CERTIFIED ETHICAL HACKER REVIEW

INTRODUCTION

OSI Reference Model

Layer	PDU	Description
Application	Data	Use protocols allowing user to access information
Presentation		Put message in standard format
Session		Open, maintain, and close a session
Transport	Segment	Reliable delivery, flow control, error correction, message confirmation, break messages into manageable pieces
Network	Packet	Separating physical address from network address. Interface with Internet. Determine path to reach destination
Data Link	Frame	How to designate who gets what message? How to keep messages separate?
Physical	Bit	What medium to use when communicate? What do I send so that it makes sense on the other side?

TCP/IP Model

Layer	Protocol
Application	HTTP, FTP, SNMP, SMTP, DNS, POP, IMAP, Telnet, SSH, DHCP…
Transport	TCP, UDP
Internet	IP, ICMP
Network Access	ARP, L2TP, STP, HDLC, FDDI

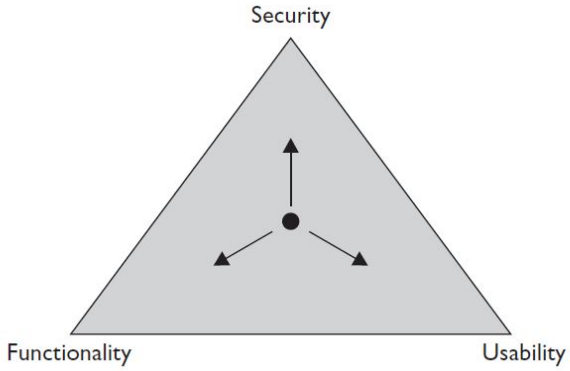


FIGURE 2: SECURITY LIMITATIONS

FIGURE 1: RISK ASSESMENT MATRIX

Asset – item of economic value owned by an organization or individual

Threat – any agent, circumstance, or situation that could cause harm or loss to an IT asset

- Natural
- Human
- Physical security
- Network
- Host
- Application

Vulnerability – any weakness that could be exploited by a threat to cause damage to an asset

Security controls – countermeasures security personnel put into place to minimize risk as much as possible

- Physical
- Technical
- Operational/Administrative

Preventative control – security measure put into place to prevent errors or incidents from occurring in the first place

Example: Authentication

Detective control – security measure put into place to identify an incident has occurred or is in progress

Corrective control – designed for after the event to limit the extent of damage and aid swift recovery

Example: Backups

IT Security (CIA)

- **Confidentiality** – addressing the secrecy and privacy of information
- **Integrity** – methods and actions taken to protect the information from unauthorized alteration or revision
- **Availability** – communication systems and data being ready for use when legitimate users need them

Access Control Systems

- **Mandatory Access Control** (MAC) – security policy is controlled by a security administrator, users can't set access controls themselves
- **Discretionary Access Control** (DAC) – allows users to set access controls on the resources they own or control

Information Security Policy – defines what is allowed, not allowed, and what the consequences are for misbehavior in regard to resources on the corporate network

- Paranoid
- Prudent
- Permissive
- Promiscuous

Standards – mandatory rules used to achieve consistency

Baselines – provide the minimum security level necessary

Guidelines – flexible recommended actions users are to take in event there is no standard to follow

Procedures – detailed step-by-step instructions for accomplishing a task or goal

Hacker Types:

- **White Hat** – ethical hackers hired by a customer for specific goal of testing and improving security or for other defensive purposes
- **Black Hat** – crackers, illegally using their skills for either personal gain or malicious intent
  - Difference between White hat: White Hats make prior agreement with client
- **Gray Hat** – something in between, maybe hacking without permission but for the good of the client
- **Hacktivist** – hacking with political agenda, cyber terrorist

Attack Types:

- Operating system
- Application-level
- Shrink-wrap code
- Misconfiguration

Hacking Phases:

1. **Reconnaissance** – gathering evidence and information on the targets (Passive)
2. **Scanning and Enumeration** – take information from recon and apply tools and techniques to gather more in-depth information on the targets (Active)
3. **Gaining Access** – attack leveled against the target
4. **Maintaining Access** – attempt to ensure they have a way back into the machine or system
5. **Covering Tracks** - conceal success and avoid detection

Penetration Testing

- **Black Box** – no knowledge of the target of evaluation
- **White Box** – full knowledge of network, system, and infrastructure in test (intended to simulate an internal hacker with elevated privileges
- **Gray Box** – something in between
- **Internal** – start test within the network
- **External** – start test outside the network, often over the internet

RECONNAISSANCE

Passive Footprinting – gather information on the target using publicly available sources

Active Footprinting – interact with target to get information (social engineering)

Domain Naming System (DNS) – provides a name-to-IP-address (and vice-versa) mapping service

DNS Record Types		Description
SRV	Service	Generalized service location record, used for newer protocols
SOA	Start of Authority	Specifies **authoritative** info about a DNS zone
PTR	Pointer	(when queried) DNS processing stops and name is returned
NS	Name Server	Delegates a DNS zone to use given authoritative name servers
MX	Mail Exchange	Maps a domain name to list of message transfer agents
CNAME	Canonical Name	Provide for aliases within the zone
A	Address	Provide IP-address-to-name mappings

SOA contains:

- Source Host
- Contact Email
- Serial Number
- Refresh Time
- Retry Time
- Expire Time
- Time to live (TTL)

DNS Poisoning – change the cache on the local name server to point to a bogus server instead of the real address

NSLookup – command line tool to query DNS servers

Syntax: nslookup [-options] {hostname | [-server]}

Tracert – command line tool to trace route (network mapping)

Advanced Google Operators
cache:URL
filetype:type
index of / string
intitle: string
inurl: string
link: string
site: domain_or_web_page_string

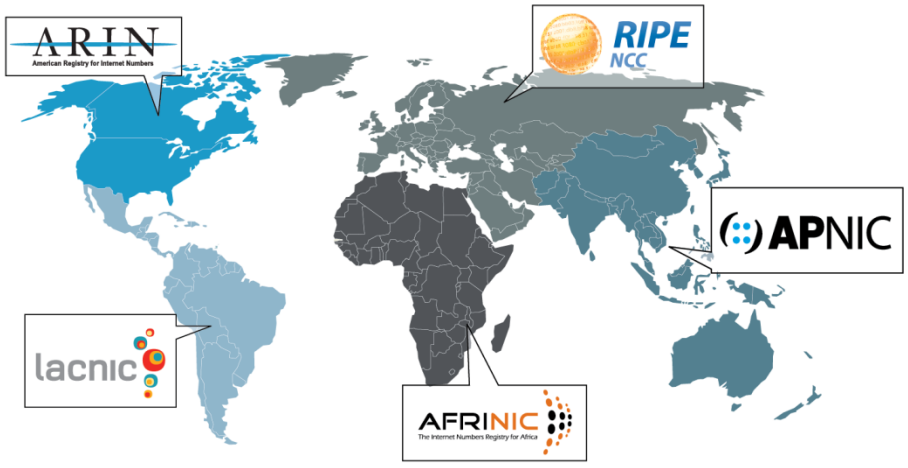


FIGURE 3: REGIONAL DNS REGISTRIES

SCANNING

Scanning – the process of discovering systems on the network and taking a look at what open ports and applications may be running

Scanning Methodology

1. Check for live systems
2. Check for open ports
3. Scan beyond IDS
4. Perform banner grabbing
5. Scan for vulnerabilities
6. Draw network diagrams
7. Prepare proxies

UDP – Connectionless communication, "Fire and Forget", datagram

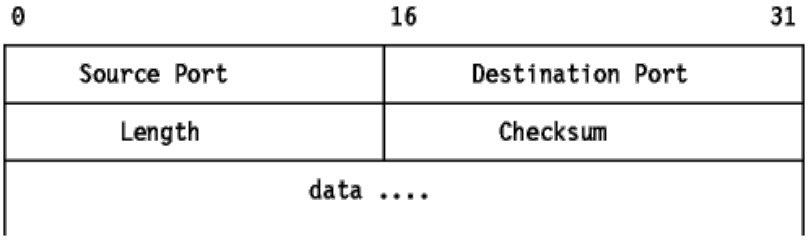


FIGURE 4: UDP DATAGRAM

TCP – Connection oriented communication (Three-Way Handshake), segment

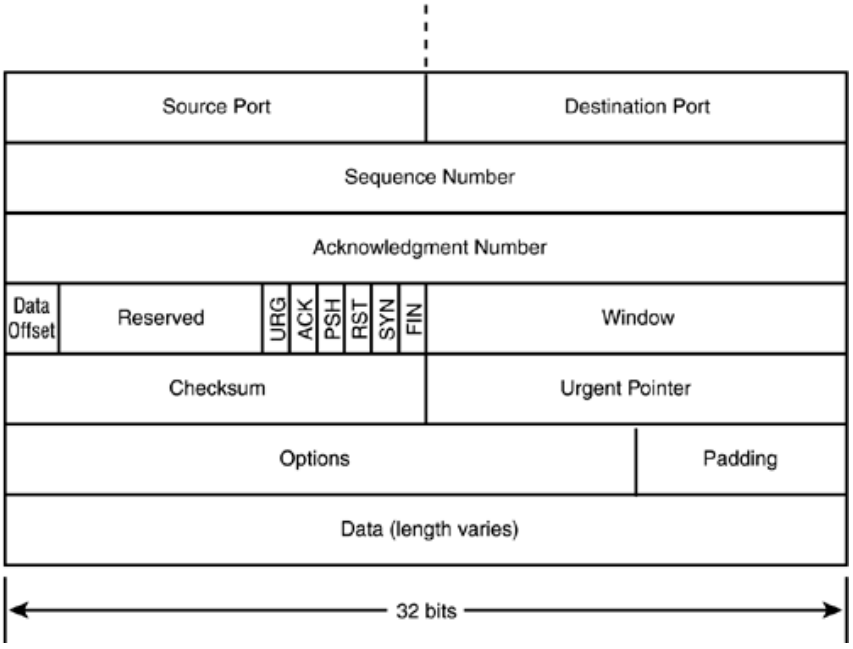


FIGURE 5: TCP SEGMENT

TCP Header Flags		Description
SYN	Synchronize	Initiates communication, indicates negotiation of parameters and sequence numbers
ACK	Acknowledgement	
RST	Reset	Forces termination of communications
FIN	Finish	Signifies ordered close to communications
PSH	Push	Force delivery of data without concern for buffering
URG	Urgent	

Important Port Numbers	
20/21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS (UPD = lookup, TCP = Zone Transfer)
67	DHCP
69	TFTP
80	HTTP
110	POP3
123 (UDP)	NTP
135	RPC
137-139	NetBIOS
143	IMAP
161-162	SNMP
389	LDAP
443	HTTPS
445	SMB
0-1023	Well Known
1024-49151	Registered
49152-65535	Dynamic

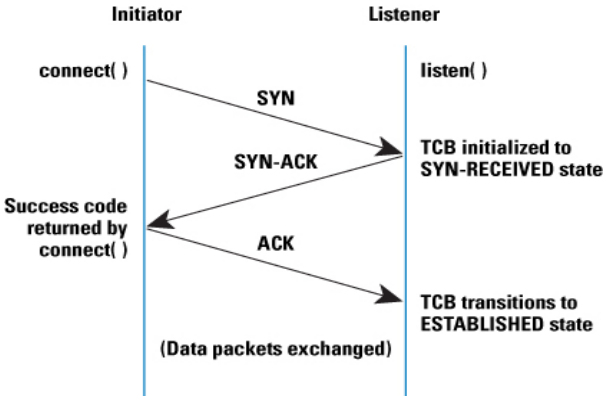


FIGURE 6: THREE WAY HANDSHAKE

Checking for live systems:

- To check which IP's are "Live", use **ICMP error messaging**, because IP is a connectionless protocol

Error Code	Error Message	Description
0	Echo Reply	Answer to Type 8 Echo Request
3	Destination Unreachable	Host or network cannot be reached
	0 Destination network unreachable	
	1 Destination host unreachable	
	6 Network unknown	
	7 Host unknown	
	9 Network administratively prohibited	
	10 Host administratively prohibited	
	13 Communication administratively prohibited	
4	Source Quench	Congestion control message
5	Redirect	Sent when there are two or more gateways available for the sender to use and the best route available to the destination is not the configured default gateway
8	Echo request	Ping message requesting Echo reply
11	Time Exceeded	Packet took too long to be routed to destination

Port Scanning (NMAP)

Syntax: nmap <scan options> <target>

NMAP Switches			
-sA	ACK scan	**-PI**	ICMP Ping
-sF	FIN scan	**-PO**	No Ping
-sI	IDLE scan	**-PS**	SYN Ping
-sL	DNS scan	**-PT**	TCP Ping
-sN	NULL scan	**-oN**	Normal output
-sO	Protocol scan	**-0X**	XML output
-sP	Ping scan	**-T0**	Serial, slowest scan
-sR	RPC scan	**-T1**	Serial, slower scan
-sS	SYN scan	**-T2**	Serial, normal speed scan
-sT	TCP Connect scan	**-T3**	Parallel, normal speed scan
-sW	Windows scan	**-T4**	Parallel, fast scan
-sX	XMAS scan		

Source routing – specified the route the packet will take to a destination, regardless of what the route tables between the two systems say

Scan Types		Response if Open	Response if Closed
Full Open Scan (TCP Connect)	Runs through full three-way handshake connection on all ports	SYN/ACK	RST
SYN (Half Open Scan)	Just send SYN packets	SYN/ACK	RST
FIN	Sends FIN packets	No Response	RST/ACK
XMAS	All Flags	No Response	RST
ACK (testing firewall)	Use ICMP destination unreachable messages to determine open ports	RST	No Response
IDLE	Use spoofed IP address with SYN scan (send SYN to target spoofing zombie, response is sent to zombie, then send SYN to zombie to check IPID)	Zombie IPID incremented by 2	Zombie IPID incremented by 1
NULL	No flags	No Response	RST/ACK

ENUMERATION

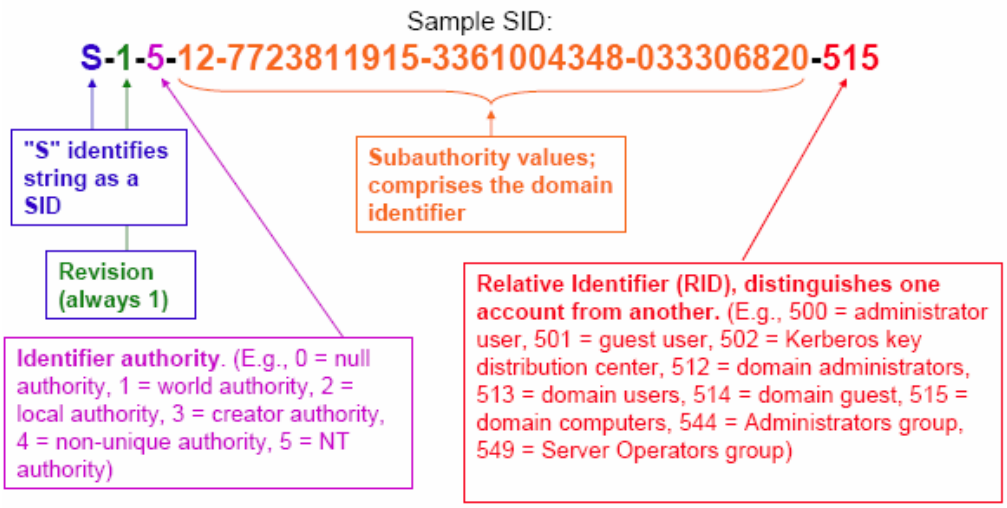
User rights – granted via an account's membership within a group and determine which system tasks an account is allowed to perform

Permissions – used to determine which resources an account has access to

Security identifier (SID) – identifies user, group, and computer accounts

Resource Identifier (RID) - portion of the SID identifying a specific user, computer, or domain

Windows RID Descriptions	
500	Administrator
501	Guest
1001	First user on system



Banner Grabbing (Fingerprinting) – send an unsolicited request to an open port to see what, if any, default message (banner) is returned, with the goal of finding out what OS is running

Example: Telnet runs on port 23, but you can telnet specifying any port just to test for connectivity

Syntax: telnet <IP> <port>

Example: Netcat

Syntax: nc <flags> <IP> <port>

Null Session Enumeration – log in to a system with no user ID and password at all

Note: requires TCP ports 135, 137, 139, and 445 to work

NetBIOS Enumeration – (Network Basic Input/Output System), hosts information about all the machines within the domain or TCP/IP network segment

Syntax: nbtstat

Result: Name_ _Code_ _Type_ _Status

NetBIOS Codes	
<00>	Identifies computer's name and the workgroup it's assigned to
<20>	File and print sharing is turned on
<1E>	Participates in NetBIOS browser elections
<1D>	This machine is currently the master browser for this segment (domain master browser)
<1C>	Domain controller
<1B>	Master browser for subnet

SNIFFING

Network Interface Card (NIC) – works by listening on a medium, waiting to hear a MAC address that matches its own, then takes that message to the processor

Sniffer – tells NIC to grab every message, not just those with the matching address (promiscuous mode)

Collision domain – composed of all the machines sharing a transport medium (only one can talk at a time)

Address Resolution Protocol (ARP) – used by the NIC when a frame is being built which asks "Does anyone have a physical address for the IP address I have here in this packet? If so, please let me know so I can build a frame and send it on"

IPv4 – expressed in decimal, consisting of four octets, separated by period

Example: 192.168.60.11

IPv6 – expressed in hexadecimal, consisting of eight quartets, separated by colon

Example: 2001:09bd:0000:0000:0000:ff00:0052:1829

Truncation (eliminate leading zeros): 2001:09bd:0:0:0:ff00:52:1829

Truncation (replace consecutive zeros with ::): 2001:09bd::ff00:52:1829

- IPv6 does not use a broadcast prefix

IPv6 address types:

- **Unicast** – addressed for one, intended to be received by one
- **Multicast** – addressed for many, intended to be received by many (broadcast)
- **Anycast** – addressed for many, intended to be received by one (closest)

IPv6 scopes:

- **Link local** – applies to only hosts on the same subnet
- **Site local** – applies to only hosts within the same organization
- **Global** – includes everything

Passive Sniffing – if connected to a Hub (routes all messages to all connections), sniffing doesn't require anything except reading packets

Active Sniffing – if connected to a Switch (routes messages only to their intended recipients), a technique needs to be used to observe the communication

- **Port Mirroring** – convince the switch that every time it gets a frame, send a copy to your port
- **MAC flooding** – send so many unsolicited MACs to the switch, filling up the CAM table (cached addresses used for forwarding), rolling off other entries, convincing the switch that the legitimate MACs aren't cached, so it behaves like a hub.
- **ARP poisoning** (ARP spoofing) – maliciously changing an ARP cache on a machine to inject faulty entries
- **DHCP starvation** – malicious attempt to exhaust all available addresses from the server

Wireshark – sniffing tool

Important Wireshark filters	
telnet	Show only telnet traffic
Host 192.168.1.102	Display traffic to or from 192.168.1.102
Net 191.168.1.0/24	Display traffic to or from the subnet 192.168.1.1-255
Port 80	Display all port 80 traffic
ip.src == 102.168.0.2	Disiplay traffic from 192.168.0.2
tcp contains keyword	Display traffic containing keyword
tcp.flags == 0xn	Displays traffic with flags using flag code n

Wireshark Flag Codes	
FIN	1
SYN	2
RST	4
PSH	8
ACK	16
URG	32

TCP Dump – sniffing tool

- -i = listening mode
- -w = write to file

EVASION

Intrusion Detection System (IDS) – hardware and/or software devices that examine streams of packets for unusual or malicious behavior

- **Signature** list based IDS – compare packets against list of known traffic patterns that indicate an attack
- **Anomaly**/behavior based IDS – compare packets against normal traffic
- **Host**-based IDS (HIDS) – resides on the host itself, usually monitoring just that host
- **Network**-based IDS (NIDS) – sits on network perimeter

Example IDS: Snort (open source)

IDS Evasion tactics:

- Slow down scans
- Flood network
- Fake attacks (diversion)
- Splice/fragment session into smaller unrecognizable packets

Firewall – appliance within a network that is designed to protect internal resources from unauthorized external access (work based on an access control list detailing what is allowed through)

Network Address Translation (NAT) – gives the ability for an internal IP address (192.168.0.0/24) to communicate across the internet with an external IP address

Stateful Inspection – the firewall has the means to track the entire status of a connection

Example: packet arrives with an ACK, but not history of a SYN, indicating a malicious attempt

HTTP Tunneling – firewalls almost never filter port 80 (HTTP), so information can be wrapped in an HTTP shell and sent through that port

Firewalking – "walking" through every port against a firewall to determine what is open

ATTACKING A SYSTEM

Security Accounts Manager (SAM) file – stores the hash value of passwords

Location: C:\Windows\system32\Config\SAM

Hash – one-way algorithmic encryption

1. Take the password and make it all caps
2. Add blanks until it is 14 digits long
3. Split into 2 equal parts
4. Encrypt each part
5. Combine parts to complete the hash

Note: if the password is less than 8 characters long, the last half of the hash will always be ***AAD3B435B51404EE***

- **SYSKEY** uses 128 bits in encrypting SAM file
- **NTLMv2** uses MD5 to hash passwords

Kerberos – makes use of both symmetric and asymmetric encryption technologies to securely transmit passwords and keys across a network

- Key Distribution Center (KDC)
- Authentication Service (AS)
- Ticket Granting Service (TGS)
- Ticket Granting Ticket\

1. Client asks the KDC (which holds the AS and TGS) for a ticket (TGT)
2. Server responds with a secret key, which is hashed by the password copy kept on the server (Active Directory)
3. If the client can decrypt the Ticket, the TGT is sent back to the server requesting a TGS service ticket
4. The server responds with a service ticket, allowing the client to log on and access network resources

Registry – a collection of all the settings and configurations that make the system run (key value pairs in hierarchy)

Syntax: regedit.exe

Root-level keys in registry	
HKEY_LOCAL_MACHINE (HKLM)	hardware and software
HKEY_CLASSES_ROOT (HKCR)	File associations and Object Linking and Embedding classes (OLE)
HKEY_CURRENT_USER (HKCU)	Profile information for the user currently logged on
HKEY_USERS (HKU)	User configuration information for all currently active users on the computer
HKEY_CURRENT_CONFIG (HKCC)	Contains pointer to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet|HardwareProfiles\Current

Key Registry 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

Linux Security Architecture	
/	Root directory
/bin	Holds all sorts of basic Linux commands (like C:\\Windows\System32)
/dev	Contains pointer locations to the various storage and i/o systems you will need to mount if you want to use them
/etc	Contains all administration files and passwords/shadow files
/home	Holds user home directories
/mnt	Holds access locations you've actually mounted
/sbin	System binaries folder, holds more administrative commands and is the repository for most of the routines Linux runs (daemons)
/usr	Holds almost all information, commands, and files unique to the users

Linux Commands	
adduser	adds a user to the system
cat	display contents of a file, extract a file
cp	copies files
ifconfig	(like ipconfig on windows) shows network configuration information about NIC
kill	kill a running process
ls	display contents of a folder (with –l displays current security settings for contents of directory)
man	displays "manual" page for a command (help file)
passwd	used to change your password
ps	process status (with –ef to show all running processes)
rm	removes files
su	perform functions as another user (sudo -> super user/root)
chmod	change mode, change access permissions to file system objects

Linux permissions

Syntax: [folderOrFile][userRead][uWrite][uExecute][groupRead][gWrite][gExecute][allRead][allWrite][allExecute]

Example: -rw-r—r—means File (- for file, d for folder), read and write for user, read for group, read for all others

Change Permissions on linux

Syntax: ***chmod*** *[userCode][groupCode][allOtherCode] where* ***read*** *= 4,* ***write*** *= 2,* ***execute*** *= 1*

Example: chmod 464 file1 means change file1 permissions to read for user, read/write for group, read for all others

Linux Users:

User	**UID**	**GID**
root	0	0
user 1	500	500
user 2	501	501

Linux Passwords can either be in the passwd file (unencrypted) or the shadow file (encrypted)

GNU Compiler Collection (GCC) – can compile and execute from several languages, used to compile linux

Syntax (C++ source file): g++ sample.cpp newapp.exe

Syntax (C source file): gcc sample.c newapp.exe

Password Complexity Tips:

- Password must not contain any part of the user's name
- Password must have a minimum of eight characters
- Password must contain characters from at least 3 of the 4 major components of complexity
    - Special symbols
    - Uppercase letters
    - Lower case letters
    - Numbers

Password Attacks

- **Passive online attack** – sniffing a wire in the hopes of either intercepting a password in clear text or attempting a replay or man-in-the-middle attack
- **Sidejacking** – steal cookies exchanged between two systems and ferret out which one to use as a replay-style attack
- **Active online attack** – usually just trying passwords (guessing)
- Offline attack – hacker steals a copy of the password file and works the cracking efforts on a separate system
    - **Dictionary** attack – compares hashes to hashes of list of prepared passwords
    - **Hybrid** attack – dictionary attack with substituting complex characters
    - **Brute-force** attack – every conceivable combination of letters, numbers, and special characters is compared against the hash to determine a match (only option if you know the password will be particularly complicated)
- **Keylogging**
- **Nonelectric** (social engineering)

Privacy Escalation/Executing Applications

- **Vertical** privilege escalation – lower-level user executes code at a higher privilege level than they should have access to
- **Horizontal** privilege escalation – executing code at the same user level but from a location that should be protected from access

Ways to escalate privileges:

- Crack password of administrator/root
- Take advantage of an OS vulnerability
- Use a tool (Metasploit)
- Send an executable via email

Stealth Alternate Data Stream (NTFS) – hiding something inside another file

Syntax to hide: type HideMe.txt > cover.txt:Hidden.txt

Syntax to find: start c:\cover.txt:Hidden.txt

Root Kit – collection of software put in place by an attacker that is designed to obscure system compromise

- Application level – replace valid applications with Trojan binaries
- Kernel level – replace OS kernel code with backdoor code
- Library level – system-level calls to hide their existence

Covering tracks

- Application log – holds entries specifically related to the applications
- System log – registers system events
- Security log – holds login attempts, access and activities regarding resources

Location: C:\System32\Config with .evt extension

WEB BASED HACKING

Web Server Attack Methodology:

1. Information Gathering
2. Footprinting
3. Mirroring Websites
4. Vulnerability Scanning
5. Session Hijacking
6. Password Cracking

Apache Servers:

- Built **modularly**, with a core to hold all the magic and modules to perform a wide variety of functions
- Open source
- Configuration almost always done as part of a module within special files (http.conf sets server status)
- Modules appropriately named (mod_negotiation)
- Extension .apxs

IIS Server

- Windows-based
- Spawn all shells as LOCAL_SYSTEM (not root)

Vulnerabilities:

- Misconfiguration
- Error reporting

HTTP Entities	
** **	(blank)
"	“
'	‘
&	&
<	<
>	>

HTTP Requests	
HTTP Head	grabs metadata
HTTP Get	shown in browser
HTTP Post	not shown in browser, but can still capture with wireshark

Canary word – created specifically to look for and indicate buffer overflow attacks

If application stopped processing and canary word was changed in log = attack logged but not successful

ATTACKING WEB SERVERS

Directory traversal

Example: http://www.example.com/../../../../etc/passwd traverses up to root and back down to password file

Unicode equivalents	
%2e	.
%2f	/

URL Tampering – adjust URL parameters and resend request

URL Obfuscation – using binary equivalent of IP address

Example: http://200.58.77.66

Convert to binaries and combine: 11001000 00111010 01001101 01000010

Convert total back to decimal: http://3359264066

ATTACKING WEB APPLICATIONS

Buffer Overflow – attempt to write more data into an application's prebuilt buffer area in order to overwrite adjacent memory, execute code, or crash a system

- Stack
- Heap
- NOP Sled

Cross-Site Scripting (XSS)

Example: http://IPADDRESS/";!--"<XSS>=&{()}

Poison Cookies

LDAP Injection – execute entry directly as an LDAP query

Username: Matt)(&) where & ends the query, preventing the password check

SQL Injection – execute entry directly as a SQL Query

Username: ' OR 1=1 where ' ends the query, only checking if 1=1

WIRELESS HACKING

Standard	Speed	Frequency (GHz)	Modulation Type
802.11a	54	5	OFDM
802.11b	11	2.4	DSSS
802.11g	54	2.4	OFDM, DSSS
802.11n	100+	2.4, 5	OFDM

Modulation Types:

- **Orthogonal Frequency-Division Multiplexing (OFDM)** – signal contains separate channels of frequency bands
- **Direct-Sequence Spread Spectrum (DSSS)** – combining all waveforms into a single purpose

Wireless Setups:

- **Ad-hoc** – system connects directly to another system
- **Infrastructure** – makes use of an access point to funnel all wireless connections through

Wireless Security Terms

- **Service Set Identifier (SSID)** – does nothing for security, other than identify which network you're on
- **Association** – action of a client connecting to an access point (AP)
- **Authentication** – identifies client before it can access anything

Wireless Security Standards

- **Wired Equivalent Privacy (WEP)**
  - 64 bit uses a 40-bit key
  - 128 bit uses a 104-bit key
  - 256 bit version uses a 232-bit key
- **Wifi Protected Access (WPA)**
  - Uses Temporal Key Integrity Protocol (TKIP) (128-bit key) during an Extensible Authentication Protocol (EAP) authentication session
  - Can be hacked by capturing the password pairwise master key (PMK) during the handshake

Attacks:

- "Evil Twin" – rogue access point, mis-association attack
- Denial of Service – jamming
- MAC Spoofing
- WEP cracking – generate enough traffic to guess password (requires knowing the MAC address of the AP and the SSID)
- Mobile phone hacks
- Bluetooth:
  - BlueSmacking – DOS against Bluetooth device
  - BlueJacking – sending unsolicited messages to, and from, mobile devices
  - BlueSniffing – sniffing Bluetooth traffic
  - BlueSnarfing – theft of data from mobile device through Bluetooth

MALWARE

Malware – software designed to harm or secretly access a computer system without the owner's informed consent

Trojan – appears to perform a desirable function for the user, but instead serves to steal data or otherwise harm the system:

- Defacement
- Proxy Server
- FTP
- VNC
- Command Shell Trojan (ex. Netcat)

Netcat example: nc –L 56 –t –e cmd.exe

Common Trojans and their Ports	
TCPWrappers	421
Doom	666
Snipernet	667
Tini	7777
WinHole	1080-81
RAT	1095, 1097-8
SpySender	1807
DeepThroat	2140, 3150
NetBus	12345-6
Whack a Mole	12362, 12363
Back Orifice	31337, 31338

Virus – self-replicating program that reproduces its code by attaching copies into other executable codes

- **Boot sector** virus (system virus) – moves the boot sector to another location on the hard drive, forcing the virus code to be executed first
- **Shell** virus – wraps itself around an application's code, inserting its own code before the application's
- **Multipartite** virus – attempts to infect both files and the boot sector (virus with multiple infection vectors)
- **Macro** virus – infects template files created by Microsoft Office (VBA)
- **Polymorphic code** virus – mutates its code using a built-in polymorphic engine
- **Metamorphic** virus – rewrites itself every time it infects a new file
- **Stealth** virus (tunneling virus) – attempts to evade antivirus (AV) applications by intercepting AV's requests to the operating system and returning them 'clean'

Worm – self-replicating, uses a computer network to send copies of itself to other systems without human intervention

- **Conficker** worm – disabled services, denied access to administrator shared drives, locked users out of directories, and restricted access to security-related sites

Signature: "open folder to view files – publisher not specified" ***autorun executable***

- **Code Red** – named after the soft drink the Eeye Digital guys were drinking when they discovered it, exploited indexing software on **IIS** using a buffer overflow and defaced hundreds of thousands of servers
- **SQL Slammer** – denial-of-service worm attacking buffer overflow weaknesses in Microsoft **SQL** Services
- **Nimda** – **file injection virus** that modified and touched nearly all web content on a machine, spreading through e-mail, open network shares, and websites, and took advantage of backdoors left on machines infected by the Code Red worm
- **Bug Bear** – terminated AV applications, set up backdoor, keylogged, and propagated over open **network shares** and **email**
- **Pretty Park** – took advantage of **IRC** to propagate stolen passwords, spread via **email**

Signature: showed 3D Pipe screensaver on Windows machines

Protection:

- Good, up-to-date antivirus program
- Sheepdip computer – checks physical media, device drivers, and other files for malware before they are introduced to the network

OTHER ATTACKS

Botnet – network of zombie computers the hacker can use to start a distributed attack

Phlashing – DOS attack that causes permanent damage to a system

Denial of Service (DOS) attacks:

- **SYN attack** – send SYN packets with false source IP, target attempts to respond with SYN/ACK but fails because address is false
- **SYN flood** – send SYN packets and never respond to the SYN/ACK packets
- **ICMP flood** – send ICMP echo packets with spoofed source address
- **Application level** – send more "legitimate" traffic to a web application than it can handle
- **Smurf** – send pings to broadcast address of the subnet with the source IP spoofed to the target
- **Ping of Death** – fragment ICMP message, send to target, when fragments are reassembled, the resultant packet is larger than the maximum size and crashes the system
- **Teardrop** – garbled IP fragments with overlapping, oversized payloads are sent to the target machine

Session Hijacking Process

1. **Sniff** the traffic between the client and the server
2. **Monitor** the traffic and predict the sequence numbering
3. **Desynchronize** the session with the client
4. **Predict** the session token and take over the session
5. **Inject** packets to the target server

CRYPTOGRAPHY

Cryptography – the science or study of protecting information by using techniques to render the information unusable to anyone who does not possess the means to decrypt it

Encryption Algorithm – a mathematical formula used to encrypt and decrypt data

- Substitution – bits replacing other bits
- Transposition – bits changing order

Cipher Types:

- **Stream cipher** – readable bits in their regular pattern are fed into the cipher and are encrypted one at a time, usually by an XOR operation
- **Block cipher** – data bits split up into locks and fed into the cipher, where each block of data (usually 64 bits at a time) is encrypted with the key and algorithm, producing an encrypted block of the same length

Symmetric Encryption (single key, shared key) – one key is used both to encrypt and decrypt the data

Symmetric Encryption Examples	Type	Key size (bits)
DES	block	56 (with an additional 8 of parity)
3DES	block	168
AES	block	128, 192, 256
IDEA	block	128
TwoFish	block	256
BlowFish	block	32-448
RC	block	2040

Asymmetric Encryption – two keys, one to encrypt (public), one to decrypt (private)

- **Diffie-Hellman** – uses Secure Sockets Layer (SSL) and IPSec encryption (vulnerable to man-in-the-middle attacks)
- **Elliptic Curve Cryptosystem (ECC)** – uses points on an elliptic curve for encryption and signatures (low processing, good for mobile devices)
- **El Gamal** – solves discrete logarithm problems for encryption
- **RSA** – uses factoring of two large prime numbers

Weaknesses of asymmetric encryption:

- Performance (asymmetric is slower than symmetric)
- Processing power (asymmetric requires much longer key length, more suitable for smaller amounts of data)

Hash Algorithms – one-way mathematical function that takes an input and produces a fixed-length string (hash) based on the arrangement of data bits in the input

Hash Examples	Format	Output (bits)
MD5	32-digit Hexadecimal	128
SHA-1		160
SHA-2	4 separate functions	224, 256, 384, 512

Rainbow tables – lsit of hashes used for cracking and collision attacks

Salt – collection of random bits used as a key in addition to hashing algorithm, helps defend against collision attacks with rainbow tables

Hashes used for **integrity**

Steganography – concealing a message inside another medium in such a way that only the sender and recipient even know of its existence (gifshuffle)

Syntax: gifshuffle [-CQS1] [-p passwd] [-f file | -m message] [infile.gif [outfile.gif]]

C – compresses data for concealment

Q – runs tool in quiet mode (no reporting)

S – provides reporting space available

1 – retains compatibility with earlier version

Example: "I love CEH" in CEH.gif

Storage: gifshuffle –C –m "I love CEH" –p "ethical" CEH.gif hacker.gif

Extraction: gifshuffle –C –p "ethical" hacker.gif

Public Key Infrastructure (PKI) – structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange

Certificate Authority – creates and issues digital certificates that can be used to verify identity (maintains certificate revocation list (CRL), used to track which certificates have problems and which have been revoked)

Registration Authority (RA) – validates an applicant into the system, making sure they are real, valid, and allowed to use the system

Cross-certification – the ability for a CA to trust a CA in a completely different PKI

Trust model – describes how entities within an enterprise deal with keys, signatures, and certificates

1. Web of Trust – multiple entities sign certificates for one another
2. Single Authority System – CA at top creates and issues certificates, and users trust each other based on the CA
3. Hierarchical trust system – root CA at top but makes use of intermediate CAs below (registration authorities) to issue and manage certificates (most secure)

Digital Certificates – electronic file used to verify a user's identity

- Version – identifies certificate format
- Serial Number – uniquely identify certificate

- Subject – whoever is being identified by the certificate
- Algorithm ID – algorithm used to create the digital signature
- Issuer – shows the identity of the authenticity of the certificate
- Valid From and Valid To – dates of validity
- Key Usage – for what purpose the certificate was created
- Subject's public key – can be used to identify the sender
- Optional fields – include Issuer Unique Identifier, Subject Alternative Name, Extensions

X.509 standard – defines what should and should not be in a digital certificate

Digital Signature – algorithmic output that is designed to ensure the authenticity (and integrity) of the sender

Data at rest (DAR) encryption:

- Encrypting data files and folders
- Encrypting the entire drive at the sector level

Encrypted Communication:

- **Secure Shell (SSH)** – secured version of Telnet
- **Secure Sockets Layer (SSL)** – encrypts data at the transport layer and above (uses RSA encryption and digital certificates)
- **Transport Layer Security (TLS)** – successor to SSL, uses RSA of 1024 and 2048 bits
- **Internet Protocol Security (IPSec)** – network layer tunneling
    - Tunnel – entire IP packet encrypted
    - Transport – data payload encrypted
- **Point-to-Point Tunneling Protocol (PPTP)** (uses RC4 encryption)

Cryptography Attacks:

- **Known plain-text attack** – have both plain text and corresponding cipher-text messages, using both to decipher the key
- **Cipher-text-only attack** – have several different messages encrypted the same way (with the same algorithm), use statistical analysis to decode the messages
- **Replay attack** (usually in context of man-in-the-middle) – repeat portion of cryptographic exchange in hopes of fooling the system into setting up a communications channel

SOCIAL ENGINEERING

Human-based attacks:

- Dumpster-diving
- Impersonation
- Technical Support
- Shoulder Surfing
- Tailgating (fake badge)
- Piggybacking (no badge)
- Reverse social engineering (get target to contact you)

Computer-based attacks

- Phishing
    - Beware unknown, unexpected, or suspicious originators
    - Beware whom the email is addressed to
    - Verify phone numbers
    - Beware bad spelling or grammar
    - Always check links
- Spear Phishing – targeted phishing attack
- Whaling – spear phishing against high-level targets

Mobile-based attacks

- Publishing malicious apps
- Repackaging legitimate apps
- Fake security applications
- SMS

Physical Security

- **Physical** measures – include all things you can touch
- **Technical** measures – smart cards, biometrics
- **Operational** measures – background checks on employees, risk assessment on devices, policies regarding key management and storage

Access controls – physical measures designed to prevent access to controller areas

Biometric system – measured by two main factors

- False Rejection Rate (FRR)
- False Acceptance Rate (FAR)

Defense in depth (layered security)

PENETRATION TESTING

Security Audit – policy and procedure focused

Pen Tests:

- Internal – performed within the organization, from various access points
- External – analyzes publicly available information and conducts network scanning, enumeration, and testing from the network perimeter or internet

Pen Test Methodology

1. **Pre-Attack** Phase
    a. Perform all reconnaissance and data-gathering efforts
2. **Attack** Phase
    a. Attempt to penetrate the network perimeter, acquire targets, execute attacks, and elevate privileges
    b. Verify ACLs by crafting packets and checking to see whether you can use any covert tunnels into the organization
    c. Try XSS, buffer overflows, and SQL injections on the web side
    d. Password cracking and privilege escalation
    e. Execute attack code
3. **Post-Attack** Phase
    a. Cleanup
    b. Provide Deliverables to client

Security Assessment Deliverables (**Report**)

- Executive summary (tailored to the standard)
- Names of all participants and dates of all tests
- List of findings, in order of highest risk
- Analysis of each finding and recommended mitigation steps
- Log files and other evidence

Insider Threat Categories

- **Pure Insider** – employee with all rights and access associated with being employed by the company
- **Insider associate** – someone with limited authorized access (guard, cleaning services)
- **Insider affiliate** – spouse, friend, or client of employee who uses the employee's credentials to gain access
- **Outside affiliate** – someone unknown and untrusted who uses an open access channel to gain access to an organization's resources