# Essential Knowledge

# Essential Knowledge

### <u>The OSI Reference Model</u>

Layer	Description	Technologies	Data Unit
1	Physical	USB, Bluetooth	Bit
2	Data Link	ARP, PPP	Frame
3	Network	IP	Packet
4	Transport	TCP	Segment
5	Session	X255, SCP	Data
6	Presentation	AFP, MIME	Data
7	Application	FTP, HTTP, SMTP	Data

### <u>TCP/IP Model</u>

Layer	Description	OSI Layer Equivalent
1	Network Access	1, 2
2	Internet	3
3	Transport	4
4	Application	5-7

### <u>TCP Handshake</u>

SYN -> SYN-ACK -> ACK

### <u>ARP</u>

- Resolves IP address to physical address

### <u>Network Security Zones</u>

- **Internet** - uncontrollable
- **Internet DMZ** - controlled buffer network
- **Production Network Zone** - very restricted; controls direct access from uncontrolled zones; has no users
- **Intranet Zone** - controlled; has little to no heavy restrictions
- **Management Network Zone** - might find VLANs and IPSEC; highly secured; strict policies

### <u>Vulnerabilities</u>

- **Common Vulnerability Scoring System** (CVSS) - places numerical score based on severity
- **National Vulnerability Database** (NVD) - US government repository of vulnerabilities

### <u>Vulnerability Categories</u>

- **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

### <u>Vulnerability Management Tools</u>

- Nessus
- Qualys
- GFI Languard
- Nikto
- OpenVAS
- Retina CS

### <u>Terms to Know</u>

- **Hack value** - perceived value or worth of a target as seen by the attacker
- **Zero-day attack** - attack that occurs before a vendor knows or is able to patch a flaw
- **Doxing** - searching for and publishing information about an individual usually with a malicious intent
- **Enterprise Information Security Architecture** (EISA) - process that determines how systems work within an organization
- **Incident management** - deals with specific incidents to mitigate the attack

### <u>Threat Modeling</u>

- Identify security objectives
- Application Overview
- Decompose application
- Identify threats
- Identify vulnerabilities

### <u>Risk Management</u>

- Risk identification
- Risk assessment
- Risk treatment
- Risk tracking
- Risk review

  *Uses risk analysis matrix to determine threat level

### <u>Types of Security Controls</u>

Description	Examples
Physical	Guards, lights, cameras
Technical	Encryption, smart cards, access control lists
Administrative	Training awareness, policies

Description	Examples

Preventative	authentication, alarm bells
Detective	audits, backups
Corrective	restore operations

### <u>Business Analysis</u>

- Business Impact Analysis (BIA)

  - Maximum Tolerable Downtime (MTD)

- Business Continuity Plan (BCP)

  - Disaster Recovery Plan (DRP)

- Annualized Loss Expectancy (ALE)

  - Annual Rate of Occurrence (ARO)

  - Single Loss Expectancy (SLE)
    $$
    ALE = SLE * ARO
    $$

User Behavior Analysis (UBA) - tracking users and extrapolating data in light of malicious activity

### <u>CIA Triad</u>

- **Confidentiality** - passwords, encryption
- **Integrity** - hashing, digital signatures
- **Availability** - anti-dos solutions

Bit flipping is an example of an <u>integrity</u> attack. The outcome is not to gain information - it is to obscure the data from the actual user.

Confidentiality != authentication - MAC address spoofing is an authentication attack

### <u>Common Criterial for Information Technology Security Evaluation</u>

- Routinely called "Common Criteria" (CC)
- **Evaluation Assurance Level** (EAL) - goes from level 1 - 7
- **Target of Evaluation** - the system that is being tested
- **Security Target** (ST) - document describing the TOE and security requirements
- **Protection Profile** (PP) - security requirements that are specific to the type of device being tested

### <u>Access Control Types</u>

- **Mandatory** (MAC) - access is set by an administrator
- **Discretionary** (DAC) - allows users to give access to resources that they own and control

### <u>Security Policies</u>

- **Access Control** - what resources are protected and who can access them
- **Information Security** - what can systems be used for
- **Information Protection** - defines data sensitivity levels
- **Password** - all things about passwords (how long, characters required, etc.)
- **E-Mail** - proper and allowable use of email systems
- **Information Audit** - defines the framework used for auditing

### <u>Policy Categorizations</u>

- **Promiscuous** - wide open
- **Permissive** - blocks only known dangerous things
- **Prudent** - blocks most and only allows things for business purposes
- **Paranoid** - locks everything down

Standards - mandatory rules to achieve consistency

Baselines - provide the minimum security necessary

Guidelines - flexible or recommended actions

Procedures - step by step instructions

Script Kiddie - uneducated in security methods, but uses tools that are freely available to perform malicious activities

Phreaker - manipulates telephone systems

### <u>The Hats</u>

- **White Hat** - ethical hackers
- **Black Hat** - hackers that seek to perform malicious activities
- **Gray Hat** - hackers that perform good or bad activities but do not have the permission of the organization they are hacking against

Hacktivist - someone who hacks for a cause

Suicide Hackers - do not case about any impunity to themselves; hack to get the job done

Cyberterrorist - motivated by religious or political beliefs to create fear or disruption

State-Sponsored Hacker - hacker that is hired by a government

### <u>Attack Types</u>

- **Operating System** (OS) - attacks targeting OS flaws or security issues inside such as guest accounts or default passwords
- **Application Level** - attacks on programming code and software logic
- **Shrink-Wrap Code** - attack takes advantage of built-in code or scripts
- **Misconfiguration** - attack takes advantage of systems that are misconfigured due to improper configuration or default configuration

Infowar - the use of offensive and defensive techniques to create an advantage

### <u>Hacking Phases</u>

1. **Reconnaissance** - gathering evidence about targets
2. **Scanning & Enumeration** - obtaining more in-depth information about targets
3. **Gaining Access** - attacks are leveled in order to gain access to a system
4. **Maintaining Access** - items put in place to ensure future access
5. **Covering Tracks** - steps taken to conceal success and intrusion

### <u>Types of Reconnaissance</u>

- **Passive** - gathering information about the target without their knowledge
- **Active** - uses tools and techniques that may or may not be discovered

### <u>Security Incident and Event Management (SIEM)</u>

- Functions related to a security operations center (SOC)
  - Identifying
  - Monitoring
  - Recording
  - Auditing
  - Analyzing

Ethical hacker - employs tools that hackers use with a customer's permission; always obtains an agreement from the client with specific objectives <u>before</u> any testing is done

Cracker - uses tools for personal gain or destructive purposes

### <u>Penetration Test</u>

- Clearly defined, full scale test of security controls
- Phases
  - **Preparation** - contracts and team determined
  - **Assessment** - all hacking phases (reconnaissance, scanning, attacks, etc.)
  - **Post-Assessment** - reports & conclusions
- Types
  - **Black Box** - done without any knowledge of the system or network
  - **White Box** - complete knowledge of the system
  - **Gray Box** - has some knowledge of the system and/or network

### <u>Law Categories</u>

- **Criminal** - laws that protect public safety and usually have jail time attached
- **Civil** - private rights and remedies
- **Common** - laws that are based on societal customs

### <u>Laws and Standards</u>

- **OSSTM Compliance** - "Open Source Security Testing Methodology Manual" maintained by ISECOM , defines three types of compliance
  - **Legislative** - Deals with government regulations (Such as SOX and HIPAA)
  - **Contractual** - Deals with industry / group requirement (Such as PCI DSS)
  - **Standards based** - Deals with practices that must be followed by members of a given group/organization (Such as ITIL ,ISO and OSSTMM itself)

- **OSSTM Controls**
  - **OSSTM Class A - Interactive Controls**
    - *Authentication* - Provides for identification and authorization based on credentials
    - *Indemnification* - Provided contractual protection against loss or damages
    - *Subjugation* - Ensures that interactions occur according to processes defined by the asset owner
    - *Continuity* - Maintains interactivity with assets if corruption of failure occurs
    - *Resilience* - Protects assets from corruption and failure

  - **OSSTM Class B - Process Controls**
    - *Non-repudiation* - Prevents participants from denying its actions
    - *Confidentiality* - Ensures that only participants know of an asset
    - *Privacy* - Ensures that only participants have access to the asset
    - *Integrity* - Ensures that only participants know when assets and processes change
    - *Alarm* - Notifies participants when interactions occur

- **ISO 27001** - Security standard based on the British BS7799 standard, focuses on security governance

- **NIST-800-53** - Catalogs security and privacy controls for federal information systems, created to help implementation of FISMA

- **ISO 27002 AND 17799** - Based on BS799 but focuses on security objectives and provides security controls based on industry best practice

- **FISMA** - "Federal Information Security Modernization Ac Of 2002" A law updated in 2004 to codify the authority of the Department of Homeland Security with regard to implementation of information security policies

- **FITARA** - "Federal Information Technology Acquisition Reform Act" A 2013 bill that was intended to change the framework that determines how the US GOV purchases technology

- **HIPAA** - "Health Insurance Portability and Accountability Act" a law that set's privacy standards to protect patient medical records and health information shared between doctors, hospitals and insurance providers

- **PCI-DSS** - "Payment Card Industry Data Security Standard" Standard for organizations handling Credit Cards, ATM cards and other POS cards

- **COBIT** - "Control Object for Information and Related Technology" IT Governance framework and toolset, created by ISACA and ITGI

- **SOX** - "Sarbanes-Oxley Act" Law that requires publicly traded companies to submit to independent audits and to properly disclose financial information

- **GLBA** - "U.S Gramm-Leach-Bliley Act" Law that protects the confidentiality and integrity of personal information that is collected by financial institutions.

- **CSIRT** - "Computer Security Incident Response Team" CSIRT provided a single point of contact when reporting computer security incidents

- **ITIL** - "Information Technology Infrastructure Library" - An operational framework developed in the '80s that standardizes IT management procedures

### <u>Controls</u>

- **Directive** - Also known as procedural controls because they deal with company procedures such as security policies, operations plans, and guidelines.
- **Deterrent** - Controls that are used to dissuade potential attackers, such as signs that warn possible attackers about the alarm system and monitoring in place.
- **Preventive** - Controls used to stop potential attacks by preventing users from performing specific actions, such as encryption and authentication
- **Compensating** - Controls used to supplement directive controls, such as administrator reviewing logs files for violations of company policy
- **Detective** - Controls used to monitor and alert on malicious or unauthorized activity, such as IDS's and CCTV feeds monitored in real life
- **Corrective** - Controls used to repair damage caused by malicious events. Such as AntiVirus software and IPS (IPS being both a detective and corrective control)
- **Recovery**

## Reconnaissance

# Reconnaissance

### <u>Footprinting</u>

- Looking for high-level information on a target
- Types
  - **Anonymous** - information gathering without revealing anything about yourself
  - **Pseudonymous** - making someone else take the blame for your actions

### <u>Four Main Focuses</u>

- Know the security posture
- Reduce the focus area
- Identify vulnerabilities
- Draw a network map

### <u>Types of Footprinting</u>

- **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

Competitive Intelligence - information gathered by businesses about competitors

Alexa.com - resource for statistics about websites

### <u>Methods and Tools</u>

Search Engines

- **NetCraft** - information about website and possibly OS info
- **Job Search Sites** - information about technologies can be gleaned from job postings
- **Google**
  - 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
- **Metagoofil** - uses Google hacks to find information in meta tags

Website Footprinting

- **Web mirroring** - allows for discrete testing offline
  - HTTrack
  - Black Widow
  - Wget
  - WebRipper
  - Teleport Pro
  - Backstreet Browser
- **Archive.org** - provides cached websites from various dates which possibly have sensitive information that has been now removed

Email Footprinting

- **Email header** - may show servers and where the location of those servers are
- **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 reccord
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

- **Nslookup** - performs DNS queries

  - nslookup [- options] [hostname]
  - interactive zone transfer
    - nslookup
    - server <IP Address>
    - set type = any
    - ls -d domainname.com

- **Dig** - unix-based command like nslookup

  - dig @server name type

Network Footprinting

- IP address range can be obtained from regional registrar (ARIN here)
- Use traceroute to find intermediary servers
  - traceroute uses ICMP echo in Windows
- Windows command - tracert
- Linux Command - traceroute

Other Tools

- **OSRFramework** - uses open source intelligence to get information about target
- **Web Spiders** - obtain information from the website such as pages, etc.
- **Social Engineering Tools**
  - Maltego
  - Social Engineering Framework (SEF)
- **Shodan** - search engine that shows devices connected to the Internet

Computer Security Incident Response Team (CSIRT) - point of contact for all incident response services for associates of the DHS

## Scanning and Enumeration

# Scanning and Enumeration

Scanning - discovering systems on the network and looking at what ports are open as well as applications that may be running

Connectionless Communication - UDP packets are sent without creating a connection. Examples are TFTP, DNS (lookups only) and DHCP

Connection-Oriented Communication - TCP packets require a connection due to the size of the data being transmitted and to ensure deliverability

### <u>TCP Flags</u>

Flag	Name	Function
SYN	Synchronize	Set during initial communication. Negotiating of parameters and sequence numbers
ACK	Acknowledgment	Set as an acknowledgement to the SYN flag. Always set after initial SYN
RST	Reset	Forces the termination of a connection (in both directions)
FIN	Finish	Ordered close to communications
PSH	Push	Forces the delivery of data without concern for buffering
URG	Urgent	Data inside is being sent out of band. Example is cancelling a message

### <u>TCP Handshake</u>

- SYN -> SYN-ACK - ACK
- Sequence numbers increase on new communication. Example is computers A and B. A would increment B's sequence number. A would never increment it's own sequence.

### <u>Port Numbers</u>

- **Internet Assigned Numbers Authority** (IANA) - maintains Service Name and Transport Protocol Port Number Registry which lists all port number reservations

- Ranges

  - **Well-known ports** - 0 - 1023

  - **Registered ports** - 1024 - 49,151

  - **Dynamic ports** - 49,152 - 65,535

Port Number	Protocol	Transport Protocol
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
67	DHCP	UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
137-139	NetBIOS	TCP/UDP
143	IMAP	TCP
161/162	SNMP	UDP
389	LDAP	TCP/UDP
443	HTTPS	TCP
445	SMB	TCP
514	SYSLOG	UDP

  - A service is said to be **listening** for a port when it has that specific port open

  - Once a service has made a connection, the port is in an **established** state

  - Netstat

    - Shows open ports on computer
    - **netstat -an** displays connections in numerical form
    - **netstat -b** displays executables tied to the open port (admin only)

### <u>Subnetting</u>

- **IPv4 Main Address Types**
  - **Unicast** - acted on by a single recipient
  - **Multicast** - acted on by members of a specific group
  - **Broadcast** - acted on by everyone on the network
    - **Limited** - delivered to every system in the domain (255.255.255.255)
    - **Directed** - delivered to all devices on a subnet and use that broadcast address
- **Subnet mask** - determines how many address available on a specific subnet

  - Represented by three methods
    - **Decimal** - 255.240.0.0
    - **Binary** - 11111111.11110000.00000000.00000000
    - **CIDR** - x.x.x.x/12   (where x.x.x.x is an ip address on that range)
  - If all the bits in the host field are 1s, the address is the broadcast
  - If they are all 0s, it's the network address
  - Any other combination indicates an address in the range
  - ![img](https://s3.amazonaws.com/prealliance-thumbnails.oneclass.com/thumbnails/001/751/775/original/stringio.txt?1513221790)

### <u>Scanning Methodology</u>

- **Check for live systems** - ping or other type of way to determine live hosts
- **Check for open ports** - once you know live host IPs, scan them for listening ports
- **Scan beyond IDS** - if needed, use methods to scan beyond the detection systems
- **Perform banner grabbing** - grab from servers as well as perform OS fingerprinting
- **Scan for vulnerabilities** - use tools to look at the vulnerabilities of open systems
- **Draw network diagrams** - shows logical and physical pathways into networks
- **Prepare proxies** - obscures efforts to keep you hidden

### <u>Identifying Targets</u>

- The easiest way to scan for live systems is through ICMP.

- It has it's shortcomings and is sometimes blocked on hosts that are actually live.

- **Message Types and Returns**

ICMP Message Type	Description and Codes
0: Echo Reply	Answer to a Type 8 Echo Request
3: Destination Unreachable	Error message followed by these codes:<br />0 - Destination network unreachable<br />1 - Destination host unreachable<br />6 - Network unknown<br />7 - Host unknown<br />9 - Network administratively prohibited<br />10 - Host administratively prohibited<br />13 - Communication administratively prohibited
4: Source Quench	A congestion control message
5: Redirect	Sent when there are two or more gateways available for the sender to use. Followed by these codes:<br />0 - Redirect datagram for the network<br />1 - Redirect datagram for the host
8: Echo Request	A ping message, requesting an echo reply
11: Time Exceeded	Packet took too long to be routed (code 0 is TTL expired)

  - Payload of an ICMP message can be anything; RFC never set what it was supposed to be. Allows for covert channels
  - **Ping sweep** - easiest method to identify hosts
  - **ICMP Echo scanning** - sending an ICMP Echo Request to the network IP address
  - An ICMP return of type 3 with a code of 13 indicates a poorly configured firewall
  - **Ping scanning tools**
    - Nmap
    - Angry IP Scanner
    - Solar-Winds Engineer Toolkit
    - Advanced IP Scanner

    - Pinkie
  - Nmap virtually always does a ping sweep with scans unless you turn it off

### <u>Port Scan Types</u>

- **Full connect** - TCP connect or full open scan - full connection and then tears down with RST
  - Easiest to detect, but most reliable
  - nmap -sT
- **Stealth** - half-open scan or SYN scan - only SYN packets sent. Responses same as full.
  - Useful for hiding efforts and evading firewalls
  - nmap -sS
- **Inverse TCP flag** - uses FIN, URG or PSH flag. Open gives no response. Closed gives RST/ACK
  - nmap -sN (Null scan)
  - nmap -sF (FIN scan)
- **Xmas** - so named because all flags are turned on so it's "lit up" like a Christmas tree
  - Responses are same as Inverse TCP scan
  - Do not work against Windows machines
  - nmap -sX
- **ACK flag probe** - multiple methods
  - TTL version - if TTL of RST packet < 64, port is open
  - Window version - if the Window on the RST packet is anything other than 0, port open
  - Can be used to check filtering. If ACK is sent and no response, stateful firewall present.
  - nmap -sA (ACK scan)
  - nmap -sW (Window scan)
- **IDLE Scan** - uses a third party to check if a port is open
  - Looks at the IPID to see if there is a response
  - Only works if third party isn't transmitting data
  - Sends a request to the third party to check IPID id; then sends a spoofed packet to the target with a return of the third party; sends a request to the third party again to check if IPID increased.
    - IPID increase of 1 indicates port closed
    - IPID increase of 2 indicates port open
    - IPID increase of anything greater indicates the third party was not idle
  - nmap -sI <zombie host>

### <u>Nmap Switches</u>

Switch	Description
-sA	ACK scan
-sF	FIN scan
-sI	IDLE scan
-sL	DNS scan (list scan)
-sN	NULL scan
-sO	Protocol scan (tests which IP protocols respond)
-sP	Ping scan
-sR	RPC scan
-sS	SYN scan
-sT	TCP connect scan
-sW	Window scan
-sX	XMAS scan
-A	OS detection, version detection, script scanning and traceroute

-PI	ICMP ping
-Po	No ping
-PS	SYN ping
-PT	TCP ping
-oN	Normal output
-oX	XML output
-T0 through -T2	Serial scans. T0 is slowest
-T3 through -T5	Parallel scans. T3 is slowest

- Nmap runs by default at a T3 level
- **Fingerprinting** - another word for port sweeping and enumeration

### <u>Hping</u>

- Another powerful ping sweep and port scanning tool
- Also can craft packets
- hping3 -1 IPaddress

Switch	Description
-1	Sets ICMP mode
-2	Sets UDP mode
-8	Sets scan mode. Expects port range without -p flag
-9	Listen mode. Expects signature (e.g. HTTP) and interface (-I eth0)
--flood	Sends packets as fast as possible without showing incoming replies
-Q	Collects sequence numbers generated by the host
-p	Sets port number
-F	Sets the FIN flag
-S	Sets the SYN flag
-R	Sets the RST flag
-P	Sets the PSH flag
-A	Sets the ACK flag
-U	Sets the URG flag
-X	Sets the XMAS scan flags

### <u>Evasion</u>

- To evade IDS, sometimes you need to change the way you scan
- One method is to fragment packets (nmap -f switch)
- **OS Fingerprinting**
  - **Active** - sending crafted packets to the target
  - **Passive** - sniffing network traffic for things such as TTL windows, DF flags and ToS fields
- **Spoofing** - can only be used when you don't expect a response back to your machine
- **Source routing** - specifies the path a packet should take on the network; most systems don't allow this anymore
- **IP Address Decoy** - sends packets from your IP as well as multiple other decoys to confuse the IDS/Firewall as to where the attack is really coming from
  - nmap -D RND:10 x.x.x.x
  - nmap -D decoyIP1,decoyIP2....,sourceIP,.... [target]
- **Proxy** - hides true identity by filtering through another computer. Also can be used for other purposes such as content blocking evasion, etc.

  - **Proxy chains** - chaining multiple proxies together
    - Proxy Switcher
    - Proxy Workbench
    - ProxyChains
- **Tor** - a specific type of proxy that uses multiple hops to a destination; endpoints are peer computers
- **Anonymizers** - hides identity on HTTP traffic (port 80)

### <u>Vulnerability Scanning</u>

- Can be complex or simple tools run against a target to determine vulnerabilities
- Industry standard is Tenable's Nessus
- Other options include
  - GFI LanGuard
  - Qualys
  - FreeScan - best known for testing websites and applications
  - OpenVAS - best competitor to Nessus and is free

### <u>Enumeration</u>

- Defined as listing the items that are found within a specific target
- Always is active in nature

### <u>Windows System Basics</u>

- 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
  - **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**
  - **finger** - info on user and host machine
  - **rpcinfo and rpcclient** - info on RPC in the environment
  - **showmount** - displays all shared directories on the machine

### <u>Banner Grabbing</u>

- **Active** - sending specially crafted packets and comparing responses to determine OS
- **Passive** - reading error messages, sniffing traffic or looking at page extensions
- Easy way to banner grab is connect via telnet on port (e.g. 80 for web server)
- **Netcat** can also be used to banner grab
  - nc <IPaddress or FQDN> <port number>
- Can be used to get information about OS or specific server info (such as web server, mail server, etc.)

### <u>NetBIOS Enumeration</u>

- 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
- Command on Windows is **nbtstat**
  - nbtstat (gives your own info)
  - nbtstat -n (gives local table)
  - nbtstat -A IPADDRESS (gives remote information)
  - nbtstat -c (gives cache information)

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**
  - SuperScan
  - Hyena
  - NetBIOS Enumerator
  - NSAuditor

### <u>SNMP Enumeration</u>

- **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
- **Tools**
  - Engineer's Toolset
  - SNMPScanner
  - OpUtils 5
  - SNScan

### <u>Other Enumerations</u>

- **LDAP**
  - 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
  - **Tools**
    - Softerra
    - JXplorer
    - Lex
    - LDAP Admin Tool
- **NTP**
  - 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, ntpdc and ntpq
- **SMTP**
  - VRFY - validates user
  - EXPN - provides actual delivery address of mailing list and aliases
  - RCPT TO - defines recipients

# Sniffing and Evasion

# Sniffing and Evasion

### <u>Basic Knowledge</u>

 - 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

### <u>Protocols Susceptible</u>

- 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

### <u>ARP</u>

- Stands for Address Resolution Protocol
- Resolves IP address to a MAC address
- Packets are ARP_REQUEST and ARP_REPLY
- Each computer maintains it's 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

### <u>IPv6</u>

- Uses 128-bit address
- Has eight groups of four hexadecimal digits
- Sections with all 0s can be shorted 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)
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**

### <u>Wiretapping</u>

- **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

### <u>Active and Passive Sniffing</u>

- **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

### <u>MAC Flooding</u>

- 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.

### <u>ARP Poisoning</u>

- 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

### <u>DHCP Starvation</u>

- 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**

  - Yersinia

  - 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.

### <u>Spoofing</u>

- **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

### <u>Sniffing Tools</u>

- **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**

### <u>Devices To Evade</u>

- **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

### <u>Evasion Techniques</u>

- **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

### <u>Firewall Evasion</u>

- 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

### <u>Honeypots</u>

- 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

# Attacking a System

# Attacking a System

<u>Windows Security Architecture</u>

- 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**

    - KerbSniff

    - KerbCrack

    - 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

    - **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)

### <u>Linux Security Architecture</u>

- 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 curennt 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

### <u>System Hacking Goals</u>

- **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

### <u>Authentication and Passwords</u>

- **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 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

### <u>Password Attacks</u>

- **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

### <u>Privilege Escalation and Executing Applications</u>

- **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

### <u>Hiding Files and Covering Tracks</u>

- 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

### <u>Rootkits</u>

- 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

Web-Based Hacking - Servers and Applications

# Wireless Network Hacking

### <u>Wireless Basics</u>

- **802.11 Series** - defines the standards for wireless networks

- **802.15.1** - Bluetooth

- **802.15.4** - Zigbee - low power, low data rate, close proximity ad-hoc networks

- **802.16** - WiMAX - broadband wireless metropolitan area networks

Wireless Standard	Operating Speed (Mbps)	Frequency (GHz)	Modulation Type
802.11a	54	5	OFDM
802.11b	11	2.4	DSSS

802.11d	Variation of a & b	Global use	
802.11e	QoS Initiative	Data and voice	
802.11g	54	2.4	OFDM and DSSS
802.11i	WPA/WPA2 Encryption		
802.11n	100+	2.4-5	OFDM
802.11ac	1000	5	QAM

- **Orthogonal Frequency-Division Multiplexing** (OFDM) - carries waves in various channels
- **Direct-Sequence Spread Spectrum** (DSSS) - combines all available waveforms into a single purpose
- **Basic Service Set** (BSS) - communication between a single AP and its clients
- **Basic Service Set Identifier** (BSSID) - MAC address of the wireless access point
- **Spectrum Analyzer** - verifies wireless quality, detects rogue access points and detects attacks
- **Directional antenna** - signals in one direction; Yagi antenna is a type
- **Omnidirectional antenna** - signals in all directions
- **Service Set Identifier** (SSID) - a text word (<= 32 char) that identifies network; provides no security
- **Three Types of Authentication**
  - **Open System** - no authentication
  - **Shared Key Authentication** - authentication through a shared key (password)
  - **Centralized Authentication** - authentication through something like RADIUS
- **Association** is the act of connecting; **authentication** is the act of identifying the client

### <u>Wireless Encryption</u>

- **Wired Equivalent Privacy** (WEP)
  - Doesn't effectively encrypt anything
  - Uses RC4 for encryption
  - Original intent was to give wireless the same level of protection of an Ethernet hub
  - **Initialization Vector** (IV) - used to calculate a 32-bit integrity check value (ICV)
    - IVs are generally small and are frequently reused
    - Sent in clear text as a part of the header
    - This combined with RC4 makes it easy to decrypt the WEP key
    - An attacker can send disassociate requests to the AP to generate a lot of these
- **Wi-Fi Protected Access** (WPA or WPA2)
  - WPA uses TKIP with a 128-bit key

  - WPA changes the key every 10,000 packets
  - WPA transfers keys back and forth during an **Extensible Authentication Protocol** (EAP)
  - **WPA2 Enterprise** - can tie an EAP or RADIUS server into the authentication
  - **WPA2 Personal** - uses a pre-shared key to authenticate
  - WPA2 uses AES for encryption
  - WPA2 ensures FIPS 140-2 compliance
  - WPA2 uses CCMP instead of TKIP
  - **Message Integrity Codes** (MIC) - hashes for CCMP to protect integrity
  - **Cipher Block Chaining Message Authentication Code** (CBC-MAC) - integrity process of WPA2

Wireless Standard	Encryption	IV Size (Bits)	Key Length (Bits)	Integrity Check
WEP	RC4	24	40/104	CRC-32
WPA	RC4 + TKIP	48	128	Michael/CRC-32
WPA2	AES-CCMP	48	128	CBC-MAC (CCMP)

### <u>Wireless Hacking</u>

- **Threats**
  - Access Control Attacks
  - Integrity Attacks
  - Confidentiality Attacks
  - Availability Attacks
  - Authentication Attacks
- **Network Discovery**
  - Wardriving, warflying, warwalking, etc.
  - Tools such as WiFiExplorer, WiFiFoFum, OpenSignalMaps, WiFinder
  - **WIGLE** - map for wireless networks
  - **NetStumbler** - tool to find networks
  - **Kismet** - wireless packet analyzer/sniffer that can be used for discovery
    - Works without sending any packets (passively)
    - Can detects access points that have not been configured
    - Works by channel hopping
    - Can discover networks not sending beacon frames

    - Ability to sniff packets and save them to a log file (readable by Wireshark/tcpdump)
  - **NetSurveyor** - tool for Windows that does similar features to NetStumbler and Kismet
    - Doesn't require special drivers
- **WiFi Adapter**
  - AirPcap is mentioned for Windows, but isn't made anymore
  - **pcap** - driver library for Windows
  - **libpcap** - driver library for Linux

### <u>Wireless Attacks</u>

- **Rogue Access Point** - places an access point controlled by an attacker
- **Evil Twin** - a rogue AP with a SSID similar to the name of a popular network
  - Also known as a mis-association attack
- **Honeyspot** - faking a well-known hotspot with a rogue AP
- **Ad Hoc Connection Attack** - connecting directly to another phone via ad-hoc network
  - Not very successful as the other user has to accept connection
- **DoS Attack** - either sends de-auth packets to the AP or jam the wireless signal
  - With a de-auth, you can have the users connect to your AP instead if it has the same name
  - Jammers are very dangerous as they are illegal
- **MAC Filter** - only allows certain MAC addresses on a network
  - Easily broken because you can sniff out MAC addresses already connected and spoof it
  - Tools for spoofing include **SMAC** and **TMAC**

### <u>Wireless Encryption Attacks</u>

- **WEP Cracking**
  - Easy to do because of weak IVs
  - **Process**
    1. Start a compatible adapter with injection and sniffing capabilities
    2. Start a sniffer to capture packets
    3. Force the creation of thousands of packets (generally with de-auth)
    4. Analyze captured packets
  - **Tools**
    - **Aircrack-ng** - sniffer, detector, traffic analysis tool and a password cracker

      - Uses dictionary attacks for WPA and WPA 2. Other attacks are for WEP only

      - **Cain and Abel** - sniffs packets and cracks passwords (may take longer)

    - Relies on statistical measures and the PTW technique to break WEP

      - **KisMAC** - MacOS tool to brute force WEP or WPA passwords

      - **WEPAttack**

      - **WEPCrack**

      - **Portable Penetrator**

      - **Elcomsoft's Wireless Security Auditor**

  - Methods to crack include **PTW**, **FMS**, and **Korek** technique

- **WPA Cracking**

  - Much more difficult than WEP

  - Uses a constantly changing temporal key and user-defined password

  - **Key Reinstallation Attack** (KRACK) - replay attack that uses third handshake of another device's session

  - Most other attacks are simply brute-forcing the password

### <u>Wireless Sniffing</u>

- Very similar to sniffing a wired network

- **Tools**

  - **NetStumbler**

  - **Kismet**

  - **OmniPeek** - provides data like Wireshark in addition to network activity and monitoring

  - **AirMagnet WiFi Analyzer Pro** - sniffer, traffic analyzer and network-auditing suite

  - **WiFi Pilot**

# Mobile Communications and IoT

# Mobile Communications and IoT

### <u>Mobile Platform Hacking</u>

- **Three Main Avenues of Attack**

  - **Device Attacks** - browser based, SMS, application attacks, rooted/jailbroken devices

  - **Network Attacks** - DNS cache poisoning, rogue APs, packet sniffing

  - **Data Center (Cloud) Attacks** - databases, photos, etc.

- **OWASP Top 10 Mobile Risks**

  - **M1 - Improper Platform Usage** - misuse of features or security controls (Android intents, TouchID, Keychain)

  - **M2 - Insecure Data Storage** - improperly stored data and data leakage

  - **M3 - Insecure Communication** - poor handshaking, incorrect SSL, clear-text communication

  - **M4 - Insecure Authentication** - authenticating end user or bad session management

  - **M5 - Insufficient Cryptography** - code that applies cryptography to an asset, but is insufficient (does NOT include SSL/TLS)

  - **M6 - Insecure Authorization** - failures in authorization (access rights)

  - **M7 - Client Code Quality** - catchall for code-level implementation problems

  - **M8 - Code Tampering** - binary patching, resource modification, dynamic memory modification

  - **M9 - Reverse Engineering** - reversing core binaries to find problems and exploits

  - **M10 - Extraneous Functionality** - catchall for backdoors that were inadvertently placed by coders

### <u>Mobile Platforms</u>

- **Android** - platform built by Google

  - **Rooting** - name given to the ability to have root access on an Android device

    - **Tools**

      - KingoRoot

      - TunesGo

      - OneClickRoot

      - MTK Droid

- **iOS** - platform built by Apple

  - **Jailbreaking** - different levels of rooting an iOS device

    - **Tools**

      - evasi0n7

      - GeekSn0w

      - Pangu

      - Redsn0w

      - Absinthe

      - Cydia

    - **Techniques**

      - **Untethered** - kernel remains patched after reboot, with or without a system connection

      - **Semi-Tethered** - reboot no longer retains patch; must use installed jailbreak software to re-jailbreak

      - **Tethered** - reboot removes all jailbreaking patches; phone may get in boot loop requiring USB to repair

    - **Types**

      - **Userland exploit** - found in the system itself; gains root access; does not provide admin; can be patched by Apple

      - **iBoot exploit** - found in bootloader called iBoot; uses vulnerability to turn codesign off; semi-tethered; can be patched

      - **BootROM exploit** - allows access to file system, iBoot and custom boot logos; found in device's first bootloader; cannot be patched

- **App Store attacks** - since some App stores are not vetted, malicious apps can be placed there

- **Phishing attacks** - mobile phones have more data to be stolen and are just as vulnerable as desktops

- **Android Device Administration API** - allows for security-aware apps that may help

- **Bring Your Own Device** (BYOD) - dangerous for organizations because not all phones can be locked down by default

- **Mobile Device Management** - like group policy on Windows; helps enforce security and deploy apps from enterprise

  - MDM solutions include XenMobile, IBM, MaaS360, AirWatch and MobiControl

- **Bluetooth attacks** - if a mobile device can be connected to easily, it can fall prey to Bluetooth attacks

  - **Discovery mode** - how the device reacts to inquiries from other devices

    - **Discoverable** - answers all inquiries

    - **Limited Discoverable** - restricts the action

    - **Nondiscoverable** - ignores all inquiries

  - **Pairing mode** - how the device deals with pairing requests

    - **Pairable** - accepts all requests

    - **Nonpairable** - rejects all connection requests

### <u>Mobile Attacks</u>

- **SMS Phishing** - sending texts with malicious links

  - People tend to trust these more because they happen less

  - **Trojans Available to Send**

    - Obad

    - Fakedefender

    - TRAMPS

    - ZitMo

  - **Spyware**

    - Mobile Spy

    - Spyera

- Mobile platform features such as Find my iPhone, Android device tracking and the like can be hacked to find devices, etc.

- **Mobile Attack Platforms** - tools that allow you to attack from your phone

  - Network Spoofer

  - DroidSheep

  - Nmap

- **Bluetooth Attacks**

  - **Bluesmacking** - denial of service against device

  - **Bluejacking** - sending unsolicited messages

  - **Bluesniffing** - attempt to discover Bluetooth devices

  - **Bluebugging** - remotely using a device's features

  - **Bluesnarfing** - theft of data from a device

  - **Blueprinting** - collecting device information over Bluetooth

- **Bluetooth Attack Tools**

  - **BlueScanner** - finds devices around you

  - **BT Browser** - another tool for finding and enumerating devices

  - **Bluesniff** and **btCrawler** - sniffing programs with GUI

  - **Bloover** - can perform Bluebugging

  - **PhoneSnoop** - good spyware option for Blackberry

  - **Super Bluetooth Hack** - all-in-one package that allows you to do almost anything

### <u>IoT Architecture</u>

- **Definition** - a collection of devices using sensors, software, storage and electronics to collect, analyze, store and share data

- **Three Basic Components**

  - Sensing Technology

  - IoT gateways

  - The cloud

- **Operating Systems**

  - **RIOT OS** - embedded systems, actuator boards, sensors; is energy efficient

  - **ARM Mbed OS** - mostly used on wearables and other low-powered devices

  - **RealSense OS X** - Intel's depth sensing version; mostly found in cameras and other sensors

  - **Nucleus RTOS** - used in aerospace, medical and industrial applications

  - **Brillo** - Android-based OS; generally found in thermostats

  - **Contiki** - OS made for low-power devices; found mostly in street lighting and sound monitoring

  - **Zephyr** - option for low-power devices and devices without many resources

  - **Ubuntu Core** - used in robots and drones; known as "snappy"

  - **Integrity RTOS** - found in aerospace, medical, defense, industrial and automotive sensors

  - **Apache Mynewt** - used in devices using Bluetooth Low Energy Protocol

- **Methods of Communicating**

  - **Device to Device** - communicates directly with other IoT devices

  - **Device to Cloud** - communicates directly to a cloud service

  - **Device to Gateway** - communicates with a gateway before sending to the cloud

  - **Back-End Data Sharing** - like device to cloud but adds abilities for parties to collect and use the data

- **Architecture Levels**

  - **Edge Technology Layer** - consists of sensors, RFID tags, readers and the devices

  - **Access Gateway Layer** - first data handling, message identification and routing

  - **Internet Layer** - crucial layer which serves as main component to allow communication

  - **Middleware Layer** - sits between application and hardware; handles data and device management, data analysis and aggregation

  - **Application Layer** - responsible for delivery of services and data to the user

### <u>IoT Vulnerabilities and Attacks</u>

- **I1 - Insecure Web Interface** - problems such as account enumeration, weak credentials, and no account lockout

- **I2 - Insufficient Authentication/Authorization** - assumes interfaces will only be exposed on internal networks and thus is a flaw

- **I3 - Insecure Network Services** - may be susceptible to buffer overflow or DoS attacks

- **I4 - Lack of Transport Encryption/Integrity Verification** - data transported without encryption

- **I5 - Privacy Concerns** - due to collection of personal data

- **I6 - Insecure Cloud Interface** - easy-to-guess credentials make enumeration easy

- **I7 - Insecure Mobile Interface** - easy-to-guess credentials on mobile interface

- **I8 - Insufficient Security Configurability** - cannot change security which causes default passwords and configuration

- **I9 - Insecure Software/Firmware** - lack of a device to be updated or devices that do not check for updates

- **I10 - Poor Physical Security** - because of the nature of devices, these can easily be stolen

- **Sybil Attack** - uses multiple forged identities to create the illusion of traffic

- **HVAC Attacks** - attacks on HVAC systems

- **Rolling Code** - the ability to jam a key fob's communications, steal the code and then create a subsequent code

- **BlueBorne Attack** - attacks against Bluetooth devices

- Other attacks already enumerated in other sections still apply such as MITM, ransomware, side channel

### <u>IoT Hacking Methodology</u>

- **Steps**

  - **Information Gathering** - gathering information about the devices; useful resource is Shodan (Google for IoT devices connected to Internet)

    - **Foren6** - IoT traffic sniffer

  - **Vulnerability Scanning** - same as normal methodology - looks for vulnerabilities

    - **Tools**

      - Nmap

      - RIoT Vulnerability Scanner

      - beSTORM

      - IoTsploit

      - IoT Inspector

  - **Launching Attacks**

    - **Tools**

      - Firmalyzer

      - KillerBee

      - JTAGulator

      - Attify

  - **Gaining Access** - same objectives as normal methodology

  - **Maintaining Access** - same objectives as normal methodology

# Security in Cloud Computing

# Security in Cloud Computing

### <u>Cloud Computing Basics</u>

- **Three Types**
  - **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
  - **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
  - **Software as a Service** (SaaS)
    - Provider supplies on-demand applications to subscribers
    - Offloads the need for patch management, compatability and version control
- **Deployment Models**
  - **Public Cloud** - services provided over a network that is open for public to use
  - **Private Cloud** - cloud solely for use by one tenant; usually done in larger organizations
  - **Community Cloud** - cloud shared by several organizations, but not open to public
  - **Hybrid Cloud** - a composition of two or more cloud deployment models
- **NIST Cloud Architecture**
  - **Cloud Carrier** - organization with responsibility of transferring data; akin to power distributor for electric grid
  - **Cloud Consumer** - aquires and uses cloud products and services
  - **Cloud Provider** - purveyor of products and services
  - **Cloud Broker** - manages use, performance and delivery of services as well as relationships betwen providers and subscribers
  - **Cloud Auditor** - independent assor of cloud service an security controls
- **FedRAMP** - regulatory effort regarding cloud computing
- **PCI DSS** - deals with debit and credit cards, but also has a cloud SIG

### <u>Cloud Security</u>

- 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

- **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

- **Tools**

  - **CloudInspect** - pen-testing application for AWS EC2 users

  - **CloudPassage 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**

### <u>Threats and Attacks</u>

- **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 int he background

- Others include malicious insiders, inadequate design and DDoS

- **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

- **Side Channel Attack** - using an existing VM on the same physical host to attack another

  - This is more broadly defined as using something other than the direct interface to attack a system

Trojans and Other Attacks

Malware Basics

- **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
- **Crypters** - use a combination of encryption and code manipulation to render malware undetectable to security programs
- **Packers** - use compression to pack the executable which helps evage signature based detection
- **Exploit Kits** - help deliver exploits and payloads
  - Infinity
  - Bleeding Life
  - Crimepack
  - Blackhole Exploit Kit

### <u>Trojans</u>

- **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
- **Types**
  - **Defacement trojan**
  - **Proxy server trojan**
  - **Botnet trojan**
    - Chewbacca
    - Skynet
  - **Remote access trojans**
    - RAT

    - MoSucker
    - Optix Pro
    - Blackhole
  - **E-banking trojans**
      - Zeus
      - Spyeye
  - **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
- **Netcat**
  - "Swiss army knife" of tcp/ip hacking
  - Provides all sorts of control over a remote shell on a target
  - Connects via **nc -e IPaddress Port#**
  - From attack machine **nc -l -p 5555** opens a listening port on 5555
  - Can connect over TCP or UDP, from any port
  - Offers DNS forwarding, port mapping and forwarding and proxying
- **Trojan Port Numbers**

Trojan Name	Port
Death	2
Senna Spy	20
Hackers Paradise	31,456
TCP Wrappers	421
Doom, Santaz Back	666
Silencer, WebEx	1001
RAT	1095-98
SubSeven	1243
Shiva-Burka	1600
Trojan Cow	2001
Deep Throat	6670-71
Tini	7777
NetBus	12345-6

| Whack a Mole | 12361-3|

| Back Orifice | 31337,8|

- **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

### <u>Viruses and Worms</u>

- **Virus** - self-replicating program that reproduces by attaching copies of itself into other executable code
  - Usually installed by user clicking on malicious file attachments or downloads
  - **Fake Antivirus** - tries to convince a user has a virus and have them download an AV that is a virus itself
- **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
- **Other Virus Types**

  - **Boot Sector Virus** - known as system virus; moves boot sector to another location and then inserts its code int he 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

  - **Multipartite Virus** - attempts to infect both boot sector and files; generally refers to viruses with multiple infection methods

  - **Macro Virus** - written in VBA; infects template files - mostly Word and Excel

  - **Polymorphic Code Virus** - mutates its code by using a polymorphic engine; difficult to find because code is always changing

  - **Encryption Virus** - uses encryption to hide the code from antivirus

  - **Metamorphic Virus** - rewrites itself every time it infects a new file

  - **Stealth Virus** - known as a tunneling virus; attempts to evade AVs by intercepting their requests and returning them instead of letting them pass to the OS

  - **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

### <u>Analyzing Malware</u>

- **Steps**

  1. Make sure you have a good test bed

     - 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

     - Tools - binText and UPX help with looking at binary

  3. Run the malware and check out processes

     - Use Process Monitor, etc. to look at processes

     - Use NetResident, TCPview or even Wireshark to look at network activity

  4. Check and see what files were added, changed, or deleted

     - Tools - IDA Pro, VirusTotal, Anubis, Threat Analyzer

- **Preventing Malware**

  - Make sure you know what is going on in your system

  - Have a good antivirus that is up to date

  - **Sheepdip** - system that is used to check things introduced into a network

    - Is airgapped

### <u>Denial of Service Attacks</u>

- Seeks to take down a system or deny access to it by authorized users

- **Botnet** - network of zombie computers a hacker uses to start a distributed attack

  - Can be controlled over HTTP, HTTPS, IRC, or ICQ

- **Basic Categories**

  - **Fragmentation attacks** - attacks take advantage of the system's ability to reconstruct fragmented packets

  - **Volumetric attacks** - bandwidth attacks; consume all bandwidth for the system or service

  - **Application attacks** - consume the resources necessary for the application to run

    - Note - application level attakcs are against weak code; application attacks are just the general term

  - **TCP state-exhaustion attacks** - go after load balancers, firewalls and application servers

  - **SYN attack** - sends thousands of SYN packets to the machine with a false source address; eventually engages all resources and exhausts the machine

  - **SYN flood** - sends thousands of SYN packets; does not spoof IP but doesn't respond to the SYN/ACK packets; eventually bogs down the computer, runs out of resources

  - **ICMP flood** - sends ICMP Echo packets with a spoofed address; eventually reaches limit of packets per second sent

  - **Smurf** - large number of pings to the broadcast address of the subnet with source IP spoofed as the target; entire subnet responds exhausting the target

  - **Fraggle** - same as smurf but with UDP packets

  - **Ping of Death** - fragments ICMP messages; after reassembled, the ICMP packet is larger than the maximum size and crashes the system

  - **Teardrop** - overlaps a large number of garbled IP fragments with oversized payloads; causes older systems to crash due to fragment reassembly

  - **Peer to peer** - clients of peer-to-peer file-sharing hub are disconnected and directed to connect to the target system

  - **Phlashing** - a DoS attack that causes permanent damage to a system; also called bricking a system

  - **LAND attack** - sends a SYN packet to the target with a spoofed IP the same as the target; if vulnerable, target loops endlessly and crashes

- **Low Orbit Ion Cannon** (LOIC) - DDoS tool that floods a target with TCP, UDP or HTTP requests

- **Other Tools**

  - Trinity - Linux based DDoS tool

  - Tribe Flood Network - uses voluntary botnet systems to launch massive flood attacks

  - R-U-Dead-Yet (RUDY) - DoS with HTTP POST via long-form field submissions

### <u>Session Hijacking</u>

- Attacker waits for a session to begin and after the victim authenticates, steals the session for himself

- **Steps**

  1. Sniff the traffic between the client and 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

- Can be done via brute force, calculation or stealing

- Predicting can be done by knowing the window size and the packet sequence number

- Sequence numbers increment on **acknowledgement**

  - For example, an acknowledgement of 105 with a window of 200 means you could expect sequence numbering from 105 to 305

- **Tools**

  - **Ettercap** - man-in-the-middel tool and packet sniffer on steroids

  - **Hunt** - sniff, hijack and reset connections

  - **T-Sight** - easily hijack sessions and monitor network connections

  - **Zaproxy**

  - **Paros**

  - **Burp Suite**

  - **Juggernaut**

  - **Hamster**

  - **Ferret**

- **Countermeasures**

  - Using unpredictable session IDs

  - Limiting incoming connections

  - Minimizing remote access

  - Regenerating the session key after authentication

  - Use IPSec to encrypt

- **IPSec**

  - **Transport Mode** - payload and ESP trailer are encrypted; IP header is not

  - **Tunnel mode** - everything is encrypted; cannot be used with NAT

  - **Architecture Protocols**

    - **Authentication Header** - guarantees the integrity and authentication of IP packet sender

    - **Encapsulating Security Payload** (ESP) - provides origin authenticity and integrity as well as confidentiality

    - **Internet Key Exchange** (IKE) - produces the keys for the encryption process

    - **Oakley** - uses Diffie-Hellman to create master and session keys

    - ** Internet Security Association Key Management Protocol** (ISAKMP) - software that facilitates encrypted communication between two endpoints

# Cryptography

# Cryptography 101

### <u>Cryptograph Basics</u>

- **Cryptography** - science or study of protecting information whether in transit or at rest

  - Renders the information unusable to anyone who can't decrypt it

  - Takes plain text, applies cryptographic method, turn it into cipher text

- **Cryptanalysis** - study and methods used to crack cipher text

- **Linear Cryptanalysis** - works best on block ciphers

- **Differential Cryptanalysis** - applies to symmetric key algorithms

  - Compares differences in the inputs to how each one affects the outcome

- **Integral cryptanalysis** - input vs output comparison same as differential; however, runs multiple computations of the same block size input

- Plain text doesn't necessarily mean ASCII format - it simply means unencrypted data

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

### <u>Encryption Algorithms and Techniques</u>

- **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
- **Steam 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

### <u>Symmetric Encryption</u>

- **Symmetric Encryption** - known as single key or shared key
  - One key is used to encrypt and decrypt the data
  - Problems include key distribution and management
  - Suitable for large amounts of data
  - Harder for groups of people because more keys are needed as group increases
  - Does nothing for nonrepudiation; only performs confidentiality
- **Algorithms**
  - **DES** - block cipher; 56 bit key; quickly outdated and now considered not very secure
  - **3DES** - block cipher; 168 bit key; more effective than DES but much slower
  - **AES** (Advanced Encryption Standard) - block cipher; 128, 192 or 256 bit key; replaces DES; much faster than DES and 3DES
  - **IDEA** (International Data Encryption Algorithm) - block cipher; 128 bit key; originally used in PGP 2.0
  - **Twofish** - block cipher; up to 256 bit key
  - **Blowfish** - fast block cipher; replaced by AES; 64 bit block size; 32 to 448 bit key; considered public domain

  - **RC** (Rivest Cipher) - RC2 to RC6; block cipher; comparable key length up to 2040 bits; RC6 (latest version) uses 128 bit blocks and 4 bit working registers; RC5 uses variable block sizes and 2 bit working registers. RC4 is a stream cipher

### <u>Asymmetric Encryption</u>

- Uses two types of keys for encryption and decryption

- **Public Key** - generally used for encryption; can be sent to anyone

- **Private Key** - kept secret; used for decryption

- Comes down to what one key encrypts, the other decrypts

- The private key is used to digitally sign a message

- **Algorithms**

  - **Diffie-Hellman** - developed as a key exchange protocol; used in SSL and IPSec; if digital signatures are waived, vulnerable to MITM attacks

  - **Elliptic Curve Cryptosystem** (ECC) - uses points on elliptical curve along with logarithmic problems; uses less processing power; good for mobile devices

  - **El Gamal** - not based on prime number factoring; uses solving of discrete logarithm problems

  - **RSA** - achieves strong encryption through the use of two large prime numbers; factoring these create key sizes up to 4096 bits; modern de facto standard

- Only downside is it's slower than symmetric especially on bulk encryption and processing power

### <u>Hash Algorithms</u>

- **Hash** - one-way mathematical function that produces a fix-length string (hash) based on the arrangement of data bits in the input

- **Algorithms**

  - **MD5** (Message Digest algorithm) - produces 128 bit hash expressed as 32 digit hexadecimal number; has serious flaws; still used for file download verification

  - **SHA-1** - developed by NSA; 160 bit value output

  - **SHA-2** - four separate hash functions; produce outputs of 224, 256, 384 and 512 bits; not widely used

  - **SHA-3** - uses sponge construction

  - **RIPEMD-#** - works through 80 stages, executing 5 blocks 16 times each; uses modulo 32 addition

- **Collision** - occurs when two or more files create the same output

  - Can happen and can be used an attack; rare, though

- **DUHK Attack** (Don't Use Hard-Coded Keys) - allows attackers to access keys in certain VPN implementations; affects devices using ANSI X9.31 with a hard-coded seed key

- **Rainbow Tables** - contain precomputed hashes to try and find out passwords

- **Salt** - used with a hash to obscure the hash; collection of random bits

- **Things to Remember**

  - Hashes are used for integrity

  - Hashes are one-way functions

- **Tools**

  - HashCalc

  - MD5 Calculator

  - HashMyFiles

### <u>Steganography</u>

- **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

### <u>PKI System</u>

- **Public Key Infrastructure** (PKI) - structure designed to verify and authenticate the identity of individuals

- **Registration Authority** - verifies user identity

- **Certificate Authority** - third party to the organization; creates and issues digital certificates

- **Certificate Revocation List** (CRL) - used to track which certificates have problems and which have been revoked

- **Validation Authority** - used to validate certificates via Online Certificate Status Protocol (OCSP)

- **Trust Model** - how entities within an enterprise deal with keys, signatures and certificates

- **Cross-Certification** - allows a CA to trust another CS in a completely different PKI; allows both CAs to validate certificates from either side

- **Single-authority system** - CA at the top

- **Hierarchical trust system** - CA at the top (root CA); makes use of one or more RAs (subordinate CAs) underneath it to issue and manage certificates

### <u>Digital Certificates</u>

- **Certificate** - electronic file that is used to verify a user's identity; provides nonrepudiation

- **X.509** - standard used for digital certificates

- **Contents of a Digital Certificate**

  - **Version** - identifies certificate format

  - **Serial Number** - used to uniquely identify certificate

  - **Subject** - who or what is being identified

  - **Algorithm ID** (Signature Algorithm) - shows the algorithm that was used to create the certificate

  - **Issuer** - shows the entity that verifies authenticity

  - **Valid From and Valid To** - dates certificate is good for

  - **Key Usage** - what purpose the certificate serves

  - **Subject's Public Key** - copy of the subject's public key

  - **Optional Fields** - Issuer Unique Identifier, Subject Alternative Name, and Extensions

- Some root CAs are automatically added to OSes that they already trust; normally are reputable companies

- **Self-Signed Certificates** - certificates that are not signed by a CA; generally not used for public; used for development purposes

  - Signed by the same entity it certifies

### <u>Digital Signatures</u>

- When signing a message, you sign it with your **private** key and the recipient decrypts the hash with your **public** key

- **Digital Signature Algorithm** (DSA) - used in generation and verification of digital signatures per FIPS 186-2

### <u>Full Disk Encryption</u>

- **Data at Rest** (DAR) - data that is in a stored state and not currently accessible
  - Usually protected by **full disk encryption** (FDE) with pre-boot authentication
  - Example of FDE is Microsoft BitLocker and McAfee Endpoint Encryption
  - FDE also gives protection against boot-n-root

### <u>Encrypted Communication</u>

- **Often-Used Encrypted Communication Methods**
  - **Secure Shell** (SSH) - secured version of telnet; uses port 22; relies on public key cryptography; SSH2 is successor and includes SFTP
  - **Secure Sockets Layer** (SSL) - encrypts data at transport layer and above; uses RSA encryption and digital certificates; has a six-step process; largely has been replaced by TLS
  - **Transport Layer Security** (TLS) - uses RSA 1024 and 2048 bits; successor to SSL; allows both client and server to authenticate to each other; TLS Record Protocol provides secured communication channel
  - **Internet Protocol Security** (IPSEC) - network layer tunneling protocol; used in tunnel and transport modes; ESP encrypts each packet
  - **PGP** - Pretty Good Privacy; used for signing, compress and encryption of emails, files and directories; known as hybrid cryptosystem - features conventional and public key cryptography
  - **S/MIME** - standard for public key encryption and signing of MIME data; only difference between this and PGP is PGP can encrypt files and drives unlike S/MIME
- **Heartbleed** - attack on OpenSSL heartbeat which verifies data was received correctly
  - Vulnerability is that a single byte of data gets 64kb from the server
  - This data is random; could include usernames, passwords, private keys, cookies; very easy to pull off
  - nmap -d --script ssl-heartbleed --script-args vulns.showall -sV [host]
  - Vulnerable versions include Open SSL 1.0.1 and 1.0.1f
  - CVE-2014-0160
- **FREAK** (Factoring Attack on RSA-EXPORT Keys) - man-in-the-middle attack that forces a downgrade of RSA key to a weaker length
- **POODLE** (Paddling Oracle On Downgraded Legacy Encryption) - downgrade attack that used the vulnerability that TLS downgrades to SSL if a connection cannot be made
  - SSl 3 uses RC4, which is easy to crack
  - CVE-2014-3566
  - Also called PoodleBleed

- **DROWN** (Decrypting RSA with Obsolete and Weakened eNcyption) - affects SSL and TLS services

  - Allows attackers to break the encryption and steal sensitive data

  - Uses flaws in SSL v2

  - Not only web servers; can be IMAP and POP servers as well

### <u>Cryptography Attacks</u>

- **Known plain-text attack** - has both plain text and cipher-text; plain-text scanned for repeatable sequences which is compared to cipher text

- **Chosen plain-text attack** - attacker encrypts multiple plain-text copies in order to gain the key

- **Adaptive chosen plain-text attack** - attacker makes a series of interactive queries choosing subsequent plaintexts based on the information from the previous encryptions; idea is to glean more and more information about the full target cipher text and key

- **Cipher-text-only attack** - gains copies of several encrypted messages with the same algorithm; statistical analysis is then used to reveal eventually repeating code

- **Replay attack**

  - Usually performed within context of MITM attack

  - Hacker repeats a portion of cryptographic exchange in hopes of fooling the system to setup a communications channel

  - Doesn't know the actual data - just has to get timing right

- **Chosen Cipher Attack**

  - Chooses a particular cipher-text message

  - Attempts to discern the key through comparative analysis

  - RSA is particularly vulnerable to this

- **Side-Channel Attack**

  - Monitors environmental factors such as power consumption, timing and delay

- **Tools**

  - Carnivore and Magic Lantern - used by law enforcement for cracking codes

  - L0phtcrack - used mainly against Windows SAM files

  - John the Ripper - UNIX/Linux tool for the same purpose

  - PGPcrack - designed to go after PGP-encrypted systems

  - CrypTool

  - Cryptobench

  - Jipher

- Keys should still change on a regular basis even though they may be "unhackable"

- Per U.S. government, an algorithm using at least a 256-bit key cannot be cracked

# Low Tech: Social Engineering and Physical Security

# Low Tech: Social Engineering and Physical Security

### <u>Social Engineering</u>

- The art of manipulating a person or group into providing information or a service they would otherwise not have given
- **Phases**
  1. Research (dumpster dive, visit websites, tour the company, etc.)
  2. Select the victim (identify frustrated employee or other target)
  3. Develop a relationship
  4. Exploit the relationship (collect sensitive information)
- **Reasons This Works**
  - Human nature (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

### <u>Human-Based Attacks</u>

- **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 has a fake badge and walks in behind someone who has a valid one
- **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

- **Rebecca** or **Jessica** - targets for social engineering

- **Insider Attack** - an attack from an employee, generally disgruntled

  - Sometimes subclassified (negligent insider, professional insider)

### <u>Computer-Based Attacks</u>

- 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** - use of malicious code that redirects a user's traffic

- **Spimming** - sending spam over instant message

- **Tools** - Netcraft Toolbar and PhishTank Toolbar

- **Fave Antivirus** - very prevalent attack; pretends to be an anti-virus but is a malicious tool

### <u>Mobile-Based Attacks</u>

- **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**)

### <u>Physical Security Basics</u>

- **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.)

## The Pen Test: Putting It All Together

# The Pen Test: Putting It All Together

- **Security Assessment** - test performed in order to assess the level of security on a network or system
- **Security Audit** - policy and procedure focused; tests whether organization is following specific standards and policies
- **Vulnerability Assessment** - scans and tests for vulnerabilities but does not intentionally exploit them
- **Penetration Test** - looks for vulnerabilities and actively seeks to exploit them
- Need to make sure you have a great contract in place to protect you from liability
- **Types of Pen Tests**
  - **External assessment** - analyzes publicly available information; conducts network scanning, enumeration and testing from the network perimeter
  - **Internal Assessment** - performed from within the organization, from various network access points
- **Red Team** - pen test team that is doing the attacking
- **Blue Team** - pen test team that is doing the defending
- **Purple Team** - pen test team that is doing both attacking and defending
- **Automated Testing Tools**
  - **Codenomicon** - utilizes fuzz testing that learns the tested system automatically; allows for pen testers to enter new domains such as VoIP assessment, etc.
  - **Core Impact Pro** - best known, all-inclusive automated testing framework; tests everything from web applications and individual systems to network devices and wireless
  - **Metasploit** - framework for developing and executing code against a remote target machine

  - **CANVAS** - hundreds of exploits, automated exploitation system and extensive exploit development framework
- **Phases of Pen Test**
  - **Pre-Attack Phase** - reconnaissance and data-gathering
  - **Attack Phase** - attempts to penetrate the network and execute attacks
  - **Post-Attack Phase** - Cleanup to return a system to the pre-attack condition and deliver reports

### <u>Security Assessment Deliverables</u>

- Usually begins with a brief to management
  - Provides information about your team and the overview of the original agreement
  - Explain what tests were done and the results of them
- **Comprehensive Report Parts**
  - Executive summary of the organization's security posture
  - Names of all participants and dates of tests
  - List of all findings, presented in order of risk
  - Analysis of each finding and recommended mitigation steps
  - Log files and other evidence (screenshots, etc.)
- Example reports and methodology can be found in the **Open Source Testing Methodology Manual** (OSSTMM)

### <u>Terminology</u>

- **Types of Insiders**
  - **Pure Insider** - employee with all rights and access associated with being an employee
    - **Elevated Pure Insider** - employee who has admin privileges
  - **Insider Associate** - someone with limited authorized access such as a contractor, guard or cleaning service person
  - **Insider Affiliate** - spouse, friend or client of an employee who uses the employee's credentials to gain access
  - **Outside Affiliate** - someone outside the organization who uses an open access channel to gain access to an organization's resources