CompTIA Security+

Attacks, Threats, and Vulnerabilities

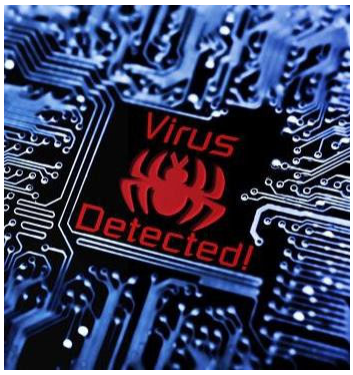
Domain 1 – 24%

CyberProtex

1

Basic Malware Terminology

- Spyware – Malware that monitors user activity and reports to a third party
- Adware – Malware that provides unwanted ads
- Worm – Self-replicating and propagating code
- Software Exploitation
  – Identifying and gaining unauthorized access to system resources through gaps in software security

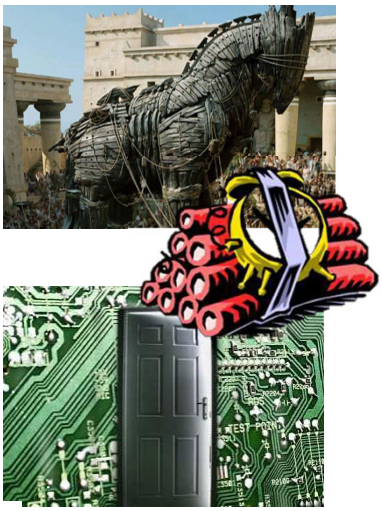


CyberProtex

Image courtesy of: http://home.bt.com/tech-gadgets/computing/what-to-do-if-your-pc-is-infected-by-malware-11363945220841

2

Malware Terminology



- Trojan – Malware that is added to a legitimate program and that operates on its own after installation
  - ✓ RAT – Remote Access Trojan
- Logic Bomb – Malware that executes on a predefined time
- Backdoor
  - ✓Benign – Software "Hooks"
  - ✓Malicious – Embedded malware that allows unauthorized access to a system

CyberProtex

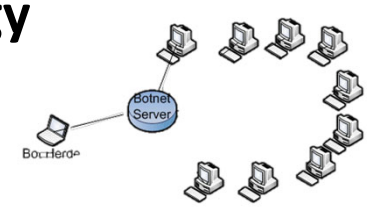
Image courtesy of: http://securityaffairs.co/wordpress/

3

3

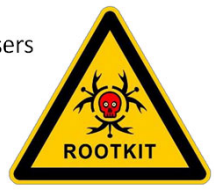
Malware Terminology

- Botnets – Botnets – Malware running on multiple exploited systems that are used in a coordinated fashion



- Ransomware – Malware that often encrypts victim resources and demands payment to decrypt

- Rootkits – Malware that hides malicious processes and activities from users and administrators



CyberProtex

Images courtesy of: http://www.rit.edu/its/news/archive/07feb/botnet.html

4

4

Application Attacks

- What kind of attacks do attackers employ against networks?
  - Zero day - An attack based on a previously unknown and unpatched vulnerability.
  - Spoofing Attacks – MAC, IP, DNS, Email
  - Pass the Hash – use hash directly without cracking
  - Replay Attacks – Collection of and replay of old network traffic to look like live traffic
  - Man-In-The-Middle Attack (MITM)– Interception and forwarding of traffic between nodes
    - ✓ Unencrypted and Encrypted

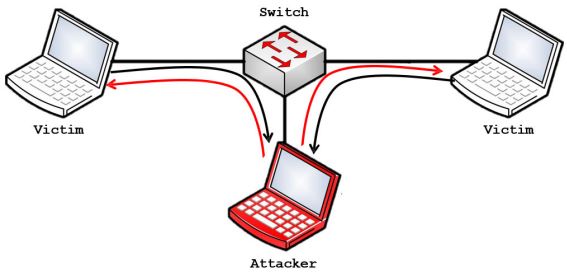


Image courtesy of: https://www.youtube.com/watch?v=Vvln4_HfIVg

CyberProtex

5

5

Application Attacks

- What kind of attacks do attackers employ against networks?
  - ✓ Buffer Overflow Attack – More data put in fixed length buffer than the buffer can handle
  - ✓ Christmas Attack – Network mapping scan to circumvent firewall detection
    - Sets FIN-PSH-URG Flags
  - ✓ Pharming – Traffic redirection
  - ✓ Phishing – Email social engineering
    - Spear Phishing
  - ✓ Vishing
    - Phishing with VoIP

CyberProtex

6

6

Application Attacks

- Cross-site scripting

Injections

- Structured query language (SQL)
- Dynamic link library (DLL)
- Lightweight directory access protocol (LDAP)
- Extensible markup language (XML)

- Directory traversal
- Buffer overflows
- Race conditions
  - Time of check/time of use
- Error handling
- Improper input handling
- Replay attack
  - Session replays
- Integer overflow
- Request forgeries
  - Server-side
  - Cross-site
- Application programming interface (API) attacks
- Resource exhaustion
- Memory leak

Memory Structure

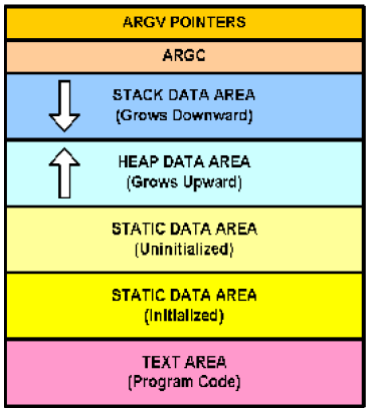


Image courtesy of: Donaldson, M. Inside the Buffer, overflow Attack: Mechanism, Method, and Prevention. https://www.sans.org/reading-room/whitepapers/securecode/buffer-overflow-attack-mechanism-method-prevention-386

Type of memory	Actions causing error
Stack (local variables) memory errors	Reading/writing to memory out of the bounds of a static array. (array index overflow - index too large/underflow - negative index) Function pointer corruption: Invalid passing of function pointer and thus a bad call to a function
Heap memory errors	Attempting to free memory already freed. Freeing memory that was not allocated. Attempting to read/write memory already freed. Attempting to read/write to memory which was never allocated. Memory allocation error. Reading/writing to memory out of the bounds of a dynamically allocated array

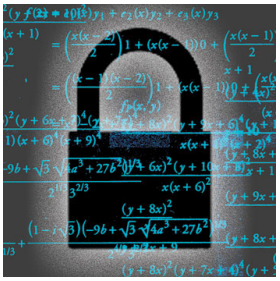
CyberProtex

Buffer Overflow

Step	Description	Supplemental Material
Step 1	Discover the vulnerability – this vulnerability is normally found with user input and any associated function	Key functions for moving data between memory locations include strcpy, strncpy, strcat, sprint, scanf, fgets, gets, getws, memcpy, memove
Step 2	Determine field parameters for minimum and maximum of the user input	The hacker tries different input until the overflow occurs
Step 3	Push exploit code into memory by overrunning the buffer to open a shell and execute arbitrary commands	Unix: target programs with the UID of 0 Windows: target programs that run as SYSTEM
Step 4	Validate exploit code fits inside buffer and does not filter out	

CyberProtex

System Attacks



- INJECTION
  - ✓ Code injection technique
  - ✓ Used to attack data-driven applications
  - ✓ SQL injection - in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- Cross-site request forgery
  - ✓ Tricks a user into executing an unwanted action in a web application
- Cross-site scripting (XSS)
  - ✓ Typically found in web applications
  - ✓ XSS enables attackers to inject client-side scripts into web pages viewed by other users
  - ✓ Used by attackers to bypass access controls such as the same-origin policy

CyberProtex

Wireless Network Attacks

- Rogue Access points
  - access point installed on a wired enterprise network
  - without authorization from the network administrator.
- Jamming/Interference
  - denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic.

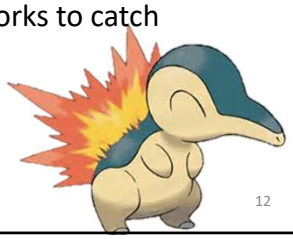
CyberProtex

11

11

Wireless Network Attacks

- ➢IV – Initialization Vector attack
  - ✓IV (Initialization Vector) helps start and end symmetric encryption
  - ✓Modifies IV of encrypted wireless packet during transmission
- ➢Evil twin
  - ✓A hotspot that looks legitimate but really is a fake copy that is used to collect personal information
- ➢War Driving
  - ✓Searching for open Wi-Fi networks to join for malicious means
  - ✓Think Pokémon Go hunting, but you are looking for networks to catch



CyberProtex

12

12

Wireless Network Attacks

- RFID – Radio Frequency Identification
  - ✓Steal digital data, disable tag, modify data
- NFC – Near Field Communications
  - ✓Attack on nearby cell phone
- WPS
  - ✓Wi-Fi Protected Setup (WPS)
  - ✓To crack a WiFi password that has WPS enabled.
- Bluejacking
  - ✓Using Bluetooth to send unsolicited messages
- Bluesnarfing
  - ✓ Theft of information from a wireless device through a Bluetooth connection.

CyberProtex

Password Attacks

- Brute-Force Attack
  - ✓ Online vs. Offline
- Dictionary Attack
- Hybrid Attack
- Birthday Attack
- Rainbow Tables

CyberProtex

Image courtesy of: http://arstechnica.com/security/2013/03/how-i-became-a-password-cracker/

Cryptographic Attacks

hello CyberProtex students! Study hard!

ᑎᗝᒪᒪᕮ ᒪᐸᑌᗝᖴᓀᖴᕮᐳᗝᐳ ᐯᐳᐸᑐᗝᗝᐳᐯ! ᐯᐳ ᐸᑐᐸ ᑎᒍᖴᑐ!

- Known plain text/cipher text
- Collision
- Downgrade
- Weak Implementations

CyberProtex

Image courtesy of: http://arstechnica.com/security/2013/03/how-i-became-a-password-cracker/ 15

15

Privilege Escalation

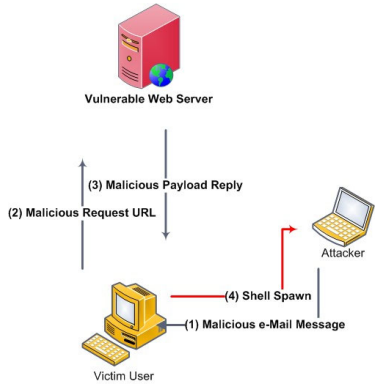
- Raising a non- privileged user or system account to administrative access
- Due to the lack of access for the non- privileged user or system account

CyberProtex

Image courtesy of: https://latesthackingnews.com/2014/06/05/privilege-escalation-in-windows/ 16

16

Client-Side Attacks



- Client-Side attacks take advantage of users through:
  - ✓Clicking links
  - ✓Opening documents
  - ✓Redirecting to a malicious websites

CyberProtex

Image courtesy of: http://securityhorror.blogspot.com/2012/09/industrializing-client-side-attacks.html

Hijacking Attacks

- Typo Squatting
  - ✓ Synonymous with URL hijacking
  - ✓ Creating domains/registering sites closely related to legitimate sites
- Session Hijacking
- Clickjacking
- Domain hijacking

CyberProtex

Image courtesy of: http://www.duetsblog.com/2011/01/articles/domain-names/typosquatting-not-just-a-for-profit-problem/

Watering Hole Attack

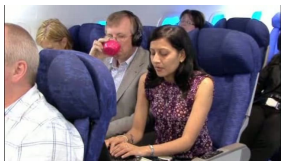
- Attacker analysis of sites to identify potential vulnerabilities
- Attacker exploit of the vulnerable site
- Attacker waits for victims to visit the site and exploit those systems

CyberProtex

Image courtesy of: https://gcn.com/blogs/pulse/2013/01/microsoft-acts-to-plug-watering-hole-attack.aspx

19

19



Social Engineering Attacks

- Shoulder Surfing
- Dumpster Diving
- Tailgating
- Impersonation
- Authority Figure
- Help Desk Spoof
- Outside Support
  - ✓Support Contractors

Technical Attacks

- Vishing
- Phishing
- Spearfishing
  - ✓ Whaling
- Hoaxes

CyberProtex

Image courtesy of: https://www.social-engineer.com/phishing-service

20

20

Social Engineering Tools

- Social Engineering is aided in many ways by trust and that trust can also be manipulated by the use of:
  - ✓ Authority
  - ✓ Intimidation
  - ✓ Social Proof
  - ✓ Scarcity
  - ✓ Urgency
  - ✓ Familiarity
  - ✓ Trust

CyberProtex

21

21

Indicators for Network Attacks

Malicious code or script execution

- PowerShell
- Python
- Bash
- Macros
- Visual Basic for Applications (VBA)

Layer 2 attacks

- Address resolution protocol (ARP) poisoning
- Media access control (MAC) flooding
- MAC cloning

22

22

Network Attacks
DNS and ARP Poisoning

DNS poisoning

- Also known as DNS cache poisoning or DNS spoofing
- Uses vulnerabilities in the domain name system (DNS)
- Divert Internet traffic away from legitimate servers and towards fake ones.

ARP poisoning

- Attacker sends forged ARP replies
  - ✓ Address Resolution Protocol (ARP) Usually aimed at a certain IP or MAC address
  - ✓ Causes victim's traffic to go directly to attacker
- Used to launch DoS, man-in-the-middle, and MAC flooding attacks
- Requires local access

CyberProtex

23

23

Network Attacks
Denial of Service (DoS) Attacks

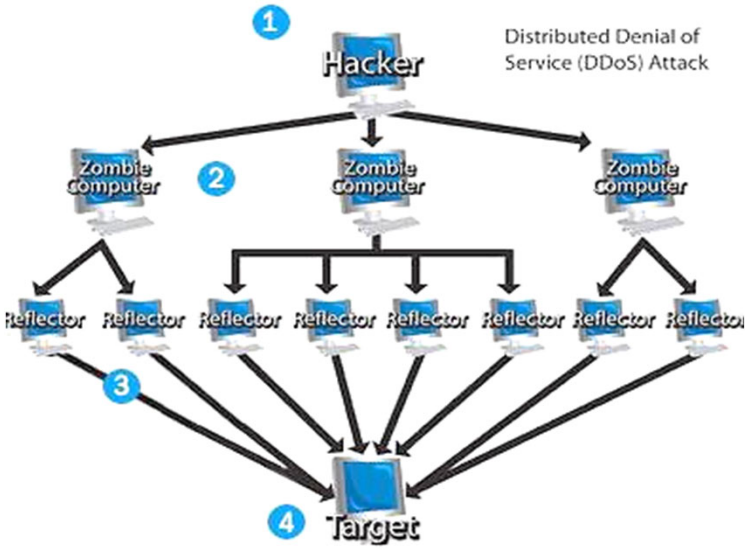
- Attacks that prevent legitimate users from gaining access to resources
- Based on the scale of the attack Denial of Service can be distributed utilizing a wide variety of victim systems
  - ✓ Distributed Denial of Service (DDoS)
- Disassociation
- Amplification
- Examples
  - ✓ Ping of Death -Manipulation of ping packets by increasing packet size and attempting to overwhelm the network resources of a victim system
  - ✓ Smurf Attack - A DDoS attack in which a victim system or network is flooded with spoofed ICMP packets
  - ✓ Fraggle Attack - A DDoS attack in which a victim system or network is flooded with spoofed UDP packets
  - ✓ Land Attack - A DoS attack in which SYN packets are manipulated to have the same source and destination IP address of an intended victim

CyberProtex

24

24

DDoS Attacks



CyberProtex

Image courtesy of http://computer.howstuffworks.com/zombie-computer3.htm

25

25

Threat Actors

- Script kiddies
- Hacktivist
- Organized Crime
- Nation States
  - ✓ Advanced persistent threats (*APT*) groups
- Competitors
- Insiders
  - ✓ Attackers from inside organizations continues to rise
  - ✓ Organizations should implement an insider threat program

CyberProtex

Image courtesy of: http://www.gtscoalition.com/insider-threat-programs-5-easy-steps-to-protect-your-company/

26

26

Techniques used in Security Assessments

Threat hunting

- Intelligence fusion
- Threat feeds
- Advisories and bulletins
- Maneuver

Vulnerability scans
- False positives
- False negatives
- Log reviews
- Credentialed vs. non-credentialed
- Intrusive vs. non-intrusive
- Application
- Web application
- Network
- Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS)
- Configuration review

Techniques used in Security Assessments

Syslog/Security information and event management (SIEM)
- Review reports
- Packet capture
- Data inputs
- User behavior analysis
- Sentiment analysis
- Security monitoring
- Log aggregation
- Log collectors

• Security orchestration, automation, and response (SOAR)

Penetration & Vulnerability Testing

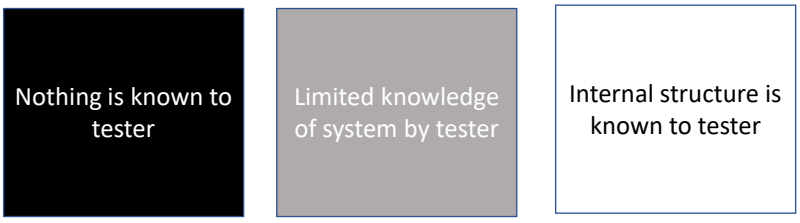
- *Penetration testing*
- *Personnel testing*
- *Physical testing*
- *System and network testing*

Phases of Penetration Testing

Technique	Description
Reconnaissance	• Tester gathers as much info about targets as possible. • Helps tester craft their simulated attack.
Initial exploitation	• Tester begins exploitation after reconnaissance. • Gain access to network or hosts, obtain credentials, etc.
Escalation of privilege	• Tester tries to gain greater control over systems. • Can do more damage with higher privileges.
Pivoting	• Tester compromises a central host. • Tester can spread to other hosts and network segments.
Persistence	• Tester maintains access to the network. • Evaluate ease of gaining a covert foothold in the network.

Penetration Testing

Black box – Gray box – White box



CyberProtex

31

31

Penetration Testing Techniques

Penetration testing
- Known environment
- Unknown environment
- Partially known environment
- Rules of engagement
- Lateral movement
- Privilege escalation
- Persistence
- Cleanup
- Bug bounty
- Pivoting

Passive and active reconnaissance
- Drones
- War flying
- War driving
- Footprinting
- OSINT

Exercise types
- Red-team
- Blue-team
- White-team
- Purple-team

32

32

Types of Sniffers

Types of Sniffers	Description	Example
Local Area Network (LAN)	Monitors internal network to yield live systems	MRTG
Protocol	1. List of protocols generated from captured data 2. Specialized sniffers configured based on step 1 hone attack vector	SoftPerfect
Address Resolution Protocol (ARP)	Captures IP addresses and associated MAC addresses	XArp
TCP Session Stealing	Captures traffic between two hosts to become man in the middle	TCPDump
Application-Level	Generated from data packets to determine operating system, SQL, application specific TCP port data	Wireshark

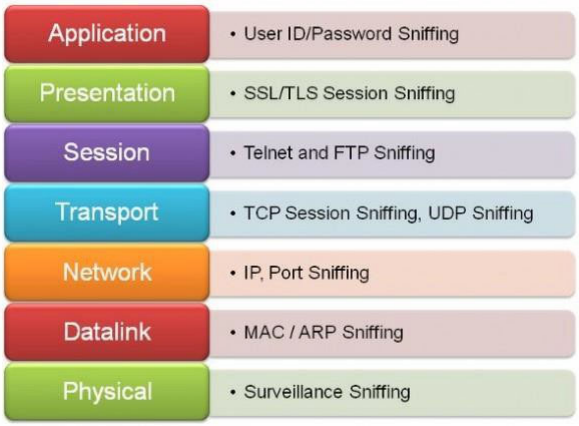
CyberProtex

33

33

Sniffing Across the Open System Interconnect Model

The kind of information that can be sniffed across a network interface depends where in the OSI model you are considering



CyberProtex

Image courtesy of: http://opensourceforu.com/2012/01/cyber-attacks-explained-network-sniffing

34

34

Vulnerability Scanning

- Passively test security controls
- Identify
  - ✓ Vulnerability
  - ✓ Lack of security controls
  - ✓ Common misconfigurations
- Intrusive vs. non-intrusive
- Credentialed vs. non-credentialed
- False Positive

CyberProtex

35

35

Types of Vulnerability Scanners

Types of Scanners	Description	Example
Network Port Scanning	Scans internal network to yield live systems, open ports, server types, and application banners	MRTG, Commands as ping sweeps and traceroute
Vulnerability Scanning	Detect vulnerabilities of operating systems and applications	Nessus, Foundstone

CyberProtex

36

36