C|EH 01 Ethical Hacking Phases Dean Bushmiller

1. Concept

- 1.1. Attacker / Adversary
  - Dose not have a contract with victim
  - Must continually defend against discovery by victim or law enforcement
  - Compromise system security
  - Breaking computer crime law
- 1.2. Ethical Hackers
  - Follows EC Council's exam definition
- 1.3. Penetration Testers
  - Professional
  - Has contract before first interaction
  - Degree of compromise is defined in scope

2. Definitions / Terms

- 2.1. General
  - Attacker
    - Computer used to perform testing activities
    - Contains tools for hacking
  - Victim
    - Target of attacker
      - Computer
      - User
  - Control
    - Computer or tool used to protect Victim from Attacker
  - Client
    - End-user workstation
  - Server
    - Central repository of data
  - Listener
    - Neutral packet collection station between Attacker & Victim
- 2.2. CEHv11
  - ECC is inconsistent in process and definition of Ethical Hacker and Adversary

3. Methodology = High-level Process

- 3.1. Business
  - Scope
- 3.2. Ethical Hacker
  - Reconnaissance
    - Collecting publicly available information
  - Scanning
    - Identifying openings in customer's systems
    - Mapping openings to potential vulnerabilities
  - Exploitation
    - compromising system vulnerabilities
    - gaining access
  - Maintaining access
    - installing backdoors to gain alternative access
    - if defender is actively repelling
  - Covering tracks
    - removing evidence of activities
- 3.3. Business
  - Artifacts = Packets / Screenshots
  - Report

4. Tools

- 4.1. Scope
  - Contract
- 4.2. Reconnaissance
  - Maltego
  - Google
- 4.3. Scanning
  - Nmap
  - OpenVAS
- 4.4. Exploitation
  - Metaspoit
- 4.5. Maintaining access
  - Metasploit
  - NETCAT
- 4.6. Covering tracks
  - STOP/ NO / DON'T
- 4.7. Report
  - Encrypted PDF
  - Artifacts = Packets / Screenshots

C|EH 02 Footprinting & Recon. Dean Bushmiller

1. Concept

1.1. Collect information about a target network for identifying various ways to intrude into the system
- 50/50 find something
  - Valuable to Victim (7)
  - Valuable to Attackers

1.2. Information Obtained
- Organization Information
- Employee details
- Network Information
- System Information
- Locations

1.3. Recon data warrens
- Search engines
- Social networking sites
- Website
  - Web services
- Email
- DNS
- Network subnets

2. Definitions / Terms

2.1. Types
- Passive
  - Victim has no idea- no stimulus
  - Nothing to capture unless you own your DNS servers
- Active
  - I need to own the subnets
  - I need to be listening
  - This all looks normal
  - "Hello from the other side of the world" (1)
  - "Hello, is it me your looking for?" (1)

3. Technique = Specific Steps

3.1. Social engineering (whole module)

3.2. search advanced operators
- [cache:] (1)
- [link:] (1)
- [related:] (1)
- [info:] (1)
- [site:] (1)
- [allintitle:] (1)
- [intitle:] (1)
- [allinurl:] (1)
- [inurl:] (1)
- [location:] (1)

3.3. Site Report

4. Methodology = High-level Process

4.1. **Reconnaissance**
- Collecting publicly available information

4.2. Scanning

4.3. Exploitation

4.4. Maintaining access

4.5. Covering tracks

5. Tools

5.1. After you know the Victim
- Domain names
- Websites

5.2. Google Hacking Database

6. Testing Implementation

6.1. MALTEGO

6.2. SHODAN

C|EH 3 Scanning Dean Bushmiller

1. Concept

- 1.1. Stimulus & Response
- 1.2. Wireshark as a listener
- 1.3. Objectives of Network Scanning to discover
  - live hosts
    - IP address
    - Open Ports = services running
    - operating systems
    - system architecture
    - Software
  - Network Range
    - Hidden Host
  - vulnerabilities in OS if unpatched
- 1.4. Each OS/ implements network stack uniquely > give attacker under-standing

2. Definitions / Terms

- 2.1. Scanning
  - Perform
    - Ping sweep
    - OS fingerprinting
    - Banner grabbing
- 2.2. Outputs
  - Network diagrams
  - Document all the findings

3. Technique = Specific Steps

- 3.1. TCP Connect/Full Open Scan
  - Most reliable forms of TCP scanning
  - Most Costly
- 3.2. Stealth scan
  - resetting the TCP connection between client and server abruptly
  - before completion of the three-way handshake signals
- 3.3. Probe packets
  - A FIN probe with the FIN TCP flag set
  - [all on] XMAS probe with the FIN, URG, and PUSH TCP flags set
  - A NULL probe with no TCP flags set
- 3.4. Inverse TCP Flag Scanning
  - [1 of each] Attackers send TCP probe packets with one of each TCP flag (FIN, URG, PSH) set
  - **not effective against Microsoft
  - works on BSD
- 3.5. IDLE/IPID Header scan is a TCP port
  - send a spoofed source address
  - complete blind scanning of a remote host
  - 3rd party host that is not doing anything = IDLE
  - view incremented packet ID as moving forward or not
  - syn/ack to 3rd party = port open = increase ipid
  - rst to 3rd party = port closed = no increase
- 3.6. FIREWALL TEST ACK SCAN
  - Attackers send TCP probe packets with the ACK flag set to a remote device
  - analyze the header information (TTL and WINDOW field) of received RST packets
  - find out if the port is open or closed

4. Methodology = High-level Process

- 4.1. Reconnaissance
- 4.2. **Scanning**
  - **Identifying openings in customer's systems**
  - Mapping openings to potential vulnerabilities
- 4.3. Exploitation
- 4.4. Maintaining access
- 4.5. Covering tracks

5. Tools

- 5.1. NMAP
- 5.2. HPING
- 5.3. Firewalk

6. Testing Implementation

- 6.1. Artifact: Network Diagrams

7. Attacker: Techniques

- 7.1. Packet Crafter tool

8. Standard / Protocol / Algorithm

- 8.1. Protocol ID
- 8.2. IP v4 / v6
- 8.3. TCP
- 8.4. UDP

9. Guardian: Controls / Countermeasures

- 9.1. IP Spoofing Controls
  - Encryption
  - NO IP-based authentication
  - Multiple firewalls
  - Ingress Filtering
  - Egress Filtering
  - Random initial sequence number
- 9.2. Banner Grabbing Control
  - Disabling or Changing Banner

C|EH 4 Enumeration Dean Bushmiller

1. Concept

1.1. Enumeration
- On open port = listening service
- Create active connection with system
- Perform directed queries
- Collect all data
  - Examples
    - Users and groups
    - Machine names
    - Machine Configuration
    - Network resources
    - Routing tables
    - Audit settings
    - Application versions
    - Service settings
- Use for
  - Further enumeration
  - Direct knowledge of vulnerability

1.2. Authentication & Encryption
- Each service has authentication
  - Cleartext
  - Default
  - local / remote
  - Operating System / Protocol
- Some services have encryption
  - Built in
  - Bolted on = TLS
- Degree of rigor varies by
  - Protocol
  - Vendor Implementation
  - User setup

2. Definitions / Terms

2.1. Ports matched to services
- NetBIOS 135/137/139/445
- SNMP 161/ 162
- LDAP 389 / 636 / 3268
- NTP 123
- SMTP 25/465/587
- DNS
  - UDP 53
  - TCP 53
- VoIP 5060
- RPC / Portmapper 111 & Variable ports

3. Techniques Core Service Enumeration

3.1. NetBIOS
- NetBIOS data (3)
- Enumerate
  - OS, users, groups, SIDs, password policies, services, service packs and hotfixes
  - NetBIOS shares, transports, sessions, disks and security event logs
  - explore and scan network within a given range of IP addresses
  - lists of computers to identify vulnerabilities

3.2. SNMP
- user accounts and devices on a target system
- consists of a manager and an agent (2)
- two passwords
  - Read community string (2)
  - Read/write community string (2)
- default community strings extracts
  - hosts, routers, devices, shares, ARP tables, routing tables
- Commands
  - GetRequest: manager - request information from agent
  - GetNextRequest: manager - continuously to retrieve all the data stored in the array or table.
  - GetResponse: agent to satisfy a request made by the SNMP manager.
  - SetRequest: manager to modify the value of a parameter within agent's (MIB).
  - Trap: agent to inform the pre-configured SNMP manager of a certain event.

3.3. LDAP
- Lightweight Directory Access Protocol
- accessing distributed directory services
- Directory services provide (8)
- A client starts a LDAP session by connecting to a Directory System Agent (DSA) on TCP port 389 (3)

3.4. NTP
- Network Time Protocol
- Synchronize clocks of networked computers
- Rarely used in Enumeration

3.5. SMTP
- SMTP provides 3 built-in-commands
  - VRFY - Validates users
  - EXPN -delivery addresses of aliases and mailing lists
  - RCPT TO - Defines the recipients of the message
- Data
  - usernames typically equal login credentials
  - valid users

3.6. DNS
- IP to FQDN
- Public not sensitive
- Early in process to ID targets not in same IP range as other targets

3.7. VoIP H9
- Protocols
  - Real-time Transport Protocol (RTP)
  - Real-Time Control Protocol (RTCP)
  - SIP (Session Initiation Protocol)
- Sensitive information
  - VoIP gateway/servers
  - IP-PBX systems
  - client software (softphones)
  - VoIP phones User-agent IP addresses
  - user extensions
- attacks
  - Denial-of-Service (DoS)
  - Session Hijacking
  - Caller ID spoofing
  - Eavesdropping
  - Spamming over Internet Telephony (SPIT)
  - VoIP phishing (Vishing)

3.8. RPC
- Remote Procedure Call
- Valid credentials are required to access the RPC interface
- technology used for creating distributed client/server programs on LAN
- inter-process communication mechanism
- components
  - client, server, endpoint, endpoint mapper, client stub and server stub
  - portmapper service listens on TCP and UDP port 111 in order to detect the endpoints and present clients details of listening RPC services.

4. Methodology = High-level Process

4.1. Reconnaissance
- Collecting publicly available information

4.2. Scanning
- Identifying openings in customer's systems
- **Mapping openings to potential vulnerabilities**

4.3. Exploitation

5. Tools

5.1. Windows Helper tool PStools
- helps to control and manage remote systems from the command line
- PsExec - execute processes remotely
- PsFile - shows files opened remotely PsGetSid-display the SID of a computer or a user
- PsKill - kill processes by name or process ID
- PsInfo - list information about a system
- PsLoggedOn - see who's logged on locally and via resource sharing
- PsLogList - dump event log records PsPasswd - changes account passwords
- PsShutdown - shuts down and optionally reboots a computer

5.2. NetBIOS (9)

5.3. SNMP (17)

5.4. LDAP
- Softerra LDAP Administrator
- http://www.ldapadministrator.com
- Active Directory, Novell Directory Services, Netscape/iPlanet

5.5. NTP
- MOSTLY DDOS & BuffOverflow

5.6. SMTP
- NetScanTools Pro Source: https://www.netscantools.com

5.7. DNS
- DIG
- nslookup
- Mxtoolbox

5.8. VoIP
- suite of SIP tools called SIPVICIOUS

5.9. RPC
- Metasploit
- msf > use exploit/multi/misc/msf_rpc_console
- Late stage attack for pivot

6. Guardian: Controls / Countermeasures

6.1. Controls
- Authentication
  - 2FA for admin functions
- SNMP
  - Remove the SNMP agent or turn off the SNMP service
  - change default community string names
  - Upgrade to SNMP3
  - Windows Group Policy security option "Additional restrictions for anonymous connections"
- DNS
  - Disable the DNS zone transfers to the untrusted hosts
  - Make sure that the private hosts and their IP addresses are not published in DNS zone files of public DNS server
  - Use premium DNS registration services that hide sensitive information such as host information (HINFO) from public
- SMTP
  - Ignore email messages to unknown recipients
  - Disable open relay feature
  - Limit the number of accepted connections from a source in order to prevent brute force attacks
- LDAP
  - STARTTLS technology to encrypt the traffic
  - Select a user name different from your email address and enable account lockout
- SMB
  - Disable SMB protocol on Web and DNS Servers
  - Disable ports TCP 139 and TCP 445 used by the SMB protocol
  - Restrict anonymous access through RestrictNullSessAccess parameter from the Windows Registry

C|EH 5 Vulnerability Analysis Dean Bushmiller

1. Concept

- 1.1. Business process
  - Operations: Can you install an agent?
    - OpenVAS / Nessus
  - Are you an outsider / attacker?
    - Banner grab leads to
      - Research
      - Throw everything we can at it
- 1.2. Vulnerability research
  - Process of discovering weaknesses
  - Review recently discovered vulnerabilities and exploits
  - Being informed about new products and technologies
- 1.3. Classify vulnerabilities
  - Severity level (low, medium, or high)
  - Exploit range (local or remote)
  - CWE Top 25
- 1.4. Approaches to network vulnerability scanning
  - Active or Passive
  - Internal or External
  - Host or Network
- 1.5. Requires current database
  - Community effort

2. Definitions / Terms

3. Technique = Specific Steps

- 3.1. Search Common Vulnerabilities and Exposures (CVE)
- 3.2. Understanding scan requires research
- 3.3. Link the CVE to CAPEC
- 3.4. Go to proof of Concept sites

4. Methodology = Business Process

- 4.1. Pre assessment = Creating a Baseline with Client
  1. Identify and understand business processes
  2. Identify the applications, data, and services that support business processes
  3. Create an inventory of all assets, and prioritize/rank the critical assets
  4. Map the network infrastructure
  5. Identify the controls already in place
  6. Understand policy implementation and standards compliance to the business processes
  7. Define the scope of the assessment
  8. Create information protection procedures to support effective planning, scheduling, coordination, and logistics
- 4.2. Assessment phase = interrogation
  1. Examine and evaluate physical security
  2. Check for misconfigurations and human errors
  3. Run vulnerability scans using tools
  4. Identify and prioritize vulnerabilities
  5. Apply business and technology context to scanner results
  6. Perform OSINT information gathering to validate the vulnerabilities
  7. Create a vulnerability scan report
- 4.3. Post assessment
  - risk assessment
    - Perform risk characterization
    - Assess the level of impact
    - Determine the threat and risk level
  - remediation
    - Prioritize recommendations
    - Develop an action plan to implement the recommendation
    - Perform root-cause analysis
    - Apply patches/fixes
    - Capture lessons learned
    - Conduct awareness training
  - verification
    - Perform dynamic analysis
    - Attack surface review
  - monitoring
    - Monitoring intrusion detection and intrusion prevention logs
    - Implementation of policies, procedures, and control
- 4.4. Simplified
  - Scanning
    - **Mapping openings to potential vulnerabilities**

5. Tools

- 5.1. Nessus Professional
- 5.2. OpenVAS

6. Testing Implementation

7. Standard / Protocol / Algorithm

- 7.1. Scoring & Catalogs
  - Common Vulnerability Scoring System (CVSS)
  - Common Vulnerabilities and Exposures (CVE)
  - Common Weakness Enumeration (CWE)
  - National Vulnerability Database (NVD)

8. Guardian: Controls / Countermeasures

- 8.1. Best Practices
  - Imitates outside view of attackers for an object
  - Suggests reasonable remedies and workarounds to address vulnerabilities
  - Supports relevant network type
    - SCADA
    - IOT
    - LAN/WAN
    - CLOUD
  - Automatic scan against constantly updated databases
  - Creates brief, actionable, customizable reports
  - Ensures correct outcomes by testing everything
    - network, network resources, ports, protocols, and operating systems
  - Inference-Based Assessment
    - starts by building an inventory of protocols found on the machine
    - scanning process to detect ports are attached to services
    - selects vulnerabilities on each machine and starts to execute only relevant tests

C|EH 6 System Hacking Dean Bushmiller

1. Concept

- 1.1. **If you do this step without a contract = prison.**
- 1.2. Inputs
  - Footprinting
  - Scanning
  - Enumeration
  - Vulnerability Analysis
- 1.3. Prior to this - no law in U.S. has been broken against corporate assets
- 1.4. Stimulus
  - true attack input
- 1.5. Response
  - Control over asset by attacker
  - Leak of confidential information

2. Definitions / Terms

- 2.1. Gaining Access
  - using weaknesses in access control mechanism or implementation
- 2.2. Escalating Privileges
  - moving from using a low-privileged account to administrator or root
- 2.3. Executing Applications
  - install Trojans, Backdoors, Rootkits, and Keyloggers
  - Goal of granting remote system access
- 2.4. Hiding Files
  - Steganography
  - Encryption to exfiltrate
    - Cryptcat
- 2.5. Covering Tracks
  - To remain undetected, erase all evidence of security compromise from the system.

3. Technique = Specific Steps

- 3.1. Gain Access
  - Cracking Passwords
    - Non-Electronic Attacks
      - Shoulder Surfing
      - Active Online Attacks
      - Social Engineering
      - Dumpster Diving
    - Active Online Attacks
      - Password guessing
      - Dictionary
      - Brute Forcing
      - Default password
      - Trojan/Spyware/Keyloggers
    - Rainbow Table Attack (Pre-Computed Hashes)
    - Capturing Hash
  - Cracking Database of Passwords
    - Pull copy of encrypted database
    - Microsoft Authentication Security Accounts Manager (SAM) Database
    - Active Directory database/ LDAP connections
    - Shadow File
- 3.2. Escalating Privileges
  - From Anonymous to Guest to User to Administrator to Root / System
  - DLL Hijacking
    - Most Windows applications do not use the fully qualified path when loading an external DLL library instead they search directory from which they have been loaded first
    - If attackers can place a malicious DLL in the application directory, it will be executed in place of the real DLL
  - Buffer Overflow
    - Software performs operations on a memory buffer, but it can read or write to memory location outside intended boundary of buffer.
    - Certain languages allow direct addressing of memory locations
    - Do not automatically ensure that locations are valid for memory buffer that is being referenced
    - Cause read or write operations to be performed on memory locations that may be associated with other variables, data structures, or internal program data
    - Attacker able to execute arbitrary code
- 3.3. Executing Applications
  - Malicious programs attackers execute on target systems
  - Keyloggers
    - Hardware
    - PC/BIOS Embedded
    - Keyboard Keylogger
    - External
    - Passthru-PS/2 and USB
    - Acoustic/CAM
    - Bluetooth
    - Wi-Fi
    - Software
    - Form Grabbing
    - Hypervisor-based
    - Kernel/Rootkit/Device Driver
    - Application
  - Spyware
    - Program records user's interaction without user's knowledge
    - Hides process and files in order to avoid detection and removal
  - Rootkits
    - Programs that hide their presence and activities
    - Rootkits
      - Replace operating system calls and utilities with its own modified versions
      - Granting attacker full access now and in future
    - How it works
      - System hooking is a process of changing and replacing the original function pointer with the pointer provided by the rootkit in stealth mode.
      - Inline function hooking is a technique where a rootkit changes some of the bytes of a function inside the core system DLLs (kernel32.dll and ntdll. dll),
      - Placing an instruction so that any process calls hit the rootkit first
- 3.4. Exfiltration
  - Techniques that adversaries may use to steal data from your network
  - Adversaries often package victim data to avoid detection while removing it
  - How
    - Covert channels
    - Transferring over command and control channel
    - Setting size limits on the transmission
  - Techniques
    - NTFS ADS
      - Alternate Data Stream
      - Metadata: attributes, word count, author name
      - Fork data into existing files without changing or altering their visible attributes
    - Steganography
      - Hiding secret within an ordinary message
      - Transmit as if "normal"
      - Extracting it at the destination
      - Maintain confidentiality of communication
      - Invisible ink
- 3.5. Covering Tracks
  - Manipulating Logs
  - Disabling Auditing
  - Wipe Disk

4. Methodology = High-level Process

- compromising system vulnerabilities
- gaining access
- 4.1. **Exploitation**

5. Tools

- 5.1. Metasploit
- 5.2. Armitage GUI for Metasploit

6. Testing Implementation

- 6.1. Metasploit pro lic = $15K U.S.

7. Standard / Protocol / Algorithm

- 7.1. Common Attack Pattern Enumeration and Classification CAPEC
- 7.2. ATT&CK

8. Guardian: Controls / Countermeasures

- 8.1. Security plus data
  - 51

C|EH 7 Malware Dean Bushmiller

1. Concept

- 1.1. Today
  - **mal**icious soft**ware** (2)
  - How attacker gains control remotely
  - Most malware has a mixture of programming techniques (3)
  - About attackers getting paid (2)
- 1.2. Do not work in this area- understand and Research only
  - Tools carried across borders can land you in jail
- 1.3. Insertion Vectors (any communications / typically user initiated or authorized)
  - Instant Messenger applications
  - Portable hardware media / removable devices
  - Browser and email software bugs
  - Insecure patch management
  - Rogue / decoy applications
  - Untrusted sites
  - Freeware
  - Downloading files
  - Email attachments
  - Network propagation
  - File sharing services
  - Installation by other malware
  - Bluetooth and wireless
- 1.4. Increasing chances of insertion
  - Social Engineered Click-jacking
  - Spearphishing
  - Compromised Legitimate Websites
  - Drive-by Downloads
  - Spam Emails
  - Malvertising

2. Definitions / Terms

- 2.1. Components of Malware
  - Crypter (1)
  - Downloader (1)
  - Dropper (1)
  - Exploit (1)
  - Injector (1)
  - Obfuscator/Wrapper (1)
  - Packer (1)
  - Payload (1)
  - Exploit kit (1)
- 2.2. Trojan
  - DEF (3)
  - Covert Channel (2)
  - Use / Functions (10)
  - Types of Trojans (11)
- 2.3. Virus
  - requires user interaction = click to install, view
  - Types of Viruses (20)
- 2.4. Worm
  - NO user required to infect = service listening on a port
  - (Virus = requires user interaction)
- 2.5. Ransomware
  - Malware which restricts access to computer and demands payment in order to remove the restrictions
  - ATT&CK techniques (8)

3. Methodology = High-level Process

- 3.1. Simplified
  - Reconnaissance
  - Scanning
  - **Exploitation** (2)
  - Maintaining access
  - Covering tracks

4. Tools

- 4.1. Using these tools will be detected
- 4.2. worm — Internet Worm Maker Thing
- 4.3. Virus — JPS Virus Maker
- 4.4. Trojan Horse Construction
  - Process Building Trojan (6)
  - DarkHorse Trojan Virus Maker
  - Generic tool : wrapper (4)
  - TOOL: (3)
  - Tool Crypter

5. Testing Implementation

- 5.1. Malware Analysis
  - DEF:
    - process of reverse engineering a specific piece of malware to determine the origin, functionality, and potential impact of a given type of malware
  - Types of Malware Analysis
    - static and dynamic
    - static analysis
      - Static
        - not running the malware code so there is no need of creating a safe environment
        - Activities (1)
        - Local and online malware scanning
        - Performing strings search
        - Identifying packing/obfuscation methods
        - Finding the portable executables (PE) information
        - Identifying file dependencies
        - Malware disassembly
      - Dynamic
        - malware will be executed on a system to understand its behavior after infection
        - requires safe environment = Testbed
        - stages (2)
        - Monitoring Activities (12)
  - Preparing Testbed
    - Allocate a physical system for the analysis lab
    - Install Virtual machine (VMware, Hyper-V, etc.) on the system
    - Install guest OSs in the Virtual machine(s)
    - Isolate the system from the network by ensuring that the NIC is in “host only” mode
    - Simulate internet services using tools such as iNetSim
    - Disable the ‘shared folders’ and the ‘guest isolation’
    - Install malware analysis tools
    - Generate hash value of each OS and tool
    - Copy the malware over to the guest OS
  - Malware analysis examples (2)

6. Guardian: Controls / Countermeasures

- 6.1. Control for malware
  - Backup
  - Patch
- 6.2. End user controls
  - Trojan
    - Avoid opening email attachments received from unknown senders
    - Block all unnecessary ports at the host and firewall
    - Avoid accepting programs transferred by instant messaging
    - Harden configuration settings
    - Monitor the internal network traffic for odd ports or encrypted traffic
    - Avoid downloading and executing applications from untrusted sources
    - Install patches and security updates
    - Scan external drives
    - Restrict permissions of installation
    - Manage local workstation file integrity through checksums, auditing, and port scanning
    - Run host-based antivirus, firewall, and intrusion detection software
  - Virus and Worms
    - Generate an anti-virus policy for safe computing and distribute it to the staff
    - Pay attention to the instructions while downloading files or any programs from the Internet
    - Update anti-virus software regularly
    - Avoid opening attachments received from an unknown sender as viruses spread via e-mail attachments
    - Since virus infections can corrupt data, ensure you are performing regular data backups
    - Schedule regular scans for all drives after the installation of anti-virus software
    - Do not accept disks or programs without checking them first using a current version of an anti-virus program
    - Ensure that any executable code used within the organization has been approved
    - Do not boot the machine with infected bootable system disk
    - Stay informed about the latest virus threats
    - Check DVDs and CDs for virus infection
    - Ensure pop-up blockers are turned on and use an Internet firewall
    - Run disk clean up and registry scanner once a week

C|EH 8 Sniffing Dean Bushmiller

1. Concept

- 1.1. Listen
- 1.2. allows an attacker to gather sensitive information
- 1.3. Most networks are fully switched
  - Only broadcast traffic will reach all host on segment
- 1.4. Most traffic is encrypted
  - If it is not encrypted you can sniff it
    - Passwords and data are sent in clear text
      - IMAP HTTP SMTP NNTP POP FTP Telnet and Rlogin
    - Solution = Encrypt it
- 1.5. How do attackers force listening?
  - sniffing requires extra steps / attacks
    - Arp Spoofing
    - MAC flooding
  - Can attacker overcome physical security?
    - Compromise a host, turn into sniffer
    - Insert a splitter and collection computer at relevant location
    - Insert small computer with LTE interface
  - Attacking Switch Configuration
    - Switched Port Analyzer (SPAN) is a Cisco switch feature, also known as port mirroring (used for IDS)
  - Attacking Telephone network
    - Wiretapping or telephone tapping is a method of monitoring telephone = it is a U.S. FEDERAL CRIME for anyone except for those with a WARRANT

2. Definitions / Terms

- 2.1. Packet Sniffing
  - process of monitoring and capturing all packets passing through a given network SEGMENT
- 2.2. Software sniffer
  - turns the NIC to promiscuous mode so that it listens to all the data transmitted on its segment
  - L2 standard is to listen only for broadcast and own MAC address as DEST
  - Some Operating Systems will not permit this activity
- 2.3. Hardware sniffer (protocol analyzer)
  - Copy of electric signal
- 2.4. Switched Vs Shared
  - shared: (HUB) single bus connects all the hosts that compete for bandwidth - easy sniffing
  - Switched: maintains a table that tracks each computer's MAC address and physical port on which that MAC address is connected

3. Technique = Specific Steps

- 3.1. MAC attacks
  - CAM (Content Addressable Memory) table is a dynamic table of fixed size
    - Tool: macof
    - Attacker Goal: Interception / redirection (MITM)
    - Technique: Switch Port Stealing sniffing technique using MAC flooding
    - Defense: Configuring Port Security
- 3.2. DHCP attacks
  - Know DHCP Request/Reply Messages = DORA
  - DHCP starvation attack
    - sending a large number of DHCP requests and uses all of the available IP addresses that the DHCP server can issue
    - Tool: Yersinia
    - Attacker Goal: DOS
  - Rogue DHCP Server
    - impersonates a legitimate server and offers IP addresses and other network information to other clients in the network (default gateway)
  - Defense: Configuring Port Security & Enable DHCP snooping with dynamic ARP inspection (DAI)
- 3.3. ARP poisoning
  - LAST write wins
  - Attacker Goal: Interception / redirection (MITM)
- 3.4. IRDP Spoofing
  - ICMP Router Discovery Protocol (IRDP) is a routing protocol that allows host to discover the IP addresses of active routers on their subnet

4. Methodology = High-level Process

- 4.1. Reconnaissance
- 4.2. Scanning
- 4.3. Maintaining access
  - **Listening**

5. Tools

- 5.1. Wireshark
  - Capture Filter
  - Display filter
  - Follow TCP Stream
- 5.2. DNS poisoning
  - substitution of a false IP address to name in DNS server or client cache
  - Intranet DNS Spoofing
    - attacker must sniff the DNS request from the intranet, then can send a malicious reply to the sender before the actual DNS server = race condition
  - Internet DNS Spoofing
    - attacker changes the primary DNS entries of the victim's computer (works well with DHCP attacks)
  - Proxy Server DNS Poisoning
    - attacker also configures a fraudulent DNS and makes its IP address a primary DNS entry in the proxy server
  - DNS Cache Poisoning
    - adding forged DNS records into the DNS resolver cache

6. Guardian: Controls / Countermeasures

- 6.1. Countermeasures
  - 802.1X suites: port-based Network Access Control (PNAC)
    - VLAN authentication
  - Encryption
  - Restrict the physical access
- 6.2. Detection
  - If your IDS has access to that segment you are good
    - ARPing is noisy to IDS
  - Nmap's NSE script allows you to check local Ethernet has its network card in promiscuous mode.
    - Command: nmap --script=sniffer-detect [Target IP Address/Range of IP addresses
- 6.3. DNS poisoning
  - DOH
  - Resolve all DNS queries to local DNS server
  - Block DNS requests being sent to external servers
  - Configure firewall to restrict external DNS lookup
- 6.4. DNS- service
  - Umbrella

C|EH 9 Social Engineering Dean Bushmiller

1. Concept

- 1.1. art of convincing people to reveal confidential information
- 1.2. Common targets
  - users
  - help desk personnel
  - technical support executives
  - system administrators
- 1.3. depend on people being unaware of their valuable information
- 1.4. Why is Social Engineering Effective?
  - Most people what to help the helpless
  - difficult to detect social engineering attempts
  - Requires diligence & recurring training

2. Definitions / Terms

- 2.1. Human-based Social Engineering
  - face to face on-site
  - On pretext of a legitimate person
  - Types
    - Impersonating — pretends to be someone legitimate or an authorized person
    - Eavesdropping
    - Shoulder Surfing
    - Dumpster Diving
    - Reverse Social Engineering ECC — attacker presents as an authority and the target seeks their advice after or before offering the information that he needs
      - "THIS is your problem, I am making it go away, (sidebar- tell me how to help you by giving me more information)"
    - Piggybacking
    - Tailgating
    - Vishing - voice phishing
      - Over-Helpfulness to the Help Desk
      - Third-party Authorization on behalf of
      - Tech Support to the user
- 2.2. Computer-based Social Engineering
  - with the help of computers
  - Techniques:
    - Pop-up Window
    - Spam
    - Chat
    - Phishing
      - Spear Phishing
      - Whaling
      - Pharming
      - Spimming
- 2.3. Principles
  - Reciprocity — You are beautiful, since I complimented you, can I have your password?
  - Obligation — obligation is same feeling as reciprocation, but it's based on social norms or expected behaviors
  - Concession — admit to even a minor detail, to concede to one fact, it is nearly impossible for that person to go back
  - Scarcity — Act now, this offer expires at midnight
  - Authority — I am the big boss, give me what I want
  - Consistency and Commitment
    - You said you wanted democracy, why don't you vote democratic
    - You said you wanted a republic, why don't you vote republican
  - Liking — People like people who are like them (1)
  - Social Proof — Everyone else is doing it, get with the program

3. Technique = Specific Steps

- 3.1. Process
  - Research on Target Company — Dumpster diving, websites, employees, tour company
  - Select Victim — Identify the frustrated employees of the target company
  - Develop Relationship — Develop relationship with the selected employees
  - Exploit the Relationship — Collect sensitive account and financial information, and current technologies

4. Methodology = High-level Process

- 4.1. Impersonation on Social Networking Sites
  - As a professional
    - Start build fakes now
      - one per gender
      - one per industry you hope to test against
      - monthly / weekly updates
    - Start corrupting your own now
- 4.2. Simplified
  - Reconnaissance
  - **Scanning** — Identifying openings in customer's systems
  - **Exploitation** — gaining access
  - **Maintaining access** — installing backdoors to gain alternative access
  - Covering tracks

5. Tools

- 5.1. Social Engineering Toolkit (SET)

6. Attacker: Techniques

- 6.1. NOT SOCIAL ENG BUT
  - Insider Threats
    - Privileged Users
    - Disgruntled Employees
    - Terminated Employees
    - Accident-Prone Employees
    - Third Parties
    - Undertrained Staff
  - Identity theft
    - Personal hacking
    - imposter obtains personal identifying information to commit fraud = $ $
    - Attackers can use identity theft to impersonate employees of a target organization and physically access the facility

CEH 11 Session Hijacking Dean Bushmiller

1. Concept

1.1. Why bother attacking directly?
- Weakest link might be the other side of the connection

1.2. What is used to maintain state/ session?
- Exploitation of Trusted Identifiers
  - session ID
  - resource ID
  - cookie
- Session Replay
  - reuse of valid session ID to spoof the target system in order to gain privileges

1.3. Why it works
- Layer abstraction
- Victim Client / Victim Server: connection
  - Layer: 3/4
  - Layer 5
  - C:IP/PORT
  - SYN# /ACK
  - S:IP/PORT
  - SYN /ACK#
  - A:IP/PORT
  - If A supplies Correct NEXT of C
  - S doesn't care or know
- Layering / Abstraction separates IP address and PORT from session sequence #
  - Attacker replaces their IP for victim
  - Attacker keeps victim PORT/ Session
  - Attacker and Server keep going
  - Victim's is cut out communication = Hijack
  - If Attacker keeps session on both sides of connection =MITM

2. Definitions / Terms

2.1. Session hijacking
- an attacker takes over a valid communication session between two computers
- can be done at most layers
- exploits weaknesses in an application's use of sessions in performing authentication improperly
- Attacker is able to steal or manipulate an active session and use it to gain unauthorized access to the application

2.2. Spoofing
- pretends to be another user or machine (victim) to gain access
- Authentication reuse = initiates a new session using the victim's stolen credentials
- Does not take over an existing active session
- Much less Synchronous activity = less chance of IDS on client side

3. Technique = Specific Steps

3.1. Network Hijacking
- Active Session Hijacking
  - three phases
    - Tracking connection
      - Network sniffer to track a victim
      - Nmap to scan network for a target with a TCP sequence that is easy to predict
    - Desynchronizing
      - state occurs when
        - connection between target and host has been established
        - stable with no data transmission
        - when server's sequence number is not equal to the client's acknowledg-ment number
        - attacker has interrupted connection between server and target
    - Injecting packet
      - actively participate as the man-in-the-middle
      - passing data between target and server
      - while reading and injecting data at will
  - interception of packets during transmission between client and server

3.2. Application Hijacking
- Gaining control over the HTTP's user session by obtaining the session IDs
- Passive Session Hijacking = sniffing / cookie collection
  - Cookie = state
    - = token
    - = Crappy authentication
  - If cookie last beyond use by victim
  - Attacker reuses cookie
    - Without or without MITM
    - At same time or after victim's session
- Session token can be compromised by
  - Session sniffing
  - Man-in-the-middle
  - Session replay
  - Predictable session token
  - Session fixation
- Client side Attacks
  - Cross-site scripting (XSS)
  - Cross-site request forgery
  - Man-in-the-browser
- Proxy attack
  - click on a bogus link that redirects the user to the attacker server
  - Attacker forwards request to the legitimate server on the behalf of the victim
  - Attacker serves as a proxy for the entire transaction

4. Methodology = High-level Process

4.1. Exploitation
- perform malicious activities
  - malicious applications
  - stealing
  - hiding
  - tampering
- gaining access

5. Tools

- 5.1. Ettercap / Bettercap
- 5.2. SSH forwarding hijack
- 5.3. RDP Hijacking
  - You can do this without much setup

6. Guardian: Controls / Countermeasures

- 6.1. Encryption
- 6.2. Application = random and short session variables, HSTS HTTP Strict Transport Security

C|EH 99 2-Day Reading Links Dean Bushmiller

1-1 Ethical Hacking
- Information Security
- Threats and Attack Vectors
- Hacking Concepts, Types, and Phases
- Ethical Hacking Concepts and Scope
- Controls
- Penetration Testing
- Laws and Standards
- Resources
  - O'REILLY
    - Policy
    - Kill Chain
    - MITRE ATT&CK
    - Indicators of compromise (IOCs)
    - Cyber Threat Intelligence
    - Incident Handling
  - PUBLIC 4

1-02 Footprinting and Reconnaissance
- Search Engines
- Web Services
- Social Networking Sites Website
- Email
- Competitive Intelligence
- Whois
- DNS
- Network
- Social Engineering
- Resources
  - O'REILLY
    - Google Hacking for Penetration Testers, 3rd
  - PUBLIC
    - Google Hacking Database
    - Advanced Operators - Google

1-03 Scanning Networks
- Diagram-whiteboard idip
- Techniques
- Beyond IDS and Firewall
- Banner Grabbing
- Draw Network Diagrams
- Resources
  - O'REILLY 5
  - PUBLIC 3

1-08 Sniffing
- Sniffing Technique (Methodology) 5
- Detection Techniques
- Resources
  - O'REILLY 1
  - PUBLIC 7

2-04 Enumeration
- NetBIOS
- SNMP
- LDAP
- NTP
- SMTP
- DNS
- Resources
  - O'REILLY 2
  - PUBLIC 2

2-05 Vulnerability Analysis
- Solutions
- Scoring Systems
- Reports
- Resources
  - O'REILLY 3
  - PUBLIC 19

3-06 System Hacking
- Cracking Passwords
- Escalating Privileges
- Executing Applications
- Hiding Files
- Covering Tracks
- Readings 30

3-11 Session Hijacking
- Application Hijacking (Methodology)
- Network Hijacking (Methodology)
- Resources
  - O'REILLY 2
  - PUBLIC 8

4-13 Web Servers
- Attacks
- Attack Methodology
- Attack Tools
- Patch Management
- Resources
  - O'REILLY 1
  - PUBLIC 1

4-14 Web Applications
- Threats
- Methodology
- Hacking Tools
- Testing Tools
- Resources
  - O'REILLY 3
  - PUBLIC 3

4-15 SQL Injection
- Types of Injection Attacks
- Methodology
- Evasion Techniques
- Resources
  - O'REILLY 1
  - PUBLIC 7