScript takes data from an attacker-controllable source, such as the URL, and passes it to a sink that supports dynamic code execution, such as eval() or innerHTML. This enables attackers to execute malicious JavaScript, which typically allows them to hijack other users' accounts.

To deliver a DOM-based XSS attack, you need to place data into a source so that it is propagated to a sink and causes execution of arbitrary JavaScript.

The most common source for DOM XSS is the URL, which is typically accessed with the window.location object. An attacker can construct a link to send a victim to a vulnerable page with a payload in the query string and fragment portions of the URL. In certain circumstances, such as when targeting a 404 page or a website running PHP, the payload can also be placed in the path.

For a detailed explanation of the taint flow between sources and sinks, please refer to the [DOM-based vulnerabilities](#) page.

How to test for DOM-based cross-site scripting

The majority of DOM XSS vulnerabilities can be found quickly and reliably using Burp Suite's [web vulnerability scanner](#). To test for DOM-based cross-site scripting manually, you generally need to use a browser with developer tools, such as Chrome. You need to work through each available source in turn, and test each one individually.

Testing HTML sinks

To test for DOM XSS in an HTML sink, place a random alphanumeric string into the source (such as `location.search`), then use developer tools to inspect the HTML and find where your string appears. Note that the browser's "View source" option won't work for DOM XSS testing because it doesn't take account of changes that have been performed in the HTML by JavaScript. In Chrome's developer tools, you can use Control+F (or Command+F on MacOS) to search the DOM for your string.

For each location where your string appears within the DOM, you need to identify the context. Based on this context, you need to refine your input to see how it is processed. For example, if your string appears within a double-quoted attribute then try to inject double quotes in your string to see if you can break out of the attribute.

Note that browsers behave differently with regards to URL-encoding. Chrome, Firefox, and Safari will URL-encode `location.search` and `location.hash`, while IE11 and Microsoft Edge (pre-Chromium) will not URL-encode these sources. If your data gets URL-encoded before being processed, then an XSS attack is unlikely to work.

Testing JavaScript execution sinks

Testing JavaScript execution sinks for DOM-based XSS is a little harder. With these sinks, your input doesn't necessarily appear anywhere within the DOM, so you can't search for it. Instead you'll need to use the JavaScript debugger to determine whether and how your input is sent to a sink.

For each potential source, such as `location`, you first need to find cases within the page's JavaScript code where the source is being referenced. In Chrome's developer tools, you can use Control+Shift+F (or Command+Alt+F on MacOS) to search all the page's JavaScript code for the source.

Once you've found where the source is being read, you can use the JavaScript debugger to add a break point and follow how the source's value is used. You might find that the source gets assigned to other variables. If this is the case, you'll need to use the search function again to track these variables and see if they're passed to a sink. When you find a sink that is being assigned data that originated from the source, you can use the debugger to inspect the value by hovering over the variable to show its value before it is sent to the sink. Then, as with HTML sinks, you need to refine your input to see if you can deliver a successful XSS attack.

Testing for DOM XSS using DOM Invader

Identifying and exploiting DOM XSS in the wild can be a tedious process, often requiring you to manually trawl through complex, minified JavaScript. If you use Burp's embedded browser, however, you can take advantage of its built-in DOM Invader extension, which does a lot of the hard work for you.

Exploiting DOM XSS with different sources and sinks

In principle, a website is vulnerable to DOM-based cross-site scripting if there is an executable path via which data can propagate from source to sink. In practice, different sources and sinks have differing properties and behavior that can affect exploitability, and determine what techniques are necessary. Additionally, the website's scripts might perform validation or other processing of data that must be accommodated when attempting to exploit a vulnerability. There are a variety of sinks that are relevant to DOM-based vulnerabilities. Please refer to the [list](#) below for details.

The document.write sink works with script elements, so you can use a simple payload, such as the one below:

```
document.write('... <script>alert(document.domain)</script> ...');
```

LAB

APPRENTICE [DOM XSS in document.write sink using source location.search](#)

Note, however, that in some situations the content that is written to document.write includes some surrounding context that you need to take account of in your exploit. For example, you might need to close some existing elements before using your JavaScript payload.

LAB

PRACTITIONER [DOM XSS in document.write sink using source location.search inside a select element](#)

The innerHTML sink doesn't accept script elements on any modern browser, nor will svg onload events fire. This means you will need to use alternative elements like img or iframe. Event handlers such as onload and onerror can be used in conjunction with these elements. For example:

```
element.innerHTML='... <img src=1 onerror=alert(document.domain)> ...'
```

LAB

APPRENTICE [DOM XSS in innerHTML sink using source location.search](#)

Sources and sinks in third-party dependencies

Modern web applications are typically built using a number of third-party libraries and frameworks, which often provide additional functions and capabilities for developers. It's important to remember that some of these are also potential sources and sinks for DOM XSS.

[DOM XSS in jQuery](#)

If a JavaScript library such as jQuery is being used, look out for sinks that can alter DOM elements on the page. For instance, jQuery's attr() function can change the attributes of DOM elements. If data is read from a user-controlled source like the URL, then passed to the attr()



function, then it may be possible to manipulate the value sent to cause XSS. For example, here we have some JavaScript that changes an anchor element's href attribute using data from the URL:

```
$(function() { $('#backLink').attr("href", (new URLSearchParams(window.location.search)).get('returnUrl'))});
```

You can exploit this by modifying the URL so that the location.search source contains a malicious JavaScript URL. After the page's JavaScript applies this malicious URL to the back link's href, clicking on the back link will execute it:

```
?returnUrl=javascript:alert(document.domain)
```

LAB

APPRENTICE [DOM XSS in jQuery anchor href attribute sink using location.search source](#)

Another potential sink to look out for is jQuery's \$() selector function, which can be used to inject malicious objects into the DOM.

jQuery used to be extremely popular, and a classic DOM XSS vulnerability was caused by websites using this selector in conjunction with the location.hash source for animations or auto-scrolling to a particular element on the page. This behavior was often implemented using a vulnerable hashchange event handler, similar to the following:

```
$(window).on('hashchange', function() { var element = $(location.hash); element[0].scrollIntoView(); });
```

As the hash is user controllable, an attacker could use this to inject an XSS vector into the \$() selector sink. More recent versions of jQuery have patched this particular vulnerability by preventing you from injecting HTML into a selector when the input begins with a hash character (#). However, you may still find vulnerable code in the wild.

To actually exploit this classic vulnerability, you'll need to find a way to trigger a hashchange event without user interaction. One of the simplest ways of doing this is to deliver your exploit via an iframe:

```
<iframe src="https://vulnerable-website.com#" onload="this.src+='<img src=1 onerror=alert(1)>'>
```

In this example, the src attribute points to the vulnerable page with an empty hash value. When the iframe is loaded, an XSS vector is appended to the hash, causing the hashchange event to fire.

Note

Even newer versions of jQuery can still be vulnerable via the \$() selector sink, provided you have full control over its input from a source that doesn't require a # prefix.

LAB

APPRENTICE [DOM XSS in jQuery selector sink using a hashchange event](#)



DOM XSS in AngularJS

If a framework like AngularJS is used, it may be possible to execute JavaScript without angle brackets or events. When a site uses the ng-app attribute on an HTML element, it will be processed by AngularJS. In this case, AngularJS will execute JavaScript inside double curly braces that can occur directly in HTML or inside attributes.

LAB

PRACTITIONER [DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded](#)

DOM XSS combined with reflected and stored data

Some pure DOM-based vulnerabilities are self-contained within a single page. If a script reads some data from the URL and writes it to a dangerous sink, then the vulnerability is entirely client-side.

However, sources aren't limited to data that is directly exposed by browsers - they can also originate from the website. For example, websites often reflect URL parameters in the HTML response from the server. This is commonly associated with normal XSS, but it can also lead to so-called reflected+DOM vulnerabilities.

In a reflected+DOM vulnerability, the server processes data from the request, and echoes the data into the response. The reflected data might be placed into a JavaScript string literal, or a data item within the DOM, such as a form field. A script on the page then processes the reflected data in an unsafe way, ultimately writing it to a dangerous sink.

```
eval(var data = "reflected string");
```

LAB

PRACTITIONER [Reflected DOM XSS](#)

Websites may also store data on the server and reflect it elsewhere. In a stored+DOM vulnerability, the server receives data from one request, stores it, and then includes the data in a later response. A script within the later response contains a sink which then processes the data in an unsafe way.

```
element.innerHTML = comment.author
```

LAB

PRACTITIONER [Stored DOM XSS](#)

Which sinks can lead to DOM-XSS vulnerabilities?

The following are some of the main sinks that can lead to DOM-XSS vulnerabilities:



```
document.write() document.writeln() document.domain element.innerHTML element.outerHTML  
element.insertAdjacentHTML element.onevent
```

The following jQuery functions are also sinks that can lead to DOM-XSS vulnerabilities:

```
add() after() append() animate() insertAfter() insertBefore() before() html() prepend() replaceAll() replaceWith()  
wrap() wrapInner() wrapAll() has() constructor() init() index() jQuery.parseHTML() $.parseHTML()
```

How to prevent DOM-XSS vulnerabilities

In addition to the general measures described on the DOM-based vulnerabilities page, you should avoid allowing data from any untrusted source to be dynamically written to the HTML document.

What can XSS be used for?

An attacker who exploits a cross-site scripting vulnerability is typically able to:

- Impersonate or masquerade as the victim user.
- Carry out any action that the user is able to perform.
- Read any data that the user is able to access.
- Capture the user's login credentials.
- Perform virtual defacement of the web site.
- Inject trojan functionality into the web site.

Impact of XSS vulnerabilities

The actual impact of an XSS attack generally depends on the nature of the application, its functionality and data, and the status of the compromised user. For example:

- In a brochureware application, where all users are anonymous and all information is public, the impact will often be minimal.
- In an application holding sensitive data, such as banking transactions, emails, or healthcare records, the impact will usually be serious.
- If the compromised user has elevated privileges within the application, then the impact will generally be critical, allowing the attacker to take full control of the vulnerable application and compromise all users and their data.

How to find and test for XSS vulnerabilities

The vast majority of XSS vulnerabilities can be found quickly and reliably using Burp Suite's web vulnerability scanner.

Manually testing for reflected and stored XSS normally involves submitting some simple unique input (such as a short alphanumeric string) into every entry point in the application, identifying every location where the submitted input is returned in HTTP responses, and testing each



location individually to determine whether suitably crafted input can be used to execute arbitrary JavaScript. In this way, you can determine the [context](#) in which the XSS occurs and select a suitable payload to exploit it.

Manually testing for DOM-based XSS arising from URL parameters involves a similar process: placing some simple unique input in the parameter, using the browser's developer tools to search the DOM for this input, and testing each location to determine whether it is exploitable.

However, other types of DOM XSS are harder to detect. To find DOM-based vulnerabilities in non-URL-based input (such as `document.cookie`) or non-HTML-based sinks (like `setTimeout`), there is no substitute for reviewing JavaScript code, which can be extremely time-consuming. Burp Suite's web vulnerability scanner combines static and dynamic analysis of JavaScript to reliably automate the detection of DOM-based vulnerabilities.

Content security policy

Content security policy (CSP) is a browser mechanism that aims to mitigate the impact of cross-site scripting and some other vulnerabilities. If an application that employs CSP contains XSS-like behavior, then the CSP might hinder or prevent exploitation of the vulnerability. Often, the CSP can be circumvented to enable exploitation of the underlying vulnerability.

[Content security policy](#)

Dangling markup injection

Dangling markup injection is a technique that can be used to capture data cross-domain in situations where a full cross-site scripting exploit is not possible, due to input filters or other defenses. It can often be exploited to capture sensitive information that is visible to other users, including CSRF tokens that can be used to perform unauthorized actions on behalf of the user.

[Dangling markup injection](#)

How to prevent XSS attacks

Preventing cross-site scripting is trivial in some cases but can be much harder depending on the complexity of the application and the ways it handles user-controllable data.

In general, effectively preventing XSS vulnerabilities is likely to involve a combination of the following measures:

- **Filter input on arrival.** At the point where user input is received, filter as strictly as possible based on what is expected or valid input.
- **Encode data on output.** At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.

- **Use appropriate response headers.** To prevent XSS in HTTP responses that aren't intended to contain any HTML or JavaScript, you can use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret the responses in the way you intend.
- **Content Security Policy.** As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

Common questions about cross-site scripting

How common are XSS vulnerabilities? XSS vulnerabilities are very common, and XSS is probably the most frequently occurring web security vulnerability.

How common are XSS attacks? It is difficult to get reliable data about real-world XSS attacks, but it is probably less frequently exploited than other vulnerabilities.

What is the difference between XSS and CSRF? XSS involves causing a web site to return malicious JavaScript, while CSRF involves inducing a victim user to perform actions they do not intend to do.

What is the difference between XSS and SQL injection? XSS is a client-side vulnerability that targets other application users, while SQL injection is a server-side vulnerability that targets the application's database.

How do I prevent XSS in PHP? Filter your inputs with a whitelist of allowed characters and use type hints or type casting. Escape your outputs with htmlentities and ENT_QUOTES for HTML contexts, or JavaScript Unicode escapes for JavaScript contexts.

How do I prevent XSS in Java? Filter your inputs with a whitelist of allowed characters and use a library such as Google Guava to HTML-encode your output for HTML contexts, or use JavaScript Unicode escapes for JavaScript contexts.

Windows Security Architecture

- Authentication credentials stored in SAM file
- File is located at C:\windows\system32\config
- Older systems use LM hashing. Current uses NTLM v2 (MD5)
- Windows network authentication uses Kerberos
- **LM Hashing**
 - Splits the password up. If it's over 7 characters, it is encoded in two sections.
 - If one section is blank, the hash will be AAD3B435B51404EE
 - Easy to break if password is 7 characters or under because you can split the hash
- SAM file presents as UserName:SID:LM_Hash:NTLM_Hash:::
- **Ntds.dit** - database file on a domain controller that stores passwords
 - Located in %SystemRoot%\NTDS\Ntds.dit or
 - Located in %SystemRoot%\System32\Ntds.dit

- Includes the entire Active Directory
- **Kerberos**
 - Steps of exchange
 1. Client asks **Key Distribution Center** (KDC) for a ticket. Sent in clear text.
 2. Server responds with **Ticket Granting Ticket** (TGT). This is a secret key which is hashed by the password copy stored on the server.
 3. If client can decrypt it, the TGT is sent back to the server requesting a **Ticket Granting Service** (TGS) service ticket.
 4. Server sends TGS service ticket which client uses to access resources.
 - **Tools**
 1. KerbSniff
 2. KerbCrack
 3. Both take a long time to crack
- **Registry**
 - Collection of all settings and configurations that make the system run
 - Made up of keys and values
 - Root level keys
 1. **HKEY_LOCAL_MACHINE** (HKLM) - information on hardware and software
 2. **HKEY_CLASSES_ROOT** (HKCR) - information on file associates and OLE classes
 3. **HKEY_CURRENT_USER** (HKCU) - profile information for the current user including preferences
 4. **HKEY_USERS** (HKU) - specific user configuration information for all currently active users
 5. **HKEY_CURRENT_CONFIG** (HKCC) - pointer to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current
 - Type of values
 1. **REG_SZ** - character string
 2. **REG_EXPAND_SZ** - expandable string value
 3. **REG_BINARY** - a binary value
 4. **REG_DWORD** - 32-bit unsigned integer
 5. **REG_LINK** - symbolic link to another key
 - Important Locations
 1. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run ServicesOnce
 2. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Services
 3. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Once
 4. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
 - Executables to edit
 1. regedit.exe
 2. regedt32.exe (preferred by Microsoft)
- **MMC**
 - Microsoft Management Console - used by Windows to administer system
 - Has "snap-ins" that allow you to modify sets (such as Group Policy Editor)

Linux Security Architecture

- Linux root is just a slash (/)
- Important locations
 - / - root directory
 - /bin - basic Linux commands
 - /dev - contains pointer locations to various storage and input/output systems
 - /etc - all administration files and passwords. Both password and shadow files are here
 - /home - holds the user home directories
 - /mnt - holds the access locations you've mounted
 - /sbin - system binaries folder which holds more administrative commands
 - /usr - holds almost all of the information, commands and files unique to the users
- Linux Commands

Command	Description
adduser	Adds a user to the system
cat	Displays contents of file
cp	Copies
ifconfig	Displays network configuration information
kill	Kills a running process
ls	Displays the contents of a folder. -l option provides most information.
man	Displays the manual page for a command
passwd	Used to change password
ps	Process status. -ef option shows all processes
rm	Removes files. -r option recursively removes all directories and subdirectories
su	Allows you to perform functions as another user (super user)

- Adding an ampersand after a process name indicates it should run in the background.
- **pwd** - displays current directory
- **chmod** - changes the permissions of a folder or file
 - Read is 4, write is 2 and execute is 1
 - First number is user, second is group, third is others
 - Example - 755 is everything for users, read/execute for group, and read/execute for others
- Root has UID and GID of 0
- First user has UID and GID of 500
- Passwords are stored in /etc/shadow for most current systems
- /etc/password stores passwords in hashes.
- /etc/shadow stores passwords encrypted (hashed and salted) and is only accessible by root

System Hacking Goals



- **Gaining Access** - uses information gathered to exploit the system
- **Escalating Privileges** - granting the account you've hacked admin or pivoting to an admin account
- **Executing Applications** - putting back doors into the system so that you can maintain access
- **Hiding Files** - making sure the files you leave behind are not discoverable
- **Covering Tracks** - cleaning up everything else (log files, etc.)
 - **clearev** - meterpreter shell command to clear log files
 - Clear MRU list in Windows
 - In Linux, append a dot in front of a file to hide it

Authentication and Passwords

- **Three Different Types**
 - **Something You Are** - uses biometrics to validate identity (retina, fingerprint, etc.)
 - Downside is there can be lots of false negatives
 - **False acceptance rate (FAR)** - rate that a system accepts access for people that shouldn't have it
 - **False rejection rate (FRR)** - rate that a system rejects access for someone who should have it
 - **Crossover error rate (CER)** - combination of the two; the lower the CER, the better the system
 - **Active** - requires interaction (retina scan or fingerprint scanner)
 - **Passive** - requires no interaction (iris scan)
 - **Something You Have** - usually consists of a token of some kind (swipe badge, ATM card, etc.)
 - This type usually requires something alongside it (such as a PIN for an ATM card)
 - Some tokens are single-factor (such as a plug-and-play authentication)
 - **Something You Know** - better known as a password
 - Most systems use this because it is universal and well-known
- **Two-Factor** - when you have two types of authentications such as something you know (password) and something you have (access card)
- **Strength of passwords** - determined by length and complexity
 - ECC says that both should be combined for the best outcome
 - Complexity is defined by number of character sets used (lower case, upper case, numbers, symbols, etc.)
- **Default passwords** - always should be changed and never left what they came with. Databases such as cirt.net, default-password.info and open-sez.me all have databases of these

Password Attacks

- **Non-electronic** - social engineering attacks - most effective.
 - Includes shoulder surfing and dumpster diving
- **Active online** - done by directly communicating with the victim's machine
 - Includes dictionary and brute-force attacks, hash injections, phishing, Trojans, spyware, keyloggers and password guessing
 - **Keylogging** - process of using a hardware device or software application to capture keystrokes of a user

- **LLMNR/NBT-NS** - attack based off Windows technologies that caches DNS locally. Responding to these poisons the local cache. If an NTLM v2 hash is sent over, it can be sniffed out and then cracked
 - **Tools**
 - NBNSpoof
 - Pupy
 - Metasploit
 - Responder
 - LLMNR uses UDP 5355
 - NBT-NS uses UDP 137
 - Active online attacks are easier to detect and take a longer time
 - Can combine "net" commands with a tool such as **NetBIOS Auditing tool** or **Legion** to automate the testing of user IDs and passwords
 - **Tools**
 - Hydra
 - Metasploit
- **Passive online** - sniffing the wire in hopes of intercepting a password in clear text or attempting a replay attack or man-in-the-middle attack
 - **Tools**
 - **Cain and Abel** - can poison ARP and then monitor the victim's traffic
 - **Ettercap** - works very similar to Cain and Abel. However, can also help against SSL encryption
 - **KerbCrack** - built-in sniffer and password cracker looking for port 88 Kerberos traffic
 - **ScoopLM** - specifically looks for Windows authentication traffic on the wire and has a password cracker
- **Offline** - when the hacker steals a copy of the password file and does the cracking on a separate system
 - **Dictionary Attack** - uses a word list to attack the password. Fastest method of attacking
 - **Brute force attack** - tries every combination of characters to crack a password
 - Can be faster if you know parameters (such as at least 7 characters, should have a special character, etc.)
 - **Hybrid attack** - Takes a dictionary attack and replaces characters (such as a 0 for an o) or adding numbers to the end
 - **Rainbow tables** - uses pre-hashed passwords to compare against a password hash. Is faster because the hashes are already computed.
 - **Tools**
 - Cain
 - KerbCrack
 - Legion
 - John the Ripper

Privilege Escalation and Executing Applications

- **Vertical** - lower-level user executes code at a higher privilege level
- **Horizontal** - executing code at the same user level but from a location that would be protected from that access
- **Four Methods**
 - Crack the password of an admin - primary aim
 - Take advantage of an OS vulnerability

- **DLL Hijacking** - replacing a DLL in the application directory with your own version which gives you the access you need
 - Use a tool that will provide you the access such as Metasploit
 - Social engineering a user to run an application
- ECC refers executing applications as "owning" a system
- **Executing applications** - starting things such as keyloggers, spyware, back doors and crackers

Hiding Files and Covering Tracks

- In Windows, **Alternate Data Stream** (ADS) can hide files
 - Hides a file from directory listing on an NTFS file system
 - **readme.txt: badfile.exe**
 - Can be run by start **readme.txt: badfile.exe**
 - You can also create a link to this and make it look real (e.g., mklink innocent.exe **readme.txt: badfile.exe**)
 - Every forensic kit looks for this, however
 - To show ADS, dir. /r does the trick
 - You can also blow away all ADS by copying files to a FAT partition
- You can also hide files by attributes
 - In Windows: attrib +h filename
 - In Linux, simply add a . to the beginning of the filename
- Can hide data and files with steganography
- Also need to worry about clearing logs
 - In Windows, you need to clear application, system and security logs
 - Don't just delete; key sign that an attack has happened
 - Option is to corrupt a log file - this happens all the time
 - Best option is be selective and delete the entries pertaining to your actions.
- Can also disable auditing ahead of time to prevent logs from being captured

Rootkits

- Software put in place by attacker to obscure system compromise
- Hides processes and files
- Also allows for future access
- **Examples**
 - Horsepill - Linus kernel rootkit inside initrd
 - Grayfish - Windows rootkit that injects in boot record
 - Firefex - multi-component family of malware
 - Azazel
 - Avatar
 - Necurs
 - ZeroAccess
- **Hypervisor level** - rootkits that modify the boot sequence of a host system to load a VM as the host OS
- **Hardware** - hide malware in devices or firmware
- **Boot loader level** - replace boot loader with one controlled by hacker
- **Application level** - directed to replace valid application files with Trojans
- **Kernel level** - attack boot sectors and kernel level replacing kernel code with back-door code; most dangerous
- **Library level** - use system-level calls to hide themselves

- One way to detect rootkits is to map all the files on a system and then boot a system from a clean CD version and compare the two file systems

Social Engineering

⚡ This chapter has [practical labs](#)

Social Engineering is the art of manipulating a person or group into providing information or a service they would otherwise not have given.

Phases

1. 🔎 **Research target company**
 - Dumpster dive, visit websites, tour the company, etc
2. 🏹 **Select the victim**
 - Identify frustrated employee or another target
3. 💬 **Build a relationship**
 - Develop relationship with target employee
4. 💰 **Exploit the relationship**
 - Collect sensitive information and current technologies

Principles

1. **Authority**
 - Impersonate or imply a position of authority
2. **Intimidation**
 - Frighten by threat
3. **Consensus / Social proof**
 - To convince of a general group agreement
4. **Scarcity**
 - The situation will not be this way for long
5. **Urgency**
 - Works alongside scarcity / act quickly, don't think
6. **Familiarity**
 - To imply a closer relationship
7. **Trust**
 - To assure reliance on their honesty and integrity

Behaviors

- **Human nature/Trust** - trusting others
- **Ignorance** of social engineering efforts
- **Fear** of consequences of not providing the information
- **Greed** - promised gain for providing requested information

- A sense of **moral obligation**

Companies Common Risks:

- **Insufficient training**
- **Lack of controls**
 - Technical
 - e.g.: Firewall rule, ACL rules, patch management (...)
 - Administrative
 - e.g.: Mandatory Vacations, Job Rotation, Separation of Duties (...)
 - Physical
 - e.g.: Proper Lighting, Cameras, Guards, Mantraps (...)
- **Size of the Company Matters**
- **Lack of Policies**
 - Promiscuous Policy
 - Permissive Policy
 - Prudent Policy
 - Paranoid Policy

Social Engineering Attacks:

Human-Based Attacks

- **Dumpster Diving** - Looking for sensitive information in the trash
 - Shredded papers can sometimes indicate sensitive info
- **Impersonation** - Pretending to be someone you're not
 - Can be anything from a help desk person up to an authoritative figure (FBI agent)
 - Posing as a tech support professional can really quickly gain trust with a person
- **Shoulder Surfing** - Looking over someone's shoulder to get info
 - Can be done long distance with binoculars, etc.
- **Eavesdropping** - Listening in on conversations about sensitive information
- **Tailgating** - Attacker walks in behind someone who has a valid badge. (e.g.: Holding boxes or simply by following without getting notice)
- **Piggybacking** - Attacker pretends they lost their badge and asks someone to hold the door
- **RFID Identity Theft (RFID skimming)** - Stealing an RFID card signature with a specialized device
- **Reverse Social Engineering** - Getting someone to call you and give information
 - Often happens with tech support - an email is sent to user stating they need them to call back (due to technical issue) and the user calls back
 - Can also be combined with a DoS attack to cause a problem that the user would need to call about
 - Always be pleasant - it gets more information
- **Insider Attack** - An attack from an employee, generally disgruntled
 - Sometimes subclassified (negligent insider, professional insider)

Computer-Based Attacks

Can begin with sites like Facebook where information about a person is available; For instance - if you know Bob is working on a project, an email crafted to him about that project would seem quite normal if you spoof it from a person on his project.

- **Phishing** - crafting an email that appears legitimate but contains links to fake websites or to download malicious content.
 - **Ways to Avoid Phishing**
 - Beware unknown, unexpected or suspicious originators
 - Beware of who the email is addressed to
 - Verify phone numbers
 - Beware bad spelling or grammar
 - Always check links
- **Spear Phishing** - Targeting a person or a group with a phishing attack.
 - Can be more useful because attack can be targeted
- **Whaling** - Going after **CEOs** or other **C-level executives**.
- **Pharming** - Make a user's traffic redirects to a clone website; may use DNS poisoning.
- **Spamming** - Sending spam over instant message.
- **Fake Antivirus** - Very prevalent attack; pretends to be an anti-virus but is a malicious tool.

Tools

- **SET (Social Engineering Toolkit)** - Pentest tool design to perform advanced attacks against human by exploiting their behavior.
- **Phish Tank** - For phishing detection
- **WIFI phisher** - Automated phishing attacks against Wi-Fi networks in order to obtain credentials or inject malware.
- **SPF Speed Phish framework** - Quick recon and deployment of simple social eng. exercises

Mobile-Based Attacks

- **ZitMo** (Zeus-in-the-Mobile) - banking malware that was ported to Android
- SMS messages can be sent to request premium services
- **Attacks**
 - Publishing malicious apps
 - Repackaging legitimate apps
 - Fake security applications
 - SMS (**smishing**)

Physical Security Basics

- **Physical measures** - everything you can touch, taste, smell or get shocked by
 - Includes things like air quality, power concerns, humidity-control systems
- **Technical measures** - smartcards and biometrics
- **Operational measures** - policies and procedures you set up to enforce a security-minded operation
- **Access controls** - physical measures designed to prevent access to controlled areas
 - **Biometrics** - measures taken for authentication that come from the "something you are" concept
 - **False rejection rate (FRR)** - when a biometric rejects a valid user
 - **False acceptance rate (FAR)** - when a biometric accepts an invalid user
 - **Crossover error rate (CER)** - combination of the two; determines how good a system is
- Even though hackers normally don't worry about environmental disasters, this is something to think of from a pen test standpoint (hurricanes, tornadoes, floods, etc.)

Prevention

- Separation of duties
- Rotation of duties
- Controlled Access
 - Least privilege
- Logging & Auditing
- Policies

Privilege Escalation and Executing Applications

⚡ Check out the [practical lab on PrivEsc](#)

Vertical - Lower-level user executes code at a higher privilege level (*e.g.: common user to root/administrator*).

Horizontal - executing code at the same user level but from a location that would be protected from that access

- Crack the password of an admin - primary aim
- Taking advantage of an OS vulnerability
 - One way to perform a priv esc is using CVE's in order to perform local shells, c shells, web shells and so on.
 - Examples:
 - Linux: [DirtyCow](#) race-condition vulnerability;
 - Windows: [EternalBlue](#) exploits the old Samba version 1 to leverage a Remote code execution (RCE);
- **DLL Hijacking** - replacing a DLL in the application directory with your own version which gives you the access you need

- In Linux machines is possible to look for **crontabs** and find misconfigurations on privileges.
- In Linux, **insecure sudo** can lead a privilege escalation to root; You can check this by typing: `sudo -l`. If there's any system command that allows **NOPASSWD option** this may lead to escalation.
- Nmap old versions you can start **interactive mode** and issue the `!/bin/bash` to elevate root privileges.
- Use a tool that will provide you the access such as Metasploit
- Social engineering a user to run an application
- ECC refers executing applications as "owning" a system
- **Executing applications** - starting things such as keyloggers, spyware, back doors and crackers

Covert data gathering

Keyloggers - record keys strokes of a individual computer keyboard or a network of computers.

- Keylogger when associated with spyware, helps to transmit your information to an unknown third party.
- **Types of Keyloggers:**
- **Hardware keylogger**
 - PC/BIOS embedded
 - Keyboard
 - External device
 - PS/2 and USB
 - Acoustic/CAM
 - Bluetooth
 - Wi-Fi
 - **Hardware Keylogger Tools:**
 - KeyGrabber - electronic device capable of capturing keystrokes from PS/2 USB keyboard.
- **Software keylogger**
 - Application
 - Kernel
 - Hypervisor-based
 - Form Grabbing based (records from web form data)
 - **Software Keylogger Tools:**
 - KeyCarbon
 - Keylama Keylogger
 - Keyboard logger
 - KeyGhost

Spywares - watching user's action and logging them without the user's knowledge.



- Hide its process, files and other objects
- **Spywares can steals user's PII, monitors activity, display annoying pop-ups, redirect web pages to ads, changes the browser's settings, steal passwords, modifies the DLLs, changes firewall settings and so on.**
- **Types of spyware:**
 - Desktop
 - Email
 - Internet
 - Child-Monitoring
 - Screen Capturing
 - USB
 - Audio and Video
 - Printers
 - Mobile devices / Telephones / Cellphones
 - GPS
- **Spyware Tools:**
 - [SpyAgent](#) - allows you to secretly monitor and record all activities on your computer, which is completely legal.
 - [Power Spy](#) - allows you to secretly monitor and record all activities on your computer, which is completely legal.
 - [mSpy](#) - GPS spyware that trace the location of particular mobile devices.
 - [USBDevview](#) - monitors and analyzes data transferred between any USB device connected to a computer.

Defending against Keyloggers and Spywares

- Restrict physical access to computer systems
- Use anti-keylogger between the keyboard and its driver
- Use pop-up blocker and avoid opening junk emails
- Use anti-spyware/antivirus
- Firewall and anti-keylogging software(Zemana AntiLogger)
- Update and patch!
- Recognize phishing emails
- Host-based IDS
- Automatic form-filling password manager or virtual keyboard

Hiding Files

↳ Check out the practical labs(2) on [Hiding Files using NTFS streams and Steganography](#)

- In Windows, you can use **Alternate Data Stream (ADS)** to hide files:
 - Hides a file from directory listing on an NTFS file system
 - type badfile.exe: > plaintext.txt:badfile.exe
 - Next create a symlink mklink normalApp.exe readme.txt:badfile.exe)
 - You can also clear out all ADS by copying files to a FAT partition

- To show ADS, `dir /r` does the trick;
 - You can use `streams` from **Sysinternals** to show streams.
 - Also you can use **FTK (Forensics ToolKit)** to look for this
- **You can also hide files by attributes**
 - In Windows: `attrib +h filename`
 - In Linux, simply add a `.` to the beginning of the filename (`.file.tar`)
- **Can hide data and files with steganography**
 - Tools for steganography:
 - CLI (Linux):
 - **steghide**
 - GUI (Windows):
 - **Snow**
 - **OpenStego**
 - **OpenPuff**

Steganography:

- **Steganography** - practice of concealing a message inside another medium so that only the sender and recipient know of its existence
- **Ways to Identify**
 - Text - character positions are key - blank spaces, text patterns
 - Image - file larger in size; some may have color palette faults
 - Audio & Video - require statistical analysis
- **Methods**
 - Least significant bit insertion - changes least meaningful bit
 - Masking and filtering (grayscale images) - like watermarking
 - Algorithmic transformation - hides in mathematical functions used in image compression
- **Tools**
 - QuickStego
 - gifshuffle
 - SNOW
 - Steganography Studio
 - OpenStego

Rootkits

- Software put in place by attacker to obscure system compromise
- Hides processes and files
- Also allows for future access
- **Examples**
 - Horsepill - Linus kernel rootkit inside initrd
 - Grayfish - Windows rootkit that injects in boot record
 - Firefef - multi-component family of malware
 - Azazel
 - Avatar

- Necurs
 - ZeroAccess
- **Hypervisor level** - rootkits that modify the boot sequence of a host system to load a VM as the host OS
- **Hardware** - hide malware in devices or firmware
- **Boot loader level** - replace boot loader with one controlled by hacker
- **Application level** - directed to replace valid application files with Trojans
- **Kernel level** - attack boot sectors and kernel level replacing kernel code with back-door code; most dangerous
- **Library level** - use system-level calls to hide themselves
- One way to detect rootkits is to map all the files on a system and then boot a system from a clean CD version and compare the two file systems

Covering Tracks

Clearing logs is the main idea behind covering tracks.

1. Find and clear the logs.
2. Falsify/Modify logs.

On Linux:

- Linux keep the **command line history** on `.bash_history` file
 - To clear out the command line history use `rm -rf` to force remove. You also can use `shred -zu` that deletes the file and **overwrite on memory**.
 - You can also use `history -c` to clear all command line history on entire system or `history -w` to clear out all session history.
- **Turn off the command logs:**
 - `export HISTSIZE=0`
 - `echo $HISTSIZE` will return 0 limiting the number of commands which can be saved in `$HISTFILE`.
- **clearrev** - Meterpreter shell command to clear log files (issued inside Metasploit Framework)

Most common logs on Linux:

- `/var/log/messages` or `/var/log/syslog/`
 - General messages, as well as system-related information.
- `/var/log/auth.log` or `/var/log/secure`
 - Store authentication logs, including both successful and failed logins and authentication methods.
- `/var/log/boot.log`
 - Related to booting and any messages logged during startup.
- `/var/log/maillog` or `var/log/mail.log`
 - stores all logs related to mail servers.
- **Clearing and Modifying logs on Linux:**

- It is possible to echo whitespace to clear the event log file:
 - `echo " " > /var/log/auth.log`
- Also you can perform this by using 'black hole dev/null':
 - `echo /dev/null > auth.log`
- To tamper/modify the log files, you can use `sed` stream editor to delete, replace and insert data.
 - `sed -i '/opened/d' /var/log/auth.log` - this command will delete every line that contains the '**opened**' word, that refers to opened sessions on Linux system.

On Windows:

- To clear out all **command line history**:
 - On **Cmd Prompt**: press [alt] + [F7]
 - On **PowerShell**: type `Clear-History`

In Windows, you need to clear **application, system and security logs**.

- **Auditpol** for changing settings on log files (used for manipulate audit policies).
- Main commands:
 - `auditpol /get /category:*` --> display all audit policies in detail if is enable (*Object Acces, System, Logon/Logoff, Privilege Use, and so on*).
 - `auditpol /clear` --> reset (disable) the system audit policy for all subcategories.
 - `auditpol /remove` --> Removes all per-user audit policy settings and disables all system audit policy settings.

⚡ Check out the [practical lab on Auditpol](#)

- **MRU** (Most Recently Used) programs that registry recently used programs/files and saves on Windows Registry.
- **Is possible to manually clear the logs on Event Viewer.**

Conclusion on Covering Tracks

- Option is to corrupt a log file - this happens all the time
- Best option is be selective and delete the entries pertaining to your actions.
- **Can also disable auditing ahead of time to prevent logs from being captured**
- Tools:
 - ccleaner --> automate the system cleaning, scrub online history, log files, etc. [Windows]
 - MRUblaster [Windows]
 - Meterpreter on MSF have **clearev** to clear all event logs remotely. [Kali Linux using MSF]

07) Web security

- Securing web
- LAN security
- Component
- Topologies
- Threats and vulnerability of LAN
- Firewall security
- Internet security

What is Web Security?

Web security is also known as “Cybersecurity”. It basically means protecting a website or web application by detecting, preventing and responding to cyber threats.

Websites and web applications are just as prone to security breaches as physical homes, stores, and government locations. Unfortunately, cybercrime happens every day, and great web security measures are needed to protect websites and web applications from becoming compromised.

That’s exactly what web security does – it is a system of protection measures and protocols that can protect your website or web application from being hacked or entered by unauthorized personnel. This integral division of Information Security is vital to the protection of websites, web applications, and web services. Anything that is applied over the Internet should have some form of web security to protect it.

Details of Web Security

There are a lot of factors that go into web security and web protection. Any website or application that is secure is surely backed by different types of checkpoints and techniques for keeping it safe.

There are a variety of security standards that must be followed at all times, and these standards are implemented and highlighted by the OWASP. Most experienced web developers from top cybersecurity companies will follow the standards of the OWASP as well as keep a close eye on the Web Hacking Incident Database to see when, how, and why different people are hacking different websites and services.



Essential steps in protecting web apps from attacks include applying up-to-date encryption, setting proper authentication, continuously patching discovered vulnerabilities, avoiding data theft by having secure software development practices. The reality is that clever attackers may be competent enough to find flaws even in a fairly robust secured environment, and so a holistic security strategy is advised.

Available Technology

There are different types of technologies available for maintaining the best security standards. Some popular technical solutions for testing, building, and preventing threats include:

- Black box testing tools
- Fuzzing tools
- White box testing tools
- Web application firewalls (WAF)
- Security or vulnerability scanners
- Password cracking tools

Likelihood of Threat

Your website or web application's security depends on the level of protection tools that have been equipped and tested on it. There are a few major threats to security which are the most common ways in which a website or web application becomes hacked. Some of the top vulnerabilities for all web-based services include:

- SQL injection
- Password breach
- Cross-site scripting
- Data breach
- Remote file inclusion
- Code injection

Preventing these common threats is the key to making sure that your web-based service is practicing the best methods of security.

The Best Strategies

There are two big defense strategies that a developer can use to protect their website or web application. The two main methods are as follows:

- **Resource assignment** – By assigning all necessary resources to causes that are dedicated to alerting the developer about new web security issues and threats, the developer can receive a constant and updated alert system that will help them detect and eradicate any threats before security is officially breached.
- **Web scanning** – There are several web scanning solutions already in existence that are available for purchase or download. These solutions, however, are only good for known

vulnerability threats – seeking unknown threats can be much more complicated. This method can protect against many breaches, however, and is proven to keep websites safe in the long run.

Web Security also protects the visitors from the below-mentioned points –

- **Stolen Data:** Cyber-criminals frequently hacks visitor's data that is stored on a website like email addresses, payment information, and a few other details.
- **Phishing schemes:** This is not just related to email, but through phishing, hackers design a layout that looks exactly like the website to trick the user by compelling them to give their sensitive details.
- **Session hijacking:** Certain cyber attackers can take over a user's session and compel them to take undesired actions on a site.
- **Malicious redirects.** Sometimes the attacks can redirect visitors from the site they visited to a malicious website.
- **SEO Spam.** Unusual links, pages, and comments can be displayed on a site by the hackers to distract your visitors and drive traffic to malicious websites.

Thus, web security is easy to install and it also helps the business people to make their website safe and secure. A web application firewall prevents automated attacks that usually target small or lesser-known websites. These attacks are born out by malicious bots or malware that automatically scan for vulnerabilities they can misuse, or cause DDoS attacks that slow down or crash your website.

Thus, Web security is extremely important, especially for websites or web applications that deal with confidential, private, or protected information. Security methods are evolving to match the different types of vulnerabilities that come into existence.

UNIT 1

LAN SECURITY

The internet has revolutionized the computer and communications world like nothing before. The telegraph, telephone, radio, and computer have all set the stage for the internet 's unprecedented integration of capabilities. The Internet is at once a worldwide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location.

Internet is what is referred to as a public network which is accessible from anywhere across the globe with the help of its inter-network structure. It is defined as a network of networks. Contrary to popular belief, the Internet is a collection of interconnected computer networks, linked by copper wires, fiber-optic cables, wireless connections etc.; the Web is a collection of interconnected documents, linked by hyperlinks and URLs. The World Wide Web is accessible via the Internet, along with many other services including E-mail, file sharing and other services. So how does the

Internet work?

It is important to remember the Internet is a network of computer networks interconnected by communications lines of various compositions and speeds.

“The Internet was conceived in the era of time-sharing, but has survived into the era of personal computers, client/server and peer-to-peer computing, and the network computer.”

INTRODUCTION TO LAN

A LAN is a high-speed data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers, servers, and other devices. LANs offer computer users many advantages, including shared access to devices and applications, file exchange between connected users, and communication between users via electronic mail and other applications.

It makes sense, most often for financial reasons but also for others, to network groups of computers where they share a common workload. All the computers in an administrative office, all the computers to do with a certain ward or discipline. Networking computers means that the people using them can share files easily send each other messages and share each other's printers. This idea has developed into Local Area Networks (LANs). Nowadays most organizations have a local area network. LANs can be as small as just one shared office or as large as a whole city. Although single LANs are geographically limited (to a department or office building, for example), separate LANs can be connected to form larger networks. Alternatively, LANs can be configured utilizing a client-server architecture which makes use of -distributed intelligence by splitting the processing of an application between two distinct components: a -front-end client and a -backend server

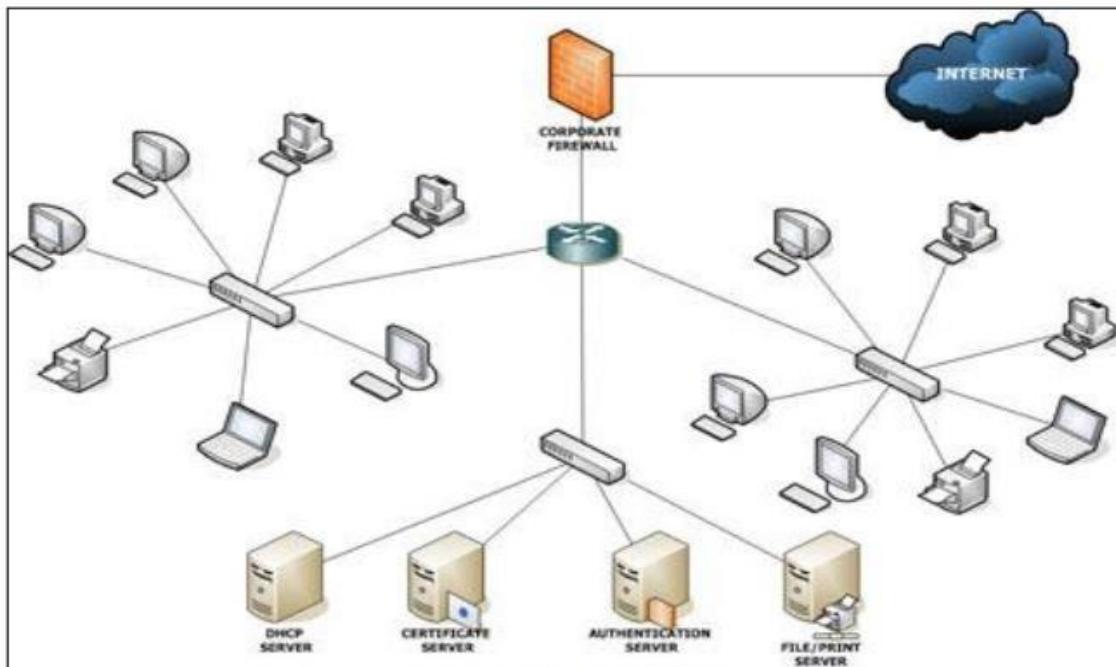


Figure: LAN Connection

WHY LAN SECURITY IS IMPORTANT

Local area networks (LANs) have become a major tool to many organizations in meeting data processing and data communication needs. Prior to the use of LANs, most processing and communications were centralized; the information and control of that information were centralized as well.

Now LANs logically and physically extend data, processing and communication facilities across the organization.

Security services that protect the data, processing and communication facilities must also be distributed throughout the LAN.

For example, sending sensitive files that are protected with stringent access controls on one system, over a LAN to another system that has no access control protection, defeats the efforts made on the first system. Users must ensure that their data and the LAN itself are adequately protected.

LAN security should be an integral part of the whole LAN, and should be important to all users.

Electronic mail (email), a major application provided by most LANs, replaces much of the Interoffice and even inter-organizational mail that is written on paper and placed in an envelope.

This envelope provides some confidentiality between the sender and receiver, and it can even be argued that the integrity of the paper envelope provides the receiver with some degree of assurance that the message was not altered.

Using electronic mail does not provide these assurances.

Simple transfers on unprotected LANs of inadequately protected electronic mail messages can be captured and read or perhaps even altered.

LAN/WAN COMPONENTS

The four primary devices used in LANs are as follows:

- Hubs
- Bridges
- Switches
- Routers

Respective to the OSI model, these devices operate at the following layers:

- OSI Layer 1 (physical)—Hubs, repeaters (hubs are considered to be multiport repeaters)
- OSI Layer 2 (data link)—Bridges, switches
- OSI Layer 3 (network)—Routers\

TOPOLOGY

LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star.

Advantages of a Star Topology

- Easy to install and wire.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages of a Star Topology

- Requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the concentrators.

Advantages of a Tree Topology

- Point-to-point wiring for individual segments.
- Supported by several hardware and software vendors.

Disadvantages of a Tree Topology

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down. More difficult to configure and wire than other topologies.

PROTOCOLS

A protocol is a formal set of rules that computers use to control the flow of messages between them. Networking involves such a complex variety of protocols that the International Standards

Organization (ISO) defined the now-popular seven-layer communications model. The Open Systems Interconnection (OSI) model describes communication processes as a hierarchy of layers, each dependent on the layer beneath it. Each layer has a defined interface with the layer above and below; this

interface is made flexible so that designers can implement various communications protocols with security features and still follow the standard.

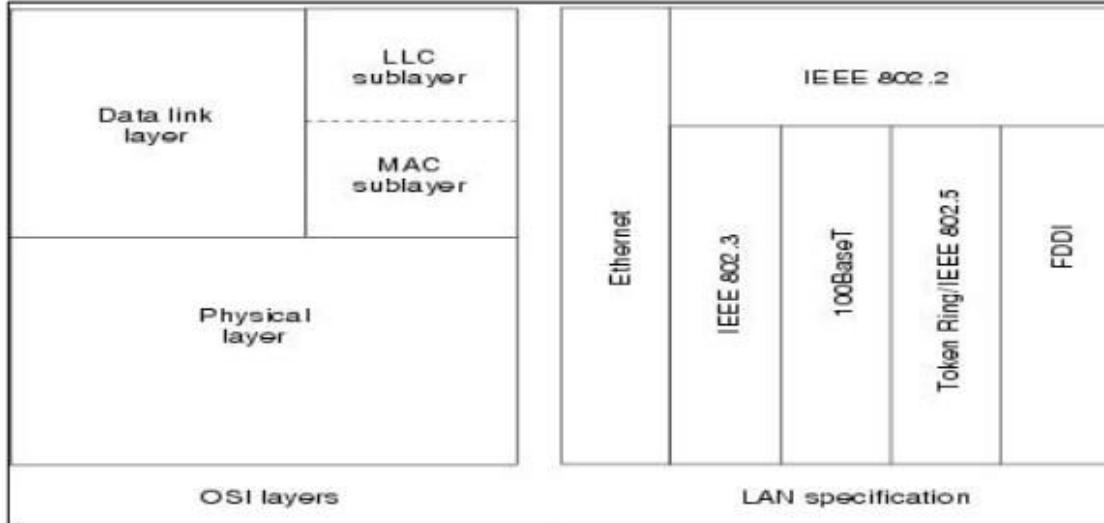


Figure: LAN Protocols in OSI

THREATS AND VULNERABILITIES

A threat can be any person, object, or event that, if realized, could potentially cause damage to the LAN. Threats can be malicious, such as the intentional modification of sensitive information, or can be accidental, such as an error in a calculation, or the accidental deletion of a file. Threats can also be acts of nature, i.e., flooding, wind, lightning, etc. The immediate damage caused by a threat is referred to as an impact.

THE LAN SECURITY PROBLEM

The advantages of utilizing a LAN were briefly discussed in the above. With these advantages however, come additional risks that contribute to the LAN security problem.

Distributed File Storing –

Concerns Remote Computing –

Concerns Topologies and Protocols –

Concerns Messaging Services –

Concerns Other LAN Security Concerns.

SECURITY THREATS OF LAN

- **Unauthorized LAN access** - results from an unauthorized individual gaining access to the LAN.
- **Inappropriate access to LAN resources**- results from an individual, authorized or unauthorized, gaining access to LAN resources in an unauthorized manner.
- **Disclosure of data** - results from an individual accessing or reading information and possibly revealing the information in an accidental or unauthorized intentional manner.
- **Unauthorized Modification to data and software** - results from an individual modifying, deleting or destroying LAN data and software in an unauthorized or accidental manner.
- **Disclosure of LAN traffic** - results from an individual accessing or reading information and possibly revealing the information in an accidental or unauthorized intentional manner as it moves through the LAN.
- **Spoofing of LAN traffic**- results when a message appears to have been sent from a legitimate, named sender, when actually the message had not been.
- Disruption of LAN functions - results from threats that block LAN resources from being available in a timely manner.
- **Unauthorized LAN Access**
- **Inadequate protection mechanism**
- **Natural calamities**
- **Deletion of data**

SECURITY SERVICES AND MECHANISMS

A security service is the collection of mechanisms, procedures and other controls that are implemented to help reduce the risk associated with threat. For example, the identification and authentication service help reduce the risk of the unauthorized user threat. Some services provide protection from threats, while other services provide for detection of the threat occurrence. An example of this would be a logging or monitoring service. The following services will be discussed in this section:

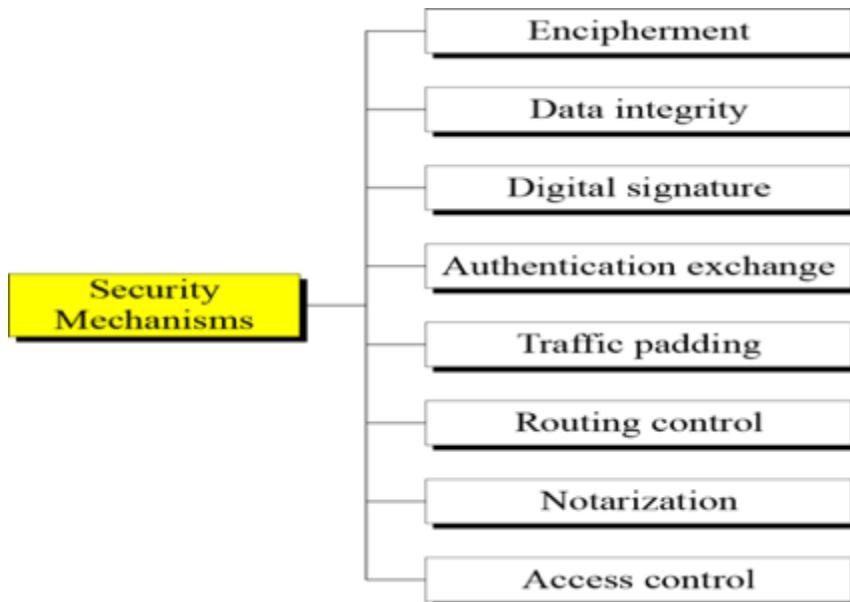
Security services



- **Authentication:** assures recipient that the **message is from the source** that it **claims to be from**.

- **Identification and authentication** - is the security service that helps ensure that the LAN is accessed by only authorized individuals.
- **Access control** - is the security service that helps ensure that LAN resources are being utilized in an authorized manner.
- **Data and message confidentiality** - is the security service that helps ensure that LAN data, software and messages are not disclosed to unauthorized parties.
- **Data and message integrity** - is the security service that helps ensure that LAN data, software and messages are not modified by unauthorized parties.
- **Non-repudiation** - is the security service by which the entities involved in a communication cannot deny having participated. Specifically, the sending entity cannot deny having sent a message (non-repudiation with proof of origin) and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery).
- **Logging and Monitoring** - is the security service by which uses of LAN resources can be traced throughout the LAN.
- **Bit stuffing:** This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.
- **Digital Signature:** This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified
- **Encipherment:** This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.
- **Access Control:** This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.
- **Notarization:** This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.
- **Data Integrity:** This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.

Security Mechanisms



Relation between security services and mechanisms

<i>Security Service</i>	<i>Security Mechanism</i>
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

ACCESS CONTROL

This service protects against the unauthorized use of LAN resources, and can be provided by the use of access control mechanisms and privilege mechanisms. Most file servers and multi-user workstations provide this service to some extent. However, PCs which mount drives from the file servers usually do not. Users must recognize that files used locally from a mounted drive are under the access control of the PC.

For this reason, it may be important to incorporate access control, confidentiality and integrity services on PCs to whatever extent possible. Access control mechanisms exist that support access granularity for acknowledging an owner, a specified group of users, and the world (all other authorized users). This allows the owner of the file (or directory) to have different access rights than all other users, and allows the owner to specify different access rights for a specified group of people, and also for the world.

The types of security mechanisms that could be implemented to provide the access control service are listed below.

Mechanisms access control mechanism using access rights (defining owner, group,

- world permissions), access control mechanism using access control lists, user profiles,
- capability lists, access control using mandatory access control mechanisms (labels), granular privilege mechanism

The types of security

Mechanisms that could be implemented to provide the data and message integrity service are listed below.

Mechanisms

Message authentication codes used for software or files,

- Use of secret key based electronic signature,
- Use of public key digital signature,
- Granular privilege mechanism,
- Appropriate access control settings (i.e., no unnecessary write permissions),
- Virus detection software,
- Workstations with no local storage (to prevent local storage of software and files),
- Workstations with no diskette drive/tape drive to prevent introduction of suspect software.
- Use of public key digital signatures.

Access control system.

What is Access Control?

The purpose of access control is to grant entrance to a building or office only to those who are authorized to be there. The deadbolt lock, along with its matching brass key, was the gold standard of access control for many years; however, modern businesses want more. Yes, they want to control who passes through their doors, but they also want a way to monitor and manage access. Keys have now passed the baton to computer-based electronic access control systems that provide quick, convenient access to authorized persons while denying access to unauthorized ones.



Today, instead of keys, we carry access cards or ID badges to gain entry to secured areas. Access control systems can also be used to restrict access to workstations, file rooms housing sensitive data, printers, and entry doors. In larger buildings, exterior door access is usually managed by a landlord or management agency, while interior office door access is controlled by the tenant company.

People new to access control may think the system is made up only of the card and the card reader mounted on the wall next to the door. But there are a few more parts behind the scenes, all working together to make the magic that grants access to the right person. That's what this guide is about. Reading it will give you a full and comprehensive understanding of how access control systems work and the language required to communicate with vendors.

What are the Components of Access Control?

At a high level, access control is about restricting access to a resource. Any access control system, whether physical or logical, has five main components:

1. **Authentication:** The act of proving an assertion, such as the identity of a person or computer user. It might involve validating personal identity documents, verifying the authenticity of a website with a digital certificate, or checking login credentials against stored details. (Something you know, something you have, something you are & somewhere you are)
2. **Authorization:** The function of specifying access rights or privileges to resources. For example, human resources staff are normally authorized to access employee records and this policy is usually formalized as access control rules in a computer system. (**Read R**- the subject can read content and list directory content, **write W**- the subject can change edit add create and rename a file or content, **execute X**- the subject can execute the file or content)
3. **Access:** Once authenticated and authorized, the person or computer can access the resource along with their rights and their objects.
4. **Manage:** Managing an access control system includes adding and removing authentication and authorization of users or systems. Some systems will sync with G Suite or Azure Active Directory, streamlining the management process.
5. **Audit:** Frequently used as part of access control to enforce the principle of least privilege. Over time, users can end up with access they no longer need, e.g., when they change roles. Regular audits minimize this risk.

Access Control Components

Access control systems aim to control who has access to a building, facility, or a “for authorized persons only” area. This is typically carried out by assigning employees, executives, freelancers, and vendors to different types of groups or access levels. Everyone may be able to use their access cards to enter the main door, but not be able to access areas containing secure or privileged information. (ACL corresponds to a column of ACL includes access control matrix a table in each row represents a subject each column represents an object and each entry is the set of access rights for the subject to that object. **Separation of duty SOD** is the principle the no user should be given more privileges to misuse the system. Safety involves measure that the access control configuration will not result to the leakage if permission to unauthorized personnel. Domain and type the grouping of processes into domain and objects into types of access operation such as RWX are restricted from domains.)

For clarity, we divide the components into three groups: user-facing components, admin-facing components, and infrastructure components. Let's dive into the nuances of the three categories.

User facing

The most familiar parts of access control systems are the cards, ID badges, and, more recently, the smartphone apps that elicit an OK beep when presented at a card reader and unlock the door. These are also known as credentials, since they bear the user's data that tells the reader to grant you permission to be on the premise, or in other words, that you are an authorized entrant.

Access cards are typically proximity cards that, rather than being swiped or inserted like credit cards, are held two to six inches in front of the card reader. The same procedure is followed for phone apps. The benefit of using credentials is that they are personalized, so any unlock event can be traced back to the person associated with it.

Admin facing

The admin-facing side is the management dashboard, or portal, where the office administrator, head of security, or IT manager sets the parameters of persons allowed to access the premises and under which circumstances they can do so. This involves a management dashboard, often in the cloud, and a way to provision access—such as a card programming device.

In more advanced systems, the manual operations aspect can be automated. For example, the provisioning (creating and deleting access) can be done automatically by connecting the access dashboard to the company directory of employees. When a new hire shows up in the system, new access is automatically positioned via an API or integrating database service like Google Apps, Microsoft Azure, SAML, or Okta.

Infrastructure

The infrastructure components are the ones that rely on your building infrastructure in order to function. The most obvious parts are locks, but there are other components, such as the controller, server, and cables.

Access Control Locks

Electronic locks are used to electrically unlock the door on which it's installed. They usually have a wire that powers them. Some locks will lock when they are supplied with power, while others unlock when supplied with power. The first ones are known as fail-safe locks and the second ones are known as fail-secure.

The choice of which to use depends on the area being secured. Entry doors call for fail-safe locks, since they need to comply with building codes and fire regulations that call for people to be able to exit at any time, even in the event of a power outage. IT rooms should be wired fail-secure because they need to remain locked at all times, even in the case of emergencies. Fail

secure doors also need to be equipped with electrified push bars to allow people to exit quickly in case of a fire.

Access Control Panel (or Controller)

Also known as the access control field panel or intelligent controller, the access control panel is not visible to most people in a facility because it's installed in the IT room or the electrical, telephone, or communications closet. The reason for this precaution is because all the locks are wired to it. When a valid credential is presented at the door reader, the panel receives its request to unlock a specific relay, which is connected to the specific door wire.

Access Control Server

Every access control system needs a server where the permissions are stored in an access database. As such it acts as the center, or “brain,” of the access control system. It is really the server that makes the decision whether the door should unlock or not by matching the credential presented to the credentials authorized for that door. The server can be a dedicated local Windows or Linux computer, a cloud server, or even a decentralized server (when the permissions are stored in the door reader). The server also tracks and records activity and events regarding access, and it allows administrators to pull reports of past data events for a given time period.

If a locally-hosted access control server is used, there is typically a dedicated machine that runs the access software on it. Managing it requires the administrator to be on-site. Since having to contend with several local servers can become complicated for multi-facility management, cloud-based servers are gaining a lot of traction in this area.

Low-Voltage Cables

Cables are a critical part of access control and can prove to be very expensive if installed improperly, so they should never be overlooked in planning an access control system. When building out space, it's important that all the cables are specified so that the general contractor knows what to do. If the cables are not planned for at this point, they will need to be added in later: This means someone will have to drill into, or lay cables on, all the newly-painted walls.

Types of Access Control

Access Control Models

The most common set of simple access control models includes discretionary access control, mandatory access control, rule-based access control, role-based access control, and attribute-based access control.

Discretionary Access Control

Discretionary Access Control (DAC) is a model of access control based on access being determined by the owner of the target resource. The owner of the resource can decide who does and does not have access, and exactly what access they are allowed to have. Their no restriction applied to the usage of information when received. Non-DAC ... policies in this category have rules that have not been established at the discrete of the user, establishes controls that cannot be changed by users but only through administrative actions. It provides separation of duty (SOD)

Mandatory Access Control

Mandatory Access Control (MAC) is a model of access control in which the owner of the resource does not get to decide who gets to access it, but instead access is decided by a group or individual who has the authority to set access on resources. Access control policies are made by a central authority. We can often find MAC implemented in government organizations, where access to a given resource is largely dictated by:

- the sensitivity label applied to data (secret, top secret, etc.),
- by the level of sensitive information, the individual is allowed to access (perhaps only secret), and
- by whether the individual actually has a need to access the resource which is the principle of least privilege.

Role-Based Access Control

Role-Based Access Control (RBAC) is a model of access control that, similar to MAC, functions on access controls set by an authority, rather than by the owner of the resource. The difference between RBAC and MAC is that access control in RBAC is based on the role of the individual accessing the resource.

Attribute-Based Access Control

Attribute-Based Access Control (ABAC) is based on attributes. These can be the attributes of a particular person, of a resource, or of an environment. Attributes may be Subject (height of a person in an amusement park), Resource (software that only runs on a particular operating system or website), or Environmental (time of day or length of activity time passed).

Multilevel access control models may be used by military and government organizations where the simpler access control models that we just discussed may not be considered robust enough to protect the information to which we are controlling access.

Physical Access Controls

When discussing physical access controls, we are often largely concerned with controlling the access of individuals, devices, and vehicles. (Prevents attackers from accessing a facility to get resource stored in a particular facility).

Access control for individuals often revolves around controlling movement into and out of buildings or facilities. We can see simple examples of such controls on the buildings of many organizations in the form of badges that control door access to facilities (something we have). Such badges are typically configured on an ACL that permits or denies their use for certain doors and regulates the time of day that they can be used.

Physical access control for vehicles often revolves around keeping said vehicles from moving into or through restricted areas.

The following are the main components of a physical access control system:

- **Access point:** The entrance points where the barrier is needed. Common physical access control examples of access points include security gates, turnstiles and door locks. A secure space can have a single access point, like an office inside a larger complex, or many access points.
- **Personal credentials:** Most PACS require a user to have identifying credentials to enter a facility or access data. Physical access control examples of credentials include fobs and key card entry systems, encrypted badges, mobile credentials, PIN codes and passwords. Personal credentials tell the system who is trying to gain entry.
- **Readers and/or keypads:** Stationed at the access point, readers send data from credentials to a control panel to authenticate the credential and request access authorization. If using a keypad or biometric reader (such as a fingerprint scan, facial ID, or retina scan), users will enter their PIN or complete a scan prior to obtaining access.
- **Control panel:** The PACS control panel receives the credential data from the reader and verifies if the credential is valid. If the credential data is approved, the control panel transmits authorization data to the access point via the access control server, and the door will unlock. If the credential data is not approved, the user will not be able to gain entry.
- **Access control server:** The access control server stores user data, access privileges, and audit logs. Depending on your system, the server might be on-premises, or managed in the cloud. System maintenance and software updates should be performed regularly to protect the system from hacking and possible security breaches.

The two main types are physical and logical.

- **Physical access control** refers to the selective restriction of access to a location, a task most often accomplished with a variety of security methods that control and track who is entering a location and who is leaving.
- **Logical access control** is defined as restricting virtual access to data; it consists of identification, authentication, and authorization protocols utilized worldwide to protect hardware from unauthorized access, including password programs, smart cards, or tokens to identify and screen users and access levels.

What to look for in physical access control systems?



With recent advancements in security technology, physical access control systems are now available with many enhanced features and options. One choice you will need to make when planning and budgeting for a physical access control system is the type of credentials you want to use. If you are opting for a more budget-conscious credential selection, keycards seem like the right choice up front. However, keycards may end up costing you more over time, simply because they are frequently lost and need replacing. Not to mention that a lost keycard can pose a security threat if it ends up in the wrong hands. If keycards or fobs are still the right choice for your business, make sure you purchase encrypted keycards, or use two-factor authentication for an added layer of protection. For the best in security and value, a mobile credential gives your users the convenience of using their mobile phone to enter and exit the building, with multi-factor biometric authentication built right in. You won't have to replace keycards, and smartphones are less likely to be lost, left at home, or passed around the office.

Another factor to consider when planning your physical access control procedures is maintenance and system management. Many legacy access control systems use cumbersome readers and on-site servers, which require in-person management and maintenance. Delays in system updates can put your system at higher risk of a breach, and older readers are prone to tampering. Plus, if credentials need to be reassigned or newly created, an administrator will likely need to be on-site to handle the request. If you anticipate needing access to your system remotely, or want the latest security updates in real-time, you should consider systems that use more modern software. When selecting a PACS for your building, there are added benefits to using a physical access control system that runs on a cloud-based platform.

What to Look for When Choosing an Access Control System?

There are several factors to take into consideration when comparing different providers. Below is an overview of some of the main questions you may want to look at, divided into three categories: compatibility, features, and maintenance.

Compatibility

Compatibility is very important when choosing an access control system. Making sure that the system you want to purchase is compatible with your facility can save you a lot of time and money during the installation process. A highly compatible system, like the Kisi one, also makes it easier to maintain the facility and ensure a high level of security. Some compatibility-related questions may be:

- Is it compatible with third-party hardware and free from lock-in?
- Does it integrate with surveillance and other security systems?
- How easy is it to use and configure?
- Does it offer an open API?

Features and maintenance

Features are obviously the deal breaker when choosing any type of security system for your office. What can be more difficult, however, is understanding which features need to be

prioritized in order to find a solution that not only covers your basic needs, but also saves you time in the long run.

We recommend that you choose a system based on cloud technology that gives you multiple unlocking options (not limited to only keycards or fobs). This saves you time, as you don't have to issue a new keycard every time there is a new visitor or employee. It also reduces the number of security issues caused by employees forgetting or misusing keycards and fobs.

Lastly, we would recommend choosing a company with solid customer service in order to quickly clear any doubts that might emerge during installation or during everyday use of the system.

Some other feature-related questions you should consider:

- Is the hardware IP-based?
- Is offline mode supported?
- Is two-factor authentication (2FA) supported?
- Is lockdown supported? If so, is it at door or place level, or both?
- What communication channels does it run on (e.g., Bluetooth, NFC, RFID, PoE, and others)?
- Does it support multiple types of authentication input such as mobile apps, remote unlocks, cards, key fobs, and more?
- Are all access methods offering end-to-end data encryption?
- Is customer support included?
- What access restrictions are available (e.g.: time-based access, role-based access, level-based access, count-based access, and others)?

Access control in information security

Information security means protecting information and information systems from unauthorized access use disclosure and disruption modification of destruction. The fountain in which access control mechanisms are build start with **identification** and **authentication** (I&A). Identification is an assertion of who the person is. Authentication is the act of verifying a claim of identity.

The need-to-know principle can be accessed with user control authorization is to ensure that only authorized individuals gain access to the systems. It includes; identification authorization and authentication.

NETWORK SCANNERS

Network scanning builds a clearer picture of accessible hosts and their network services. Network scanning and reconnaissance is the real data gathering exercise of an Internet-based security assessment. The rationale behind IP network scanning is to gain insight into the following elements of a given network:



- ICMP message types that generate responses from target hosts
- Accessible TCP and UDP network services running on the target hosts
- Operating platforms of target hosts and their configuration
- Areas of vulnerability within target host IP stack implementations (including sequence number predictability for TCP spoofing and session hijacking)
- Configuration of filtering and security systems (including firewalls, border routers, switches, and IDS sensors)

TYPES OF SCANNING

There are three types of scanning:

- 1.** Port Scanning
- 2.** Network Scanning
- 3.** Vulnerability Scanning

SCANNING METHODOLOGY

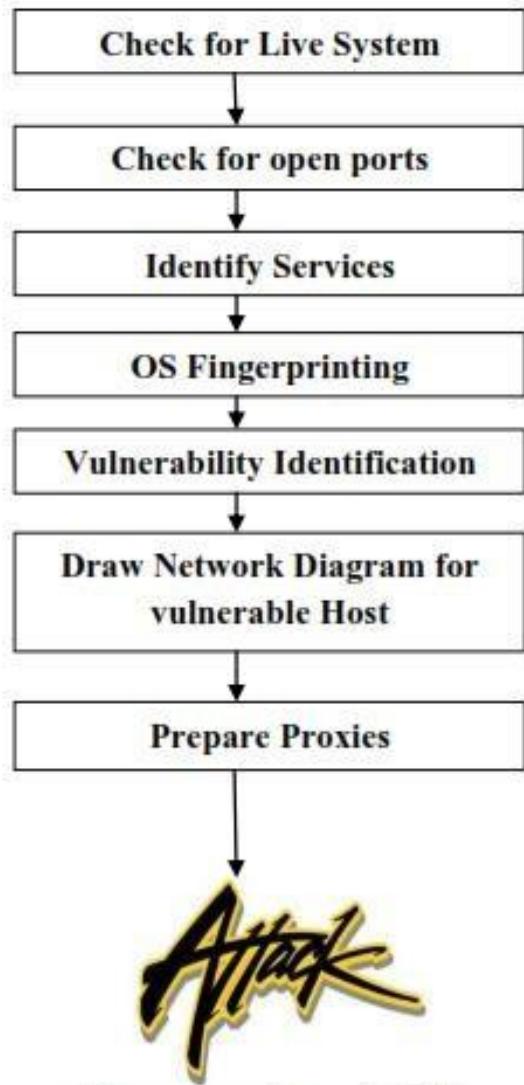


Figure: scanning methodology

PORT SCANNING

When live systems are discovered, an attacker will usually attempt to discover which services are available for exploitation. This is accomplished by a technique commonly known as *port scanning*.

The sections in this chapter titled -The TCP/IP Protocol| and -The UDP Protocol| respectively details both the TCP and UDP protocol and clarifies how ports are used; suffice to say, however, that every application has a specific port number associated with it that identifies that application.

SSH Security Basics

SSH stands for [Secure Shell](#). The name “SSH” is used interchangeably to mean either the SSH protocol itself or the software tools that allow system administrators and users to make secure connections to remote computers using that protocol.

The SSH protocol is an encrypted protocol designed to give a secure connection over an insecure network, such as the internet. SSH in Linux is built on a portable version of the [OpenSSH](#) project. It is implemented in a [classic client-server model](#), with an SSH server accepting connections from SSH clients. The client is used to connect to the server and to *display* the session to the remote user. The server accepts the connection and *executes* the session.

In its default configuration, an SSH server will listen for incoming connections on Transmission Control Protocol ([TCP](#)) port 22. Because this is a standardized, [well-known port](#), it is a target for [threat actors](#) and [malicious bots](#).

Threat actors launch bots that scan a range of IP addresses looking for open ports. The ports are then probed to see if there are vulnerabilities that can be exploited. Thinking, “I’m safe, there are bigger and better targets than me for the bad guys to aim at,” is false reasoning. The bots aren’t selecting targets based on any merit; they’re methodically looking for systems they can breach.

Security Friction

Security friction is the irritation—of whatever degree—those users and others will experience when you implement security measures. We’ve got long memories and can remember introducing new users to a computer system, and hearing them ask in a horrified voice whether they *really* had to enter a password *every time* they logged in to the mainframe. That—to them—was security friction.

(Incidentally, the invention of the password is credited to [Fernando J. Corbató](#), another figure in the pantheon of computer scientists whose combined work contributed to the circumstances that led to the birth of [Unix](#).)

Introducing security measures usually involves some form of friction for someone. Business owners have to pay for it. The computer users may have to change their familiar practices, or remember another set of authentication details, or add extra steps to connect successfully. The system administrators will have additional work to do to implement and maintain the new security measures.

Hardening and locking down a Linux or Unix-like operating system can get very involved, very quickly. What we're presenting here is a set of easy to implement steps that will improve the security of your computer without the need for third-party applications and without digging through your firewall.

These steps aren't the final word in SSH security, but they'll move you a long way forward from the default settings, and without too much friction.

Avoid Port 22

Port 22 is the standard port for SSH connections. If you use a different port, it adds a little bit of security through obscurity to your system. Security through obscurity is never considered a true security measure, and I have railed against it in other articles. In fact, some of the smarter attack bots probe all open ports and determine which service they are carrying, rather than relying on a simple look-up list of ports and assuming they provide the usual services. But using a non-standard port can help with lowering the noise and bad traffic on port 22.

To configure a non-standard port, edit your [SSH configuration file](#):

```
sudo gedit /etc/ssh/sshd_config
```

```
# $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Protocol 2

Port 479
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Remove the hash # from the start of the “Port” line and replace the “22” with the port number of your choice. Save your configuration file and restart the SSH daemon:

```
sudo systemctl restart sshd
```

Let’s see what effect that has had. Over on our other computer, we’ll use the ssh command to connect to our server. The ssh command defaults to using port 22:

```
ssh dave@howtogeek.local
```

```
[dave@Nostromo ~]$ ssh dave@howtogeek.local
ssh: connect to host howtogeek.local port 22: Connection refused
[dave@Nostromo ~]$ █
```

Our connection is refused. Let’s try again and specify port 470, using the -p (port) option:

```
ssh -p 479 dave@howtogeek.local
```

```
[dave@Nostromo ~]$ ssh -p 479 dave@howtogeek.local
dave@howtogeek.local's password: █
```

Our connection is accepted.

Filter Connections Using TCP Wrappers

TCP Wrappers is an easy to understand access control list. It allows you to exclude and permit connections based on characteristics of the connection request, such as IP address or hostname. TCP wrappers should be used in conjunction with, and not instead of, a properly configured firewall. In our specific scenario, we can tighten things up considerably by using TCP wrappers.

TCP wrappers was already installed on the Ubuntu 18.04 LTS machine used to research this article. It had to be installed on Manjaro 18.10 and Fedora 30.

To install on Fedora, use this command:

```
sudo yum install tcp_wrappers
```

```
[dave@howtogeek ~]$ sudo yum install tcp_wrappers █
```

To install on Manjaro, use this command:



```
sudo pacman -Syu tcp-wrappers
```

```
[dave@howtogeek ~]$ sudo pacman -Syu tcp-wrappers
```

There are two files involved. One holds the allowed list, and the other holds the denied list. Edit the deny list using:

```
sudo gedit /etc/hosts.deny
```

```
dave@howtogeek:~$ sudo gedit /etc/hosts.deny
```

This will open the gedit editor with the deny file loaded in it.

```
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system
# See the manual pages hosts_access(5) and hosts_options(5)
#
# Example:      ALL: some.host.name, .some.domain
#                  ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
ALL : ALL
```

You need to add the line:

```
ALL : ALL
```

And save the file. That blocks all access that hasn't been authorized. We now need to authorize the connections you wish to accept. To do that, you need to edit the allow file:

```
sudo gedit /etc/hosts.allow
```



```
dave@howtogeek:~$ sudo gedit /etc/hosts.allow
```

This will open the gedit editor with the allow file loaded in it.

```
# /etc/hosts.allow: list of hosts that are allowed to access the system
# See the manual pages hosts_access(5) and hosts_options(5)
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information
#
sshd : 192.168.4.23
```

ADVERTISEMENT

We've added in the SSH daemon name, SSHD, and the IP address of the computer we're going to allow to make a connection. Save the file, and let's see if the restrictions and permissions are in force.

First, we'll try to connect from a computer that isn't in the hosts.allow file:

```
[dave@howtogeek ~]$ ssh -p 479 dave@192.168.4.24
ssh: connect to host 192.168.4.24 port 479: Connection refused
[dave@howtogeek ~]$
```

The connection is refused. We'll now try to connect from the machine at IP address 192.168.4.23:

```
[dave@Nostromo ~]$ ssh -p 479 dave@howtogeek.local
dave@howtogeek.local's password:
```

Our connection is accepted.

Our example here is a bit brutal—only a single computer can connect. TCP wrappers is quite versatile and more flexible than this. It supports hostnames, wildcards, and subnet masks to accept connections from ranges of IP addresses.

Reject Connection Requests with No Passwords

Although it is a bad practice, a Linux system administrator can create a user account with no password. That means remote connection requests from that account will have no password to check against. Those connections will be accepted but unauthenticated.

The default settings for SSH accept connection requests without passwords. We can change that very easily, and ensure all connections are authenticated.

We need to edit your SSH configuration file:

```
sudo gedit /etc/ssh/sshd_config
```

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues w:
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
```

ADVERTISEMENT

Scroll through the file until you see the line that reads with “#PermitEmptyPasswords no.” Remove the hash # from the start of the line and save the file. Restart the SSH daemon:

```
sudo systemctl restart sshd
```

Use SSH Keys Instead of Passwords

SSH keys provide a secure means of logging into an SSH server. Passwords can be guessed, cracked, or brute-forced. SSH keys are not open to such types of attack.



When you generate SSH keys, you create a pair of keys. One is the public key, and the other is the private key. The public key is installed on the servers you wish to connect to. The private key, as the name would suggest, is kept secure on your own computer.

SSH keys allow you to make connections without a password that are—counterintuitively—more secure than connections that use password authentication.

When you make a connection request, the remote computer uses its copy of your public key to create an encrypted message that is sent back to your computer. Because it was encrypted with your public key, your computer can unencrypt it with your private key.

Your computer then extracts some information from the message, notably the session ID, encrypts that, and sends it back to the server. If the server can decrypt it with its copy of your public key, and if the information inside the message matches what the server sent to you, your connection is confirmed to be coming from you.

ADVERTISEMENT

Here, a connection is being made to the server at 192.168.4.11, by a user with SSH keys. Note that they are not prompted for a password.

```
ssh dave@192.168.4.11
```

```
[dave@Nostromo ~]$ ssh dave@192.168.4.11
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.0.0-29-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

10 packages can be updated.
0 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Tue Oct  1 17:26:42 2019 from 192.168.4.16
dave@howtogeek:~$ █
```

Disable Password Authentication Altogether

Of course, the logical extension of using SSH keys is that if all remote users are forced to adopt them, you can turn off password authentication completely.

We need to edit your SSH configuration file:

```
sudo gedit /etc/ssh/sshd_config
```

```
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication no
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues w:
# some PAM modules and threads)
ChallengeResponseAuthentication no
```

Scroll through the file until you see the line that starts with “#PasswordAuthentication yes.” Remove the hash # from the start of the line, change the “yes” to “no”, and save the file. Restart the SSH daemon:

```
sudo systemctl restart sshd
```

Disable X11 Forwarding

X11 forwarding allows remote users to run graphical applications from your server over an SSH session. In the hands of a threat actor or malicious user, a GUI interface can make their malign purposes easier.

A standard mantra in cybersecurity is if you don’t have a bonafide reason to have it turned on, turn it off. We’ll do so by editing your [SSH config file](#):

```
sudo gedit /etc/ssh/sshd_config
```

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#PermitUserEnvironment no
```

ADVERTISEMENT

Scroll through the file until you see the line that starts with “#X11Forwarding no.” Remove the hash # from the start of the line and save the file. Restart the SSH daemon:

```
sudo systemctl restart sshd
```

Set an Idle Timeout Value

If there is an established SSH connection to your computer, and there has been no activity on it for a period of time, it could pose a security risk. There is a chance that the user has left their desk and is busy elsewhere. Anyone else who passes by their desk can sit down and start using their computer and, via SSH, your computer.

It’s much safer to establish a timeout limit. The SSH connection will be dropped if the inactive period matches the time limit. Once more, we’ll edit your SSH configuration file:

```
sudo gedit /etc/ssh/sshd_config
```

```
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#PermitUserEnvironment no
#Compression delayed
ClientAliveInterval 300
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none
```

Scroll through the file until you see the line that starts with “#ClientAliveInterval 0” Remove the hash # from the start of the line, change the digit 0 to your desired value. We’ve used 300 seconds, which is 5 minutes. Save the file, and restart the SSH daemon:

```
sudo systemctl restart sshd
```

Set a Limit for Password Attempts

Defining a limit on the number of authentication attempts can help thwart password guessing and brute-force attacks. After the designated number of authentication requests, the user will be disconnected from the SSH server. By default, there is no limit. But that is quickly remedied.

Again, we need edit your SSH configuration file:

```
sudo gedit /etc/ssh/sshd_config
```

```
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
MaxAuthTries 3
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none
```

Scroll through the file until you see the line that starts with “#MaxAuthTries 0”. Remove the hash # from the start of the line, change the digit 0 to your desired value. We’ve used 3 here. Save the file when you made your changes and restart the SSH daemon:

```
sudo systemctl restart sshd
```

ADVERTISEMENT

We can test this by attempting to connect and deliberately entering an incorrect password.

```
[dave@Nostromo ~]$ ssh dave@192.168.4.11
dave@192.168.4.11's password:
Received disconnect from 192.168.4.11 port 22:2: Too many authentication failures
Disconnected from 192.168.4.11 port 22
[dave@Nostromo ~]$
```

Note that MaxAuthTries number seemed to be one more than the number of tries the user was permitted. After two bad attempts, our test user is disconnected. This was with MaxAuthTries set to three.

Disable Root Log Ins

It is bad practice to log in as root on your Linux computer. You should log in as a normal user and use sudo to perform actions that require root privileges. Even more so, you shouldn't allow root to log into your SSH server. Only regular users should be allowed to connect. If they need to perform an administrative task, they should use sudo too. If you're forced to allow a root user to log in, you can at least force them to use SSH keys.

For the final time, we're going to have to edit your SSH configuration file:

```
sudo gedit /etc/ssh/sshd_config
```

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin prohibit-password
#StrictModes yes
MaxAuthTries 3
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
```

Scroll through the file until you see the line that starts with “#PermitRootLogin prohibit-password” Remove the hash # from the start of the line.

- If you want to prevent root from logging in at all, replace “prohibit-password” with “no”.
- If you are going to allow root to log in but force them to use SSH keys, leave “prohibit-password” in place.

Save your changes and restart the SSH daemon:

```
sudo systemctl restart sshd
```

The Ultimate Step

Of course, if you don't need SSH running on your computer at all, make sure it is disabled.

```
sudo systemctl stop sshd  
sudo systemctl disable sshd
```

ADVERTISEMENT

If you don't open the window, no one can climb in.

TECHNIQUES

Over time, a number of techniques have been developed for surveying the protocols and ports on which a target machine is listening. They all offer different benefits and problems. Here is a lineup of the most common:

TCP connect () scanning: This is the most basic form of TCP scanning. The connect () system call provided by your operating system is used to open a connection to every interesting port on the machine. If the port is listening, connect () will succeed, otherwise the port isn't reachable. One strong advantage to this technique is that you don't need any special privileges. Any user on most UNIX boxes is free to use this call. Another advantage is speed.

TCP SYN scanning: This technique is often referred to as "half-open" scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and wait for a response. A SYN|ACK indicates the port is listening. A RST is indicative of a non-listener.

TCP FIN scanning: There are times when even SYN scanning isn't clandestine enough.

Some firewalls and packet filters watch for SYNs to an unallowed port, and programs like syn-logger and Courtney are available to detect these scans. FIN packets, on the other hand, may be able to pass through unmolested. The idea is that closed ports tend to reply to your FIN packet with the proper RST. Open ports, on the other hand, tend to ignore the packet in question.

Fragmentation scanning: This is not a new scanning method in and of itself, but a modification of other techniques. Instead of just sending the probe packet, you break it into a couple of small IP fragments.

FIREWALLS

A firewall is a **security device — computer hardware or software** — that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer. ... Firewalls can provide different levels of protection.

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet

There are three basic types of firewalls depending on:



- Whether the communication is being done between a single node and the network, or between two or more networks.
- Whether the communication is intercepted at the network layer, or at the application layer.
- Whether the communication state is being tracked at the firewall or not.

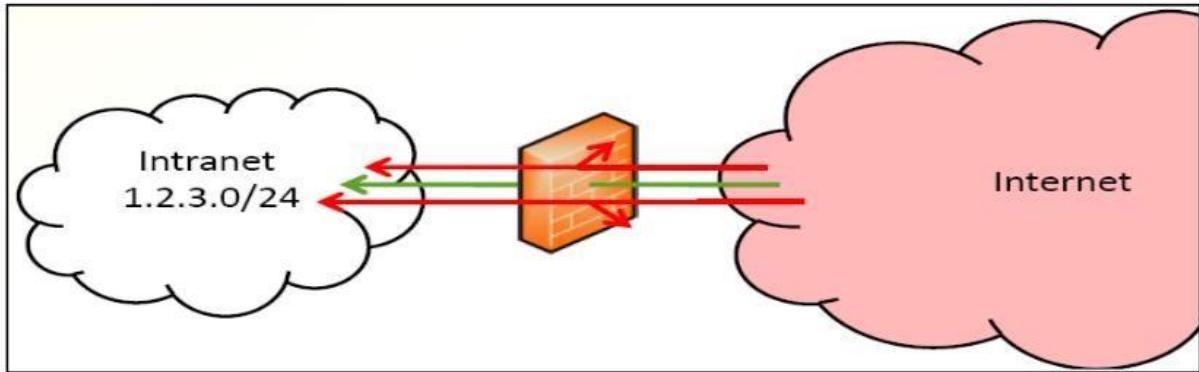


Figure: Firewall

TYPES OF FIREWALLS

There are two types of firewalls.

1. Packet Filtering Firewalls - that block selected network packets.
2. Proxy Servers (sometimes called firewalls) - that make network connections for you

ADVANTAGES

Packet filtering has a number of advantages:

One screening router can help protect an entire network **Packet filtering doesn't require user knowledge or cooperation** **Packet filtering is widely available in many routers**

DISADVANTAGES

Although packet filtering provides many advantages, there are some disadvantages to using packet filtering as well:

Current filtering tools are not perfect **Some protocols are not well suited to packet filtering** **Some policies can't readily be enforced by normal packet filtering routers**

Configuring SSH access through firewalls

SSH is one of the few protocols that are frequently permitted through firewalls. Unrestricted outbound SSH is very common, especially in smaller and more technical organizations. Inbound SSH is usually restricted to one or very few servers.

Outbound SSH

Configuring outbound SSH in a firewall is very easy. If there are restrictions on outgoing traffic at all, just create a rule that allows TCP port 22 to go out. That is all. If you want to restrict the destination addresses, you can also limit the rule to only permit access to your organization's external servers in the cloud, or to a jump server that guards cloud access.

Back-tunneling is a risk

Unrestricted outbound SSH can, however, be risky. The SSH protocol supports [tunneling](#). The basic idea is that it is possible to have the SSH server on an external server listen to connections from anywhere, forward those back into the organization, and then make a connection to some Internal server.

This can be very convenient in some environments. Developers and system administrators frequently use it to open a tunnel that they can use to gain remote access from their home or from their laptop when they are travelling.

However, it generally violates policy and takes control away from firewall administrators and the security team. It can, for example, violate [PCI](#), [HIPAA](#), or [NIST SP 800-53](#). It can be used by hackers and foreign intelligence agencies to leave backdoors into organizations

Inbound SSH access

For inbound access, there are a few practical alternatives:

- Configure firewall to forward all connections to port 22 to a particular IP address on the internal network or [DMZ](#).
- Use different ports on the firewall to access different servers.
- Only allow SSH access after you have logged in using a VPN (Virtual Private Network), typically using the [IPsec](#) protocol.

TYPES OF PROXY SERVERS

There are many different types of proxy servers out there, but following are some commonly known proxies.

Anonymous Proxy Distorting Proxy High Anonymity Proxy Intercepting Proxy Reverse Proxy Transparent Proxy Web Proxy

A **web proxy** focuses on traffic over the World Wide Web. Many times, these proxies are used by schools, countries, or corporations to block offensive web content, or to simply control their client's access to the internet.

Open Proxy – An open proxy is a proxy that allows anybody to connect to and use. Open proxies can also be exploited and misused by spammers. For this reason, some websites will not allow traffic to their servers from known open proxies.

FIREWALL MONITORING

1. Don't depend on your firewall completely as it's not complete answer of your network security.
2. Deny all traffic by default and only enable those ports, protocols, and services that are needed.
3. Limit the number of applications that run on the firewall in order to maximize CPU cycles and network throughput. This will let the firewall do what it's best at doing.
4. Run the firewall service as a unique user ID instead of administrator or root.
5. Set or change the default firewall administrator or root password before you ever connect it to the public Internet.

PROXY SERVER

Proxying provides Internet access to a single host, or a very small number of hosts, while appearing to provide access to all of your hosts. The hosts that have access act as proxies for the machines that don't, doing what these machines want do.

A proxy server for a particular protocol or set of protocols runs on a dual-homed host or a bastion host: some host that the user can talk to, which can, in turn, talks to the outside world. The user's client program talks to this proxy server instead of directly talking to the "real" server out on the Internet.

The proxy server evaluates requests from the client and decides which to pass on and which to disregard. If a request is approved, the proxy server talks to the real server on behalf of the client (thus the term "proxy"), and proceeds to relay requests from the client to the real server, and to relay the real server's answers back to the client.

"Proxy systems are effective only when they are used in conjunction with some method of restricting IP-level traffic between the clients and the real servers, such as a screening router or a dual-homed host that doesn't route packets. If there is IP-level connectivity between the clients and the real servers, the clients can bypass the proxy system (and presumably so can someone from the outside)."

APPLICATIONS OF FIREWALL

There are three applications of firewall:

- Network address translation or NAT
- Intrusion detection systems
 - Logging

SESSION HIJACKING

Ethical Hacking: Session Hijacking. The course is the 11th course in the LinkedIn learning path. The course is divided into 5 sections named respectively:

- Network Session Hijacking
- Web Session Hijacking
- Additional Tools
- Service Hijacking
- Hijacking the Physical World

Network Session Hijacking

Session Hijacking means the ability of the attacker to:

- take control over communications.
- Gain Access to services without authenticating.
- Exploit protocol weaknesses.
- Exploit weak wireless configuration.
- Exploit web services.

Both sides of the TCP session maintain a 32 bits sequence number used throughout the session. The session starts with a 3-way handshake to set the values of the sequence number on both sides which will be incremented throughout the session.

Shijack is a TCP connection hijacking tool for Linux, FreeBSD and Solaris.

Web Session Hijacking

HTTP is stateless protocol so there it doesn't retain any information between web pages. But whenever there is a need to track this info, state will be provided through session IDs (authentication). Session IDs can be passed either embedded in the URL or via cookies.

WebSockets provide the ability to set up a full duplex communications channel between the client and the server, this requires a handshake over HTTP or HTTPS to upgrade the protocol to WS or WSS and a WebSocket server to manage the protocol.

Man In the Browser (MITB) is a form of attack which inserts code inside the user's browser. It is a difficult attack to detect as the malware sniffs and modifies the transaction before their transmission. MITB is hard to detect and can include parts of HTML sent from the server to capture sensitive information without being noticed to even anti-virus software.

To Create a MITB you can use:

- Browser helper object.
- Browser extension.
- API hooking.
- JavaScript.

MIM attack can be used to hijack a web session, it goes often unnoticed until it's too late. The attacker intercepts the messages coming from both ends (client & server) and reply to each of them without them realizing there is a "proxy" between them.

MIM can be established in many ways:

- Web proxy in the web browser (it can be deliberate — to do testing).
- ARP poisoning.
- Malicious WiFi host-spot.

SSL stripping is an attack used in the key exchange protocol; it is used to downgrade security for the connection without interfering with the certificate. It is also known as an HTTP downgrade attack. The communication between the server and the attacker happens through HTTPS but the one between the client and the attacker is through HTTP, therefore the attacker can see the messages coming from the client clearly and the certificate on the server side was validated with no issues.

Session hijacking can happen through intercepting and re-using cookies.

Subterfuge is a framework used to hijack sessions. It can be used to hijack the session through ARP poisoning. ARP poisoning happens when an attacker sends an ARP identification associating an IP address of a machine on the network with the attacker's MAC address.

Additional Tools

Zed Attack Proxy is a web proxy tool that comes with Kali. ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Cain & Abel is used to collect credentials and crack passwords. It includes session hijacking a MIM throughout poisoning. It is available for Windows.

Service Hijacking

Secure Shell (SSH) is a common protocol used by system administrators to remotely manage enterprise servers, and is preferred over telnet, as it establishes a secure connection.

Insomnia a company from New Zealand invented a tool called **PuTTY Hijack** (works only on 0.6 version) that hijacks putty sessions and puts system administrators at risk. This tool inspired another one called **PuTTY Rider** which works on all PuTTY releases. PuTTY Rider can even monitor the session in real time.

DNS hijack can happen through altering your hosts file on your systems. This files exists on both Linux and Windows and it provides hard coded translation, it is used before checking the DNS sever.

Cloud is also not immune to hijacking. It could be account hijacking, service cloud traffic hijacking, theft of pay-for-use API keys ... The attack can happen using brute force guessing of passwords or the credentials have been compromised though another service.

Hijacking the Physical World

Since the cars and drones use have multiple networks and dozens of sensors and electronic computer units, ECUs. Replacing early point to point wiring with addressable network devices.

This gives the opportunity to attackers to remotely access and control these systems — via Bluetooth or internet. The control can vary from controlling air conditioning system to disabling brakes or accelerators.

Summary

Web applications provide an interface between end users and web servers through a set of web pages generated at the server end or that contain script code to be executed dynamically within the client Web browser.

Module Objective

The objective of this lab is to provide expert knowledge of web application vulnerabilities and web applications attacks such as:

- Parameter tampering
- Directory traversals
- Cross-Site Scripting (XSS)
- Web Spidering
- Cookie Poisoning and cookie parameter tampering
- Securing web applications from hijacking

Scenario

A web application is an application that is accessed by users over a network such as the Internet or an intranet. The term may also mean a computer software application that is coded in a browser-supported programming language (such as JavaScript, combined with a browser-rendered markup language like HTML) and reliant on a common web browser to render the application executable.

Web applications are popular due to the ubiquity of web browsers, and the convenience of using a web browser as a client. The ability to update and maintain web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity, as is the inherent support for cross-platform compatibility. Common web applications include webmail, online retail sales, online auctions, wikis and many other functions.

Web hacking refers to exploitation of applications via HTTP which can be done by manipulating the application via its graphical web interface, tampering the Uniform Resource Identifier (URI) or tampering HTTP elements not contained in the URI. Methods that can be used to hack web applications are SQL Injection attacks, Cross Site Scripting (XSS), Cross Site Request Forgeries (CSRF), Insecure Communications, etc.

As a security expert and Security Administrator, you need to test web applications for cross-site scripting vulnerabilities, cookie hijacking, command injection attacks, and secure web applications from such attacks.

I. Hacking Web Applications

According to the Daily News, Cyber-crime targeted in new ICT policy; the government is reviewing the current Information and Communication Technology (ICT) policy in the quest to incorporate other relevant issues, including addressing cyber-crime, reported being on the increase.

“Many websites and web applications are vulnerable to security threat including the government’s and nongovernment websites, we are therefore cautious to ensure that the problem is checked”, Mr Urasa said. Citing some of the reasons leading to hacking, he said inadequate auditing in website and web applications caused by lack of standard security auditing were among problems that many web developers faced.

As a security expert and Security Administrator, you should be aware of all the methods that can be employed by an attacker towards hacking web applications and accordingly you can implement a countermeasure for those attacks. Hence, in this lab, you will learn how to hack a website with vulnerabilities.

Lab Objectives

The objective of this lab is to help students learn how to test web applications for vulnerabilities. In this lab you will perform:

- Parameter tampering attacks
- Cross-site scripting (XSS or CSS)

Lab Analysis

In this lab, you have learnt how to test web applications for vulnerabilities. Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

II. Website Vulnerability Scanning Using Acunetix WVS

As an expert Penetration Tester, find out if your website is secure before hackers download sensitive data, commit a crime using your website as a launch pad, and endanger your business. You may use Acunetix Web Vulnerability Scanner (WVS) that checks the website, analyzes the web applications and finds perilous SQL injection, Cross site scripting and other vulnerabilities that expose the online business. Concise reports identify where web applications need to be fixed, thus enabling you to protect your business from impending hacker attacks!

Lab Objectives

The objective of this lab is to help students secure web applications and test websites for vulnerabilities and threats.

Lab Analysis

In this lab, you have learnt how to secure web applications and test websites for vulnerabilities and threats. Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Module Syllabus

- Web Application Security Statistics
- Introduction to Web Applications
- Web Application Components
- How Do Web Applications work?
- Web Application Architecture
- Web 2.0 Applications
- Vulnerability Stack
- Web Attack Vectors
- Web Application Threats - 1
- Web Application Threats - 2
- Unvalidated Input
- Parameter/Form Tampering

- Directory Traversal
- Security Misconfiguration
- Injection Flaws
 - SQL Injection Attacks
 - Command Injection Attacks
 - Command Injection Example
 - File Injection Attack
- What is LDAP Injection?
- How LDAP Injection Works?
- Hidden Field Manipulation Attack
- Cross-Site Scripting (XSS) Attacks
 - How do XSS Attacks work?
 - Cross-Site Scripting Attack Scenario: Attack via Email
 - XSS Example: Attack via Email
 - XSS Example: Stealing Users' Cookies
 - XSS Example: Sending an Unauthorized Request
 - XSS Attack in Blog Posting
 - XSS Attack in Comment Field
 - XSS Cheat Sheet
 - Cross-Site Request Forgery (CSRF) Attack
 - How do CSRF Attacks work?
- Web Application Denial-of-Service (DoS) Attack
 - Denial of Service (DoS) Examples
- Buffer Overflow Attacks
- Cookie/Session Poisoning
 - How Does Cookie Poisoning work?
- Session Fixation Attack
- Insufficient Transport Layer Protection
- Improper Error Handling
- Insecure Cryptographic Storage
- Broken Authentication and Session Management
- Unvalidated Redirects and Forwards
- Web Services Architecture
 - Web Services Attack
 - Web Services Footprinting Attack
 - Web Services XML Poisoning
- Footprint Web Infrastructure
 - Footprint Web Infrastructure: Server Discovery
 - Footprint Web Infrastructure: Server Identification/Banner Grabbing
 - Footprint Web Infrastructure: Hidden Content Discovery
- Web Spidering Using Burp Suite
- Hacking Web Servers
 - Web Server Hacking Tool: WebInspect
- Analyze Web Applications
 - Analyze Web Applications: Identify Entry Points for User Input
 - Analyze Web Applications: Identify Server-Side Technologies

- Analyze Web Applications: Identify Server-Side Functionality
 - Analyze Web Applications: Map the Attack Surface
- Attack Authentication Mechanism
- Username Enumeration
- Password Attacks: Password Functionality Exploits
- Password Attacks: Password Guessing
- Password Attacks: Brute-forcing
- Session Attacks: Session ID Prediction/ Brute-forcing
- Cookie Exploitation: Cookie Poisoning
- Authorization Attack
 - HTTP Request Tampering
 - Authorization Attack: Cookie Parameter Tampering
- Session Management Attack
 - Attacking Session Token Generation Mechanism
 - Attacking Session Tokens Handling Mechanism: Session Token Sniffing
- Injection Attacks
- Attack Data Connectivity
 - Connection String Injection
 - Connection String Parameter Pollution (CSPP) Attacks
 - Connection Pool DoS
- Attack Web App Client
- Attack Web Services
- Web Services Probing Attacks
 - Web Service Attacks: SOAP Injection
 - Web Service Attacks: XML Injection
 - Web Services Parsing Attacks
- Web Service Attack Tool: soapUI
- Web Service Attack Tool: XMLSpy
- Web Application Hacking Tool: Burp Suite Professional
- Web Application Hacking Tools: CookieDigger
- Web Application Hacking Tools: WebScarab
 - Web Application Hacking Tools
- Encoding Schemes
 - How to Defend Against SQL Injection Attacks?
 - How to Defend Against Command Injection Flaws?
 - How to Defend Against XSS Attacks?
 - How to Defend Against DoS Attack?
 - How to Defend Against Web Services Attack?
- Web Application Countermeasures
 - How to Defend Against Web Application Attacks?
 - Web Application Security Tool: Acunetix Web Vulnerability Scanner
 - Web Application Security Tool: Falcove Web Vulnerability Scanner
 - Web Application Security Scanner: Netsparker
 - Web Application Security Tool: N-Stalker Web Application Security Scanner
 - Web Application Security Tools
- Web Application Firewall: dotDefender

- Web Application Firewall: IBM AppScan
- Web Application Firewall: ServerDefender VP
 - Web Application Firewall
- Web Application Pen Testing
 - Information Gathering
 - Configuration Management Testing
 - Authentication Testing
 - Session Management Testing
 - Authorization Testing
 - Data Validation Testing
 - Denial of Service Testing
 - Web Services Testing
 - AJAX Testing

08) Vulnerability Analysis and Penetration Testing (VAPT)

Vulnerability Testing

Vulnerability Testing also called Vulnerability Assessment is a process of evaluating security risks in software systems to reduce the probability of threats. The purpose of vulnerability testing is reducing the possibility for intruders/hackers to get unauthorized access of systems. It depends on the mechanism named Vulnerability Assessment and Penetration Testing (VAPT) or VAPT testing.

A vulnerability is any mistake or weakness in the system's security procedures, design, implementation or any internal control that may result in the violation of the system's security policy.

- What is Vulnerability Assessment
- Why do Vulnerability Assessment
- Vulnerability Assessment and Penetration Testing (VAPT) Process
- How to do Vulnerability Testing
- Types of vulnerability scanner
- Tools for Vulnerability Scanning
- Advantages of Vulnerability Assessment
- Disadvantages of Vulnerability Assessment
- Comparison of Vulnerability Assessment and Penetration Testing
- Vulnerability Testing Methods

Why do Vulnerability Assessment



It is important for the security of the organization.

- The process of locating and reporting the vulnerabilities, which provide a way to detect and resolve security problems by ranking the vulnerabilities before someone or something can exploit them.
- In this process Operating systems, Application Software and Network are scanned in order to identify the occurrence of vulnerabilities, which include inappropriate software design, insecure authentication, etc.

Vulnerability Assessment Process

Here is the step-by-step **Vulnerability Assessment Process** to identify the system vulnerabilities.



Step 1) Goals & Objectives: – Define goals and objectives of Vulnerability Analysis.

Step 2) Scope: – While performing the Assessment and Test, Scope of the Assignment needs to be clearly defined.

The following are the three possible scopes that exist:

- **Black Box Testing:** – Testing from an external network with no prior knowledge of the internal network and systems.
- **Grey Box Testing:** – Testing from either external or internal networks with the knowledge of the internal network and system. It's the combination of both Black Box Testing and White Box Testing.
- **White Box Testing:** – Testing within the internal network with the knowledge of the internal network and system. Also known as Internal Testing.

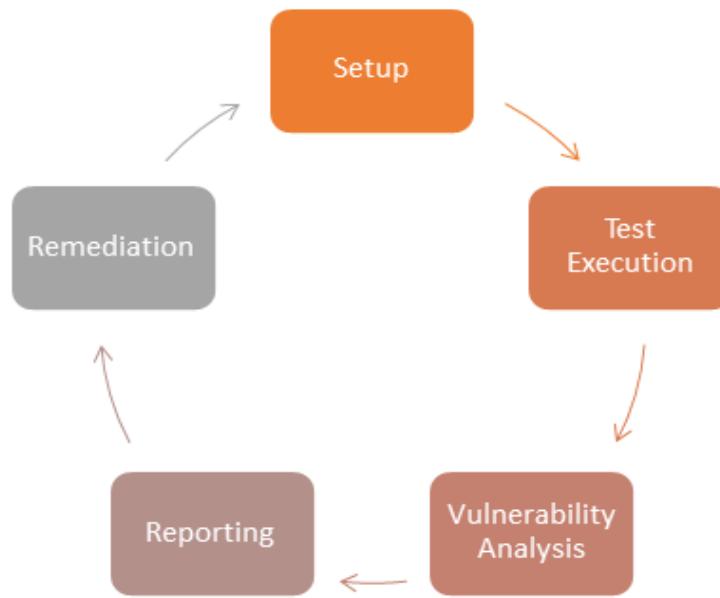
Step 3) Information Gathering: – Obtaining as much information about IT environment such as Networks, IP Address, Operating System Version, etc. It's applicable to all the three types of Scopes such as Black Box Testing, Grey Box Testing and White Box Testing.

Step 4) Vulnerability Detection: – In this process, vulnerability scanners are used to scan the IT environment and identify the vulnerabilities.

Step 5) Information Analysis and Planning: – It will analyze the identified vulnerabilities to devise a plan for penetrating into the network and systems.

How to do Vulnerability Assessment

Following is the step-by-step process on **How to do Vulnerability Assessment**:



Step 1) Setup:

- Begin Documentation
- Secure Permissions
- Update Tools
- Configure Tools

Step 2) Test Execution:

- Run the Tools
- Run the captured data packet (A packet is the unit of data that is routed between an origin and the destination. When any file, for example, e-mail message, HTML file, Uniform Resource Locator (URL) request, etc. is sent from one place to another on the internet, the TCP layer of TCP/IP divides the file into a number of “chunks” for efficient routing, and each of these chunks will be uniquely numbered and will include the Internet address of the destination. These chunks are called packets. When all the packets are arrived, they will be reassembled into the original file by the TCP layer at the receiving end while running the assessment tools)

Step 3) Vulnerability Analysis:

- Defining and classifying network or System resources.
- Assigning priority to the resources (Ex: – High, Medium, Low)
- Identifying potential threats to each resource.
- Developing a strategy to deal with the most prioritized problems first.
- Defining and implementing ways to minimize the consequences if an attack occurs.

Step 4) Reporting

Step 5) Remediation:

- The process of fixing the vulnerabilities.
- Performed for every vulnerability

Types of a vulnerability scanner

1. Host Based

- Identifies the issues in the host or the system.
- The process is carried out by using host-based scanners and diagnose the vulnerabilities.
- The host-based tools will load a mediator software onto the target system; it will trace the event and report it to the security analyst.

2. Network-Based

- It will detect the open port, and identify the unknown services running on these ports. Then it will disclose possible vulnerabilities associated with these services.
- This process is done by using Network-based Scanners.

3. Database-Based

- It will identify the security exposure in the database systems using tools and techniques to prevent from SQL Injections. (SQL Injections: – Injecting SQL statements into the database by the malicious users, which can read the sensitive data from a database and can update the data in the Database.)

Tools for Vulnerability Scanning

1) Acunetix



Intuitive and easy to use, [Acunetix](#) by Invicti helps small to medium-sized organizations ensure their web applications are secure from costly data breaches. It does so by detecting a wide range

of web security issues and helping security and development professionals act fast to resolve them.

Features:

- Advanced scanning for 7,000+ web vulnerabilities, including OWASP Top 10 such as SQLi and XSS
- Automated web asset discovery for identifying abandoned or forgotten websites
- Advanced crawler for the most complex web applications, incl. multi-form and password-protected areas
- Combined interactive and dynamic application security testing to discover vulnerabilities other tools miss
- Proof of exploit provided for many types of vulnerabilities
- DevOps automation through integrations with popular issue tracking and CI/CD tools
- Compliance reporting for regulatory standards, such as PCI DSS, NIST, HIPAA, ISO 27001, and more.

[More Information >>](#)

2) Intruder



Intruder is a powerful online vulnerability scanner that discovers security weaknesses across your IT environment. Offering industry-leading security checks, continuous monitoring and an easy-to-use platform, Intruder keeps businesses of all sizes safe from hackers.

Features:

- Best-in-class threat coverage with over 10,000 security checks
- Checks for configuration weaknesses, missing patches, application weaknesses (such as SQL injection & cross-site scripting) and more
- Automatic analysis and prioritization of scan results
- Intuitive interface, quick to set-up and run your first scans
- Proactive security monitoring for the latest vulnerabilities
- AWS, Azure and Google Cloud connectors
- API integration with your CI/CD pipeline

Category	Tool	Description
Host Based	STAT	Scan multiple systems in the network.

	TARA	Tiger Analytical Research Assistant.
	Cain & Abel	Recover password by sniffing network, cracking HTTP password.
	Metasploit	Open-source platform for developing, testing and exploit code.
Network-Based	Cisco Secure Scanner	Diagnose and Repair Security Problems.
	Wireshark	Open-Source Network Protocol Analyzer for Linux and Windows.
	Nmap	Free Open-Source utility for security auditing.
	Nessus	Agentless auditing, Reporting and patch management integration.
Database-Based	SQL diet	Dictionary Attack tool door for SQL server.
	Secure Auditor	Enable user to perform enumeration, scanning, auditing, and penetration testing and forensic on OS.
	DB-scan	Detection of Trojan of a database, detecting hidden Trojan by baseline scanning.

Advantages of Vulnerability Assessment

- Open-Source tools are available.
- Identifies almost all vulnerabilities
- Automated for Scanning.
- Easy to run on a regular basis.

Disadvantages of Vulnerability Assessment

- High false positive rate
- Can easily detect by Intrusion Detection System Firewall.
- Often fail to notice the latest vulnerabilities.

Comparison of Vulnerability Assessment and Penetration Testing

	Vulnerability Assessment	Penetration Testing
Working Mechanism	Discover Vulnerabilities	Identify and Exploit Vulnerabilities
Focus	Discovery & Scanning	Simulation
Coverage of Completeness	Breadth over Depth	Depth over Breadth
Cost	High	Low
Performed By	Low- Moderate	High
Tester Knowledge	In-house Staff	An attacker or Pen Tester
How often to Run	High	Low
Result	After each equipment is loaded	Once in a year
	Provide Partial Details about Vulnerabilities	Provide Complete Details of Vulnerabilities

Vulnerability Testing Methods

Active Testing

- Inactive Testing, a tester introduces new test data and analyzes the results.
- During the testing process, the testers create a mental model of the process, and it will grow further during the interaction with the software under test.
- While doing the test, the tester will actively involve in the process of finding out the new test cases and new ideas. That's why it is called Active Testing.

Passive Testing

- Passive testing, monitoring the result of running software under test without introducing new test cases or data

Network Testing

- Network Testing is the process of measuring and recording the current state of network operation over a period of time.
- Testing is mainly done for predicting the network operating under load or to find out the problems created by new services.
- We need to Test the following Network Characteristics: -
 - Utilization levels
 - Number of Users
 - Application Utilization

Distributed Testing

- Distributed Tests are applied for testing distributed applications, which means, the applications that are working with multiple clients simultaneously. Basically, testing a distributed application means testing its client and server parts separately, but by using a distributed testing method, we can test them all together.
- The test parts will interact with each other during the Test Run. This makes them synchronized in an appropriate manner. Synchronization is one of the most crucial points in distributed testing.

ARP poisoning

- What is IP & Mac Address
- What is Address Resolution Protocol (ARP) Poisoning?
- Hacking Activity: Configure Static ARP in Windows

What is IP and MAC Addresses

IP Address is the acronym for Internet Protocol address. An internet protocol address is used to uniquely identify a computer or device such as printers, storage disks on a computer network. There are currently two versions of IP addresses. IPv4 uses 32-bit numbers. Due to the massive growth of the internet, IPv6 has been developed, and it uses 128-bit numbers.

IPv4 addresses are formatted in four groups of numbers separated by dots. The minimum number is 0, and the maximum number is 255. An example of an IPv4 address looks like this;

127.0.0.1

IPv6 addresses are formatted in groups of six numbers separated by full colons. The group numbers are written as 4 hexadecimal digits. An example of an IPv6 address looks like this;

2001:0db8:85a3:0000:0000:8a2e:0370:7334

In order to simplify the representation of the IP addresses in text format, leading zeros are omitted, and the group of zeros is completely omitted. The above address in a simplified format is displayed as;

2001:db8:85a3::8a2e:370:7334

MAC Address is the acronym for media access control address. MAC addresses are used to uniquely identify network interfaces for communication at the physical layer of the network. MAC addresses are usually embedded into the network card.

A MAC address is like a serial number of a phone while the IP address is like the phone number.

Exercise

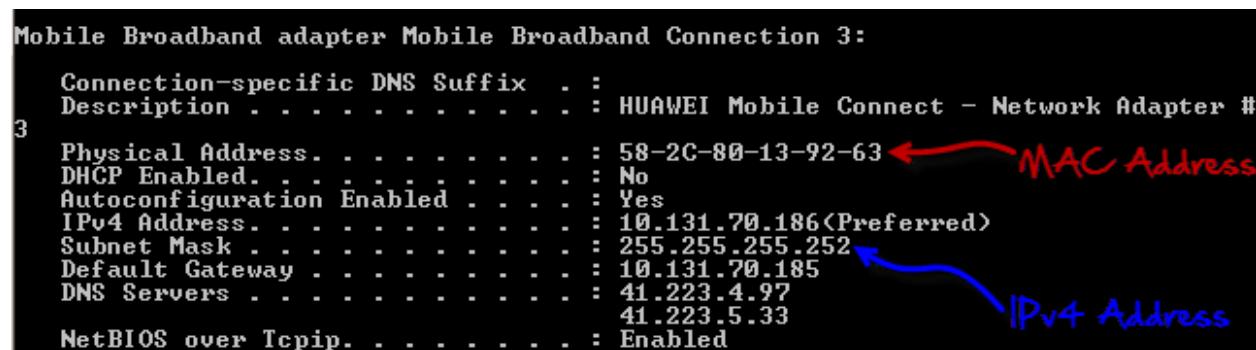
We will assume you are using windows for this exercise. Open the command prompt.

Enter the command

ipconfig /all

You will get detailed information about all the network connections available on your computer. The results shown below are for a broadband modem to show the MAC address and IPv4 format and wireless network to show IPv6 format.

```
Mobile Broadband adapter Mobile Broadband Connection 3:
  Connection-specific DNS Suffix . . . . . : 
  Description . . . . . : HUAWEI Mobile Connect - Network Adapter #3
  Physical Address. . . . . : 58-2C-80-13-92-63 ← MAC Address
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  IPv4 Address. . . . . : 10.131.70.186<Preferred>
  Subnet Mask . . . . . : 255.255.255.252 ←
  Default Gateway . . . . . : 10.131.70.185
  DNS Servers . . . . . : 41.223.4.97
                                         41.223.5.33
  NetBIOS over Tcpip. . . . . : Enabled
```



Ultimate guide to network sniffer



What is ARP Poisoning?

ARP is the acronym for Address Resolution Protocol. It is used to convert IP address to physical addresses [MAC address] on a switch. The host sends an ARP broadcast on the network, and the recipient computer responds with its physical address [MAC Address]. The resolved IP/MAC address is then used to communicate. **ARP poisoning is sending fake MAC addresses to the switch so that it can associate the fake MAC addresses with the IP address of a genuine computer on a network and hijack the traffic.**

ARP Poisoning Countermeasures

Static ARP entries: these can be defined in the local ARP cache and the switch configured to ignore all auto ARP reply packets. The disadvantage of this method is, it's difficult to maintain on large networks. IP/MAC address mapping has to be distributed to all the computers on the network.

ARP poisoning detection software: these systems can be used to cross check the IP/MAC address resolution and certify them if they are authenticated. Uncertified IP/MAC address resolutions can then be blocked.

Operating System Security: this measure is dependent on the operating system been used. The following are the basic techniques used by various operating systems.

- **Linux based:** these work by ignoring unsolicited ARP reply packets.
- **Microsoft Windows:** the ARP cache behavior can be configured via the registry. The following list includes some of the software that can be used to protect networks against sniffing;
 - **AntiARP**—provides protection against both passive and active sniffing
 - **Agnitum Outpost Firewall**—provides protection against passive sniffing
 - **XArp**—provides protection against both passive and active sniffing
- **Mac OS:** ArpGuard can be used to provide protection. It protects against both active and passive sniffing.

Hacking Activity: Configure ARP entries in Windows

We are using Windows 7 for this exercise, but the commands should be able to work on other versions of windows as well.

Open the command prompt and enter the following command

arp -a

HERE,

- **aprcalls** the ARP configure program located in Windows/System32 directory



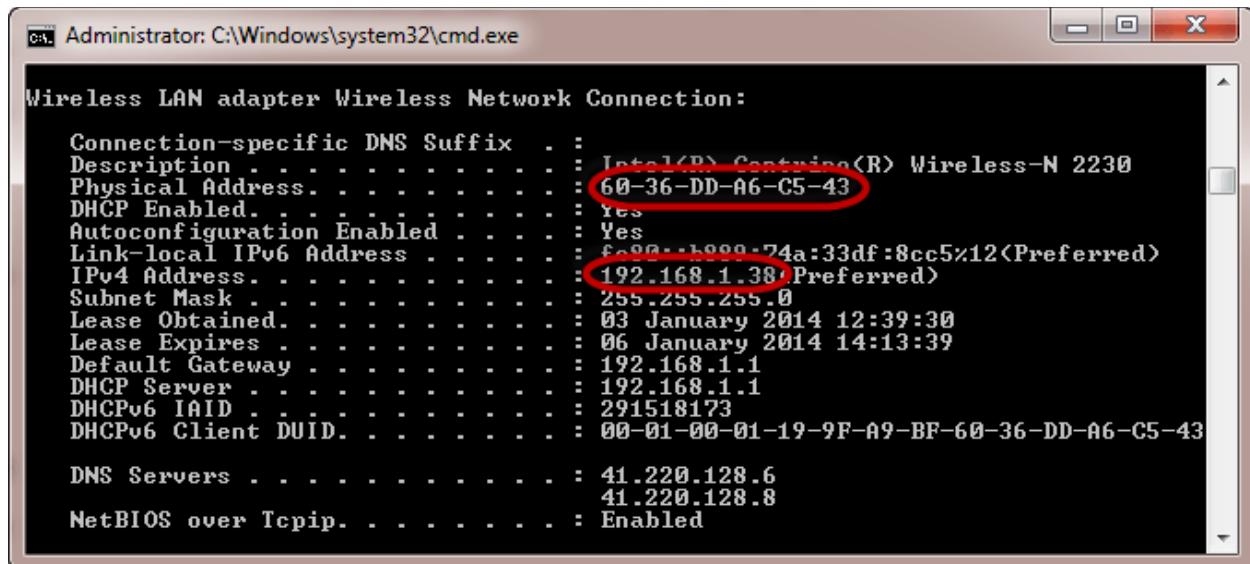
- **-a** is the parameter to display the contents of the ARP cache

Note: dynamic entries are added and deleted automatically when using TCP/IP sessions with remote computers.

Static entries are added manually and are deleted when the computer is restarted, and the network interface card restarted or other activities that affect it.

Adding static entries

Open the command prompt then use the ipconfig /all command to get the IP and MAC address

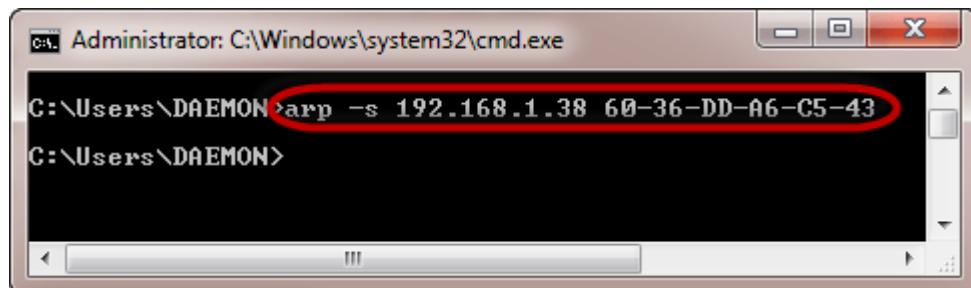


```
Administrator: C:\Windows\system32\cmd.exe
Wireless LAN adapter Wireless Network Connection:
  Connection-specific DNS Suffix . : Intel(R) Centrino(R) Wireless-N 2230
  Description . . . . . : Intel(R) Centrino(R) Wireless-N 2230
  Physical Address. . . . . : 60-36-DD-A6-C5-43
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::b999:74a3%3 (Preferred)
  IPv4 Address. . . . . : 192.168.1.38 (Preferred)
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained. . . . . : 03 January 2014 12:39:30
  Lease Expires . . . . . : 06 January 2014 14:13:39
  Default Gateway . . . . . : 192.168.1.1
  DHCP Server . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . : 291518173
  DHCPv6 Client DUID. . . . . : 00-01-00-01-19-9F-A9-BF-60-36-DD-A6-C5-43
  DNS Servers . . . . . : 41.220.128.6
                           41.220.128.8
  NetBIOS over Tcpip. . . . . : Enabled
```

The MAC address is represented using the Physical Address and the IP address is IPv4Address

Enter the following command

arp -s 192.168.1.38 60-36-DD-A6-C5-43



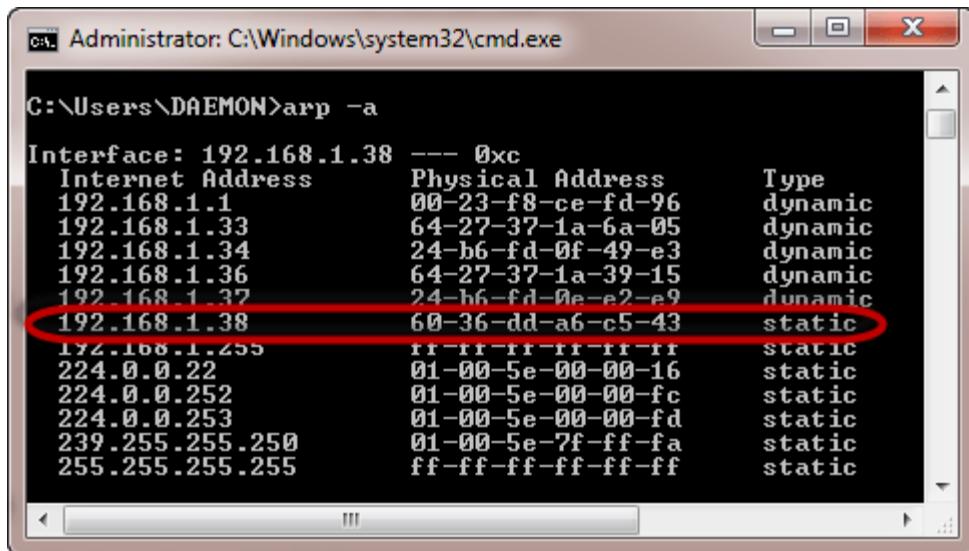
```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\DAEMON>arp -s 192.168.1.38 60-36-DD-A6-C5-43
C:\Users\DAEMON>
```

Note: The IP and MAC address will be different from the ones used here. This is because they are unique.

Use the following command to view the ARP cache

```
arp -a
```

You will get the following results



```
C:\Users\DAEMON>arp -a

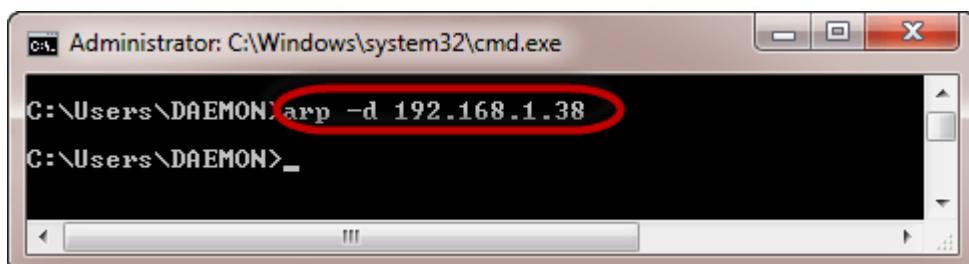
Interface: 192.168.1.38 --- 0xc
  Internet Address      Physical Address      Type
  192.168.1.1           00-23-f8-ce-fd-96    dynamic
  192.168.1.33          64-27-37-1a-6a-05    dynamic
  192.168.1.34          24-b6-fd-0f-49-e3    dynamic
  192.168.1.36          64-27-37-1a-39-15    dynamic
  192.168.1.37          24-b6-fd-0e-e2-e9    dynamic
  192.168.1.38          60-36-dd-a6-c5-43    static
  192.168.1.255         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
  224.0.0.253            01-00-5e-00-00-fd    static
  239.255.255.250        01-00-5e-7f-ff-fa    static
  255.255.255.255        ff-ff-ff-ff-ff-ff    static
```

Note the IP address has been resolved to the MAC address we provided and it is of a static type.

Deleting an ARP cache entry

Use the following command to remove an entry

```
arp -d 192.168.1.38
```



```
C:\Users\DAEMON>arp -d 192.168.1.38
C:\Users\DAEMON>
```

P.S. ARP poisoning works by sending fake MAC addresses to the switch

Conclusion

In Software Engineering, Vulnerability Testing depends upon two mechanisms namely Vulnerability Assessment and Penetration Testing. Both these tests differ from each other in



strength and tasks that they perform. However, to achieve a comprehensive report on Vulnerability Testing, the combination of both procedures is recommended.

Penetration Testing

Penetration Testing - Introduction

What is Penetration Testing?

Penetration testing is a type of security testing that is used to test the insecurity of an application. It is conducted to find the security risk which might be present in the system.

If a system is not secured, then any attacker can disrupt or take authorized access to that system. Security risk is normally an accidental error that occurs while developing and implementing the software. For example, configuration errors, design errors, and software bugs, etc.

Why is Penetration Testing Required?

Penetration testing normally evaluates a system's ability to protect its networks, applications, endpoints and users from external or internal threats. It also attempts to protect the security controls and ensures only authorized access.

Penetration testing is essential because –

- It identifies a simulation environment i.e., how an intruder may attack the system through **white hat attack**.
- It helps to find weak areas where an intruder can attack to gain access to the computer's features and data.
- It supports to avoid **black hat attack** and protects the original data.
- It estimates the magnitude of the attack on potential business.
- It provides evidence to suggest, why it is important to increase investments in security aspect of technology

When to Perform Penetration Testing?

Penetration testing is an essential feature that needs to be performed regularly for securing the functioning of a system. In addition to this, it should be performed whenever –

- Security system discovers new threats by attackers.
- You add a new network infrastructure.
- You update your system or install new software.
- You relocate your office.
- You set up a new end-user program/policy.



How is Penetration Testing Beneficial?

Penetration testing offers the following benefits –

- **Enhancement of the Management System** – It provides detailed information about the security threats. In addition to this, it also categorizes the degree of vulnerabilities and suggests you, which one is more vulnerable and which one is less. So, you can easily and accurately manage your security system by allocating the security resources accordingly.
- **Avoid Fines** – Penetration testing keeps your organization's major activities updated and complies with the auditing system. So, penetration testing protects you from giving fines.
- **Protection from Financial Damage** – A simple breach of security system may cause millions of dollars of damage. Penetration testing can protect your organization from such damages.
- **Customer Protection** – Breach of even a single customer's data may cause big financial damage as well as reputation damage. It protects the organizations who deal with the customers and keep their data intact.

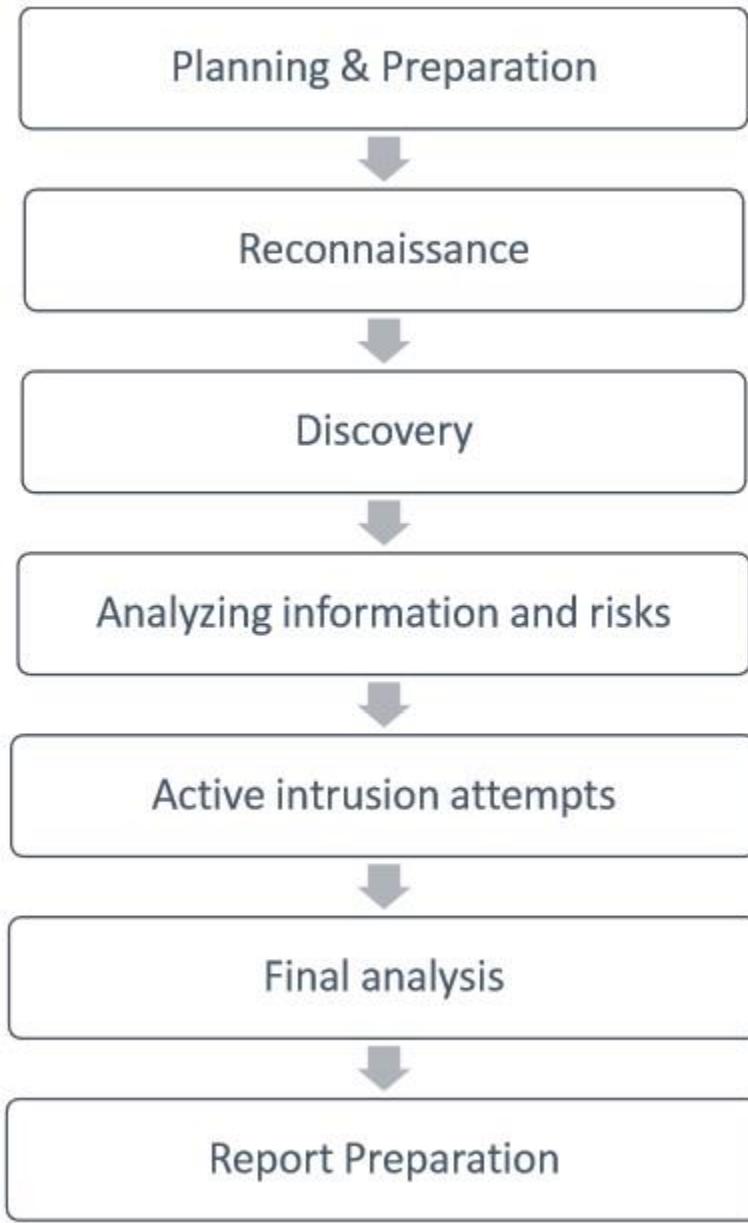
Penetration Testing - Method

Penetration testing is a combination of techniques that considers various issues of the systems and tests, analyzes, and gives solutions. It is based on a structured procedure that performs penetration testing step-by-step.

This chapter describes various steps or phases of penetration testing method.

Steps of Penetration Testing Method

The following are the seven steps of penetration testing –



Planning & Preparation

Planning and preparation starts with defining the goals and objectives of the penetration testing.

The client and the tester jointly define the goals so that both the parties have the same objectives and understanding. The common objectives of penetration testing are –

- To identify the vulnerability and improve the security of the technical systems.
- Have IT security confirmed by an external third party.
- Increase the security of the organizational/personnel infrastructure.

Reconnaissance

Reconnaissance includes an analysis of the preliminary information. Many times, a tester doesn't have much information other than the preliminary information, i.e., an IP address or IP address block. The tester starts by analyzing the available information and, if required, requests for more information such as system descriptions, network plans, etc. from the client. This step is the passive penetration test, a sort of. The sole objective is to obtain a complete and detailed information of the systems.

Discovery

In this step, a penetration tester will most likely use the automated tools to scan target assets for discovering vulnerabilities. These tools normally have their own databases giving the details of the latest vulnerabilities. However, tester discover

- **Network Discovery** – Such as discovery of additional systems, servers, and other devices.
- **Host Discovery** – It determines open ports on these devices.
- **Service Interrogation** – It interrogates ports to discover actual services which are running on them.

Analyzing Information and Risks

In this step, tester analyzes and assesses the information gathered before the test steps for dynamically penetrating the system. Because of larger number of systems and size of infrastructure, it is extremely time consuming. While analyzing, the tester considers the following elements –

- The defined goals of the penetration test.
- The potential risks to the system.
- The estimated time required for evaluating potential security flaws for the subsequent active penetration testing.

However, from the list of identified systems, the tester may choose to test only those which contain potential vulnerabilities.

Active Intrusion Attempts

This is the most important step that has to be performed with due care. This step entails the extent to which the potential vulnerabilities that was identified in the discovery step which possess the actual risks. This step must be performed when a verification of potential vulnerabilities is needed. For those systems having very high integrity requirements, the potential vulnerability and risk needs to be carefully considered before conducting critical clean up procedures.

Final Analysis

This step primarily considers all the steps conducted (discussed above) till that time and an evaluation of the vulnerabilities present in the form of potential risks. Further, the tester recommends to eliminate the vulnerabilities and risks. Above all, the tester must assure the transparency of the tests and the vulnerabilities that it disclosed.

Report Preparation

Report preparation must start with overall testing procedures, followed by an analysis of vulnerabilities and risks. The high risks and critical vulnerabilities must have priorities and then followed by the lower order.

However, while documenting the final report, the following points needs to be considered –

- Overall summary of penetration testing.
- Details of each step and the information gathered during the pen testing.
- Details of all the vulnerabilities and risks discovered.
- Details of cleaning and fixing the systems.
- Suggestions for future security.

Penetration Testing Vs. Vulnerability

Generally, these two terms, i.e., Penetration Testing and Vulnerability assessment are used interchangeably by many people, either because of misunderstanding or marketing hype. But, both the terms are different from each other in terms of their objectives and other means. However, before describing the differences, let us first understand both the terms one-by one.

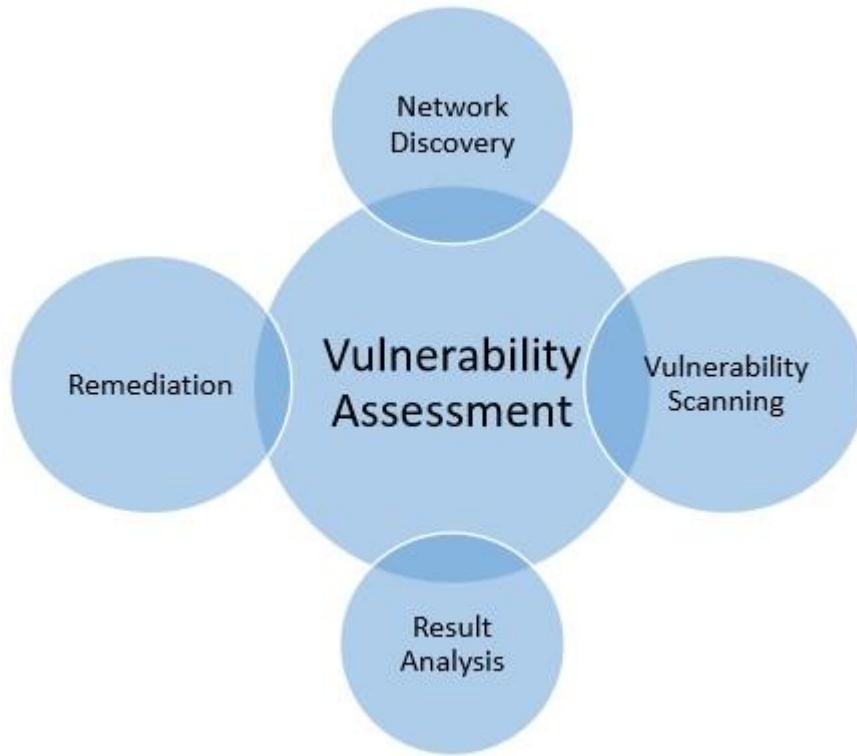
Penetration Testing

Penetration testing replicates the actions of an external or/and internal cyber attacker/s that is intended to break the information security and hack the valuable data or disrupt the normal functioning of the organization. So, with the help of advanced tools and techniques, a penetration tester (also known as **ethical hacker**) makes an effort to control critical systems and acquire access to sensitive data.

Vulnerability Assessment

On the other hand, a vulnerability assessment is the technique of identifying (discovery) and measuring security vulnerabilities (scanning) in a given environment. It is a comprehensive assessment of the information security position (result analysis). Further, it identifies the potential weaknesses and provides the proper mitigation measures (remediation) to either remove those weaknesses or reduce below the risk level.

The following diagram summarizes the vulnerability assessment –



The following table illustrates the fundamental differences between penetration testing and vulnerability assessments –

Penetration Testing	Vulnerability Assessments
Determines the scope of an attack.	Makes a directory of assets and resources in a given system.
Tests sensitive data collection.	Discovers the potential threats to each resource.
Gathers targeted information and/or inspect the system.	Allocates quantifiable value and significance to the available resources.
Cleans up the system and gives final report.	Attempts to mitigate or eliminate the potential vulnerabilities of valuable resources.
It is non-intrusive, documentation and environmental review and analysis.	Comprehensive analysis and through review of the target system and its environment.
It is ideal for physical environments and network architecture.	It is ideal for lab environments.
It is meant for critical real-time systems.	It is meant for non-critical systems.

Which Option is Ideal to Practice?

Both the methods have different functionality and approach, so it depends upon the security position of the respective system. However, because of the basic difference between penetration testing and vulnerability assessment, the second technique is more beneficial over the first one.

Vulnerability assessment identifies the weaknesses and gives solution to fix them. On the other hand, penetration testing only answers the question that "can anyone break-in the system security and if so, then what harm he can do?"

Further, a vulnerability assessment attempts to improve security system and develops a more mature, integrated security program. On the other hand, a penetration testing only gives a picture of your security program's effectiveness.

As we have seen here, the vulnerability assessment is more beneficial and gives better result in comparison to penetration testing. But experts suggest that, as a part of security management system, both techniques should be performed routinely to ensure a perfect secured environment.

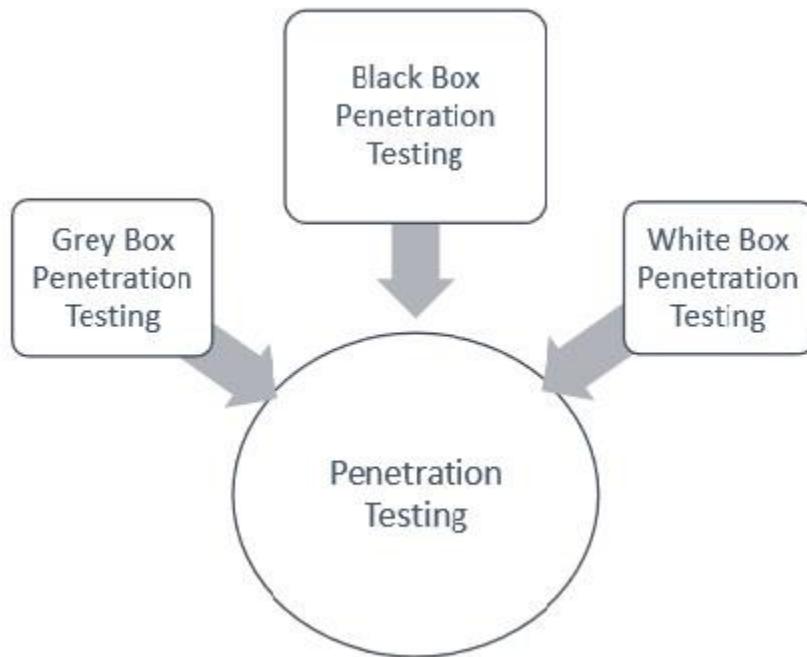
Types of Penetration Testing

The type of penetration testing normally depends on the scope and the organizational wants and requirements. This chapter discusses about different types of Penetration testing. It is also known as **Pen Testing**.

Types of Pen Testing

Following are the important types of pen testing –

- Black Box Penetration Testing
- White Box Penetration Testing
- Grey Box Penetration Testing



For better understanding, let us discuss each of them in detail –

Black Box Penetration Testing

In black box penetration testing, tester has no idea about the systems that he is going to test. He is interested to gather information about the target network or system. For example, in this testing, a tester only knows what should be the expected outcome and he does not know how the outcomes arrives. He does not examine any programming codes.

Advantages of Black Box Penetration Testing

It has the following advantages –

- Tester need not necessarily be an expert, as it does not demand specific language knowledge
- Tester verifies contradictions in the actual system and the specifications
- Test is generally conducted with the perspective of a user, not the designer

Disadvantages of Black Box Penetration Testing

Its disadvantages are –

- Particularly, these kinds of test cases are difficult to design.
- Possibly, it is not worth, incase designer has already conducted a test case.
- It does not conduct everything.

White Box Penetration Testing

This is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc. It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box, and open box testing.

White box penetration testing examines the code coverage and does data flow testing, path testing, loop testing, etc.

Advantages of White Box Penetration Testing

It carries the following advantages –

- It ensures that all independent paths of a module have been exercised.
- It ensures that all logical decisions have been verified along with their true and false value.
- It discovers the typographical errors and does syntax checking.
- It finds the design errors that may have occurred because of the difference between logical flow of the program and the actual execution.

Grey Box Penetration Testing

In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.

Advantages of Grey Box Penetration Testing

It has the following advantages –

- As the tester does not require the access of source code, it is non-intrusive and unbiased
- As there is clear difference between a developer and a tester, so there is least risk of personal conflict
- You don't need to provide the internal information about the program functions and other operations

Areas of Penetration Testing

Penetration testing is normally done in the following three areas –

- **Network Penetration Testing** – In this testing, the physical structure of a system needs to be tested to identify the vulnerability and risk which ensures the security in a network. In the networking environment, a tester identifies security flaws in design, implementation, or operation of the respective company/organization's network. The



devices, which are tested by a tester can be computers, modems, or even remote access devices, etc

- **Application Penetration Testing** – In this testing, the logical structure of the system needs to be tested. It is an attack simulation designed to expose the efficiency of an application's security controls by identifying vulnerability and risk. The firewall and other monitoring systems are used to protect the security system, but sometime, it needs focused testing especially when traffic is allowed to pass through the firewall.
- **The response or workflow of the system** – This is the third area that needs to be tested. Social engineering gathers information on human interaction to obtain information about an organization and its computers. It is beneficial to test the ability of the respective organization to prevent unauthorized access to its information systems. Likewise, this test is exclusively designed for the workflow of the organization/company.

Penetration Testing - Manual & Automated

Both manual penetration testing and automated penetration testing are conducted for the same purpose. The only difference between them is the way they are conducted. As the name suggests, manual penetration testing is done by human beings (experts of this field) and automated penetration testing is done by machine itself.

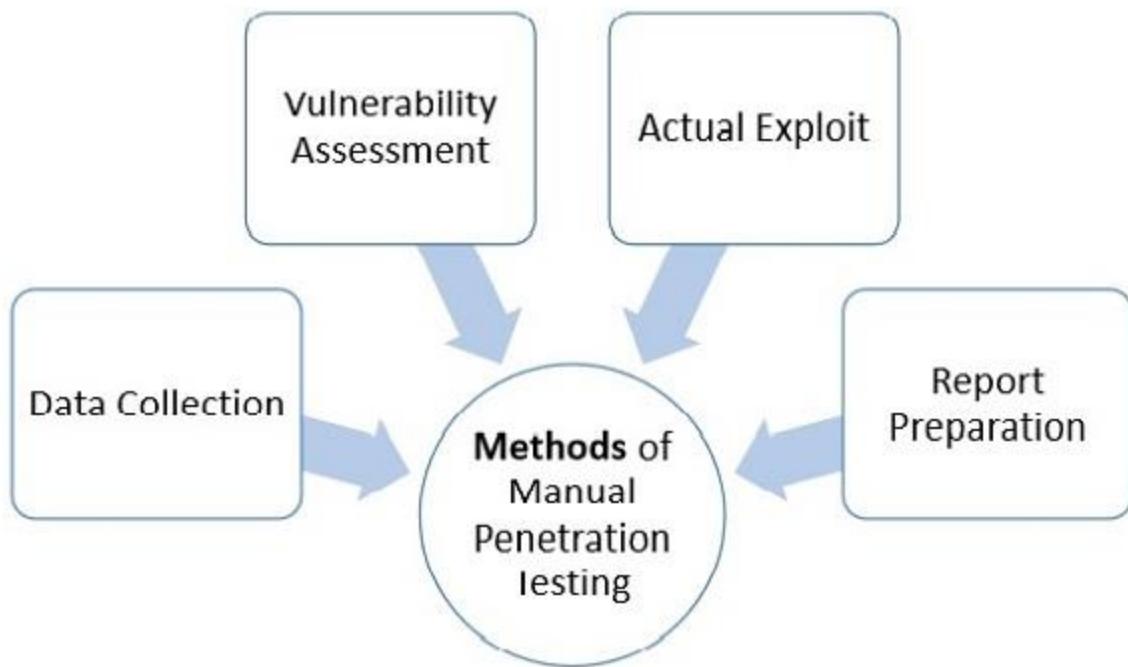
This chapter will help you learn the concept, differences, and applicability of both the terms.

What is Manual Penetration Testing?

Manual penetration testing is the testing that is done by human beings. In such type of testing, vulnerability and risk of a machine is tested by an expert engineer.

Generally, testing engineers perform the following methods –

- **Data Collection** – Data collection plays a key role for testing. One can either collect data manually or can use tool services (such as webpage source code analysis technique, etc.) freely available online. These tools help to collect information like table names, DB versions, database, software, hardware, or even about different third party plugins, etc
- **Vulnerability Assessment** – Once the data is collected, it helps the testers to identify the security weakness and take preventive steps accordingly.
- **Actual Exploit** – This is a typical method that an expert tester uses to launch an attack on a target system and likewise, reduces the risk of attack.
- **Report Preparation** – Once the penetration is done, the tester prepares a final report that describes everything about the system. Finally the report is analyzed to take corrective steps to protect the target system.



Types of Manual Penetration Testing

Manual penetration testing is normally categorized in two following ways –

- **Focused Manual Penetration Testing** – It is a much-focused method that tests specific vulnerabilities and risks. Automated penetration testing cannot perform this testing; it is done only by human experts who examine specific application vulnerabilities within the given domains.
- **Comprehensive Manual Penetration Testing** – It is through testing of whole systems connected with each other to identify all sorts of risk and vulnerability. However, the function of this testing is more situational, such as investigating whether multiple lower-risk faults can bring more vulnerable attack scenario, etc

What is Automated Penetration Testing?

Automated penetration testing is much faster, efficient, easy, and reliable that tests the vulnerability and risk of a machine automatically. This technology does not require any expert engineer, rather it can be run by any person having least knowledge of this field.

Tools for automated penetration testing are Nessus, Metasploit, OpenVAS, backtrack (series 5), etc. These are very efficient tools that changed the efficiency and meaning of penetration testing.

However, the following table illustrates the fundamental difference between the manual and automated penetration testing –

Manual Penetration Testing	Automated Penetration Testing
It requires expert engineer to perform the test.	It is automated so even a learner can run the test.
It requires different tools for the testing.	It has integrated tools does required anything from outside.
In this type of testing, results can vary from test to test.	It has fixed result.
This test requires to remember cleaning up memory by the tester.	It does not.
It is exhaustive and time taking.	It is more efficient and faster.
It has additional advantages i.e., if an expert does pen test, then he can analyze better, he can think what a hacker can think and where he can attack. Hence, he can put security accordingly.	It cannot analyze the situation.
As per the requirement, an expert can run multiple testing.	It cannot.
For critical condition, it is more reliable.	It is not.

Penetration Testing - Tools

Penetration testing, normally consists of information gathering, vulnerability and risk analysis, vulnerability exploits, and final report preparation.

It is also essential to learn the features of various of tools which are available with penetration testing. This chapter provides information and insights about these features.

What are Penetration Testing Tools?

The following table collects some of the most significant penetration tools and illustrates their features –

Tool Name	Purpose	Portability	Expected Cost
Hping	Port Scanning Remote OS fingerprinting	Linux, NetBSD, FreeBSD, OpenBSD,	Free
Nmap	Network Scanning Port Scanning OS Detection	Linux, Windows, FreeBSD, OS X, HP-UX, NetBSD, Sun, OpenBSD, Solaris, IRIX, Mac, etc.	Free

SuperScan	Runs queries including ping, whois, hostname lookups, etc. Detects open UDP/TCP ports and determines which services are running on those ports.	Windows 2000/XP/Vista/7	Free
p0f	Os fingerprinting Firewall detection	Linux, FreeBSD, NetBSD, OpenBSD, Mac OS X, Solaris, Windows, and AIX	Free
Xprobe	Remote active OS fingerprinting Port Scanning TCP fingerprinting	Linux	Free
Httprint	Web server fingerprinting SSL detection Detect web enabled devices (e.g., wireless access points, switches, modems, routers)	Linux, Mac OS X, FreeBSD, Win32 (command line & GUI)	Free
Nessus	Detect vulnerabilities that allow remote cracker to control/access sensitive data	Mac OS X, Linux, FreeBSD, Apple, Oracle Solaris, Windows	Free to limited edition
GFI LANguard	Detect network vulnerabilities	Windows Server 2003/2008, Windows 7 Ultimate/ Vista, Windows 2000 Professional, Business/XP, Sever 2000/2003/2008	Only Trial Version Free
Iss Scanner	Detect network vulnerabilities	Windows 2000 Professional with SP4, Windows Server 2003 Standard with SO1, Windows XP Professional with SP1a	Only Trial Version Free
Shadow Security Scanner	Detect network vulnerabilities, audit proxy and LDAP servers	Windows but scan servers built on any platform	Only Trial Version Free
Metasploit Framework	Develop and execute exploit code against a remote target Test vulnerability of computer systems	All versions of Unix and Windows	Free

Brutus	Telnet, ftp, and http password cracker	Windows 9x/NT/2000	Free
--------	--	--------------------	------

Penetration Testing - Infrastructure

Computer systems and associated networks normally consist of a large number of devices and most of them play a major role in conducting total works and businesses of the respective system. A minor flaw at any point of time, and at any part of these devices may cause great damage to your business. Therefore, all of them are vulnerable to risk and need to be secured properly.

What is Infrastructure Penetration Testing?

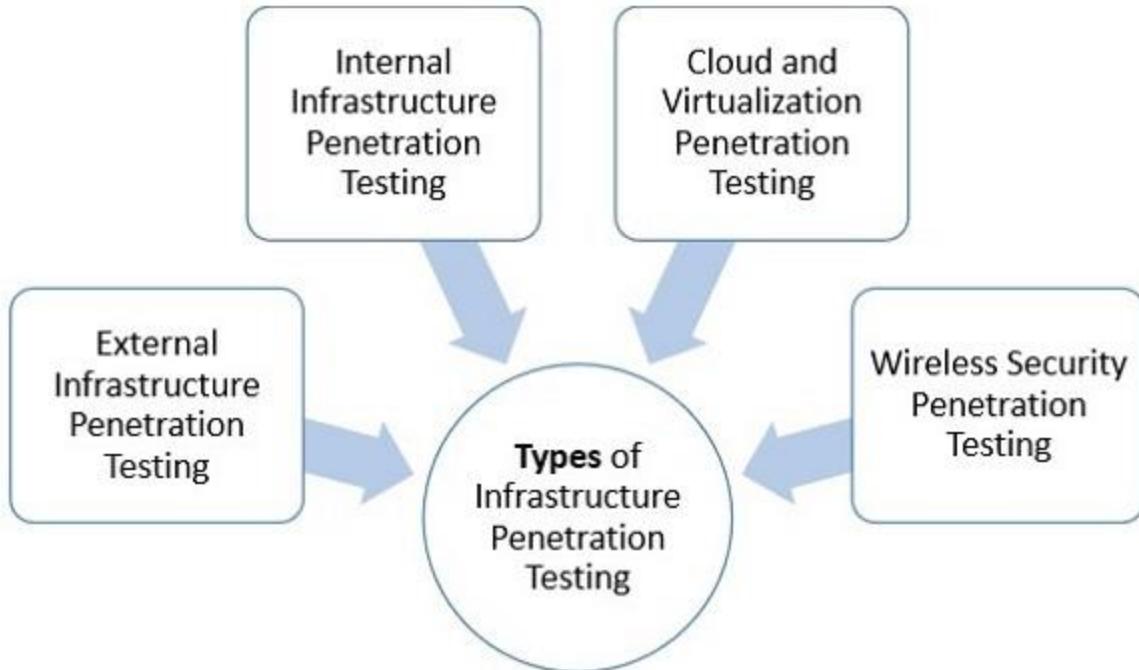
Infrastructure penetration testing includes all internal computer systems, associated external devices, internet networking, cloud and virtualization testing.

Whether hidden on your internal enterprise network or from public view, there is always a possibility that an attacker can leverage which can harm your infrastructure. So, it is better to be safe in advance rather than regret later.

Types of Infrastructure Penetration Testing

Following are the important types of infrastructure penetration testing –

- External Infrastructure Penetration Testing
- Internal Infrastructure Penetration Testing
- Cloud and Virtualization Penetration Testing
- Wireless Security Penetration Testing



External Infrastructure Testing

The penetration test, targeting the external infrastructure discovers what a hacker could do with your networks, which is easily accessible through the Internet.

In this testing, a tester normally replicates the same kind of attacks that the hackers can use by finding and mapping the security flaws in your external infrastructure.

There are various benefits of leveraging external infrastructure penetration testing, as it –

- Identifies the flaws within the firewall configuration that could be misused
- Finds out how information can be leaked out from your system by an attacker
- Suggests how these issues can be fixed
- Prepares a comprehensive report highlighting the security risk of the border networks, and suggests solutions
- Ensures overall efficiency and productivity of your business

Internal Infrastructure Penetration Testing

Due to some minor internal security flaws, hackers are illegally committing frauds in large organizations. So, with internal infrastructure penetration testing, a tester can identify the possibility of a security and from which employee, this problem has occurred.

Internal infrastructure penetration testing benefits as it –

- Identifies how an internal attacker could take advantage of even a minor security flaw.
- Identifies the potential business risk and damage that an internal attacker can inflict.
- Improves the security systems of internal infrastructure.
- Prepares a comprehensive report giving details of the security exposures of internal networks along with the detailed action plan on how to deal with it.

Cloud and Virtualization Penetration Testing

As you buy a public server or wave space, it significantly increases the risks of data breach. Further, identifying the attacker on cloud environment is difficult. An attacker can also buy hosting a Cloud facility to get access to your new Cloud data.

In fact, most of the Cloud hosting is implemented on virtual infrastructure, causing Virtualization risk that an attacker can easily access.

Cloud and Virtualization penetration testing benefits as it –

- Discovers the real risks within the virtual environment and suggests the methods and costs to fix the threats and flaws.
- Provides guidelines and an action plan how to resolve the issue/s.
- Improves the overall protection system.
- Prepares a comprehensive security system report of the Cloud computing and Virtualization, outline the security flaw, causes and possible solutions.

Wireless Security Penetration Testing

Wireless technology of your laptop and other devices provides an easy and flexible access to various networks. The easily accessible technology is vulnerable to unique risks; as physical security cannot be used to limit network access. An attacker can hack from the remote location. Hence, wireless security penetration testing is necessary for your company/organization.

The following are the reasons for having wireless technology –

- To find the potential risk caused by your wireless devices.
- To provide guidelines and an action plan on how to protect from the external threats.
- To improve the overall security system.
- For preparing a comprehensive security system report of the wireless networking, to outline the security flaw, causes, and possible solutions.

Penetration Testing - Testers

There is the issue of protecting the most critical data of the organization; therefore, the role of a penetration tester is much critical, a minor error can put both the parties (tester and his client) on risk.

Therefore, this chapter discusses various aspects of a penetration tester including his qualification, experience, and responsibilities.

Qualification of Penetration Testers

This test can be performed only by a qualified penetration tester; therefore, qualification of a penetration tester is very important.

Either qualified internal expert or a qualified external expert may perform the penetration test until they are organizationally independent. It means that the penetration tester must be organizationally independent from the management of the target systems. For example, if a third-party company is involved in the installation, maintenance, or support of target systems, then that party cannot perform penetration testing.

Here are some guidelines that will help you while calling a penetration tester.

Certification

A certified person can perform penetration testing. Certification held by the tester is the indication of his skill sets and competence of capable penetration tester.

Following are the important examples of penetration testing certification –

- Certified Ethical Hacker (CEH).
- Offensive Security Certified Professional (OSCP).
- CREST Penetration Testing Certifications.
- Communication Electronic Security Group (CESG) IT Health Check Service certification.
- Global Information Assurance Certification (GIAC) Certifications for example, GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), Advance Penetration Tester (GXPN), and GIAC Exploit Researcher.

Past Experience

The following questions will help you to hire an effective penetration tester –

- How many years of experience does the penetration tester has?
- Is he an independent penetration tester or working for an organization?
- With how many companies he worked as penetration tester?
- Has he performed penetration testing for any organization, which has similar size and scope as yours?
- What type of experience does the penetration tester has? For example, conducting network-layer penetration testing etc
- You may also ask for the reference from other customers for whom he worked.

When hiring a penetration tester, it is important to evaluate the past year testing experience of the organization for which he (tester) has worked as it is related to the technologies specifically deployed by him within the target environment.

In addition to the above, for complex situations and typical client requirements, it is recommended to evaluate a tester's capability to handle similar environment in his/her earlier project.

Role of a Penetration Tester

A penetration tester has the following roles –

- Identify inefficient allocation of tools and technology.
- Testing across internal security systems.
- Pinpoint exposures to protect the most critical data.
- Discover invaluable knowledge of vulnerabilities and risks throughout the infrastructure.
- Reporting and prioritizing remediation recommendations to ensure that the security team is utilizing their time in the most effective way, while protecting the biggest security gaps.

Penetration Testing - Report Writing

It is not necessary that an experienced penetration tester can write a good report, as writing report of penetration testing is an art that needs to be learnt separately.

What is Report Writing?

In penetration testing, report writing is a comprehensive task that includes methodology, procedures, proper explanation of report content and design, detailed example of testing report, and tester's personal experience. Once the report is prepared, it is shared among the senior management staff and technical team of target organizations. If any such kind of need arises in future, this report is used as the reference.

Report Writing Stages

Due to the comprehensive writing work involved, penetration report writing is classified into the following stages –

- Report Planning
- Information Collection
- Writing the First Draft
- Review and Finalization



Report Planning

Report planning starts with the objectives, which help readers to understand the main points of the penetration testing. This part describes why the testing is conducted, what are the benefits of pen testing, etc. Secondly, report planning also includes the time taken for the testing.

Major elements of report writing are –

- **Objectives** – It describes the overall purpose and benefits of pen testing.
- **Time** – Inclusion of time is very important, as it gives the accurate status of the system. Suppose, if anything wrong happens later, this report will save the tester, as the report will illustrate the risks and vulnerabilities in the penetration testing scope during the specific period of time.
- **Target Audience** – Pen testing report also needs to include target audience, such as information security manager, information technology manager, chief information security officer, and technical team.
- **Report Classification** – Since, it is highly confidential which carry server IP addresses, application information, vulnerability, threats, it needs to be classified properly. However, this classification needs to be done on the basis of target organization which has an information classification policy.
- **Report Distribution** – Number of copies and report distribution should be mentioned in the scope of work. It also needs to mention that the hardcopies can be controlled by printing a limited number of copies attached with its number and the receiver's name.

Information Collection

Because of the complicated and lengthy processes, pen tester is required to mention every step to make sure that he collected all the information in all the stages of testing. Along with the

methods, he also needs to mention about the systems and tools, scanning results, vulnerability assessments, details of his findings, etc.

Writing the First Draft

Once, the tester is ready with all tools and information, now he needs to start the first draft. Primarily, he needs to write the first draft in the details – mentioning everything i.e. all activities, processes, and experiences.

Review and Finalization

Once the report is drafted, it has to be reviewed first by the drafter himself and then by his seniors or colleagues who may have assisted him. While reviewing, reviewer is expected to check every detail of the report and find any flaw that needs to be corrected.

Content of Penetration Testing Report

Following is the typical content of a penetration testing report –

Executive Summary

- *Scope of work*
- *Project objectives*
- *Assumption*
- *Timeline*
- *Summary of findings*
- *Summary of recommendation*

Methodology

- *Planning*
- *Exploitation*
- *Reporting*

Detail Findings

- *Detailed systems information*
- *Windows server information*

References

- *Appendix*

Penetration Testing - Ethical Hacking

The fast growth of the internet has changed the way of life for everyone. These days, most of the private and public works are internet dependent. Government's all secret working plans, and operations are internet based. All these things made the life very simple and easily accessible.

But with the good news, there is also a dark face of this development i.e., the criminal hacker. There is no geopolitical limitation of these criminal hackers, they can hack any system from any part of the world. They can damage confidential data and credit history very badly.

Therefore, to protect from the criminal hackers, the concept of the ethical hacker evolved. This chapter discusses the concept and the role of an ethical hacker.

Who are Ethical Hackers?

Ethical hackers are the computer experts who are legally allowed to hack a computer system with the objective to protect from the criminal hackers. An ethical hacker identifies the vulnerabilities and risks of a system and suggests how to eliminate them.

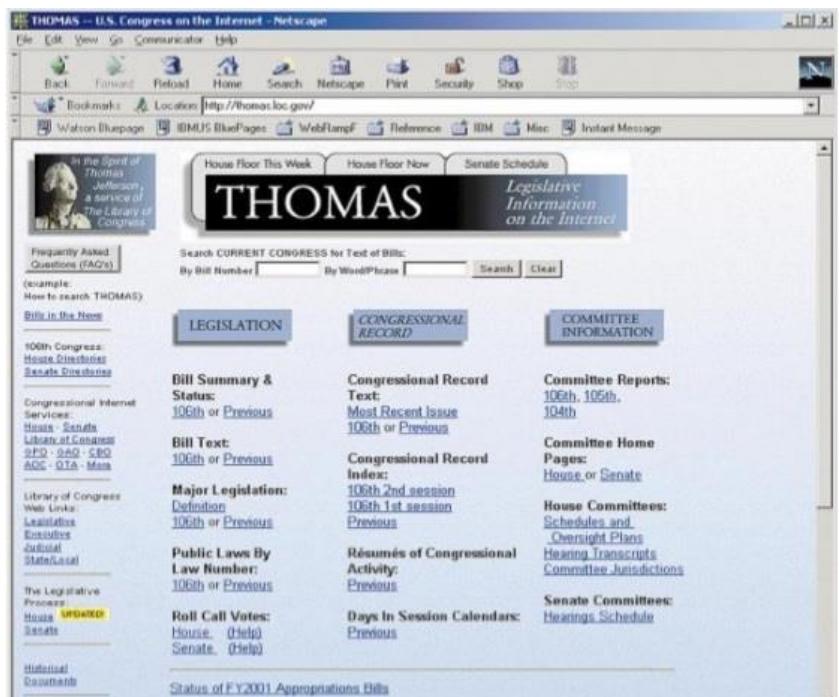
Who are Criminal Hackers?

Criminal hackers are those computer programming experts who hack others systems with the intention to steal data, steal money, defame others credit, destroy others data, blackmail someone, etc.

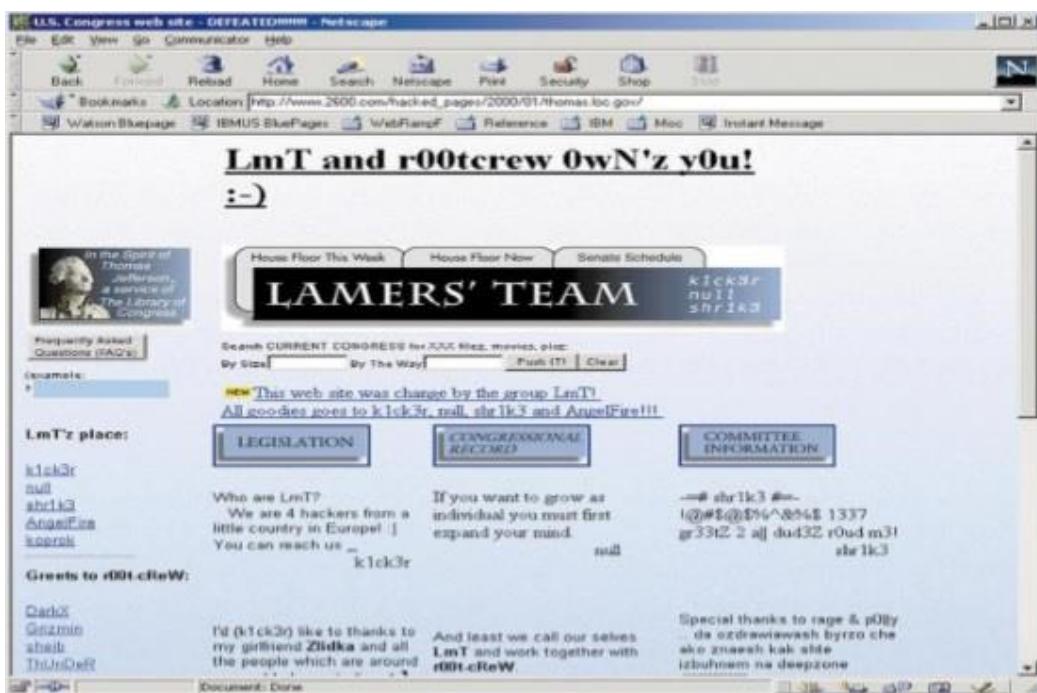
What can Criminal Hackers do?

Once a system is hacked, a criminal hacker can do anything with that system. The following two images C.C. Palmer, which is published on pdf.textfiles.com, illustrates a simple example of a hacked page –

Here is a screenshot of a webpage taken before it was hacked –



And, here is the screenshot of the same webpage after it was hacked –



What are the Skills-Set of Ethical Hackers?

Expert ethical hackers have the following skill-sets to hack the system ethically

- They must be trustworthy.
- Whatever the risks and vulnerabilities, they discover while testing the system, they have to keep them confidential.
- Clients provide confidential information about their system infrastructure such as IP address, password, etc. Ethical hackers need to keep this information confidential.
- Ethical hackers must have sound knowledge of computer programming, networking and hardware.
- They should have good analytical skills to analyze the situation and speculate the risk in advance.
- They should have the management skill along with patience, as pen testing can take one day, one week, or even more.

What do Ethical Hackers do?

Ethical hackers, while performing penetration testing, basically try to find the answers to the following questions –

- What are the weak points that a criminal hacker can hit?
- What can a criminal hacker see on the target systems?
- What can a criminal hacker do with that confidential information?

Moreover, an ethical hacker is required to address adequately the vulnerabilities and risks, which he found to exist in the target system(s). He needs to explain and suggest the avoidance procedures. Finally, prepare a final report of his all-ethical activities that he did and observed while performing penetration testing.

Types of Hackers

Hackers are normally divided into three categories.

Black Hat Hackers

A "black hat hacker" is an individual who has an extensive computer software as well as hardware and his purpose is to breach or bypass internet security of someone else. Black hat hackers are also popular as crackers or dark-side hackers.

White Hat Hackers

The term "white hat hacker" refers to an ethical computer hacker who is a computer security expert, specialized in penetration testing and in other associated testing methodologies. His primary role is to ensure the security of an organization's information system.

Grey Hat Hacker

The term "grey hat hacker" refers to a computer hacker who cracks computer security system whose ethical standards fall somewhere between purely ethical and solely malicious.

Penetration Testing Vs. Ethical Hacking

Penetration testing is very closely related to ethical hacking, so these two terms are often used interchangeably. However, there is a thin line of difference between these two terms. This chapter provides insights into some basic concepts and fundamental differences between penetration testing and ethical hacking.

Penetration Testing

Penetration testing is a specific term and focuses only on discovering the vulnerabilities, risks, and target environment with the purpose of securing and taking control of the system. Or in other words, penetration testing targets respective organization's defense systems consisting of all computer systems and its infrastructure.

Ethical Hacking

On the other hand, ethical hacking is an extensive term that covers all hacking techniques, and other associated computer attack techniques. So, along with discovering the security flaws and vulnerabilities, and ensuring the security of the target system, it is beyond hacking the system but with a permission in order to safeguard the security for future purpose. Hence, we can say that, it is an umbrella term and penetration testing is one of the features of ethical hacking.

The following are the major differences between Penetration testing and Ethical hacking which is listed in the following table –

Penetration Testing	Ethical Hacking
A narrow term focuses on penetration testing only to secure the security system.	A comprehensive term and penetration testing is one of its features.
A tester essentially does need to have a comprehensive knowledge of everything rather required to have the knowledge of only the specific area for which he conducts pen testing.	An ethical hacker essentially needs to have a comprehensive knowledge of software programming as well as hardware.
A tester not necessarily required to be a good report writer.	An ethical hacker essentially needs to be an expert on report writing.
Any tester with some inputs of penetration testing can perform pen test.	It requires to be an expert professional in the subject, who has the obligatory certification of ethical hacking to be effective.

Paper work in less compared to Ethical hacking.	A detailed paper works are required, including legal agreement etc.
To perform this type of testing, less time required.	Ethical hacking involves lot of time and effort compared to Penetration testing.
Normally, accessibility of whole computer systems and its infrastructure doesn't require. Accessibility is required only for the part for which the tester performing pen testing.	As per the situation, it normally requires a whole range of accessibility all computer systems and its infrastructure.

Since penetration techniques are used to protect from threats, the potential attackers are also swiftly becoming more and more sophisticated and inventing new weak points in the current applications. Hence, a particular sort of single penetration testing is not sufficient to protect your security of the tested systems.

As per the report, in some cases, a new security loophole is discovered and successful attack took place immediately after the penetration testing. However, it does not mean that the penetration testing is useless. It only means that, this is true that with thorough penetration testing, there is no guarantee that a successful attack will not take place, but definitely, the test will substantially reduce the possibility of a successful attack.

Penetration Testing - Limitations

Because of the swift pace of developments in the field of information and technology, the success story of penetration testing is comparatively short-lived. As more protection to the systems is required, more often than you need to perform penetration testing in order to diminish the possibility of a successful attack to the level that is appreciated by the company.

Following are the major limitations of Penetration Testing –

- **Limitation of Time** – As all of us know, penetration testing is not at all time bound exercise; nevertheless, experts of penetration testing have allotted a fixed amount of time for each test. On the other hand, attackers have no time constraints, they plan it in a week, month, or even years.
- **Limitation of Scope** – Many of the organizations do not test everything, because of their own limitations, including resource constraints, security constraints, budget constraints, etc. Likewise, a tester has limited scope and he has to leave many parts of the systems that might be much more vulnerable and can be a perfect niche for the attacker.
- **Limitation on Access** – More often testers have restricted access to the target environment. For example, if a company has carried out the penetration test against its DMZ systems from all across its internet networks, but what if the attackers attack through the normal internet gateway.
- **Limitation of Methods** – There are chances that the target system can crash during a penetration test, so some of the particular attack methods would likely be turned off the table for a professional penetration tester. For example, producing a denial of service flood to divert a system or network administrator from another attack method, usually an

ideal tactic for a really bad guy, but it is likely to fall outside of the rules of engagement for most of the professional penetration testers.

- **Limitation of Skill-sets of a Penetration Tester** – Usually, professional penetration testers are limited as they have limited skills irrespective of their expertise and past experience. Most of them are focused on a particular technology and having rare knowledge of other fields.
- **Limitation of Known Exploits** – Many of the testers are aware with only those exploits, which are public. In fact, their imaginative power is not as developed as attackers. Attackers normally think much beyond a tester's thinking and discover the flaw to attack.
- **Limitation to Experiment** – Most of the testers are time bound and follow the instructions already given to them by their organization or seniors. They do not try something new. They do not think beyond the given instructions. On the other hand, attackers are free to think, to experiment, and to create some new path to attack.

Moreover, penetration testing can neither replace the routine IT security tests, nor it can substitute a general security policy, but rather, penetration testing supplements the established review procedures and discovers new threats.

Penetration Testing - Remediation

Penetration testing efforts – however thorough they may be – cannot always ensure an exhaustive discovery of every instance where a security control's effectiveness is insufficient. Identifying a cross-site scripting vulnerability or risk in one area of an application may not definitely expose all instances of this vulnerability present in the application. This chapter illustrates the concept and utility of remediation.

What is Remediation?

Remediation is an act of offering an improvement to replace a mistake and set it right. Often the presence of vulnerability in one area may indicate weakness in process or development practices that could have replicated or enabled similar vulnerability in other locations. Therefore, while remediating, it is important for the tester to carefully investigate the tested entity or applications with ineffective security controls in mind.

Because of these reasons, the respective company should take steps to remediate any exploitable vulnerability within a reasonable period of time after the original penetration test. In fact, as soon as the company has completed these steps, the pen tester should perform a retest to validate the newly implemented controls which are capable to mitigate the original risk.

The remediation efforts extending for a longer period after the initial pen test possibly require performing a new testing engagement to ensure accurate results of the most current environment. This determination should be made after a risk analysis of how much change has occurred since the original testing was completed.

Moreover, in specific conditions, the flagged security problem may illustrate a basic flaw in respective environment or application. Therefore, the scope of a retest should consider whether any changes caused by remediation identified from the test are classified as significant. All changes should be retested; however, whether an entire system retest is necessary or not will be determined by the risk assessment of the changes.

Penetration Testing - Legal Issues

Before allowing someone to test sensitive data, companies normally take measures regarding the availability, confidentiality, and integrity of data. For this agreement to be in place, legal compliance is a necessary activity for an organization.

The most important legal regulations which have to be observed when establishing and maintaining security and authorization systems are presented below in context for using in implementing penetration tests.

What are the Legal Issues?

Following are some of the issues which may arise between a tester and his client –

- The tester is unknown to his client – so, on what ground, he should be given access of sensitive data
- Who will take the guarantee of security of the lost data?
- The client may blame for the loss of data or confidentiality to tester

Penetration testing may affect system performance, and can raise confidentiality and integrity issues; therefore, this is very important, even in an internal penetration testing, which is performed by an internal staff to get permission in writing. There should be a written agreement between a tester and the company/organization/individual to clarify all the points regarding the data security, disclosure, etc. before commencing testing.

A **statement of intent** should be drawn up and duly signed by both the parties prior to any testing work. It should be clearly outlined that the scope of the job and that, you may and may not be doing while performing vulnerability tests.

For the tester, it is important to know who owns the business or systems which are being requested to work on, and the infrastructure between testing systems and their targets that may be potentially affected by pen testing. The idea is to make sure;

- **the tester** has the permission in writing, with clearly defined parameters.
- **the company** has the details of its pen tester and an assurance that he would not leak any confidential data.

A legal agreement is beneficial for both the parties. Remember, regulations change from country to country, so keep yourself abreast with the laws of your respective country. Sign an agreement only after considering the respective laws.

09) Information Security Management System (ISMS)

A Definition of ISMS

An information security management system defines policies, methods, processes, and tools to ensure sustainable information security in companies and government agencies. This includes the introduction of specific procedures and the implementation of organizational and technical measures that must be continuously controlled, monitored, and improved.

The goal is to ensure, beyond the IT department, an appropriate level of protection for the confidentiality, availability, and integrity of information within the entire organization or the defined scope. Thus, the ISMS provides the basis for systematic implementation of information security within a company and for compliance with security standards. Potential threats relating to information security are identified, analyzed, and mitigated, making them controllable.

An effective ISMS can provide many benefits to your business. This is especially true in today's threat-heavy landscape where having robust information security is an absolute necessity in many supply chains.

Key business benefits

- Help you win new business and enter new sectors
- Strengthen your relationship with your existing customers
- Build your organisation's brand and reputation
- Protect your business from security breaches

What does an ISMS do?

Your information security management system can help support your business in many ways. You will find that an effective ISMS can:

- Safeguard your organisation's information assets
- Make it easy to demonstrate how secure your information is
- Show how seriously your organisation takes information security
- Help you stay ahead of new information security risks and opportunities
- Support your organisation's development and growth

What Is Information Security?

The term information security is often used synonymously with IT security, but strictly speaking it goes beyond that. Information security encompasses everything that protects a company's information assets against threats (e.g., cyberattacks, sabotage, espionage, and natural disasters)

and the resulting harm to its business or reputation. Legal regulations such as the German IT Security Act (IT-SiG) or the General Data Protection Regulation (GDPR) require appropriate protective measures for sensitive information, which may be in electronic, written, or printed form.

What Is the Difference between Information Security and IT Security?

Unlike IT security, information security refers not only to the security of the technology used, but also to organizational issues such as access authorizations and responsibilities. Accordingly, information security is not the sole responsibility of the IT department, but must be implemented in all areas of the company, starting with management.

What Are the Protection Goals of Information Security?

According to the international ISO 27000 family of standards, the protection goals of information security comprise three main aspects:

- **Confidentiality:** Confidential information may only be viewed and disclosed by authorized persons. Access to this information must therefore be appropriately secured. Confidentiality is violated if an attacker is able to eavesdrop on communications, for example.
- **Integrity:** Information must be protected from undetected manipulation in order to preserve its accuracy and completeness. Integrity is violated if, for example, an attacker is able to modify research data without detection.
- **Availability:** Information, services, or resources must be available and usable for legitimate users at all times. Availability can be disrupted, for example, by a DDoS attack that deliberately overloads systems.

Other aspects are authenticity, accountability, commitment, and reliability. The degree of information security achieved can be determined on the basis of how well these protection goals are fulfilled.

Who Is Responsible for Information Security in the Company?

To ensure information security in every part of the company, clear responsibilities must be defined and all necessary resources (money, personnel, time) must be made available. This is the responsibility of top management in the company. It bears overall responsibility for information security and an appropriate ISMS.

Following a top-down approach, it is the responsibility of company management to initiate the security process, set up an organizational structure, define security objectives and general conditions, and establish guidelines for enforcing information security. The detailed design and implementation of these guidelines as an ISMS can be delegated to managers and employees.

An information security officer appointed by top management acts as the point of contact for all information security issues. He/she must be integrated into the ISMS process and work closely with IT managers, for example, when selecting new IT components or applications.

What Are the Advantages of an ISMS?

With an ISMS, information security can be systematically implemented throughout the entire company and ensure that all required security standards are met. This holistic, preventive approach offers several advantages:

Protection of sensitive information:

An ISMS ensures that proprietary information assets (e.g., intellectual property, personnel data, or financial data) as well as data entrusted by customers or third parties are adequately protected against any and all threats.

Maintaining business continuity:

By using an ISMS to make information security an integral part of their business processes, companies can continuously increase their level of security and mitigate information security risks. In this way, they counteract the risk of security incidents disrupting business continuity.

Meeting compliance requirements:

Strict compliance requirements apply, particularly in highly regulated sectors such as finance or critical infrastructure. Violations of legal regulations and contractual agreements can result in heavy fines. With an ISMS, companies ensure that they meet all regulatory and contractual requirements, which also gives them more operational and legal certainty.

Verifiability of information security:

By certifying their ISMS, companies are able to verify to third parties that sensitive information is handled securely. This contributes to a better external image and to building trust, which in turn means a competitive advantage.

Improved cost-effectiveness and cost reduction:

The structured coordination and risk-oriented planning of measures in an ISMS helps to set priorities, use resources efficiently, and make investments in the right places. After initial additional costs, overheads can thus be reduced in the long term.

What Are Key Steps for Implementing an ISMS?

The efficient and effective implementation of an ISMS is a very complex process. The following steps should be taken into account:

Define the scope of services:

The first step is to clarify what the ISMS is supposed to do in the first place. To do this, company management must clearly define the areas of application, objectives, and limits of the ISMS.

Identify assets:

What assets should be protected by the ISMS? They can be information, software, services, and physical assets such as computers, but also the qualifications, skills, and experience of employees as well as other intangible assets such as reputation and standing. The main objective here is to identify business-critical assets on which the company's survival depends.

Identify and assess risks:

For every asset worth protecting, potential risks must be identified and classified based on legal requirements or compliance guidelines. Companies should ask themselves, for example, what impacts each risk would have if confidentiality, integrity, and availability were breached, or what the probabilities of the risks occurring are. In the end, they arrive at an assessment of which risks are acceptable, due to the expected amount of harm caused, for instance, and which must be addressed at all costs.

Define measures:

Based on the previous risk assessment, suitable technical and organizational measures for risk mitigation or avoidance must then be selected and implemented. This also includes defining clear competencies and responsibilities.

Check effectiveness:

The measures adopted and implemented must be continuously monitored and regularly checked for effectiveness, for example, by audits.

Make improvements:

If the review of the measures introduced reveals deficiencies or new risks have been identified, the ISMS process must be run through again from the beginning. In this way, the ISMS can be continuously adapted to changing conditions or requirements, continuously improving information security in the company.

Security Auditing

A security audit is the high-level description of the many ways organizations can test and assess their overall security posture, including cybersecurity. You might employ more than one type of security audit to achieve your desired results and meet your business objectives.

Why Are Security Audits Important?

The infographic features a dark blue background with a light blue rectangular frame. Inside the frame, the title "SECURITY AUDIT BENEFITS" is displayed in bold red capital letters at the top. Below the title is a graphic illustration consisting of several icons: a magnifying glass focusing on a computer screen, a gear, a warning sign with an exclamation mark, a small window icon, and a stack of money. To the right of the graphic is a bulleted list of seven benefits:

- Verify that your current security strategy is adequate or not
- Check that your security training efforts are working
- Uncover any extraneous hardware and software
- Reduce cost by nixing the use of unnecessary resources
- Uncover flaws introduced by new technology or processes
- Prove the organization is compliant with regulations

At the bottom of the frame, the Varonis logo is visible.

If you keep track of cybersecurity news even a little bit, you should have an intuitive understanding of why audits are important. Regular audits can catch new vulnerabilities and unintended consequences of organizational change, and on top of that, they are required by law for some industries – most notably medical and financial.

Here are some more specific benefits to running security audits.

- Verify that your current security strategy is adequate or not
- Check that your security training efforts are moving the needle from one audit to the next
- Reduce cost by shutting down or repurposing extraneous hardware and software that you uncover during the audit
- Security audits uncover vulnerabilities introduced into your organization by new technology or processes
- Prove the organization is compliant with regulations – HIPAA, SHIELD, CCPA, GDPR, etc.

How Do Security Audits Work?

AUDIT WORKFLOW



1. Define Assessment Criteria

- Determine the overall goals to be addressed in the audit
- Break those objectives down to departmental priorities
- Agree on how the audit will be performed and tracked



2. Prepare the Security Audit

- Prioritize your success criteria and business objectives
- Select the required tools and methodologies to meet goals
- Find or create a method to gather the correct data



3. Conduct the Security Audit

- Take care to provide appropriate documentation
- Monitor audit progress and data points for accuracy
- Use previous audits and new info to deep dive into findings



4. Complete and Share the Results

- Share results with all previously-determined parties
- Create a list of action items based on the audit findings
- Prioritize fixes to remediate the security items discovered

They found that companies focus audits on compliance activities and not to assess the risk to their organization. Checking boxes on a compliance form is great, but that won't stop an attacker from stealing data. By reframing the security audit to uncover risk to your organization as a whole you will be able to tick the compliance-related boxes along the way.

Gartner also found that audits tend to exist in a silo without a wide net and buy-in from many key stakeholders in the organization. They advise organizations to build a cross-functional

security audit project plan with multiple stakeholders that is updateable and repeatable so you can track your successes and failures over time.

A security audit should follow this basic format:

Define Assessment Criteria

A security audit is only as complete as its early definition. Determine the overall objectives the company needs to address in the audit, and then break those down to departmental priorities.

Get sign off on all business objectives of the security audit and keep track of out-of-scope items and exceptions.

Gartner advises companies to agree on how the assessment will be performed and tracked, and how the results will be gathered and addressed prior to the audit.

Things to consider:

- Industry and geographic standards (e.g., HIPAA, CCPA, GDPR, etc.)
- Maintain a threat catalog of all discovered risk vectors
- Are your stakeholders involved and able to participate?
- Utilize outside resources, when possible, an experienced security auditor can help you ask the correct questions and steer the audit successfully

Most importantly, the organization's priorities must not influence the outcomes of the audit.

Put simply, don't ignore bad stuff because it makes your job hard.

Prepare the Security Audit

With all of your success criteria and business objectives defined, it's time to prioritize those items. In order to do a great audit, companies have to align their efforts with the top items on their list. Not every item is a top priority, and not every top priority requires maximum effort.

During this step, select the tools and methodologies required to meet the business objectives. Find or create an appropriate questionnaire or survey to gather the correct data for your audit. Avoid square pegging tools into the round holes of your requirements and one-size-fits-all surveys.

Conduct the Security Audit

The next step is, of course, to conduct the audit.

During the audit, take care to provide appropriate documentation and perform due diligence throughout the process. Monitor the progress of the audit and also the data points collected for accuracy. Use previous audits and new information as well as the guidance of your auditing team

to carefully select which rabbit holes in which you descend. You will uncover details that require further examination but prioritize those new items with the team first.

Complete the audit and socialize the results with all of the stakeholders using the agreed-upon definitions from the earlier steps. Create a list of action items based on the audit and prioritize fixes and changes to remediate the security items discovered.

Beware of Risks and Pitfalls

There are a few possible challenges to a successful security audit.

- Avoid on the fly assessments, trust the process
- Stand by the facts of your results – people will push back and question the validity of your audit, make sure to be thorough and complete
- Beware of poorly defined scope or requirements in your audit, they can prove to be unproductive wastes of time
- An audit is supposed to uncover risk to your operation, which is different from a process audit or compliance audit, stay focused on risk

Types of Security Audits

Describes three different security audits for three different use cases.

1. One-time assessment

One-time assessments are security audits that you perform for ad-hoc or special circumstances and triggers in your operation. For example, if you are going to introduce a new software platform you have a battery of tests and audits that you run to discover any new risk you are introducing into your shop.

2. Tollgate assessment

Tollgate assessments are security audits with a binary outcome. It's a go or no-go audit to determine a new process or procedure can be introduced into your environment. You aren't determining risk as much as looking for showstoppers that will prevent you from moving forward.

3. Portfolio assessment

Portfolio security audits are the annual, bi-annual, or <enter your requirements here> regularly scheduled audit. Use these audits to verify that your security processes and procedures are being followed and that they are adequate for the current business climate and needs.

What to Look for in an IT Audit

Here is an incomplete list of things that you might find and flag during an audit.

- Insufficient password complexity
- Over permissive ACLs on folders
- Inconsistent ACLs on folders
- Non-existent or insufficient file activity auditing
- Non-existent or insufficient review of auditing data
- Correct security software and security configurations on all systems
- Only compliant software installed on systems
- Data retention policies followed
- Disaster recovery plans updated and tested
- Incident response plans updated and tested
- Sensitive data stored and protected correctly with encryption
- Change management procedures followed

10) UNDERSTANDING CYBER LAWS

Cyber laws are meant to set the definite pattern, some rules and guidelines that defined certain business activities going on through internet legal and certain illegal and hence punishable

WHAT IS CYBER LAW

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the

Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. It focuses on enhancing a jurisdiction 's legal system by establishing laws that reflect and deal with the technological changes that permeate society and describes the legal issues related to use of internetworked information technology. **Cyber law encompasses laws relating to:**

- Cyber Crimes
- Electronic and Digital Signatures
- Intellectual Property
- Data Protection and Privacy

Cybercrimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber crime

Intellectual property is refers to creations of the human mind e.g. a story, a song, a painting, a design etc. The facets of intellectual property that relate to cyber space are covered by cyber law.

These include:

- Copyright law in relation to computer software, computer source code, websites, cell phone content etc,
- Software and source code licenses
- Trademark law with relation to domain names, meta tags, mirroring, framing, linking etc
- Semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts,
- Patent law in relation to computer hardware and software.

Data protection and privacy laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc. These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

NEED FOR CYBER LAW

The cyber-crime has to be voluntary and willful, an act or omission that adversely affects a person or property. The cyber laws provide the backbone for e-commerce and India's approach has been to look at

e-governance and e-commerce primarily from the promotional aspects looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. There is the need to take in to consideration the security aspects.

Cyberspace

Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.

With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

Cyber security

Cybersecurity denotes the technologies and procedures intended to safeguard computers, networks, and data from unlawful admittance, weaknesses, and attacks transported through the Internet by cyber delinquents.

ISO 27001 (ISO27001) is the international Cybersecurity Standard that delivers a model for creating, applying, functioning, monitoring, reviewing, preserving, and improving an Information Security Management System.

The Ministry of Communication and Information Technology under the government of India provides a strategy outline called the National Cybersecurity Policy. The purpose of this government body is to protect the public and private infrastructure from cyber-attacks.

Cybersecurity Policy

The cybersecurity policy is a developing mission that caters to the entire field of Information and Communication Technology (ICT) users and providers. It includes –

- Home users
- Small, medium, and large Enterprises
- Government and non-government entities

It serves as an authority framework that defines and guides the activities associated with the security of cyberspace. It allows all sectors and organizations in designing suitable cybersecurity policies to meet their requirements. The policy provides an outline to effectively protect information, information systems and networks.

It gives an understanding into the Government's approach and strategy for security of cyber space in the country. It also sketches some pointers to allow collaborative working across the public and private sectors to safeguard information and information systems. Therefore, the aim of this policy is to create a cybersecurity framework, which leads to detailed actions and programs to increase the security carriage of cyberspace.

Security Policies

1. **Policies** - High-level statements about protecting information; Business rules to safeguard CIA triad; Security Policies can be applied on Users, Systems, Partners, Networks, and Providers.
 - o **Common Security Policies examples:**
 - Password Policy
 - Meet the password complexity requirements.
 - e.g.: Minimum 8 char length, upper and lower case and alphanumerical.
 - Wireless Security Policy
 - AUP - Acceptable Use-Policy
 - How to properly use company's assets
 - e.g.: "Do's and Dont's" with company's computer.
 - Data Retention Policy
 - e.g.: Keep the data for X time.
 - Access Control Policies
 - e.g.: Accessing servers; Firewalls
2. **Procedures** - Set of details steps to accomplish a goal; Instructions for implementation
3. **Guidelines** - Advice on actions given a situation; Recommended, not mandatory

Security Policy - Examples

- **Access Control Policy**
 - o This defines the resources being protected and the rules that control access to them
- **Remote Access Policy**
 - o This defines who can have remote access and defines access medium and remote access security controls.
- **Firewall Management Policy**
 - o This defines access, management and monitoring of firewalls in an organization.
- **Network Connection Policy**
 - o This defines who can install new resources on the network, approve the installation of new devices, document network changes etc.
- **Password Policy**
 - o This defines guidelines for using strong password protection on available resources.
- **User Account Policy**

- This defines the account creation process, authority, rights and responsibility of user accounts.
- **Information Protection Policy**
 - This defines the sensitivity levels of information, who may have access, how it is stored and transmitted, and how it should be deleted from storage media etc.
- **Special Access Policy**
 - This defines the terms and conditions of granting special access to system resources.
- **Email Security Policy**
 - This policy is designed to govern the proper usage of corporate email.
- **Acceptable Use Policy**
 - This defines the acceptable use of system resources.

Security Policy - Types

1. **Promiscuous Policy** - This policy usually has no restrictions on usage of system resources.
2. **Permissive Policy** - This policy begins wide open and only known dangerous services/attacks or behaviors are blocked. This type of policy has to be updated regularly to stay effective.
3. **Prudent Policy** - This policy provides maximum security while allowing known but necessary dangers. This type of policy will block all services and only safe/necessary services are enabled individually. Everything is logged.
4. **Paranoid Policy** - This policy forbids everything. No Internet connection or severely restricted Internet usage is allowed.

Security Policy - Creation Steps

1. Perform a Risk Assessment
2. Use security Standards and Frameworks as guide
3. Get Management and Staff input
4. Enforce the policy. Use penalties for non-compliance
5. Publish final draft to entire org.
6. Have all staff read/sign that they understood policy
7. Employ tools to help enforce policy
8. Staff training
9. Review and update regularly

Incident Management Process

An incident is an event that could lead to loss of, or disruption to, an organization's operations, services or functions.

Incident management is a term describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence.



1. **Preparation:** Select people, assign rules, define tools to handle the incident.
2. **Detection & Analysis:** Determine an incident has occurred (IDS, SIEM, AV, someone reporting, etc).
3. **Classification and Prioritization:**
4. **Notification:** Identify minor and major incident; who and how to notify an incident.
5. **Containment:** Limit the damage; Isolate hosts; Contact system owners.
6. **Forensic Investigation:** Investigate the root cause of the incident using forensic tools; System logs, real-time memory, network device logs, application logs, etc;
7. **Eradicate & Recovery:** Remove the cause of incident; Patch if needed. Recovery: get back into production; Monitor affected systems.
8. **Post-incident Activities:** Document what happened and why; Transfer knowledge.

Cyber Crime

The **Information Technology Act 2000** or any legislation in the Country does not describe or mention the term **Cyber Crime**. It can be globally considered as the gloomier face of technology. The only difference between a traditional crime and a cyber-crime is that the cyber-crime involves in a crime related to computers. Let us see the following example to understand it better –

Traditional Theft – A thief breaks into Ram's house and **steals** an object kept in the house.

Hacking – A Cyber Criminal/Hacker sitting in his own house, through his computer, hacks the computer of Ram and **steals** the data saved in Ram's computer without physically touching the computer or entering in Ram's house.

The I.T. Act, 2000 defines the terms –

- access in computer network in **section 2(a)**
- computer in **section 2(i)**
- computer network in **section 2(j)**
- data in **section 2(0)**
- information in **section 2(v)**.

To understand the concept of Cyber Crime, you should know these laws. The object of offence or target in a cyber-crime are either the computer or the data stored in the computer.

Nature of Threat

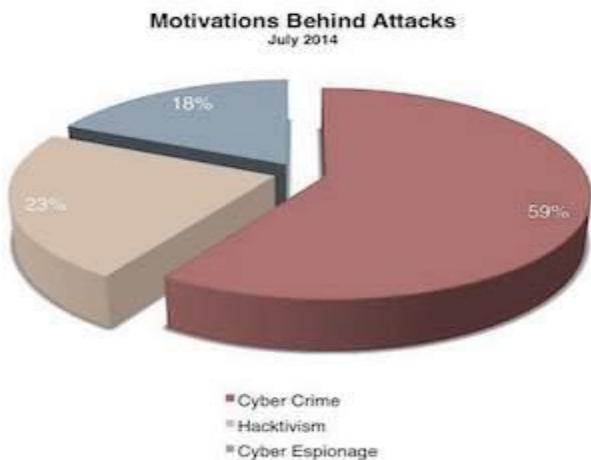
Among the most serious challenges of the 21st century are the prevailing and possible threats in the sphere of cybersecurity. Threats originate from all kinds of sources, and mark themselves in disruptive activities that target individuals, businesses, national infrastructures, and governments alike. The effects of these threats transmit significant risk for the following –

- public safety
- security of nations
- stability of the globally linked international community

Malicious use of information technology can easily be concealed. It is difficult to determine the origin or the identity of the criminal. Even the motivation for the disruption is not an easy task to find out. Criminals of these activities can only be worked out from the target, the effect, or other circumstantial evidence. Threat actors can operate with considerable freedom from virtually anywhere. The motives for disruption can be anything such as –

- simply demonstrating technical prowess
- theft of money or information
- extension of state conflict, etc.

Criminals, terrorists, and sometimes the State themselves act as the source of these threats. Criminals and hackers use different kinds of malicious tools and approaches. With the criminal activities taking new shapes every day, the possibility for harmful actions propagates.



Enabling People

The lack of information security awareness among users, who could be a simple school going kid, a system administrator, a developer, or even a CEO of a company, leads to a variety of cyber vulnerabilities. The awareness policy classifies the following actions and initiatives for the purpose of user awareness, education, and training –

- A complete awareness program to be promoted on a national level.
- A comprehensive training program that can cater to the needs of the national information security (Programs on IT security in schools, colleges, and universities).
- Enhance the effectiveness of the prevailing information security training programs. Plan domain-specific training programs (e.g., Law Enforcement, Judiciary, E-Governance, etc.)
- Endorse private-sector support for professional information security certifications.

Information Technology Act

The Government of India enacted The Information Technology Act with some major objectives which are as follows –

- To deliver lawful recognition for transactions through electronic data interchange (EDI) and other means of electronic communication, commonly referred to as **electronic commerce** or E-Commerce. The aim was to use replacements of paper-based methods of communication and storage of information.
- To facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000. The I. T. Act got the President's assent on June 9, 2000 and it was made effective from October 17, 2000. By adopting this Cyber Legislation, India became the 12th nation in the world to adopt a Cyber Law regime.

Mission and Vision Cybersecurity Program

Mission

The following mission caters to cybersecurity –

- To safeguard information and information infrastructure in cyberspace.
- To build capabilities to prevent and respond to cyber threats.
- To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

Vision

To build a secure and resilient cyberspace for citizens, businesses, and Government.

Emerging Trends of Cyber Law

Reports reveal that upcoming years will experience more cyber-attacks. So organizations are advised to strengthen their data supply chains with better inspection methods.

Some of the emerging trends of cyber law are listed below –

- Stringent regulatory rules are put in place by many countries to prevent unauthorized access to networks. Such acts are declared as penal offences.

- Stakeholders of the mobile companies will call upon the governments of the world to reinforce cyber-legal systems and administrations to regulate the emerging mobile threats and crimes.
- The growing awareness on privacy is another upcoming trend. Google's chief internet expert Vint Cerf has stated that *privacy may actually be an anomaly*.
- **Cloud computing** is another major growing trend. With more advancements in the technology, huge volumes of data will flow into the cloud which is not completely immune to cyber-crimes.
- The growth of **Bitcoins** and other virtual currency is yet another trend to watch out for. Bitcoin crimes are likely to multiply in the near future.
- The arrival and acceptance of data analytics, which is another major trend to be followed, requires that appropriate attention is given to issues concerning **Big Data**.

Create Awareness

While the U.S. government has declared October as the National Cybersecurity Awareness month, India is following the trend to implement some stringent awareness scheme for the general public.

The general public is partially aware of the crimes related to **virus transfer**. However, they are unaware of the bigger picture of the threats that could affect their cyber-lives. There is a huge lack of knowledge on e-commerce and online banking cyber-crimes among most of the internet users.

Be vigilant and follow the tips given below while you participate in online activities –

- Filter the visibility of personal information in social sites.
- Do not keep the "remember password" button active for any email address and passwords
- Make sure your online banking platform is secure.
- Keep a watchful eye while shopping online.
- Do not save passwords on mobile devices.
- Secure the login details for mobile devices and computers, etc.

Areas of Development

The "Cyberlaw Trends in India 2013" and "Cyber law Developments in India in 2014" are two prominent and trustworthy cyber-law related research works provided by Perry4Law Organization (P4LO) for the years 2013 and 2014.

There are some grave cyber law related issues that deserve immediate consideration by the government of India. The issues were put forward by the Indian cyber law roundup of 2014 provided by P4LO and Cyber Crimes Investigation Centre of India (CCICI). Following are some major issues –

- A better cyber law and effective cyber-crimes prevention strategy

- Cyber-crimes investigation training requirements
- Formulation of dedicated encryption laws
- Legal adoption of cloud computing
- Formulation and implementation of e-mail policy
- Legal issues of online payments
- Legality of online gambling and online pharmacies
- Legality of Bitcoins
- Framework for blocking websites
- Regulation of mobile applications

With the formation of cyber-law compulsions, the obligation of banks for cyber-thefts and cyber-crimes would considerably increase in the near future. Indian banks would require to keep a dedicated team of cyber law experts or seek help of external experts in this regard.

The transactions of cyber-insurance should be increased by the Indian insurance sector as a consequence of the increasing cyber-attacks and cyber-crimes.

International Network on Cybersecurity

To create an international network on cybersecurity, a conference was held in March 2014 in New Delhi, India.

The objectives set in the International Conference on Cyberlaw & Cybercrime are as follows –

- To recognize the developing trends in Cyberlaw and the legislation impacting cyberspace in the current situation.
- To generate better awareness to battle the latest kinds of cybercrimes impacting all investors in the digital and mobile network.
- To recognize the areas for stakeholders of digital and mobile network where Cyberlaw needs to be further evolved.
- To work in the direction of creating an international network of cybercrimes. Legal authorities could then be a significant voice in the further expansion of cyber-crimes and cyber law legislations throughout the globe.

Intellectual Property Right

Intellectual property rights are the legal rights that cover the privileges given to individuals who are the owners and inventors of a work, and have created something with their intellectual creativity. Individuals related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in the business practices by them.

The creator/inventor gets exclusive rights against any misuse or use of work without his/her prior information. However, the rights are granted for a limited period of time to maintain equilibrium.

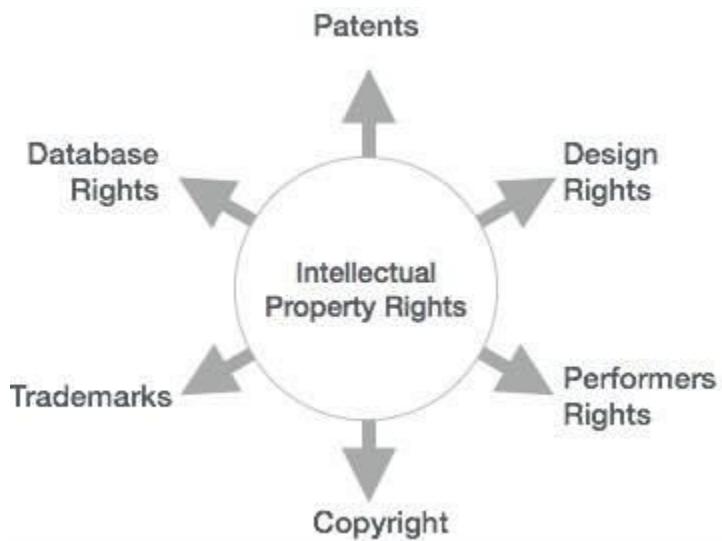
The following list of activities which are covered by the intellectual property rights are laid down by the World Intellectual Property Organization (WIPO) –

- Industrial designs
- Scientific discoveries
- Protection against unfair competition
- Literary, artistic, and scientific works
- Inventions in all fields of human endeavor
- Performances of performing artists, phonograms, and broadcasts
- Trademarks, service marks, commercial names, and designations
- All other rights resulting from intellectual activity in the industrial, scientific, literary, or artistic fields

Types of Intellectual Property Rights

Intellectual Property Rights can be further classified into the following categories –

- Copyright
- Patent
- Patent
- Trade Secrets, etc.



Advantages of Intellectual Property Rights

Intellectual property rights are advantageous in the following ways –

- Provides exclusive rights to the creators or inventors.
- Encourages individuals to distribute and share information and data instead of keeping it confidential.
- Provides legal defense and offers the creators the incentive of their work.
- Helps in social and financial development.

Intellectual Property Rights in India

To protect the intellectual property rights in the Indian territory, India has defined the formation of constitutional, administrative and jurisdictional outline whether they imply the copyright, patent, trademark, industrial designs, or any other parts of the intellectual property rights.

Back in the year 1999, the government passed an important legislation based on international practices to safeguard the intellectual property rights. Let us have a glimpse of the same –

- The **Patents** (Amendment) Act, 1999, facilitates the establishment of the mail box system for filing patents. It offers exclusive marketing rights for a time period of five years.
- The **Trade Marks** Bill, 1999, replaced the Trade and Merchandise Marks Act, 1958
- The **Copyright** (Amendment) Act, 1999, was signed by the President of India.
- The *sui generis* legislation was approved and named as the Geographical Indications of Goods (Registration and Protection) Bill, 1999.
- The **Industrial Designs** Bill, 1999, replaced the Designs Act, 1911.
- The **Patents (Second Amendment)** Bill, 1999, for further amending the Patents Act of 1970 in compliance with the TRIPS.

Intellectual Property in Cyber Space

Every new invention in the field of technology experiences a variety of threats. Internet is one such threat, which has captured the physical marketplace and have converted it into a virtual marketplace.

To safeguard the business interest, it is vital to create an effective property management and protection mechanism keeping in mind the considerable amount of business and commerce taking place in the Cyber Space.

Today it is critical for every business to develop an effective and collaborative IP management mechanism and protection strategy. The ever-looming threats in the cybernetic world can thus be monitored and confined.

Various approaches and legislations have been designed by the law-makers to up the ante in delivering a secure configuration against such cyber-threats. However, it is the duty of the intellectual property right (IPR) owner to invalidate and reduce such *mala fide* acts of criminals by taking proactive measures.

Cyber Security Strategies

To design and implement a secure cyberspace, some stringent strategies have been put in place. This chapter explains the major strategies employed to ensure cybersecurity, which include the following –

- Creating a Secure Cyber Ecosystem
- Creating an Assurance Framework
- Encouraging Open Standards
- Strengthening the Regulatory Framework

- Creating Mechanisms for IT Security
- Securing E-governance Services
- Protecting Critical Information Infrastructure

Strategy 1 – Creating a Secure Cyber Ecosystem

The cyber ecosystem involves a wide range of varied entities like devices (communication technologies and computers), individuals, governments, private organizations, etc., which interact with each other for numerous reasons.

This strategy explores the idea of having a strong and robust cyber-ecosystem where the cyber-devices can work with each other in the future to prevent cyber-attacks, reduce their effectiveness, or find solutions to recover from a cyber-attack.

Such a cyber-ecosystem would have the ability built into its cyber devices to permit secured ways of action to be organized within and among groups of devices. This cyber-ecosystem can be supervised by present monitoring techniques where software products are used to detect and report security weaknesses.

A strong cyber-ecosystem has three symbiotic structures – **Automation, Interoperability, and Authentication**.

- **Automation** – It eases the implementation of advanced security measures, enhances the swiftness, and optimizes the decision-making processes.
- **Interoperability** – It toughens the collaborative actions, improves awareness, and accelerates the learning procedure. There are three types of interoperability –
 - Semantic (i.e., shared lexicon based on common understanding)
 - Technical
 - Policy – Important in assimilating different contributors into an inclusive cyber-defense structure.
- **Authentication** – It improves the identification and verification technologies that work in order to provide –
 - Security
 - Affordability
 - Ease of use and administration
 - Scalability
 - Interoperability

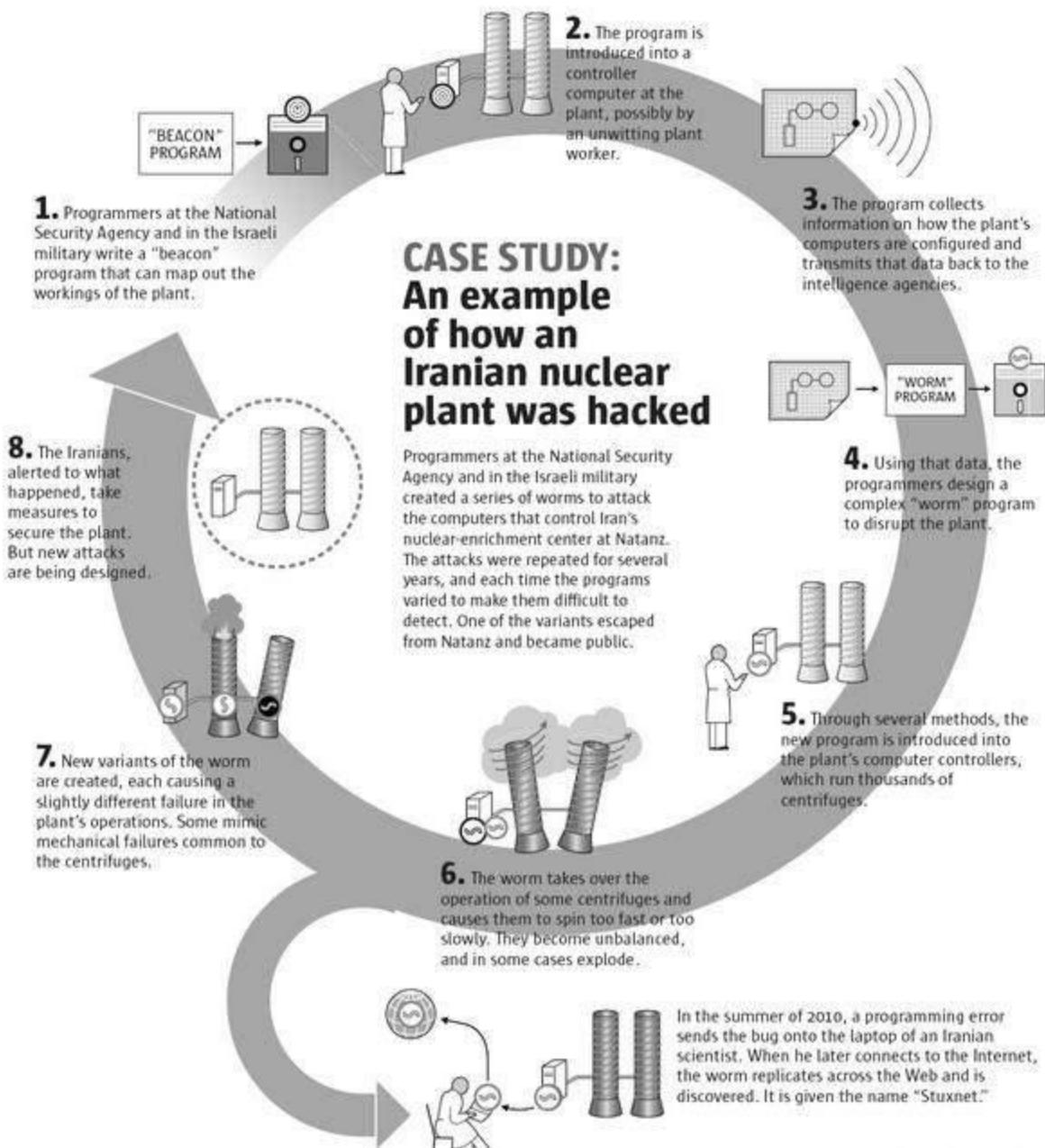
Comparison of Attacks

The following table shows the *Comparison of Attack Categories against Desired Cyber Ecosystem Capabilities* –

Desired Cyber Ecosystem Capabilities	Categories of Cyber Attack							
	Attrition	Malware	Hacking	Social Tactics	Improper Usage (Insider)	Physical Action; Loss or Theft	Multiple Component	Other
Automation	x	x	x	x	x	x	x	x
Authentication	x	x	x	x		x	x	x
Interoperability	x	x	x	x			x	
Automated Defense Identification, Selection, and Assessment	x	x	x	x	x	x	x	x
Build Security In	x	x	x	x		x	x	x
Business Rules-Based Behavior Monitoring	x	x	x	x	x	x	x	x
General Awareness and Education	x	x	x	x	x	x	x	x
Moving Target	x	x	x	x			x	x
Privacy	x	x	x	x	x	x	x	x
Risk-Based Data Management	x	x	x	x	x	x	x	x
Situational Awareness	x	x	x	x	x	x	x	x
Tailored Trustworthy Spaces	x	x	x	x			x	x

Case Study

The following diagram was prepared by *Guilbert Gates for The New York Times*, which shows how an Iranian plant was hacked through the internet.



Explanation – A program was designed to automatically run the Iranian nuclear plant. Unfortunately, a worker who was unaware of the threats introduced the program into the controller. The program collected all the data related to the plant and sent the information to the intelligence agencies who then developed and inserted a worm into the plant. Using the worm, the plant was controlled by miscreants which led to the generation of more worms and as a result, the plant failed completely.

Types of Attacks

The following table describes the attack categories –

Attack Category	Description of Attack
Attrition	Methods used to damage networks and systems. It includes the following – <ul style="list-style-type: none">• distributed denial of service attacks• impair or deny access to a service or application• resource depletion attacks
Malware	Any malicious software used to interrupt normal computer operation and harm information assets without the owner's consent. Any execution from a removable device can enhance the threat of a malware.
Hacking	An attempt to intentionally exploit weaknesses to get unethical access, usually conducted remotely. It may include – <ul style="list-style-type: none">• data-leakage attacks• injection attacks and abuse of functionality• spoofing• time-state attacks• buffer and data structure attacks• resource manipulation• stolen credentials usage• backdoors• dictionary attacks on passwords• exploitation of authentication
Social Tactics	Using social tactics such as deception and manipulation to acquire access to data, systems or controls. It includes – <ul style="list-style-type: none">• pre-texting (forged surveys)• inciting phishing• retrieving of information through conversation
Improper Usage (Insider Threat)	Misuse of rights to data and controls by an individual in an organization that would violate the organization's policies. It includes – <ul style="list-style-type: none">• installation of unauthorized software• removal of sensitive data
Physical Action/Loss or Theft of Equipment	Human-Driven attacks such as – <ul style="list-style-type: none">• stolen identity tokens and credit cards

	<ul style="list-style-type: none"> • fiddling with or replacing card readers and point of sale terminals • interfering with sensors • theft of a computing device used by the organization, such as a laptop
Multiple Component	Single attach techniques which contains several advanced attack techniques and components.
Other	<p>Attacks such as –</p> <ul style="list-style-type: none"> • supply chain attacks • network investigation

Strategy 2 – Creating an Assurance Framework

The objective of this strategy is to design an outline in compliance with the global security standards through traditional products, processes, people, and technology.

To cater to the national security requirements, a national framework known as the **Cybersecurity Assurance Framework** was developed. It accommodates critical infrastructure organizations and the governments through "Enabling and Endorsing" actions.

Enabling actions are performed by government entities that are autonomous bodies free from commercial interests. The publication of "National Security Policy Compliance Requirements" and IT security guidelines and documents to enable IT security implementation and compliance are done by these authorities.

Endorsing actions are involved in profitable services after meeting the obligatory qualification standards and they include the following –

- ISO 27001/BS 7799 ISMS certification, IS system audits etc., which are essentially the compliance certifications.
- 'Common Criteria' standard ISO 15408 and Crypto module verification standards, which are the IT Security product evaluation and certification.
- Services to assist consumers in implementation of IT security such as IT security manpower training.

Trusted Company Certification

Indian IT/ITES/BPOs need to comply with the international standards and best practices on security and privacy with the development of the outsourcing market. ISO 9000, CMM, Six Sigma, Total Quality Management, ISO 27001 etc., are some of the certifications.

Existing models such as SEI CMM levels are exclusively meant for software development processes and do not address security issues. Therefore, several efforts are made to create a

model based on self-certification concept and on the lines of Software Capability Maturity Model (SW-CMM) of CMU, USA.

The structure that has been produced through such association between industry and government, comprises of the following –

- standards
- guidelines
- practices

These parameters help the owners and operators of critical infrastructure to manage cybersecurity-related risks.

Strategy 3 – Encouraging Open Standards

Standards play a significant role in defining how we approach information security related issues across geographical regions and societies. Open standards are encouraged to –

- Enhance the efficiency of key processes,
- Enable systems incorporations,
- Provide a medium for users to measure new products or services,
- Organize the approach to arrange new technologies or business models,
- Interpret complex environments, and
- Endorse economic growth.

Standards such as ISO 27001[3] encourage the implementation of a standard organization structure, where customers can understand processes, and reduce the costs of auditing.

Strategy 4 – Strengthening the Regulatory Framework

The objective of this strategy is to create a secure cyberspace ecosystem and strengthen the regulatory framework. A 24X7 mechanism has been envisioned to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC). The Computer Emergency Response Team (CERT-In) has been designated to act as a nodal agency for crisis management.

Some highlights of this strategy are as follows –

- Promotion of research and development in cybersecurity.
- Developing human resource through education and training programs.
- Encouraging all organizations, whether public or private, to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cybersecurity initiatives.
- Indian Armed Forces are in the process of establishing a cyber-command as a part of strengthening the cybersecurity of defense network and installations.

- Effective implementation of public-private partnership is in pipeline that will go a long way in creating solutions to the ever-changing threat landscape.

Strategy 5 – Creating Mechanisms for IT Security

Some basic mechanisms that are in place for ensuring IT security are – link-oriented security measures, end-to-end security measures, association-oriented measures, and data encryption. These methods differ in their internal application features and also in the attributes of the security they provide. Let us discuss them in brief.

Link-Oriented Measures

It delivers security while transferring data between two nodes, irrespective of the eventual source and destination of the data.

End-to-End Measures

It is a medium for transporting Protocol Data Units (PDUs) in a protected manner from source to destination in such a way that disruption of any of their communication links does not violate security.

Association-Oriented Measures

Association-oriented measures are a modified set of end-to-end measures that protect every association individually.

Data Encryption

It defines some general features of conventional ciphers and the recently developed class of public-key ciphers. It encodes information in a way that only the authorized personnel can decrypt them.

Strategy 6 – Securing E-Governance Services

Electronic governance (e-governance) is the most treasured instrument with the government to provide public services in an accountable manner. Unfortunately, in the current scenario, there is no devoted legal structure for e-governance in India.

Similarly, there is no law for obligatory e-delivery of public services in India. And nothing is more hazardous and troublesome than executing e-governance projects without sufficient cybersecurity. Hence, securing the e-governance services has become a crucial task, especially when the nation is making daily transactions through cards.

Fortunately, the Reserve Bank of India has implemented security and risk mitigation measures for card transactions in India enforceable from 1st October, 2013. It has put the responsibility of ensuring secured card transactions upon banks rather than on customers.

"E-government" or electronic government refers to the use of Information and Communication Technologies (ICTs) by government bodies for the following –

- Efficient delivery of public services
- Refining internal efficiency
- Easy information exchange among citizens, organizations, and government bodies
- Re-structuring of administrative processes.

Strategy 7 – Protecting Critical Information Infrastructure

Critical information infrastructure is the backbone of a country's national and economic security. It includes power plants, highways, bridges, chemical plants, networks, as well as the buildings where millions of people work every day. These can be secured with stringent collaboration plans and disciplined implementations.

Safeguarding critical infrastructure against developing cyber-threats needs a structured approach. It is required that the government aggressively collaborates with public and private sectors on a regular basis to prevent, respond to, and coordinate mitigation efforts against attempted disruptions and adverse impacts to the nation's critical infrastructure.

It is in demand that the government works with business owners and operators to reinforce their services and groups by sharing cyber and other threat information.

A common platform should be shared with the users to submit comments and ideas, which can be worked together to build a tougher foundation for securing and protecting critical infrastructures.

The government of USA has passed an executive order "Improving Critical Infrastructure Cybersecurity" in 2013 that prioritizes the management of cybersecurity risk involved in the delivery of critical infrastructure services. This Framework provides a common classification and mechanism for organizations to –

- Define their existing cybersecurity bearing,
- Define their objectives for cybersecurity,
- Categorize and prioritize chances for development within the framework of a constant process, and
- Communicate with all the investors about cybersecurity.

Policies To Mitigate Cyber Risk

This chapter takes you through the various policies laid to minimize cyber risk. It is only with well-defined policies that the threats generated in the cyberspace can be reduced.

Promotion of R&D in Cybersecurity

Due to the ever-increasing dependence on the Internet, the biggest challenge we face today is the security of information from miscreants. Therefore, it is essential to promote research and development in cybersecurity so that we can come up with robust solutions to mitigate cyber risks.

Cybersecurity Research

Cybersecurity Research is the area that is concerned with preparing solutions to deal with cyber criminals. With increasing amount of internet attacks, advanced persistent threats and phishing, lots of research and technological developments are required in the future.

Cybersecurity Research-Indian Perspective

In the recent years, India has witnessed an enormous growth in cyber technologies. Hence it calls for an investment in the research and development activities of cybersecurity. India has also seen many successful research outcomes that were translated into businesses, through the advent of local cybersecurity companies.

Threat Intelligence

Research work to mitigate cyber-threats is already being commenced in India. There is a proactive response mechanism in place to deal with cyber threats. Research and Development activities are already underway at various research organizations in India to fight threats in cyberspace.

Next Generation Firewall

Multi-identity based expertise such as Next Generation Firewall that offers security intelligence to enterprises and enable them to apply best suited security controls at the network perimeter are also being worked on.

Secured Protocol and Algorithms

Research in protocols and algorithms is a significant phase for the consolidation of cybersecurity at a technical level. It defines the rules for information sharing and processing over cyberspace. In India, protocol and algorithm level research includes –

- Secure Routing Protocols

- Efficient Authentication Protocols
- Enhanced Routing Protocol for Wireless Networks
- Secure Transmission Control Protocol
- Attack Simulation Algorithm, etc.

Authentication Techniques

Authentication techniques such as Key Management, Two Factor Authentication, and Automated key Management provide the ability to encrypt and decrypt without a centralized key management system and file protection. There is continuous research happening to strengthen these authentication techniques.

BYOD, Cloud and Mobile Security

With the adoption of varied types of mobile devices, the research on the security and privacy related tasks on mobile devices has increased. Mobile security testing, Cloud Security, and BYOD (Bring Your Own Device) risk mitigation are some of the areas where a lot of research is being done.

Cyber Forensics

Cyber Forensics is the application of analysis techniques to collect and recover data from a system or a digital storage media. Some of the specific areas where research is being done in India are –

- Disk Forensics
- Network Forensics
- Mobile Device Forensics
- Memory Forensics
- Multimedia Forensics
- Internet Forensics

Reducing Supply Chain Risks

Formally, supply chain risk can be defined as –

Any risk that an opponent may damage, write some malicious function to it, deconstruct the design, installation, procedure, or maintenance of a supply item or a system so that the entire function can be degraded.

Supply Chain Issues

Supply chain is a global issue and there is a requirement to find out the interdependencies among the customers and suppliers. In today's scenario it is important to know – *What are the SCRM problems? and How to address the problems?*

An effective SCRM (Supply Chain Risk Management) approach requires a strong public-private partnership. Government should have strong authorities to handle supply chain issues. Even private sectors can play a key role in a number of areas.

We cannot provide a one-size-fits-all resolution for managing supply chain risks. Depending on the product and the sector, the costs for reducing risks will weigh differently. Public Private Partnerships should be encouraged to resolve risks associated with supply chain management.

Mitigate Risks through Human Resource Development

Cybersecurity policies of an organization can be effective, provided all its employees understand their value and exhibit a strong commitment towards implementing them. Human resource directors can play a key role in keeping organizations safe in cyberspace by applying the following few points.

Taking Ownership of the Security Risk Posed by Employees

As most of the employees do not take the risk factor seriously, hackers find it easy to target organizations. In this regard, HR plays a key role in educating employees about the impact their attitudes and behavior have on the organization's security.

Ensuring that Security Measures are Practical and Ethical

Policies of a company must be in sync with the way employees think and behave. For example, saving passwords on systems is a threat, however continuous monitoring can prevent it. The HR team is best placed to advise whether policies are likely to work and whether they are appropriate.

Identifying Employees who may Present a Particular Risk

It also happens that cyber-criminals take the help of insiders in a company to hack their network. Therefore it is essential to identify employees who may present a particular risk and have stringent HR policies for them.

Creating Cybersecurity Awareness

Cybersecurity in India is still in its evolution stage. This is the best time to create awareness on issues related to cyber security. It would be easy to create awareness from the grass-root level like schools where users can be made aware how Internet works and what are its potential threats.

Every cyber café, home/personal computers, and office computers should be protected through firewalls. Users should be instructed through their service providers or gateways not to breach unauthorized networks. The threats should be described in bold and the impacts should be highlighted.

Subjects on cybersecurity awareness should be introduced in schools and colleges to make it an ongoing process.

The government must formulate strong laws to enforce cybersecurity and create sufficient awareness by broadcasting the same through television/radio/internet advertisements.

Information Sharing

United States proposed a law called **Cybersecurity Information Sharing Act of 2014 (CISA)** to improve cybersecurity in the country through enhanced sharing of information about cybersecurity threats. Such laws are required in every country to share threat information among citizens.

Cybersecurity Breaches Need a Mandatory Reporting Mechanism

The recent malware named **Uroburos/Snake** is an example of growing cyber-espionage and cyber-warfare. Stealing of sensitive information is the new trend. However, it is unfortunate that the telecom companies/internet service providers (ISPs) are not sharing information pertaining to cyber-attacks against their networks. As a result, a robust cybersecurity strategy to counter cyber-attacks cannot be formulated.

This problem can be addressed by formulating a good cybersecurity law that can establish a regulatory regime for obligatory cybersecurity breach notifications on the part of telecom companies/ISPs.

Infrastructures such as automated power grids, thermal plants, satellites, etc., are vulnerable to diverse forms of cyber-attacks and hence a breach notification program would alert the agencies to work on them.

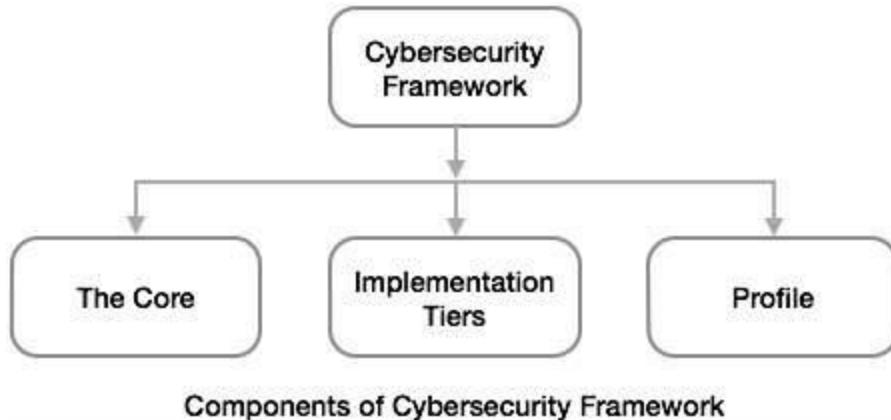
Implementing a Cybersecurity Framework

Despite the fact that companies are spending on cybersecurity initiatives, data breaches continue to occur. According to *The Wall Street Journal*, "Global cybersecurity spending by critical infrastructure industries was expected to hit \$46 billion in 2013, up 10% from a year earlier according to Allied Business Intelligence Inc." This calls for the effective implementation of the cybersecurity framework.

Components of Cybersecurity Framework

The Framework comprises of three main components –

- The Core,
- Implementation Tiers, and
- Framework Profiles.



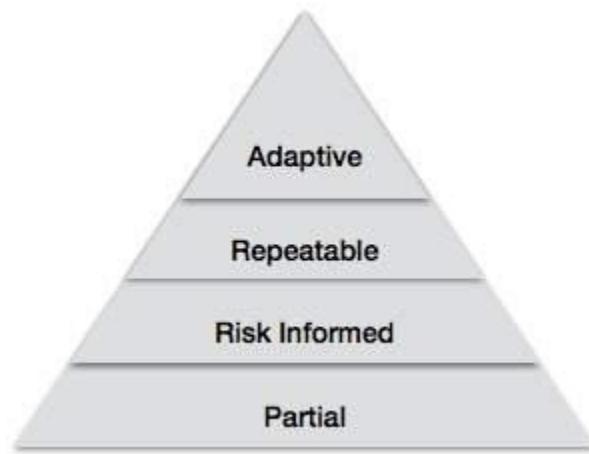
The Framework Core

The Framework Core is a set of cybersecurity activities and applicable references that have five simultaneous and constant functions – Identify, Protect, Detect, Respond, and Recover. The framework core has methods to ensure the following –

- Develop and implement procedures to protect the most critical intellectual property and assets.
- Have resources in place to identify any cybersecurity breach.
- Recover from a breach, if and when one occurs.

The Implementation Tiers

The Framework Implementation Tiers define the level of sophistication and consistency an organization employs in applying its cybersecurity practices. It has the following four levels.



Tier 1 (Partial) – In this level, the organization's cyber-risk management profiles are not defined. There is a partial consciousness of the organization's cybersecurity risk at the organization level. Organization-wide methodology to managing cybersecurity risk has not been recognized.

Tier 2 (Risk Informed) – In this level, organizations establish a cyber-risk management policy that is directly approved by the senior management. The senior management makes efforts to establish risk management objectives related to cybersecurity and implements them.

Tier 3 (Repeatable) – In this level, the organization runs with formal cybersecurity measures, which are regularly updated based on requirement. The organization recognizes its dependencies and partners. It also receives information from them, which helps in taking risk-based management decisions.

Tier 4 (Adaptive) – In this level, the organization adapts its cybersecurity practices "in real-time" derived from previous and current cybersecurity activities. Through a process of incessant development in combining advanced cybersecurity technologies, real-time collaboration with partners, and continuous monitoring of activities on their systems, the organization's cybersecurity practices can quickly respond to sophisticated threats.

The Framework Profile

The Framework Profile is a tool that provides organizations a platform for storing information concerning their cybersecurity program. A profile allows organizations to clearly express the goals of their cybersecurity program.

Where do You Start with Implementing the Framework?

The senior management including the directors should first get acquainted with the Framework. After which, the directors should have a detailed discussion with the management about the organization's Implementation Tiers.

Educating the managers and staff on the Framework will ensure that everyone understands its importance. This is an important step towards the successful implementation of a vigorous cybersecurity program. The information about existing Framework Implementations may help organizations with their own approaches.

Network Security

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Types of Network Security Devices

Active Devices



These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

Passive Devices

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

Preventative Devices

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

Firewalls

A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.

Firewalls are commonly used in private networks or *intranets* to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

Hardware and Software Firewalls

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For

larger networks – e.g., for business purpose – business networking firewall solutions are available.

Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

Antivirus

An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

Content Filtering

Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.

Content filtering can be divided into the following categories –

- Web filtering
- Screening of Web sites or pages
- E-mail filtering
- Screening of e-mail for spam
- Other objectionable content

Intrusion Detection Systems

Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.

Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. Intrusion detection systems can also perform the following actions –

- Correct Cyclic Redundancy Check (CRC) errors
- Prevent TCP sequencing issues
- Clean up unwanted transport and network layer options

Information Technology Act, 2000

As discussed in the first chapter, the Government of India enacted the Information Technology (I.T.) Act with some major objectives to deliver and facilitate lawful electronic, digital, and online transactions, and mitigate cyber-crimes.

Salient Features of I.T Act

The salient features of the I.T Act are as follows –

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It defines in a new section that *cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.*
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- It is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that *nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.*

Scheme of I.T Act

The following points define the scheme of the I.T. Act –

- The I.T. Act contains **13 chapters and 90 sections**.
- The last four sections namely sections 91 to 94 in the I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.
- It commences with Preliminary aspect in Chapter 1, which deals with the short, title, extent, commencement and application of the Act in Section 1. Section 2 provides Definition.
- Chapter 2 deals with the authentication of electronic records, digital signatures, electronic signatures, etc.
- Chapter 11 deals with offences and penalties. A series of offences have been provided along with punishment in this part of The Act.
- Thereafter the provisions about due diligence, role of intermediaries and some miscellaneous provisions are been stated.
- The Act is embedded with two schedules. The First Schedule deals with Documents or Transactions to which the Act shall not apply. The Second Schedule deals with electronic

signature or electronic authentication technique and procedure. The Third and Fourth Schedule are omitted.

Application of the I.T Act

As per the sub clause (4) of Section 1, *nothing in this Act shall apply to documents or transactions specified in First Schedule*. Following are the documents or transactions to which the Act shall not apply –

- **Negotiable Instrument** (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
- A **power-of-attorney** as defined in section 1A of the Powers-of-Attorney Act, 1882;
- A **trust** as defined in section 3 of the Indian Trusts Act, 1882;
- A **will** as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
- Any **contract** for the sale or conveyance of immovable property or any interest in such property;
- Any such class of documents or transactions as may be notified by the Central Government.

Amendments Brought in the I.T Act

The I.T. Act has brought amendment in four statutes vide section 91-94. These changes have been provided in schedule 1-4.

- The first schedule contains the amendments in the Penal Code. *It has widened the scope of the term "document" to bring within its ambit electronic documents.*
- The second schedule deals with amendments to the India Evidence Act. *It pertains to the inclusion of electronic document in the definition of evidence.*
- The third schedule amends the Banker's Books Evidence Act. *This amendment brings about change in the definition of "Banker's-book". It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device. Similar change has been brought about in the expression "Certified-copy" to include such printouts within its purview.*
- The fourth schedule amends the Reserve Bank of India Act. *It pertains to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institution.*

Intermediary Liability

Intermediary, dealing with any specific electronic records, is a person who on behalf of another person accepts, stores or transmits that record or provides any service with respect to that record.

According to the above mentioned definition, it includes the following –

- Telecom service providers
- Network service providers
- Internet service providers
- Web-hosting service providers
- Search engines
- Online payment sites
- Online auction sites
- Online market places and cyber cafes

Highlights of the Amended Act

The newly amended act came with following highlights –

- It stresses on privacy issues and highlights information security.
- It elaborates Digital Signature.
- It clarifies rational security practices for corporate.
- It focuses on the role of Intermediaries.
- New faces of Cyber Crime were added.

Digital & Electronic Signatures

Digital Signature

A digital signature is a technique to validate the legitimacy of a digital message or a document. A valid digital signature provides the surety to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message. Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.

Electronic Signature

An electronic signature or e-signature, indicates either that a person who demands to have created a message is the one who created it.

A signature can be defined as a schematic script related with a person. A signature on a document is a sign that the person accepts the purposes recorded in the document. In many engineering companies digital seals are also required for another layer of authentication and security. Digital seals and signatures are same as handwritten signatures and stamped seals.

Digital Signature to Electronic Signature

Digital Signature was the term defined in the old I.T. Act, 2000. **Electronic Signature** is the term defined by the amended act (I.T. Act, 2008). The concept of Electronic Signature is broader than Digital Signature. Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

As per the amendment, verification of electronic record by electronic signature or electronic authentication technique shall be considered reliable.

According to the **United Nations Commission on International Trade Law (UNCITRAL)**, electronic authentication and signature methods may be classified into the following categories –

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those bases on the physical features of the user, i.e., biometrics.
- Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
- Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

According to the UNCITRAL MODEL LAW on Electronic Signatures, the following technologies are presently in use –

- Digital Signature within a public key infrastructure (PKI)
- Biometric Device
- PINs
- Passwords
- Scanned handwritten signature
- Signature by Digital Pen
- Clickable “OK” or “I Accept” or “I Agree” click boxes

Offences & Penalties

The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The law defines the offenses in a detailed manner along with the penalties for each category of offence.

Offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Cyber-crime usually includes the following –

- Unauthorized access of the computers

- Data diddling
- Virus/worms attack
- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking
- Email bombing
- Salami attacks
- Physically damaging computer system.

The offences included in the I.T. Act 2000 are as follows –

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Example

Offences Under The It Act 2000

Section 65. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation – For the purpose of this section “computer source code” means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Section	Offence	Punishment	Bailability and Congizability
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC.
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC
67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
69	Failure to assist the agency referred to in sub section (3) in regard interception or	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.

	monitoring or decryption of any information through any computer resource		
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.
70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable
71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

Object – The object of the section is to protect the “intellectual property” invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law

Essential ingredients of the section

- knowingly or intentionally concealing
- knowingly or intentionally destroying
- knowingly or intentionally altering
- knowingly or intentionally causing others to conceal
- knowingly or intentionally causing another to destroy
- knowingly or intentionally causing another to alter.

This section extends towards the Copyright Act and helps the companies to protect their source code of their programs.

Penalties – Section 65 is tried by any magistrate.

This is cognizable and non-bailable offence.

Penalties – Imprisonment up to 3 years and / or

Fine – Two lakh rupees.

The following table shows the offence and penalties against all the mentioned sections of the I.T. Act –

Compounding of Offences

As per Section 77-A of the I. T. Act, any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.

No offence shall be compounded if –

- *The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR*
- *Offence affects the socio-economic conditions of the country; OR*
- *Offence has been committed against a child below the age of 18 years; OR*
- *Offence has been committed against a woman.*

The person alleged of an offence under this Act may file an application for compounding in the Court. The offence will then be pending for trial and the provisions of Sections 265-B and 265-C of Cr. P.C. shall apply.

Cyber Law - FAQ

1. What is Cybercrime?

A. Cybercrime refers to all the activities done with criminal intent in cyberspace. Because of the anonymous nature of the internet, miscreants engage in a variety of criminal activities. The field of cybercrime is just emerging and new forms of criminal activities in cyberspace are coming to the forefront with each passing day.

2. Do we have an exhaustive definition of Cybercrime?

A. No, unfortunately we don't have an exhaustive definition of cybercrime. However, any online activity which basically offends human sensibilities can be regarded as a cybercrime.

3. What are the various categories of Cybercrimes?

A. Cybercrimes can be basically divided into three major categories –

- Cybercrimes against persons,
- Cybercrimes against property, and
- Cybercrimes against Government.

4. Tell us more about Cybercrimes against persons.

A. Cybercrimes committed against persons include various crimes like transmission of child pornography, harassment using e-mails and cyber-stalking. Posting and distributing obscene material is one of the most important Cybercrimes known today.

5. Is Cyber harassment also a Cybercrime?

A. Cyber harassment is a distinct cybercrime. Various kinds of harassment does occur in cyberspace. Harassment can be sexual, racial, religious, or other. Cyber harassment as a crime also brings us to another related area of violation of privacy of netizens. Violation of privacy of online citizens is a Cybercrime of a grave nature.

6. What are Cybercrimes against property?

A. Cybercrimes against all forms of property include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.

7. Is hacking a Cybercrime?

A. Hacking is amongst the gravest Cybercrimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer system without your knowledge and has tampered with precious confidential data.

The bitter truth is that no computer system in the world is hacking proof. It is unanimously agreed that any system, however secure it might look, can be hacked. The recent denial of service attacks seen over the popular commercial sites like E-bay, Yahoo, and Amazon are a new category of Cybercrimes which are slowly emerging as being extremely dangerous.

Using one's own programming abilities to gain unauthorized access to a computer or network is a very serious crime. Similarly, the creation and dissemination of harmful computer programs which do irreparable damage to computer systems is another kind of Cybercrime.

8. What is Cybercrime against Government?

A. Cyber Terrorism is one distinct example of cybercrime against government. The growth of Internet has shown that the medium of cyberspace is being used by individuals and groups to threaten the governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual hacks into a government or military maintained website.

9. Is there any comprehensive law on Cybercrime today?

A. As of now, we don't have any comprehensive laws on cybercrime anywhere in the world. This is the reason that the investigating agencies like FBI are finding the Cyberspace to be an extremely difficult terrain. Cybercrimes fall into that grey area of Internet law which is neither fully nor partially covered by the existing laws. However, countries are taking crucial measures to establish stringent laws on cybercrime.

10. Is there any recent case which demonstrates the importance of having a cyber law on cybercrime within the national jurisdictions of countries?

A. The most recent case of the virus "I love you" demonstrates the need for having cyber laws concerning cybercrimes in different national jurisdictions. At the time of the web publication of this feature, Reuters has reported that "The Philippines has yet to arrest the suspected creator of the 'Love Bug' computer virus because it lacks laws that deal with computer crime, a senior police officer said". The fact of the matter is that there are no laws relating to cybercrime in the Philippines.

11. What is Vishing?

A. Vishing is the criminal practice of using social influence over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to sensitive information such as credit card details from the public. The term is a combination of "Voice" and phishing.

12. What is Mail Fraud?

A. Mail fraud is an offense under United States federal law, which includes any scheme that attempts to unlawfully obtain money or valuables in which the postal system is used at any point in the commission of a criminal offense.

13. What is ID Spoofing?

A. It is the practice of using the telephone network to display a number on the recipient's Caller ID display which is not that of the actual originating station.

14. What is Cyber espionage?

A. It is the act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments, and enemies for military, political, or economic advantage using illegal exploitation methods on the internet.

15. What is the meaning of Sabotage?

A. Sabotage literally means willful damage to any machinery or materials or disruption of work. In the context of cyberspace, it is a threat to the existence of computers and satellites used by military activities

16. Name the democratic country in which The Cyber Defamation law was first introduced.

A. South Korea is the first democratic country in which this law was introduced first.

17. What are Bots?

A. Bots are one of the most sophisticated types of crime-ware facing the internet today. Bots earn their unique name by performing a wide variety of automated tasks on behalf of the cyber criminals. They play a part in "denial of service" attack in internet.

18. What are Trojans and Spyware?

A. Trojans and spyware are the tools a cyber-criminal might use to obtain unauthorized access and steal information from a victim as part of an attack.

19. What are Phishing and Pharming?

A. Phishing and Pharming are the most common ways to perform identity theft which is a form of cyber-crime in which criminals use the internet to steal personal information from others.

20. Mention some tips to prevent cyber-crimes.

- Read the latest ways hackers create phishing scams to gain access to your personal information.
- Install a firewall on your computer to keep unwanted threats and attacks to a minimum.

- Use caution while opening emails and clicking links. You should read carefully while downloading content from unverified sources.
- Create strong passwords for any websites where personal information is stored.