Week #6, Lesson 4: Post-Exploitation
What happens after an attacker gets on the machine
Midterm Review class next, July 7th
Midterm is open book, but no internet, no collaboration, no AI/ChatGPT
Open Book: Bring your own handwritten notes, printed notes, or book
Online, July 12th, proctored
Review Lesson 5 (on crypto) slides
Watch Lesson 3 supplemental video
Everything for midterm exam: Lab 1&2, HW1&2, Lessons 1-5
HW2: is due on July 14th, needs to be done before the midterm exam

Exercise /#1A
What are the steps for the user (Firefox) to make a DNS request for www.nytimes.com, presuming no hosts have been on the Internet?
For an iterative query:
The user makes a request to the local DNS server. They are specifically asking for the A record (IPv4 address)
The local DNS server queries the root server. The root server responds to ask the TLD server.
The local DNS server queries the TLD server. The TLD server responds to ask the authoritative server.
The local DNS server queries the authoritative server. The authoritative server responds with the IP address.
The local DNS server gives the IP address to the user.

Exercise /#1B:
Suppose an attacker is on the User's home network. How hard is it to poison your DNS cache? What steps are required?
It is very easy if they are on the network.
Respond faster than the local DNS. Spoof the IP of local DNS. Respond with the transaction ID/sequence number of the request.
Port # and Transaction ID are both 16 bits, and both randomized.

Exercise /#1C:
Suppose an attacker wants to poison the DNS cache for all users on Verizon FIOS, and make all verizon FIOS users who go to www.nytimes.com go to 6.6.6.6. How should she do that? How hard is it?
In the initial query to the root server, the local dns caches that info so it doesn't have to do that again. When it queries the TLD server, it caches the response again. When it queries the authoritative DNS server, it caches the response, which is the IP address.

The attacker can take over the answer with the IP address from the authoritative server.
There are 3 steps:
respond faster than real DNS server
Spoof the IP address DNS server - generally easy
Need the source port # and transaction ID - 32 bits of randomness
They need to read headers of DNS packets - extremely difficult
This is all very hard to do, but it has happened

One of the goals in the cyber kill chain is persistence - they need to remain on the system after they gain initial access.
Attackers can be on the network for months - it takes a really long time of access to accomplish the goals of the attackers.

Exercise #2:
What does this scan for?
nmap -sS -O 10.10.10.10
TCP or UDP?
Which ports?
TCP SYN scan with OS detection: it will scan the top 1000 ports (most common, not ports 0 -> 999)
Reality: do not rely on defaults: specify everything, and just scan everything
nmap -sS -O 10.10.10.10 -p-

Persistence is all about staying on the system.

Trojans: any program that pretends to be something else
Non self replicating "back door" program which runs hidden on the infected computer
Can be installed by:

1. Non trusted software download
2. Email attachments
3. Application level exploits
4. Executable content on websites (Flash, Java, ActiveX)
   Trojan can be used to maintain control of the system, access password, keylog, etc.

For simplicity, all unauthorized software is called malware
Trojan creators these days are typically motivated by financial gain
Hence they typically look for credit card, account data, confidential documents, financial data, etc.

Some ports were typically used by Trojans. They became so popular that if a port was used by some program, some antivirus would block those programs

Determining which ports are listening:
-netstat -an | findstr (windows)
-netstat -anp | grep (linux)

Goal for malware is to hide itself though, so it wants to avoid this

Proxy Server Trojans: starts a hidden http proxy on the victims computer
Attacker uses the victim's computer as a transit point to attack yet another victim. Hides the location of the attacker.
Metasploit Meterpreter shell can easily install a proxy trojan.

NetBus Trojan
Remote Control trojan program - RAT
Allows anyone running the client (control program) to control any machine infected with the NetBus Trojan
Many variants were subsequently released

Rootkits
Designed to evade detection
Can run in user mode and kernel mode
User mode rootkits run in ring 3 along with other user applications
kernel mode runs in ring 0 by modifying the OS kernel

Exercise #3:
How could malware survive an operating system wipe?
If the malware infects the firmware
Embedding the malware within the BIOS or UEFI firmware of the device
Hide in backup

Exercise #4: What are some reasons for an attacker to stay on a host after it is compromised?
Continue lateral movement, planning exploitation, monitor user's activities

Loki2
Loki: arbitrary information tunneling in the data portion of ICMP_ECHO and ECHOREPLY
Attacker install Loki on compromises server: requires root, grabs incoming ICMP packets
Can also use UDP 53 to disguise as DNS
Can switch between UDP and ICMP
Encryption supported

Covert Channel:
The message is hidden within the traffic of legitimate communications channel.

Network Steganography:
The message is hidden within the traffic of a legitimate comm channel

Common Example: Tunnel inside TCP 80
Tunneling - encapsulating one protocol into another protocol.
•Very common method for even legitimate applications is to tunnel their communications over TCP 80.
•Other methods include tunneling inside SSH and GRE tunneling.
GRE: GRE protocol, or Generic Routing Encapsulation, is ==a tunneling protocol developed by Cisco that encapsulates packets of one network protocol within another.
•This causes problems for firewalls that rely on restricting traffic by IP and source/destination port
•Application layer firewalls dig deeper into the packets and can filter by the application itself.

covert_tcp:

1. IP Identification method: ID field is a 16 bit number used for TCP segmentation. Supposed to be a random number. You can fit insert a single ASCII charactr and receive it at the other end
2. TCP sequence Number method: Send SYN with ADCII character as the initial sequence number, reply with rst, rst actuall acks the receipt of the hidden character
3. TCP ACK #: sender bounces this information of an unwitting intermediate party
   Exercise #5
   Explain the three functions of covert_tcp

What are another three places (aside from the covert_tcp functions) where data can be hidden while still allowing TCP to work correctly?
. IP Identification method: ID field is a 16 bit number used for TCP segmentation. Supposed to be a random number. You can fit insert a single ASCII charactr and receive it at the other end
2. TCP sequence Number method: Send SYN with ADCII character as the initial sequence number, reply with rst, rst actuall acks the receipt of the hidden character
3. TCP ACK #: sender bounces this information of an unwitting intermediate party
You can hide in Checksum, options, source port # (supposed to be randomly generated)

Reverse WWW shell
Covert channel using HTTP
Reverse WWW shell

Advanced Exfiltration
Exfiltration canuse any common network protocols: DNS, HTTP, Email, upload to Websites (Pastebin, Dropbox)

Data Loss Prevention: a class of tools used to prevent accidental or intentional exfilitration of data
Host Based and network based (email gateway, web proxy)
Idenfitifcation of sensitive data
Regular Expression
Keywords
Data Tagging
Monitors portable devices (e.g., USB flash drives)

Removal of Evidence
Altering Event Logs - deleting is very obvious, might want to edit instead
Logs in Windows: stored in registry
EventLog is logging server
File end with .LOG
Application, Security, System
This info is moved to main event logs files, Windows usually locks these files so normal processes can't be edited

Unix Logging
Log files are usually in ASCII
With privilege they are easy to edit

Shell History Files store history of shell commands

Exercise #6:
How can we retain logs after an attacker has breached the system?
Send logs to external service (Splunk, ELK, etc), log redundancy and backups

Exercise A:
Describe three methods attackers use to maintain access on a compromised system. What are ways to detect each method?
Create a backdoor - a hidden entry point into the system. This can be detected with unusual network connections, weird processes, and anti-malware scans.
Credential Theft - stealing user credentials like username/password combinations. This can be detected with multifactor authentication.
Installing malware on operating system - can be detected with tools that monitor the kernel