Table of Contents

Terms and Definitions

Read the following terms and make sure you know their meaning. Look up any that you are not comfortable with. On your own cheat sheet, jot down any additional terms you run across that struck you as new or odd.

Term	Definition
Hax0r	Hacker
Uber hacker	Good hacker
L33t	Sp33k Replacing characters to avoid filters
Full disclosure	Revealing vulnerabilities
Hacktivism	Hacking for a cause
Suicide Hacker	Hopes to be caught
Ethical Hacker	Hacks for defensive purposes
Penetration Test	Determine true security risks
Vulnerability Assessment	Basic idea of security levels
Vulnerabilty Researcher	Tracks down vulnerabilities
White hat	Hacks with permission
Grey hat	Believes in full disclosure
Black hat	Hacks without permission
White Box	A test everyone knows about
Grey Box	A test with a very specific goal but unspecific means
Black Box	A test no one knows is happening
Threat	Potential event
Vulnerability	Weakness
Exposure	Accessibility
Exploit	Act of attacking
TOE	Target of Evaluation
Rootkit	Hides processes that create backdoors
Botnet	Robot network that can be commanded remotely
Buffer Overflow	Hijack the execution steps of a program
Shrinkwrap Code	Reused code with vulnerabilities

Methodologies

This class tells a story, and understanding that story is far more important than memorizing these lists. Think about what actions are taken during each phase, and notice how they logically progress.

The phases of an attack

1. Reconnaissance Information gathering, physical and social engineering, locate network range
2. Scanning - Enumerating Live hosts, access points, accounts and policies, vulnerability assessment
3. Gaining Access Breech systems, plant malicious code, backdoors
4. Maintaining Access Rootkits, unpatched systems
5. Clearing Tracks IDS evasion, log manipulation, decoy traffic

Information Gathering

1. Unearth initial information what/ who is the target?
2. Locate the network range what is the attack surface?
3. Ascertain active machines what hosts are alive?
4. Open ports / access points how can they be accessed?
5. Detect operating systems what platform are they?
6. Uncover services on ports what software can be attacked?
7. Map the network Tie it all together, document, and form a strategy.

Legal Issues

Be able to describe the importance of each of these items. The exam will not go into depth on this, just be prepared to identify the issues.

United States

- Computer fraud and abuse act Addresses hacking activities
- 18 U.S.C. 1029 Possession of Access Devices
- 18 U.S.C. 1030 Fraud and Related Activity in Connection with Computers
- CAN-SPAM Defines legal email marketing
- SPY-Act Protects vendors monitoring for license enforcement
- DMCA - Digital Millennium Copyright Act Protects intellectual property
- SOX - Sarbanes Oxley Controls for corporate financial processes
- GLBA - Gramm-Leech Bliley Act Controls use of personal financial data
- HIPPA - Health Information Portability and Protection Act Privacy for medical records
- FERPA - Family Educational Rights and Privacy Act Protection for education records
- FISMA - Federal Information Security Management Act Government networks must have security standards

Europe

- Computer misuse act of 1990 Addresses hacking activities
- Human Rights Act of 1990 Ensures privacy rights

Domain Name Service

DNS is critical in the footprinting of a target network. It can sometimes save the attacker a lot of time, or at least corroborate other information that has been gathered. DNS is also a target for several types of attack.

Fields in the SOA record: (Time in seconds)

1882919 7200 3600 14400 2400
Serial Refresh Retry Expiry TTL

Requesting a zone transfer

```
nslookup; ls -d example.dom
```

```
dig @ns1.example.dom AXFR
host -t AXFR example.dom ns1.example.dom
```

Using Whois

```
whois example.dom
```

Regional Internet Registrars

- ARIN (North America)
- APNIC (Asia Pacific Region)
- LACNIC (Southern and Central America and Caribbean)
- RIPE NCC (Europe, the Middle East and Central Asia)
- AfriNIC (Africa)

Attacks against DNS servers

- Zone transfers Information gathering shortcut
- Zone poisoning Breach the primary server and alter the zone file to corrupt the domain
- Cache poisoning Send false answers to cache servers until they store them
- Reflection DoS Send bogus requests into a chain of servers that do recursive queries

Google Searching

An attacker will use Google to enumerate a target without ever touching it. The advanced search syntax is easy to use but can be quirky at times. It takes practice and experimentation.

Using Advanced Search

operator:keyword additional search terms

Advanced Operators

Site: Confines keywords to search only within a domain
Ext: File extension
Loc: Maps location
Intitle: Keywords in the title tag of the page
Allintitle: Any of the keywords can be in the title
Inurl: Keywords anywhere in the URL
Allinurl: Any of the keywords can be in the URL
Incache: Search Google cache only

Keyword combinations

passsword | passlist | username | user
login | logon
Administrator | Admin | Root
Prototype | Proto | Test | Example

Examples

site:intenseschool.com (ceh ecsa lpt)
intitle:index.of
allinurl:login logon
-ext:html -ext:htm -ext:asp -ext:aspx -ext:php

Nmap Scan Types

Nmap is the de-facto tool for foot printing networks. It is capable of finding live hosts, access points, fingerprinting operating systems, and verifying services. It also has important IDS evasion capabilities.

Discovery Scans

Option	Description
-sP	Ping
-sL	List Scan
-sO	Protocol
-sV	Verify
-sL	List scan

Normal Scans

```
Windows Linux
Option Desc Flags Open Closed Open Closed
-sT Connect S SA RA SA RA
-sS Stealth S SA RA SA RA
```

Inverse Scans

Windows Linux

```
Option Desc Flags Open Closed Open     Closed
-sN    Null   RA     RA     - RA
-sX    Xmas UPF RA RA - RA
-sF    Fin F RA RA - RA
-sA    Ack A R R R R
-sW    Window A R R R R
```

Other Important Nmap Options

-O Operating System Detection

Option Description

```
-A Enable OS detection, Version detection, Script scanning and Traceroute
-n Do not lookup DNS
-v verbose output
-T [0-5] Timing - 5 is faster
-P0 Do not ping first
-F Fast mode - Scan fewer ports than the default scan
```

TCP Flags

This test will have scenarios that require you demonstrate an understanding of TCP behavior including Nmap scan types. Be sure to know each of these combinations well.

TCP Flags

```
0 0 URG ACK PSH RST SYN FIN
```

TCP Handshake (Open Port)

```
Direction Binary Hex Flags
A -> B 00000010 0x02 S Seq = 1 Ack = 0
B -> A 00010010 0x12 A S Ack = 2 Seq = 10
A -> B 00010000 0x10 A Seq = 2 Ack = 11
```

TCP Handshake (Closed Port)

```
Direction Binary Hex Flags
A -> B 00000010 0x02 S Seq = 1 Ack = 0
B -> A 00010100 0x14 A R Ack = 2 Seq = 0
```

NMap Stealth Scan (Open Port)

```
Direction Binary Hex Flags
A -> B 00000010 0x02 S
B -> A 00010010 0x12 A S
A -> B 00000100 0x04 R
```

NMap Xmas Scan (Open Port)

```
Direction Binary Hex Flags
A -> B 00101001 0x29 U P F
No response from Linux hosts, R A from Windows
```

NMap ACK Scan

```
Direction Binary Hex Flags
A -> B 00010000 0x10 A
A -> B 00000100 0x04 R
Solaris will not respond on open ports
```

Ports and Protocols

These must be memorized! Also be prepared to convert them to hexadecimal representation in case they must be identified in a packet dump, log file, IDS rule, or a sniffer capture/display filter.

Protocols

1 ICMP
6 TCP
17 UDP
47 GRE
50 ESP
51 AH

Ports

20 - 21 FTP
22 SSH
23 Telnet
25 SMTP
42 WINS
53 DNS
80 - 81 -8080 HTTP
88 Kerberos
110 POP3
111 Portmapper (Linux)
119 NNTP
135 RPC-DCOM
137 - 138 - 139 SMB
143 IMAP
161 - 162 SNMP
389 LDAP
445 CIFS
1080 SOCKS5
3389 RDP
6667 IRC
14237 Palm Pilot Remote Sync

Trojan Horses

7777 Tini
12345 NetBus
27374 Sub7
31337 Back Orifice

Enumeration

Enumeration is the act of making a list of policies, user accounts, shares and other resources. This step happens just before vulnerability assessment and helps the attack put together the best strategy for gaining access.

Establishing a Null Session

```
net use \\[target ip]\IPC$ "" /user:""
```

Protecting Information Disclosure

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous
"0" is the default for Windows 2000 and gives up everything
"1" is the default for Windows 2003 and gives up less
"2" is the most secure setting but makes a machine not very cooperative with others

Microsoft SIDs

S-1-5-21-<………>-500 Built-in Local administrator
S-1-5-21-<………>-501 Built-in Local guest
S-1-5-21-<………>-512 Built-in Domain administrator
S-1-5-21-<………>-1000 Anything above 1000 are users that have been created

Ports involved with enumerations attacks

111 Linux Portmapper Service
42 WINS
88 Kerberos
135 Windows RPC-DCOM
137 NetBIOS Name Service
138 NetBIOS Datagram Service
139 NetBIOS Sessions
161 SNMP Agent
162 SNMP Traps
389 LDAP
445 CIFS (Common Internet File System)

Misc.

"public" and "private" default community SNMP strings
1.1.1.2.1.0.0.1.3.4.1.4 is an SNMP OID
ou=sales,cn=example... is an LDAP (LDIF) name string
fingerd the finger daemon was used in older UNIX systems

Password Cracking

This test will have scenarios that require you demonstrate an understanding of TCP behavior. Be sure to know each of these combinations well.

Types of password cracking techniques

Guessing is the most efficient, assuming information gathering before hand
Dictionary Based on a predetermined list of words
Brute Force trying every possible combination of characters and takes the longest
Hybrid A combination of all other attacks

LM Hashes

Every password is ultimately 14 characters long, split into two 7 character halved
Passwords that are less than 7 characters are easily identified in the SAM file (hash starts off with **AA3B4** and ends in **404EE**)

Rainbow Tables

"Time / Memory Trade off"" Less memory than a lookup, less computing than a brute force.
Salting the hash is a way to combat rainbow tables.

Cracking Effort

Weak passwords can be cracked in seconds
Strong passwords might take the lifetime of several universes to crack
Rainbow Tables Solve the "Time / Memory Trade Off"
DNA Distributed Network Architecture

Popular Cracking Tools

John the Ripper Command line tool that runs under both Windows and Linux
L0phtcrack Commercial tool
0phtcrack Open source tool that supports rainbow tables
Cain and Abel Powerful multipurpose tool that than sniff and crack passwords af many types

Trojans and Malware

The official definition is: A legitimate application that has been modified with malicious code. A Trojan horse is a social engineering technique. It masquerades as a legitimate download and injects the victim's host with an access point, or a client that can connect outbound to a server waiting remotely. They don't necessarily exploit a vulnerability unless privilege escalation is necessary. They provide a command environment for whoever connects to them that includes: File browsers, keyloggers, web cam viewer, and many additional tools.

Terms

- Wrapper or Binder Application used to combine a malicious binary and a legitimate program
- Rootkit Can be installed via Trojan, used to hide processes that create backdoor access
- HTTP Trojan Reverses a connection outbound through an HTTP or SHTTP tunnel
- Netcat Not really a Trojan, but often used in Trojan code to setup the listening socket
- Hoax Many legit tools are rumored to be Trojans but might not be
- Keylogger Records the keystrokes on the install host and saves them in a log

Famous Trojans

- Tini Small 3Kb file, uses port 7777
- Loki Used ICMP as a tunneling protocol

- Netbus One of the first RATs (Remote Authentication Trojan)
- Sub 7 Written in Delphi, expanded on what Netbus had demonstrated
- Back Orifice First modular malware, had the capabilities to be expanded on by outside authors
- Beast All in one Client / Server binary
- MoSucker Client could select the infection method for each binary
- Nuclear RAT Reverse connecting Trojan
- Monkey Shell Provides a powerful shell environment that can reverse connections and encrypt commands.

Detecting Trojans

- netstat / fport Command line tools for viewing open ports and connections
- tcpview GUI tool for viewing open ports and connections
- Process Viewer GUI tool for showing open processes including child processes
- Autoruns Lists all programs that will run on start up and where they are called from
- Hijack This Displays a list of unusual registry entries and files on the drive
- Spybot S&D Originally volunteer supported scanning and detection tool

Virus Trivia

No one is expecting you the student to stay on top of the 40k or so known malware variants that have been discovered. But there are a few that are significant for demonstrating the capabilities of this method of attack. Think of the malware mentions in the course as examples of what thousands of others have copied or improved upon.

Phases of an outbreak

Infection -> Spreading -> Attack

Virus Lifecycle

Design - > Replication -> Launch -> Detection -> Incorporation -> Elimination

Types of Viruses

- Boot Virus Infects the boot sector of floppies or hard disks
- Macro Virus Written in Microsoft Office Macro language
- Network Virus Spreads via network shares
- Stealth Virus Hides in a file, copies itself out to deliver payload
- Polymorphic Virus Encrypts itself
- Cavity Virus Hides in the empty areas of executables
- Tunneling Virus Trace interceptor programs that monitor OS Kernel requests
- Camouflage Virus Disguise themselves as legit files
- Multipartite Virus Infects via multiple vectors
- Metamorphic Virus rewrites itself

Famous Viruses

- Elk Cloner 1st virus
- Morris 1st worm
- I Love You VBScript worm, sent via email
- Melissa Macro virus
- Klez Mass mailer with its own SMTP engine
- Slammer Targets SQL server, total size of 376 bytes
- MyDoom Mass mailer, uses port 3127, attacks the hosts file
- MonteCarlo Memory resident, copies to the end on exe files

Sniffing

Social Engineering is the most powerful attack tool. It requires no equipment or technology, and often minimal expense. Only proper user education and awareness can prevent it and even then, errors in judgment can still be exploited.

Methods for defeating a switch

- Admin the switch If the password for the switch can be guessed, a port can be placed into monitor mode
- MAC Spoofing Set the MAC address of a NIC to the same value as another
- MAC Flooding Overwhelm the CAM table of the switch so it coverts to hub mode
- ARP Poisoning Inject incorrect information into the ARP caches of two or more endpoints.

Wireshark command line tools

- tshark Command line version of Wireshark
- dumpcap Captures traffic
- capinfos Reads a saved capture file and returns statistics about it

- editcap Edit and/or translate the format of capture files
- mergecap Merges multiple capture files into one
- text2pcap Generates a capture file from an ASCII hexdump of packets
- tcpflow Extracts data streams from dump files
- tcptrace Analyzes TCP conversations
- tcpreplay Can resend capture packets

TCPDump capture filters

Capture filters will be kept simple on the test. They look basically like English phrases. Analyze the examples below to get an idea.

- `host www.example.com and not (port 80 or port 25)`
- `port not 53 and not arp`
- `ip proto 1`
- `(tcp[2:2] > 1500 and tcp[2:2] < 1550`

Wireshark display filters

- Display filters work basically like: `proto.field operator value`
- Analyse the following examples:
- `tcp.flags == 0x29`
- `ip.addr != 192.168.1.1`
- `tcp.port eq 25 or icmp`
- `ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`
- `http.request.uri matches "login.html"`

MAC Addresses

Sniffing and defeating Ethernet switches requires an understanding of hardware addresses. Due to the risks involved with these local attacks, Intrusion Detection Systems are looking for too much ARP traffic or strange MAC addresses.

The MAC 48 Format

- A Media Access Control address is 48 bits
- The first 3 bytes of the MAC is a vendor code
- The other three bytes are arbitrarily assigned
- A broadcast MAC address is
- FF:FF:FF:FF:FF:FF

Addresses can be assigned in two ways

  - BIA - Burned in Address
  - OUI - Organizationally Unique Identifier
  - The two least significant bits of the first byte in the OUI address
  - nnnnnn0n = universally administered address
  - nnnnnn1n = administratively assigned
  - nnnnnnn0 = Unicast traffic
  - nnnnnnn1 = Multicast traffic

Internet Protocol

- Internet protocol is responsible for packaging datagrams for delivery between networks. It is a "best effort" protocol with no error control or correction. For more information read RFC 791
- Internet Protocol Header
- Checklist of items to concentrate on:
- How IPIDs work
- How the fragmentation works
- How the TTL works
- Protocol IDs

- Basic IP addressing principles
- DoS attacks relating to IP

Internet Control Message Protocol

- ICMP is a transport protocol that creates message datagrams that can be exchanged by network hosts for troubleshooting, error reporting, and information. For more information read RFC 792
- For a complete list of type and codes visit http://www.spirit.com/Resources/icmp.html
- ICMP Header Example:
- Type Code Description
- 0 0 Echo Reply
- 3 Destination Unreachable
- 3 13 Administratively Prohibited
- 8 0 Echo Request
- 5 0 Redirect
- 11 0 Time Exceeded
- 13 - Timestamp Request
- Don't forget!!
- Type 3 Code 13 means administratively prohibited

User Datagram Protocol

User Datagram Protocol is a simple fast transport protocol that is used for its low overhead in situations where error correction and flow control is not needed, such as short bursts of messages. UDP is difficult to firewall off effectively because it is stateless. For more information read RFC 768

- User Datagram Protocol
- Checklist of items to concentrate on:
- Port addresses and ranges
- How ICMP and UDP assist each other
- UDP based Denial of Service Attacks

Transmission Control Message Protocol

TCP provides guaranteed transport and flow control of layer 5-7 messages. Along with IP, ICMP, and UDP, a good solid understanding of this protocol is critical for understanding: Scanning, Firewalls, Intrusion Detection, and various types of DoS attacks. For more information read RFC 793

Transmission Control Protocol

Checklist of items to concentrate on:

- Port addresses and ranges
- Order of the six flags
- How the handshake works
- How the sequence numbers work
- How session hijacking works
- Denial of service attacks related to TCP

Social Engineering

Social Engineering is the most powerful attack tool. It requires no equipment or technology, and often minimal expense. Only proper user education and awareness can prevent it and even then, errors in judgment can still be exploited.

The principles of Social Engineering

- Authority An intimidating presence

- Scarcity Create the perception of loss or lack of access to a resource
- Liking Charm and charisma
- Reciprocation The victim believes they owe the attacker a favor
- Consistency Appealing the a victims true feelings and opinions
- Social Validation Compliments and praise

Types of Social Engineers

- Insider Associates Have limited authorized access, and escalate privileges from there.
- Insider Affiliates Are insiders by virtue of an affiliation, they spoof the identity of the insider.
- Outsider Affiliates are non-trusted outsiders that use an access point that was left open.

DoS and DDoS

Denial of Services and Distributed Denial of Service attacks are embarrassing and inconvenient. They are extremely difficult to prevent from being attempted. The best defense is a well-designed network that is hard to overwhelm.

DoS Methods

- Buffer Overflows Crashes applications or services
- Smurf Spoofed traffic sent to the broadcast address of a network
- Fraggle UDP version of the Smurf, usually bouncing Chargen traffic off Echo ports
- Ping of Death Packet larger than the 64k limit
- Teardrop Offset values modified to cause fragments to overlap during reassembly, results in short packet
- Unnamed Offset values modified to cause gaps between fragments, results in long packets
- Syn Flood SYN flags sent to open ports, no completion of the hansdshake
- Land Traffic sent to a victim spoofing itselft as the source, results in ACK storms
- Winnuke Sends TCP traffic with the URG flag set, causes CPU utilization to peak

Dos Tools

- Jolt2 Floods with invalid traffic results in 100% CPU utilization
- Land and La Tierra Executes teardrop and land attacks
- Targa Provides a menu of several DoS attacks
- Blast20 Also considered to be a web server load tester
- Crazy Pinger ICMP flooder
- UDP Flood UDP flooder written by Foundstone

DDos Attacks

- Botnets - Command and Control Center communicates with "Handlers" which in term communicate with Zombies. The handlers and zombies are machines infected with malware. The C&CC is either a chatroom on IRC, or can even be a distributed system of infected machines.

DDoS Tools

- Trinoo One of the first to demonstrate "Master/slave" DDoS attacks
- Tribal Flood Network Could launch several DoS attacks from distributed positions at the same time
- TFN2K Bug fixes and updates to the original TFN
- Stacheldraht Means "Barbed Wire" in German
- Agobot A modular IRC bot, many derivatives have been created from this code

- Nuclear Bot Developed by "Nuclear Winter Crew" and written in Delphi, many features

Buffer Overflows

It isn't necessary to become a "C" programmer to pass the test, but several basic concepts and terms are critical in the understanding of BO scripts and the detection of BO attacks.

Terminology

- Stack Memory place for short term processing
- Heap Memory space for long term program execution
- Push "Push" new instructions onto the stack
- Pop "Pop" instructions off the stack when processed
- EIP Execute Instruction Pointer, memory address of next instruction to be executed
- NOOP A "do nothing" instruction that wastes a clock cycle
- NOOP Sled Placed in a buffer overflow exploit to aid in running the payload

Dangerous Functions

The following functions are dangerous because they do not check the size of the destination buffers:

- gets()
- strcpy()
- strcat()
- printf()
- The >> operator is also dangerous for the same reason

Canary bytes

- String terminating characters:
- LF Line Feed
- CR Carriage Return
- NULL Null
- EOF End of File
- A randomly chosen value can also be placed at the end of a stack and checked.

Recognizing a buffer overflow attempt

```
Apr 5 02:02:09 [3432] : nops: 62.32.54.123:3211 -> 192.168.3.4:135
0x90/0x90/0x90/0x90/0x90/0x90/0x90/0x90/0x90/
```

HTTP and URLs

HTTP is the protocol for the World Wide Web. The client (web browser) sends request to the server (Apache, IIS) which is turn passes the request to an application. There are several attack types that are possible in this exchange since all of these components can have vulnerabilities.

HTTP Error Codes

- 200 Series Everything is OK
- 400 Series Could not provide requested resource (page not found, moved, authentication failure)
- 500 Series Could not process request (script error, database connection error)

ASCII Characters

- . %2E
- / %2F
- < %3C
- %3E
- Uniform Resource Locators (URL)
- Protocol FQDN Resource Path Query String

- http://www.example.com/folder/directory/page.asp?var=something&foo=some+other+thing
- Representing IP Addresses
- Dotted Quad http://192.168.100.125
- Hex Quad http://0xC0.0xA8.0x64.0x7D
- Decimal http://3232261245
- Converting Dotted Quad to Decimal (using above example)
- 192.168.100.125

Formula (256^3 * 192) + (256^2 * 168) + (256^1 * 100) + (256^0 * 125)
Simplified (16777216 * 192) + (65536 * 168) + (256 * 100) + 125
Simplified again 3221225472 + 11010048 + 25600 + 125 =
Answer 3232261245

Wireless Technology

Wireless is fast becoming the network technology of choice because it is cheap and easy. It is also a hub-bed environment that can leak signals for miles. Configuring wireless technologies is an often misunderstood process, and often leaves many opportunities available for attack.

802.11

Spec Distance Speed Freq

- 802.11a 30M 54Mbps 5Ghz
- 802.11b 100M 11Mbps 2.4Ghz
- 802.11g 100M 54Mbps 2.4Ghz
- 802.11n 125M 600Mbps 5Ghz
- 802.11i is a rewrite of WEP called WPA/TKIP
- 802.11ac 30M with Theoretical Speed limitation of 1 Gbps.

Other Wireless Technology

• BlueTooth	Personal Area Network
• Zigbee	Designed for Longer Battery life

Wireless Security

- WEP Uses RC4 for the stream cipher with a 24b initialization vector
- Key sizes are 40b or 104b
- WPA Uses RC4 for the stream cipher but supports longer keys
- WPA/TKIP Changes the IV with each frame and includes key mixing
- WPA2 Uses AES as the stream cipher and includes all the features of TKIP
- OSA Open Systems Authentication is a non-protected AP that broadcasts its SSID
- PSK Pre-Shared Key is protected by an encryption standard

Terms and Tools

- Wardriving Driving around with portable equipment and locating wireless networks
- Warchalking Writing symbols on the sidewalk or buildings communicating found networks
- Jamming Producing white noise signals that overpower the Wifi networks
- Netstumbler Finds wireless networks, SSIDS, and channels
- Ministumbler for the pocket pc
- Macstumbler for the Macintosh
- AirPcap Hardware tools for wardriving, WEP cracking, and sniffing
- Airopeek Sniffer that specializes in wireless traffic
- AircrackNG WEP cracker
- Airsnort Another WEP cracker

- CoWPAtty WPA offline brute force cracker

Wireless Technology

Wireless is fast becoming the network technology of choice because it is cheap and easy. It is also a hubbed environment that can leak signals for miles. Configuring wireless technologies is an often misunderstood process, and often leaves many opportunities available for attack.

WLAN Channels

Each channel increments by .005Mhz

Wardriving Symbols

Cryptography

Cryptography is assumed pre-requisite for this class. Its still a good idea to review some core terminology before the exam.

Terms and Definitions

- Plaint Text The data set before encryption
- Cipher Text The result of encryption
- Cryptanalysis Attempting to "break" and encryption algorithm
- Cryptography Obscuring the meaning of a message
- Steganography Hiding a message within another
- Salt Ensures different keys are created each time
- Initialization Vector Change the characteristics of the key each time it is reused

Types of Cryptography

- Symmetric Single key both encrypts and decrypts
- Asymmetric A pair of keys, public and private are mathematically associated
- One encrypts and the other decrypts, private key is always a secret
- One-Way Hash Cannot be reversed, only brute forced
- Used to represent data, sometimes called "Digital Fingerprint" or "Message Digest".

Symmetric Algorithms

- DES Block 56 bit key used in LM Hash password storage
- 3DES Block 128 bit key used in NTLM
- RC4 Stream Used in WEP
- AES Stream Used in WPA2

Asymmetric Algorithms

- RSA Asymmetric Used in SSL/TLS
- Elliptic Curve Asymmetric Used in TLS for portable devices

One-Way Hashes

- MD5 One Way Hash 128b hash value, used for integrity checks
- SHA-1 One Way Hash 160b hash value, stronger than MD5

Linux Operating System

While it is not necessary to be a Linux administrator or developer to pass this test, there is some assumed knowledge of a few basics, particularly pertaining to Security issues.

Linux File System

- / Root of the file system

- /var Variable data, log files are found here
- /bin Binaries, commands for users
- /sbin System Binaries, commands for administration
- /root Home directory for the root user
- /home Directory for all home folders for non-privileged users
- /boot Stores the Linux Kernel image and other boot files
- /proc Direct access to the Linux kernel
- /dev direct access to hardware storage devices
- /mnt place to mount devices on onto user mode file system

Identifying Users and Processes

- INIT process ID 1
- Root UID, GID 0
- Accounts for services 1-999
- All other users Above 1000

MAC Times

- Modify Modify the contents of the file
- Access When the files was accessed last
- Change Metadata change
- Use the "touch -mac filename" command to update all of them at the same time

Permissions

- User Group Others
- R 400 040 004
- W 200 020 002
- X 100 010 001
- SUID 4000
- SGID 2000
- Examples
- User can RWX, Group can RW and Others can R 764
- User can RW, Group can R and others can R 644
- SUID bit set, User and group can RWX 4770
- SUID and GUID bit set, all users can RWX 6777

Linux Commands

Practice the following commands and be able to recognize them in a shell script or log file. Always remember to "manpage" a command. Get used to reading about options and usage.

Command Notable Options Description

Using Linux (Basic Commands)

- man / Manual pages
- ls -l Looksee into a directory
- cd Change directory
- pwd Print working directory
- touch -macr Create a file or update its attributes
- mv Move a file
- rm Remove a file
- mkdir Make a directory
- grep String search utility
- more Paginate the output to the console
- nano Simple text editor
- vi Powerful text editor

- gcc -o Compile from source code

Administration and Troubleshooting

- dd Create an image file of a volume or device
- file Query a file for its type
- netstat List state of TCP/UDP ports
- dig DNS Zone transfer
- host Look up DNS records
- lsof List open files
- ps aux View process list
- rpcinfo Enumerate portmapper
- smbclient -L List or use SMB shares
- md5sum Calculate MD5 hash

Security tools that run best under Linux (add your own to this list !)

- mailsnarf, urlsnarf, filesnarf
- ettercap -q -z MiTM sniffer
- nmap Network mapper
- hping -c count -S Packet crafter
- snort Network Intrusion Detection
- iptables -P -A -j --sport --dport -p Kernel mode firewall
- kismet WiFi scanner and sniffer
- nikto Web vulnerability scanner
- maltego Information gathering
- tcpdump -i Command line sniffer
- firewalk -u Firewall enumerator
- nc -l -e -v "Swiss army knife"

Firewalls and IPTables

The Linux firewall makes a good teaching example because once you understand it, all firewalls are easier. It is free, open source, and widely available.

Types of Firewalls

- Packet filter The simplest form of filtering, looks only at layer 3 and 4
- Stateful Inspection Understands directionality and established sockets
- Circuit Level Gateway Translates sequence numbers along with addresses and ports
- Application Proxy Deep packet inspection all the way into the payload

Attacking Firewalls

- TCP Flag combinations While some flag combinations are filtered, others may pass
- Firewalking Enumerating ACLs on a filter
- ACK floods Overwhelming an SPI firewall into thinking the traffic should pass
- 0th fragment Host based firewalls only: The 0th fragment has TCP data, the others do not
- ICMP redirection Hijack local hosts to use the attackers host as a gateway, the traffic can be altered or observed
- Tunneling and port redirection Hiding data inside encapsulation

Setting up a network firewall

A host based firewall only protect the host, a network based firewall must also be a router. In Linux, the Kernel must be told to forward packets:

```
        echo 1 > /proc/sys/net/ipv4/ip_forward
```

There are several default tables for a forwarding firewall to be aware of:

- INPUT

- OUTPUT
- FORWARD
- ACCEPT
- NAT

IPTables Example: Defending against a Smurf attack

- iptables -A FORWARD -p tcp -s 0/0 -d x.y.z.m/32 --destination-port 25 --syn -j ACCEPT iptables -A FORWARD -p tcp -s 0/0 -d x.y.z.w/32 --destination-port 80 --syn -j ACCEPT iptables -A FORWARD -p tcp -s 0/0 -d x.y.z.w/32 --destination-port 443 --syn -j ACCEPTiptables -A FORWARD -p tcp -s 0/0 -d 0/0 --destination-port 22 --syn -j ACCEPT

IDS and Snort

Intrusion Detection Systems are a key technology for protecting a network. Attackers can also use them to look to look for very specific events on the network such as logins or other attackers. As a counterpart to firewalls, IDS is a great way to bring together the many of the concepts that been discussed in this course including; sniffing, scanning, and the four major protocols (IP, ICMP, TCP, UDP).

Types of IDS

Host Based Active Listens on the hosts
Network Based Passive Listens on the network

Detection Engines

Signature Analysis Real time Uses a rules based approach
Anomaly Analysis Real time requires a baseline to compare with
Statistical Analysis Not real time Analysis of patterns and occurrences

Evasion Techniques

Encryption IDS cannot decrypt data to look at it
Fragmentation IDS might be too busy perceiving together traffic and start ignoring some
Decoy traffic false positives can confuse investigators

Snort rules

Snort rules take on the following syntax:

```
action protocol address prot -> | <> address prot (option:value;
option:value;)
```

Starting Snort

Display layer 2 and 7 to the console, use our own rules file and log here

```
snort -dve -c ./rules.local -l .
```

Examples of Snort rules

The simplest rule

```
alert tcp any any -> any any (msg:”Sample alert”; sid:1000000;)
```

Detecting a simple signature

```
alert tcp 192.168.1.6 any -> 192.168.1.5 139 \ (msg: “Possible
SMBDie Attempt"; content:”|5c 50 49 50 45|”; sid:1000000;)
```

Dynamic rules (May be phased out in favor of a new method called "tagging")

```
activate tcp any any -> any 21 (content:"Login"; activates:1;
sid:1000000;)
dynamic tcp any any -> any 21 (activated_by: 1; count:100;)
```

Command Line Tools

The key to becoming comfortable with command line tools is to practice saying in plain language what a command is trying to instruct the computer to do. It's hard to memorize switches and far easier to understand what a tool does. As you study and find more examples, add them to this list.

NMap

```
nmap -sT -T5 -n -p 1-100 192.168.1.1
```

Use nmap to run a connect scan at a fast rate without DNS resolution to ports 1-100 at host 192.168.1.1

Netcat

```
nc -v -z -w 2 192.168.1.1
```

Use netcat, show on the console a scan that sends packets every 2 seconds to host 192.168.1.1

Tcpdump

```
tcpdump -i eth0 -v -X ip proto 1
```

Use tcpdump to listen on interface eth0 andsdisplay layer 2 and 7 for ICMP traffic

Snort

```
snort -vde -c my.rules -l .
```

Use snort and show on the console layer 2 and 7 data using configuration file my.rules and log in this directory.

Hping

```
hping3 -I eth0 -c 10 -a 2.2.2.2 -t 100 192.168.3.6
```

Use hping3 on eth0 and send 10 packets spoofing 2.2.2.2 and a TTL of 100 to host 192.168.3.6

Iptables

```
iptables –A FORWARD –j ACCEPT –p tcp --dport 80
```

Use iptables and append the forward table with a rule that will jump to the accept table when tcp traffic that has a destination port of 80 is noticed.

Syntax Recognition

The exam requires that you can recognize what an attack looks like from a log file. The following are examples that can be used to help explain the principles of each type of attack:

Directory Traversal

```
http://www.example.com/scripts/../../../../winnt/system32/cmd.exe?c+dir+c:
```

XSS (Cross Site Scripting)

```
http://www.example.com/pages/form.asp?foo=%3Cscript%3Ealert("Hacked")%3C/scri
pt%3Elang=
```

SQL Injection

```
http://www.example.com/pages/form.asp?foo=blah'+or+1+=+1+--
http://www.example.com/pages/form.asp?foo=%27%3B+insert+into+usertable+("some
thing")%3B+--lang=
blah' or 1 = 1 --
```

Nimda Virus

```
http://www.example.com/MSADC/../../../../winnt/system32/cmd.exe?c+dir+c:
```

Code Red

```
GET/default.ida?NNNNNNNNNNN%u9090%u688%u8b00%u0000%u00=a HTTP/1.0
```

SNMP OID

```
1.1.1.0.2.3.1.2.4.1.5.3.0.1
```

Buffer overflow attempt

```
Apr 5 02:02:09 [3432] : nops: 62.32.54.123:3211 -> 192.168.3.4:135
0x90/0x90/0x90/0x90/0x90/0x90/0x90/0x90/0x90/
```

Zone Transfer

```
Apr 5 02:02:09 [3432] : AXFR: 143.32.4.129:4865 -> 192.168.3.4:53
```

Enumerate email accounts

```
Apr 5 02:02:09 [3432] : VRFY: 78.34.65.45:5674 -> 192.168.3.4:25
```

Snort Signature Rule

```
Alert tcp any any -> any any (msg:"Test Rule"; sid:1000000;)
```

IPTables Rule

```
iptables -A FORWARD -j ACCEPT -p udp --dport 53
```

Capture Filter

```
host 192.168.1.1 and host 192.168.1.2 ip proto 1
```

Display Filter

```
ip.addr == 192.168.1.1 && tcp.flags == 0x29
```