Network Penetration

Lesson 3: System Hacking + Malvare + Sniffers

Program

- System Hacking
- Malvare
  - Overt and covert channels
- Sniffers
  - Understanding sniffers
  - Using a sniffer
  - Switched network sniffing
- Exercises

System Hacking

Password cracking

- Vulnerable password types:
  - Passwords that use only numbers
  - Passwords that use only letters
  - Passwords that are all upper- or lowercase
  - Passwords that use proper names
  - Passwords that use dictionary words
  - Short passwords (fewer than eight characters)

Password cracking

- Vulnerable (a little less) password types:
    - Passwords that contain only letters, special characters, and numbers: stud@52
    - Passwords that contain only numbers: 23698217
    - Passwords that contain only special characters: &*#@!(%)
    - Passwords that contain only letters and numbers: meetl23
    - Passwords that contain only letters: POTHMYDE
    - Passwords that contain only letters and special characters: rex@&ba
    - Passwords that contain only special characters and numbers: 123@$4

Password-Cracking Techniques

- Dictionary Attacks (uses dictionary)
- Brute-Force Attacks (tests all keys)
- Hybrid Attack (dictionary with added steps)
- Syllable Attack (combine brute force and dictionary)
- Rule-Based Attack (logical rules followed)
- Passive Online Attacks (listening)
- Active Online Attacks (guessing, Trojan/spyware/key loggers, hash injection, and phishing)
- Offline Attacks (go for storage)
- Nontechnical Attacks (eavesdrop, shoulder surfing, social engineering)

Attack types

- Passive Online Attacks:
  - Packet Sniffing (capture + inspect packets)
  - Man-in-the-Middle (listen on both parties)
  - Replay Attack (capture + use packets)
- Active Online Attacks:
  - Password Guessing (try to guess)
  - Trojans, Spyware, and Keyloggers (using tools)
  - Hash Injection (retrive hash + use)
  - Offline Attacks (find stored passwords)
  - Precomputed Hashes or Rainbow Tables (precompute + match hashes)
  - Distributed Network Attacks (involve several computers)

Other attack types

- Default Passwords
- Guessing
- USB Password Theft
- Using Password Cracking

Authentication on Microsoft Platforms

- Security Accounts Manager
  - File lock unless boot or Blue Screen of Death
- How Passwords Are Stored within the SAM:
  - c:\windows\system32\config\SAM.
  - Link:1010:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
    - bold part before the colon is the LM hash, and the bold part after the colon represents the NTLM hash
  - Ophcrack, L0phtCrack, pwdump display and attempt to decipher these hashes

Authentication on Microsoft Platforms

- NTLM Authentication
  - NT LAN Manager
  - Security Support Provider (SSP) on top
- Kerberos authentication protocol
  - Key distribution center (KDC)
  - Authentication server (AS)
  - Ticket-granting server (TGS)

Elevating privileges

- Gaining better access and more privileges
- Horizontal Privilege Escalation:
  - An attacker attempts to take over the rights and privileges of another user who has the same privileges as the current account.
- Vertical Privilege Escalation:
  - The attacker gains access to an account and then tries to elevate the privileges of the account. It is also possible to carry out a vertical escalation by compromising an account and then trying to gain access to a higher-privileged account.
- Tools: E.g. Trinity Rescue Kit (TRK)

Executing Applications

- Backdoors (E.g. using PsExec, part of PsTools)
- Crackers
- Keyloggers
- Malware
- Remote connection tools:
  - PDQ Deploy
  - RemoteExec
  - DameWare
  - Netcat

Covering your tracks

- Disabling Auditing:
  - auditpol \\<ip address of target> /clear
- Surgically removal tools:
  - Dump Event Log, ELSave, WinZapper, Ccleaner, Wipe, MRU-Blaster, Tracks Eraser Pro, Clear My History
- Data Hiding
  - E.g hidden file types
- Alternate Data Streams (ADS)
  - Fork or hide data within files
    - type triforce.exe > smoke.doc:triforce.exe
    - start smoke.doc:triforce.exe
- Tools for uncovering:
  - Sfind, LNS, Tripwire

Malware

Categories of Malware

- Viruses
- Worms
- Trojan horses
- Rootkits
- Spyware
- Adware

Viruses

- Actions:
  - Altering data
  - Infecting other programs
  - Replicating
  - Encrypting itself
  - Transforming itself into another form
  - Altering configuration settings
  - Destroying data
  - Corrupting or destroying hardware

Viruses

- Development:
  - Design
  - Replication
  - Launch
  - Detection
  - Incorporation
  - Elimination

Virus types

- System or boot sector virus (Master boot record)
- Macro viruses (E.g. VBA scripts)
- Cluster viruses (Alter FAT to point at self)
- Stealth or tunneling virus (Intercept calls, bogus responses)
- Encryption viruses (Partly encrypted)
- Cavity or file-overwriting viruses (Hides in file, alters size)
- Sparse-infector viruses (Only activates some times)
- Companion or camouflage virus (Similar name, runs first)
- Logic bomb (Activates at event/time)
- File or multipartite viruses (Several parts)
- Shell viruses (Makes infected program a subroutine)
- Cryptoviruses (ransomware)

Worms

- Features:
  - Do not require a host application to perform their activities.
  - Do not necessarily require any user interaction, direct or otherwise, to function.
  - Replicate extremely rapidly across networks and hosts.
  - Consume bandwidth and resources.
  - Transmit information from a victim system back to another location specified by the designer.
  - Carry a payload, such as a virus, and drop off this payload on multiple systems rapidly.

Worms

- Differences from virus:
  - A worm can be considered a special type of malware that can replicate and consume memory, but at the same time it does not typically attach itself to other applications or software.
  - A worm spreads through infected networks automatically and requires only that a host is vulnerable. A virus does not have this ability.

Spyware

- Collects and forwards information, without knowledge or consent
- Methods of spyware infection:
  - Peer-to-Peer Networks (P2P)
  - Instant Messaging (IM)
  - Internet Relay Chat (IRC)
  - Email Attachments
  - Physical Access
  - Browser Defects
  - Freeware
  - Websites
  - Software Installations

Other ”wares”

- Adware
  - Displays pop-ups, adds, …
- Scareware
  - Tries to scare user into supplying credit info, …
- Ransomware
  - Encrypts data, user must pay to get it back

Trojan

- Providing covert access to system
- Goals similar to virus or worm:
  - Control system
  - Take some specific action:
    - Stealing data
    - Installing software
    - Downloading or uploading files
    - Modifying files
    - Installing keyloggers
    - Viewing the system user’s screen
    - Consuming computer storage space
    - Crashing the victim’s system
- See book for tools

Backdoors

- A backdoor typically achieves one or more of the following key goals:
  - Lets an attacker access a system later by bypassing any countermeasures the system owner may have placed.
  - Provides the ability to gain access to a system while keeping a low profile. This allows an attacker to access a system and circumvent logging and other detective methods.
  - Provides the ability to access a system with minimal effort in the least amount of time.
  - Under the right conditions, a backdoor lets an attacker gain access to a system without having to rehack.
- Types:
  - Password-cracking backdoor
  - Process-hiding backdoor

Overt and Covert Channels

- Overt channel:
  - Put in place by design and represents the legitimate or intended way for the system or process to be used
- Covert channel:
  - Uses a system or process in a way that it was not intended to be used.
  - Used most often by Trojans
  - Tools for exploitation in book

Sniffers

Sniffers

- Utilities that can capture and scan traffic moving across a network
- Any utility that has the ability to perform a packet-capturing function
- Passive sniffing:
  - Only listening/analyzing packets
- Active sniffing:
  - Altering packets
- Connected network interface must be in promiscous mode
  - Allowing the capture of all traffic
- Shows packets and provides in-depth view of info

Sniffers

- Protocols to be sniffed:
  - Telnet/rlogin
  - HTTP
  - Simple Mail Transfer Protocol (SMTP)
  - Network News Transfer Protocol (NNTP)
  - Post Office Protocol (POP)
  - File Transfer Protocol (FTP)
  - Internet Message Access Protocol (IMAP)

Sniffers

- Tools:
    - Wireshark (you know this☺)
    - Tcpdump
    - WinDump
    - OmniPeek
    - Dsniff
    - EtherApe (Linux/Unix)
    - MSN Sniffer
    - NetWitness NextGen

Switched Network Sniffing

- A wired switch doesn’t allow you to sniff the whole network.
- Methods for enabling sniffing on a switch is to turn it into a device that does allow sniffing
- We want to convert it into a hub-like environment
- A switch keeps track of MAC addresses received by writing them to a content addressable memory (CAM) table
- If flooded, fails to write CAM – makes the switch fail into a hub
- Tool:
    - Linux Macof

Other sniffing techniques

- ARP Poisoning:
  - Contaminate a network with improper gateway mappings
  - Attempting to become the hub of all network traffic
- MAC Spoofing:
  - Change the MAC address to the MAC address of an existing authenticated machine already on the network
- Port Mirror or SPAN Port
  - Getting physical access to the switch and using port mirroring or a Switched Port Analyzer (SPAN) port
  - This technique is used to send a copy of every network packet encountered on one switchport or a whole VLAN to another port where it may be monitored

Sniffing countermeasures

- Use a hardware-switched network for the most sensitive portions of your network in an effort to isolate traffic to a single segment or collision domain.
- Implement IP DHCP Snooping on switches to prevent ARP poisoning and spoofing attacks.
- Implement policies preventing promiscuous mode on network adapters.
- Be careful when deploying wireless access points, knowing that all traffic on the wireless network is subject to sniffing.
- Encrypt your sensitive traffic using an encrypting protocol such as SSH or IPsec.

Sniffing countermeasures

- Static ARP entries, which consist of preconfiguring a device with the MAC addresses of devices that it will be working with ahead of time. However, this strategy does not scale well.
- Port security is used by switches that have the ability to be programmed to allow only specific MAC addresses to send and receive data on each port.
- IPv6 has security benefits and options that IPv4 does not have.
- Replacing protocols such as FTP and Telnet with SSH is an effective defense against sniffing. If SSH is not a viable solution, consider protecting older legacy protocols with IPsec.
- Virtual private networks (VPNs) can provide an effective defense against sniffing due to their encryption aspect.
- SSL is a great defense along with IPsec.

Other defensive strategies

- Mitigating MAC Flooding
  - Preventing MAC flooding by settting max number of MAC addresses.
    - Will shut down after threshold is reached.
- Detecting sniffer attacks
  - Look for systems running network cards in promiscuous mode. Under normal circumstances there is little reason for a network card to be in promiscuous mode, and as such all cards running in this mode should be investigated.
  - Run an NIDS to detect telltale signs of sniffing and track it down.
  - Tools such as HP's Performance Insight can provide a way to view the network and identify unusual traffic.