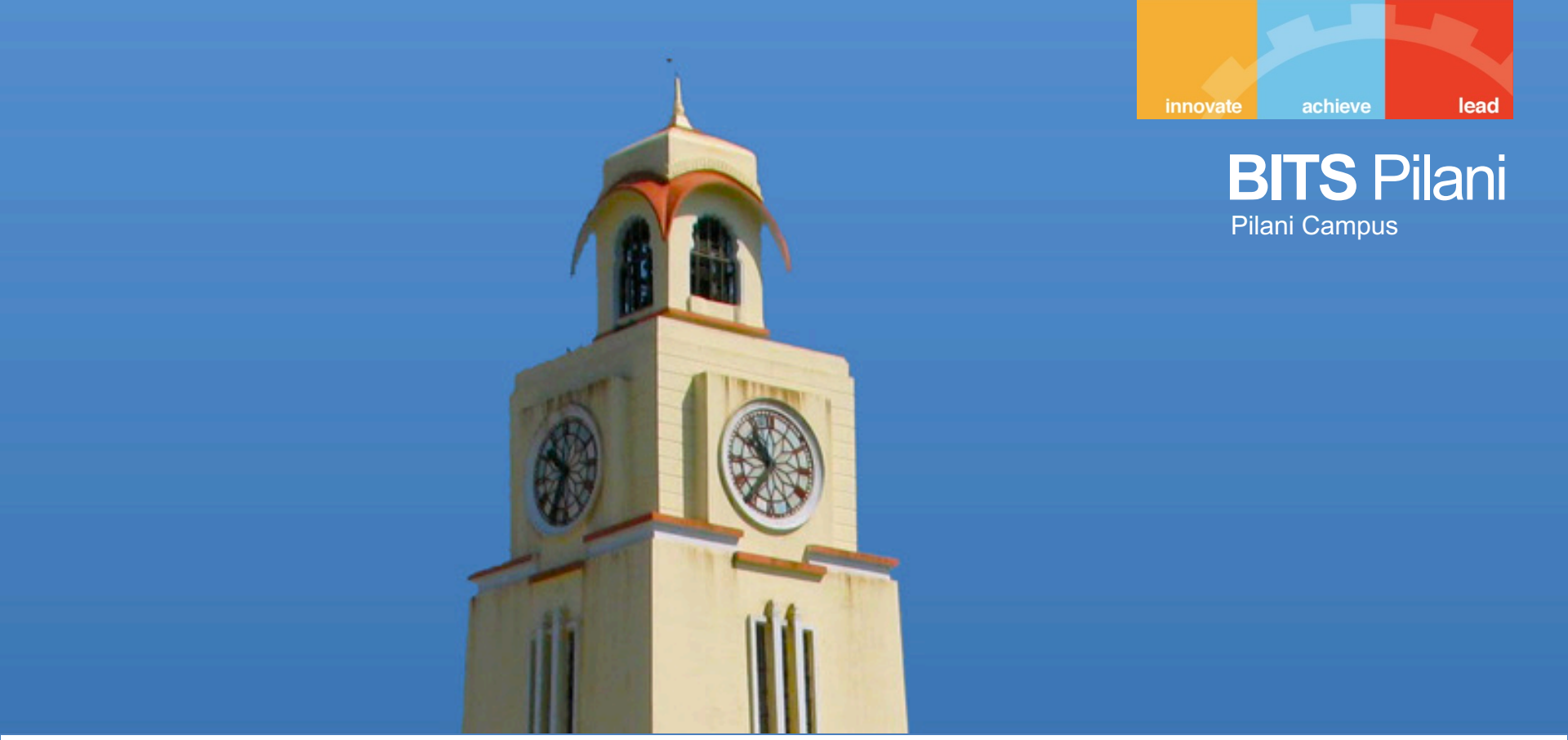
BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP



SSZG575: Ethical Hacking
Session: 02 (Tools & Techniques)

Agenda

innovate achieve lead

- Tools & Techniques
  - Rootkits
  - Covert-channels
  - Sniffing
  - MITM
  - Botnets
  - Covering the traces
  - Camouflage
  - Defeat forensics
  - Use cases and discussions
- Metasploit Overview

Introduction

What is a Rootkit?

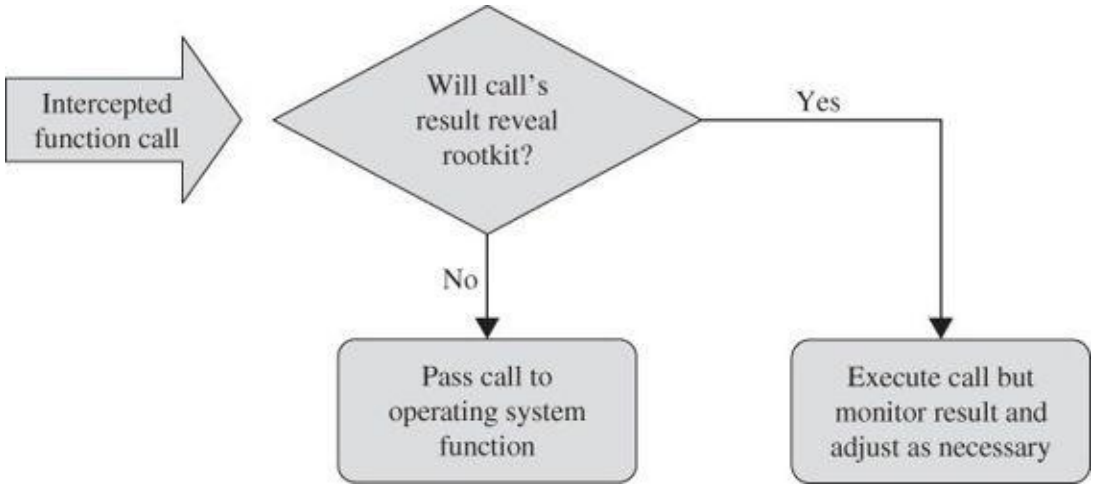
- ROOTKIT is a piece of designed to hide itself (so that it remains undetected) and its processes, data and/or activities on the system.
- ROOTKIT is used to open a backdoor so that the attacker can have uninterrupted access to the compromised machine
-
- Q: Is a rootkit virus or worm?

Rootkit Capabilities

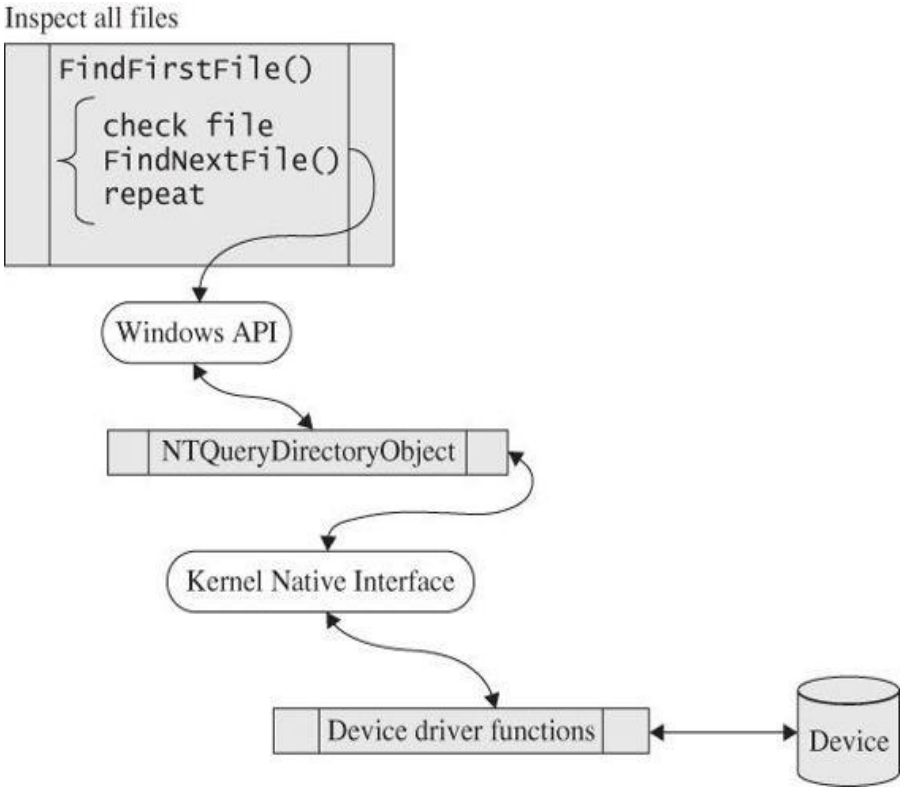
- Hides processes
- Hides files
- Hides registry entry
- Hides services
- Bypasses personal firewalls
- Undetectable by anti-virus software
- Can create covert channels – undetectable on network
- Defeats cryptographic hash checking
- Installs silently – no logs etc

How Rootkit Evades Detection?

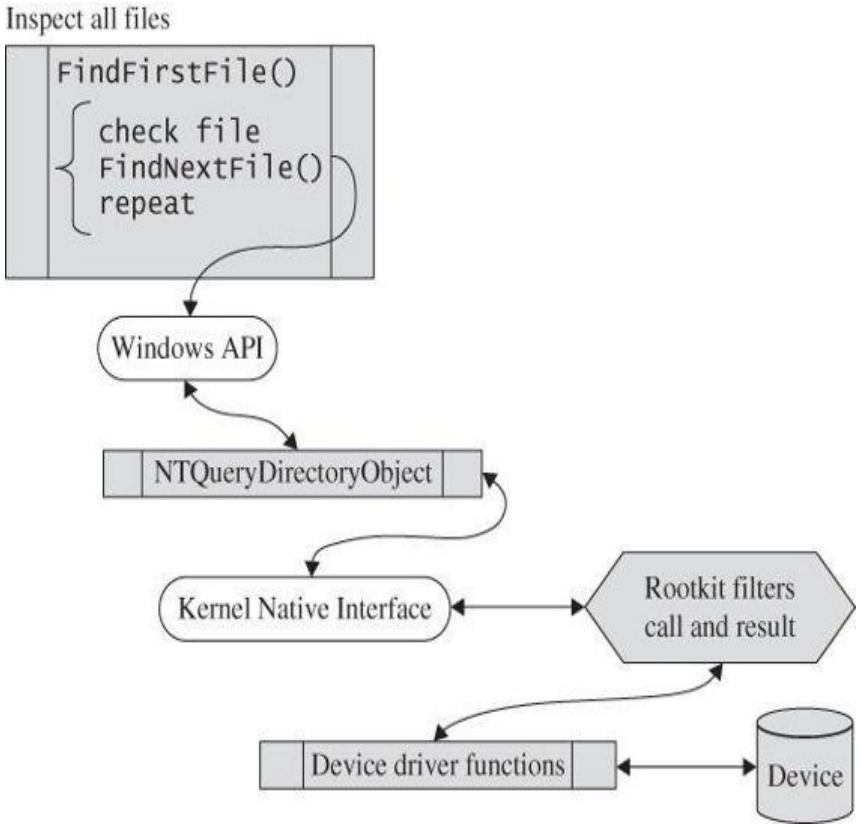
- Rootkits intercept the operating systems calls then alter results of the call if required. This allows rootkit to evade it's detection – antivirus tools or operating system tools



How Rootkit Evades Detection?…



Normal OS call execution



Rootkit controlled OS call execution

Rootkit Revealer Tools

- Ice Sword
- F-Secure Black Light
- Rootkit Revealer
- Dark Spy
- System Virginity Verifier
- RK Detector

Covert Channel

innovate achieve lead

- A covert channel is any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy.
- Covert channels transfer information using non-standard methods against the system design.
- Covert channel allows the communication of information by transferring objects through existing information channels or networks using the structure of the existing medium to convey the data in small parts.
- Covert channels are used to steal data from highly secure systems

Covert Channel: Examples

- Jeremiah Denton, a prisoner of war during the Vietnam War, used a covert channel to communicate without his captors' knowledge.
  - Denton was interviewed by a Japanese TV reporter in a videotape interview
  - USA intelligence agents noticed that Denton was blinking in an unusual manner on the tape
  - They discovered he was blinking letters in Morse code. The letters were T-O-R-T-U-R-E and Denton was blinking them over and over
  - This is a real-world example of covert channel use to send a message undetected.
- In computers, a property of a file can be used to deliver information rather than the file itself.
  - An example can be creation of a seemingly innocent computer file 16 bytes in size.
  - The file can contain any data as that is not the important information.
  - The file can then be emailed to another person.
  - The file seems meaningless but the real communication is of the number 16.
  - The file size is used to communicate the important data, not the contents of the file.

Covert Channel: Examples

- Covert channels can use a technique called tunnelling, which lets one protocol be carried over another protocol.
- Internet Control Message Protocol (ICMP) tunnelling is a method of using ICMP echo-request and echo-reply to carry any payload an attacker may wish to use, in an attempt to stealthily access or control a compromised system.
  - Ping command is a used as a troubleshooting tool using ICMP protocol.
  - For that reason, many router, switches, firewalls, and other packet filtering devices allow the ICMP protocol to be passed through the device.
- Loki is a hacking tool that provides shell access over ICMP, making it much more difficult to detect than TCP or UDP based backdoors.
  - The network thinks, a series of ICMP packets are being sent across the network.
  - Hacker sends commands from Loki client and executing them on the server.
  - https://www.skillset.com/questions/the-hacking-tool-loki-provides-shell-access-to-the-attacker-over-6083
- Reference: https://www.hackingarticles.in/covert-channel-the-hidden-network/

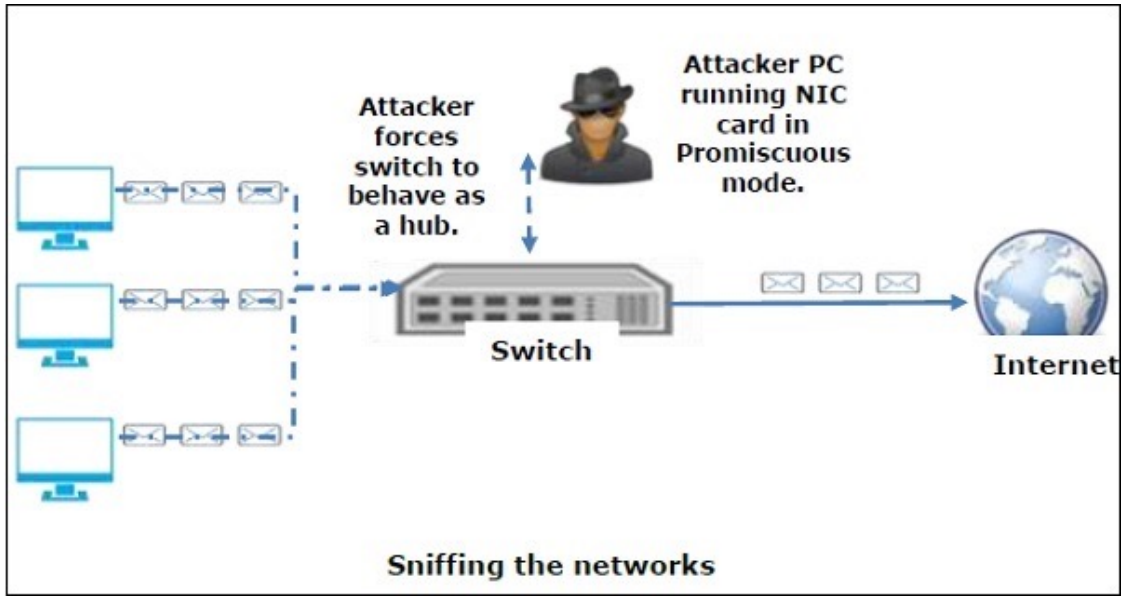
Exercise

- http://www.spammimic.com

What is Sniffing?

- Sniffing is the process of monitoring and capturing all data packets that are passing through a computer network using packet sniffers.
- Packet Sniffers (network protocol analysers) are used by network administrators to keep track of data traffic passing through their network.
- **Active Sniffing:**
  - Conducted on a switched network.
  - Switch is a device that connects two network devices together.
  - Switches use the media access control (MAC) address to forward information to their intended destination ports.
  - Attackers take advantage of this by injecting traffic into the LAN to enable sniffing.
- **Passive Sniffing:**
  - Uses hubs instead of switches.
  - Hubs perform the same way as switches only that they do use MAC address to read the destination ports of data.
  - All an attacker needs to do is to simply connect to LAN and they are able to sniff data traffic in that network.

How Does Sniffing Work?



Sniffing the networks

- Sniffing is similar to that of “tapping phone wires” and try to know the conversation details (**wiretapping)**.
- Information sniffed normally includes:
  - Email traffic
  - FTP passwords
  - Web traffics
  - Telnet passwords
  - Router configuration
  - Chat sessions
  - DNS traffic

Sniffing Tools

- **BetterCAP:** Perform various types of MITM attacks, manipulate HTTP, HTTPS and TCP traffic in real-time, sniff for credentials etc.
- **Ettercap:** Comprehensive suite for MITM attacks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.
- **Wireshark:** One of the widely used packet sniffers with many features to analyse traffic.
- **Tcpdump:** Well-known command-line packet analyzer. It provides the ability to intercept and observe TCP/IP and other packets during transmission over the network.
- **WinDump:** A Windows port of the tcpdump.
- **OmniPeek:** A commercial product that is the evolution of the product EtherPeek.
- **Dsniff:** A suite of tools designed to perform sniffing with different protocols with the intent of intercepting and revealing passwords on Unix & Linux platforms.
- **EtherApe:** Linux/Unix tool with graphical display of incoming and outgoing connections.
- **MSN Sniffer:** Sniffing utility specifically designed for sniffing MSN Messenger traffic.
- **NetWitness NextGen:** It includes a hardware-based sniffer to monitor and analyze all traffic on a network. This tool is used by the FBI and other law enforcement agencies.

How to Detect Sniffing?

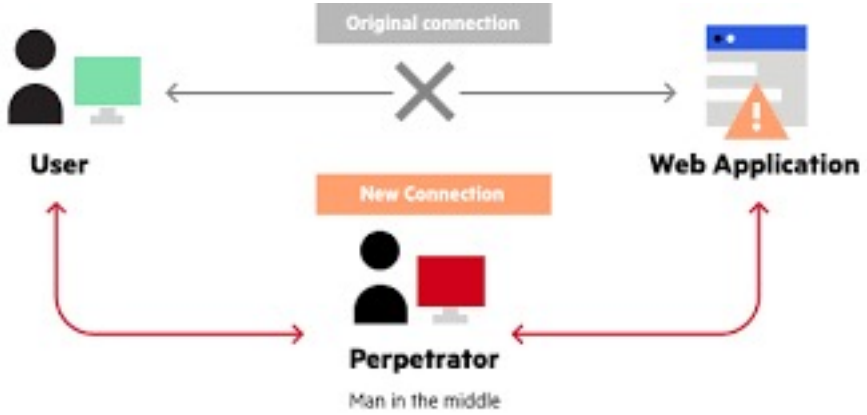
- Sniffers normally collect data and are difficult to detect.
- Easier to detect a sniffer on a switched ethernet network segment. The techniques are:
  - **Ping method:** Sniffer might respond to the ping if the suspect machine is still running. It is not a strongly reliable method.
  - **ARP method:** Machines always capture and caches ARP. Upon sending a non-broadcast ARP, the sniffer/promiscuous machine will cache the ARP and it will respond to our broadcast ping
  - **On Local Host:** Logs can be used to find if a sniffer is being used.
  - **Latency method:** Ping time is generally short. If the load is heavy by sniffer, it takes long time to reply for pings.
  - **ARP Watch:** Used to trigger alarms when it sees a duplicate cache of the ARP.
  - **Using IDS:** Intrusion detection systems monitors for ARP spoofing in the network.

Man In The Middle (MITM)

- Man-In-The-Middle attack intercepts a communication between two systems.
- Attacker splits the original connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server.
- Once the connection is intercepted, the attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication.
- MITM attack is very effective because of the nature of the http protocol and data transfer which are all ASCII based.
- MITM attack could also be done over an https connection. It consists in the establishment of two independent SSL sessions, one over each TCP connection.
- Browser sets a SSL connection with the attacker, and the attacker establishes another SSL connection with the web server.
- Normally, browser warns the user that the digital certificate used is not valid, but the user may ignore the warning because they don’t understand the threat.

MITM Attack Tools

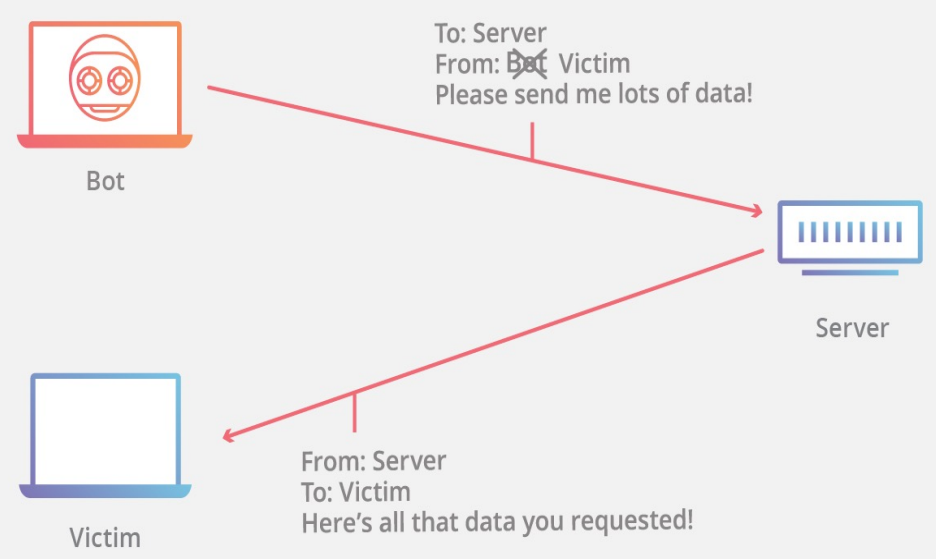
- MITM attack tools are particularly efficient in LAN network environments as they implement extra functionalities, like ARP spoof capabilities to intercept communication between hosts.
- Few popular once are:
  - PacketCreator
  - Ettercap
  - Dsniff
  - Cain and Abel



MITM Attack Types

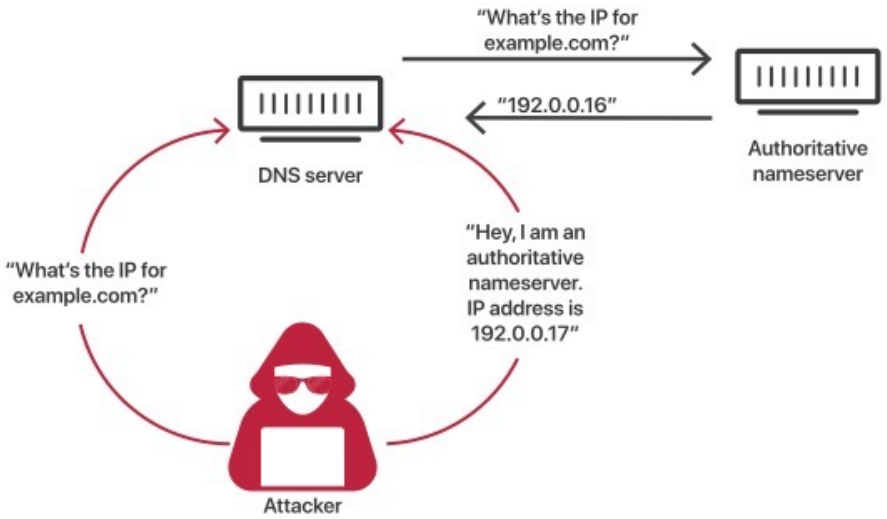
- **IP spoofing:** Spoofing of the IP address of target server which a victim wants to connect
- **DNS spoofing:** A technique that forces a user to a fake website rather than the real one the user intends to visit.
- **HTTPS spoofing:** Attacker fools a browser into believing it's visiting a trusted website
  - Browser is re-directed to an unsecure website and attacker monitors interactions with that website and steals any personal/important information.
- **SSL hijacking:** Attacker uses another computer and secure server and intercepts all the information passing between the server and the user's computer.
- **Email hijacking:** Taking over the email accounts of an important target (banks, HNIs etc)
  - Attacker monitors transactions
  - Attackers can then spoof the email address and send their own instructions to customers.
- **Wi-Fi eavesdropping:** Cybercriminals set up Wi-Fi connections with legitimate sounding names. Once a user connects to this Wi-Fi, the attacker will be able to monitor the user's online activity and be able to intercept login credentials, payment card information, and more.
- **Stealing browser cookies:** Cybercriminals hijack browser cookies which store information from user browsing session enabling attacker to gain access to passwords, address, and other sensitive information.

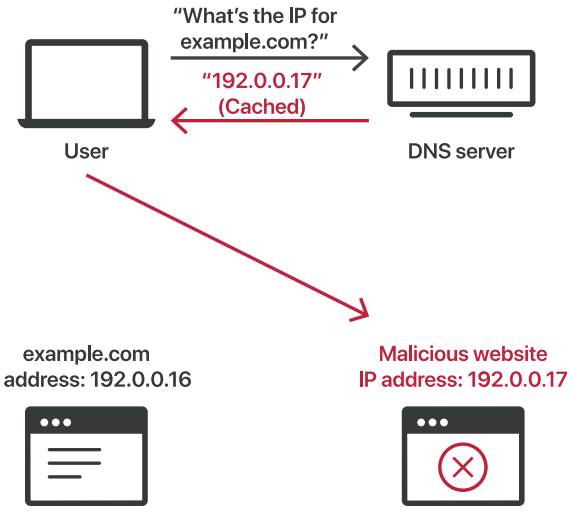
What is IP Spoofing?



- IP spoofing is the creation of IP packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both.
- Sending and receiving IP packets is a primary way in which networked computers and other devices communicate over internet.
- An IP packets contains a header which precedes the body of the packet and contains important routing information, including the source address.
- In a normal packet, the source IP address is the address of the sender of the packet. If the packet has been spoofed, the source address will be forged.

What is DNS Spoofing?





- Attackers can poison DNS caches by impersonating DNS nameservers, making a request to a DNS resolver, and then forging the reply when the DNS resolver queries a nameserver.
- This is possible because DNS servers use UDP instead of TCP, and because currently there is no verification for DNS information.

MITM Attack Prevention

- Use “HTTPS” instead of HTTP
- Be wary of potential phishing emails from attackers asking to update password or any other login credentials.
- Instead of clicking on the link provided in the email, manually type the website address into browser.
- Never connect to public Wi-Fi routers directly, if possible.
  - Use VPN to protect the private data while using public Wi-Fi.
- Install a strong security solution to detect and protect from malware. Always keep the security software up to date.
- Ensure home Wi-Fi network is secure.
  - Update all of the default usernames and passwords on home router and all connected devices to strong, unique passwords.

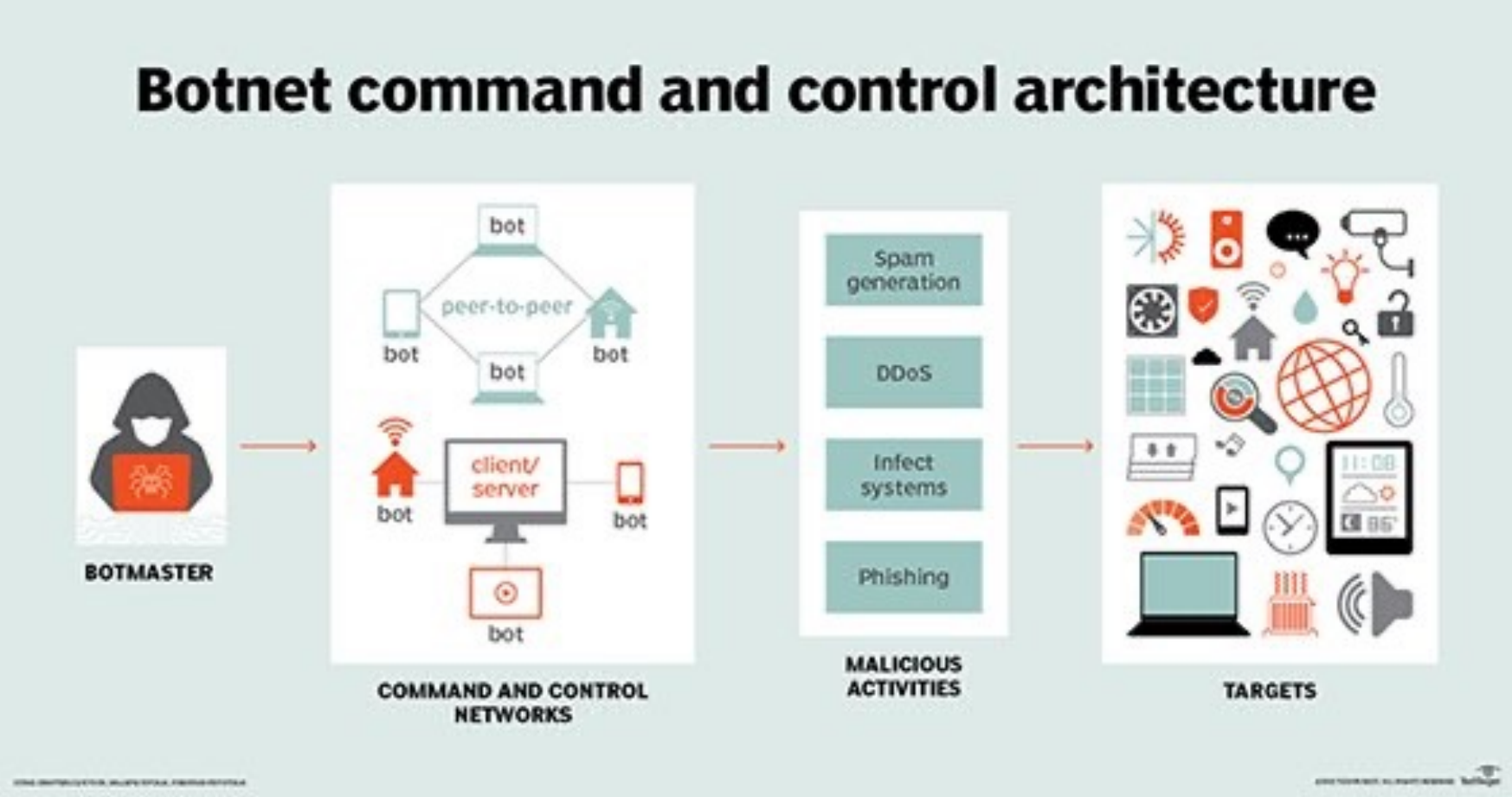
Botnets

- A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them.
- Attackers use botnets to for malicious activities such as credentials leaks, unauthorized access, data theft and DDoS attacks.
- Common botnet actions are:
  - **Email spam:** Used for sending out spam messages in huge numbers. The Cutwail botnet can send up to 74 billion messages per day. They are also used to spread bots to recruit more computers to the botnet.
  - **DDoS attacks:** Leverages the massive scale of the botnet to overload a target network or server with requests, rendering it inaccessible to its intended users.
  - **Financial breach:** Includes botnets specifically designed for the direct theft of funds from enterprises and credit card information. ZeuS botnet is one such example.
  - **Targeted intrusions:** Smaller botnets designed to compromise specific high-value systems of organizations (R&D, Financials, IP etc) from which attackers can penetrate and intrude further into the network.

Protection from Botnets

- Use a good Internet security suite that detects and removes a malware from machine and prevents future attacks.
- Update computer's operating system as early as possible. Hackers often utilize known flaws in operating system security to install botnets.
  - Set computer to install updates automatically.
- Update applications on computer, phone and tablet.
  - Hackers create programs to exploit known weaknesses of applications.
- Don't download attachments or click on links from email addresses you don't recognize.
- Use a firewall when browsing the Internet.
  - Use pre-installed firewall on Mac while install a good third party firewall on Windows based machine.
- Don't visit websites that are known distributors of malware.
  - Use an Internet security tool to warn about such sites.

Protection from Botnets



Covering the Tracks

- Hiding of digital footprints is the final stage of penetration testing.
- Ethical hackers cover their tracks to:
  - Maintain their connection in the system
  - Avoid detection by incident response teams or forensics teams
- Methods to cover tracks
  - Using reverse HTTP shells
  - Using ICMP tunnels
  - Clearing event logs
  - Erasing command history

Covering the Tracks

- **Using Reverse HTTP Shells**
  - Hacker installs reverse HTTP shells on the victim computer and uses it to send communications to the network's server.
  - Reverse shell is designed in a way that the target device will always return commands.
  - This is possible since port 80 is always open, and therefore, these commands are not flagged by the network's perimeter security devices like firewalls.
  - Hacker can now gain any information from the server undetected leaving no footprint behind since all they did was send HTTP commands.
- **Using ICMP Tunnels**
  - ICMP is used by a network device to test connectivity using echo requests.
  - Hackers encapsulate these echo requests with TCP payloads and forward them to the proxy server.
  - This request is then de-capsulated by the proxy server, which extracts the payload and sends it to the hacker.
  - Network's security devices read this communication as simple ICMP packet transfer hence facilitating the hacker in covering their tracks.

Covering the Tracks…

innovate achieve lead

- **Clearing Event Logs**
  - Using Metasploit Meterpreter but hacker must exploit a network using Metasploit.
  - Hacker uses the Meterpreter command prompt and uses the script “clearev” to clears all the event logs.
  - Event logs can also be cleared using the clearlog.exe file.
  - After deleting the event logs, the hacker removes the clearlog.exe from the system.
  - Event logs in Linux systems can also be deleted using text editors such as “kWrite”.
  - Logs in Linux systems are stored in the “/var/logs” directory.
- **Erasing Command History**
  - If the hacker is in a hurry and does not have time to go through all the event logs, they could cover their tracks by erasing and shredding the command history.
  - Hackers delete their bash history (can store upto 500 commands) by resetting its size to zero using command “export HISTSIZE=0”.
  - History file can be shredded using the command “shred -zuroot/bash_history”.

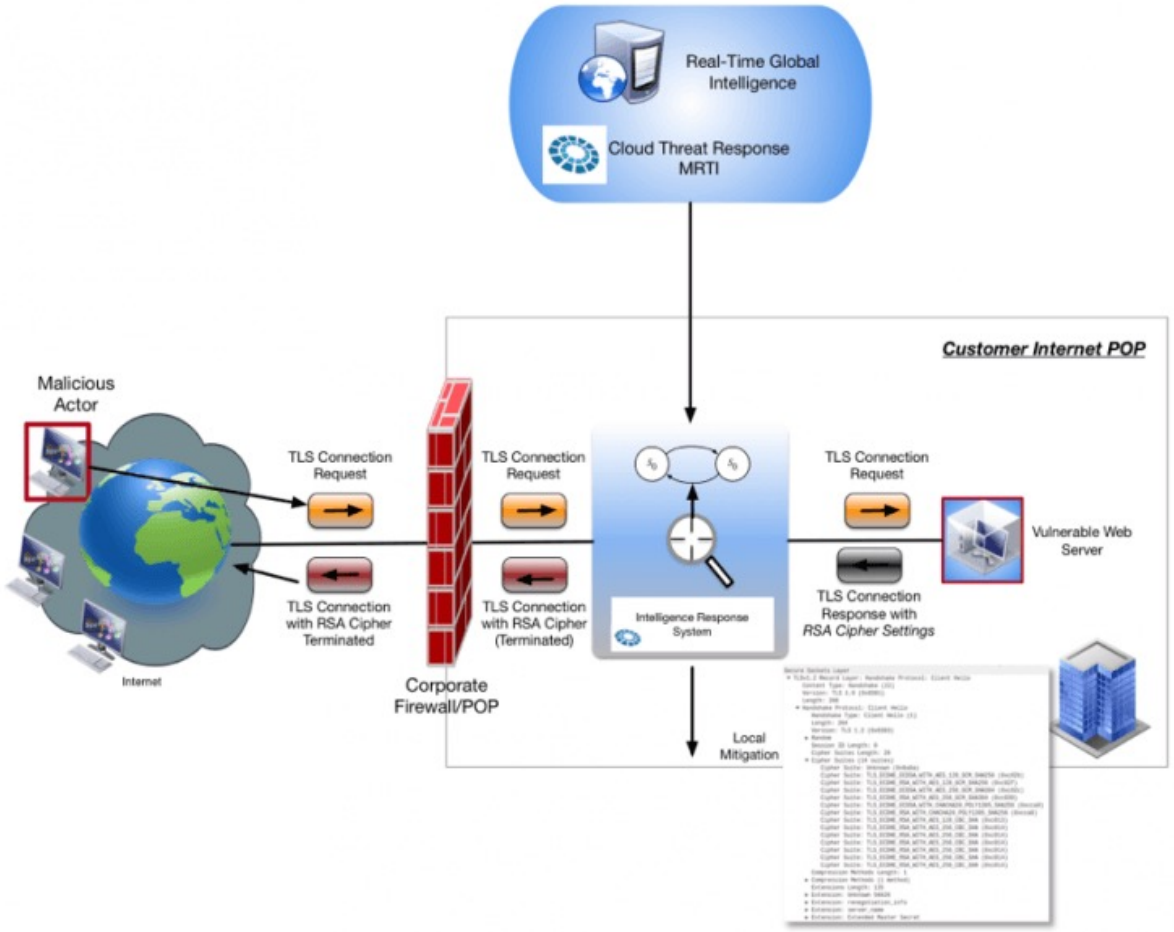
Camouflage

- **Camouflage**: The act, means, or result of obscuring things to deceive an enemy by painting or screening objects so that they are lost to view in the background, or by making up objects that from a distance have the appearance of fortifications.
- **Deception**: To mislead by a false appearance or statement.

Camouflage Defense Strategy

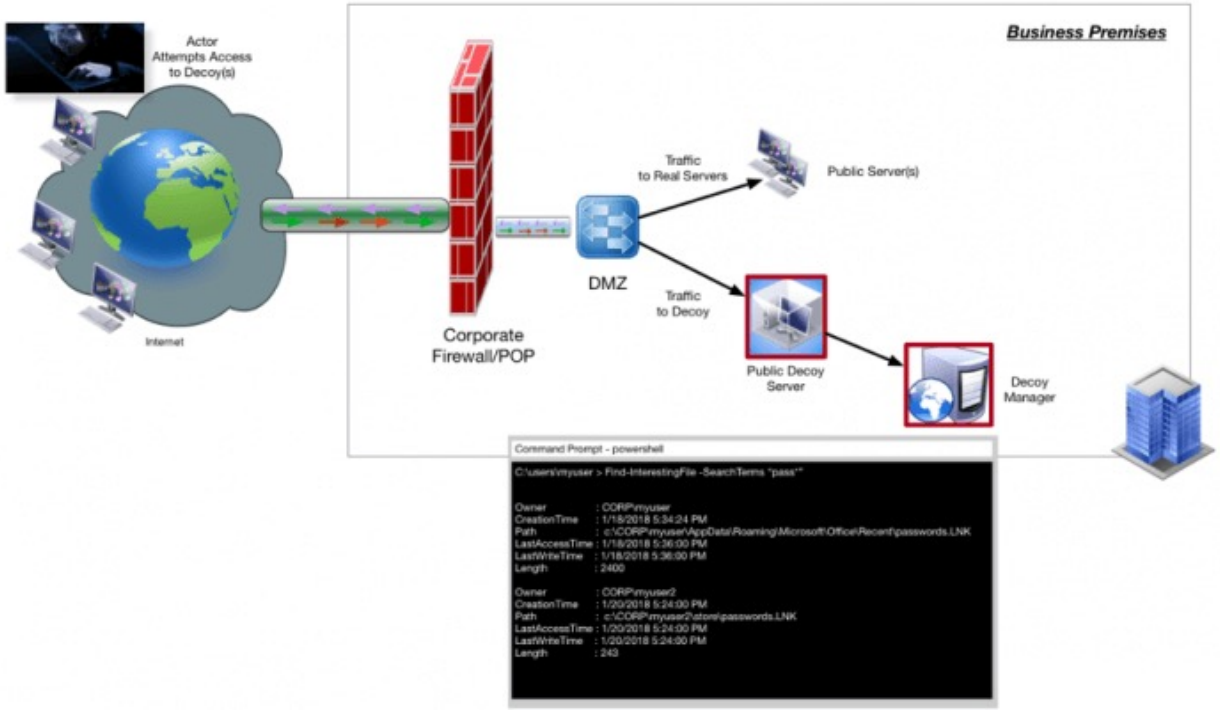
- Predicting Attacks
  - Ability to gather low-false positive threat intelligence on adversary tactics, indicator etc.
  - Ability to easily understand goals, motives, intent etc
- Detecting Activities
  - Ability to gather advanced detection when other protections fail
  - Early alerting and notification to operations without impact to business-critical systems
- Disrupting & Responding
  - Easily engage with attackers and their Tactics, Techniques & Procedures (TTPs)
  - Easy reconnaissance on the attacks
  - Manipulation of behavior and interactions that confuse, delay, or interrupt attacker's activities
  - Increase the cost, expertise required and impact on the attacker

Camouflaging Unpatched Server



- IT & security teams are often unable to keep up with the continuous challenge of maintaining software patch levels on all servers.
- Unpatched servers remain vulnerable to being exploited.
- Network-based camouflage is a way to protects against certain types of vulnerabilities.
- This involves obfuscation and camouflage by an intermediary network system configured to do so based on threat intelligence on the vulnerabilities.

Server Decoys



- Deception techniques are alternative or addition to camouflage.
- Use of decoy systems that impersonate legitimate systems that can act as an enticement to attackers.
- Endpoint decoy can provide vital insight to the TTPs performed by those actors.
- Decoys engage an attacker to explore/ spend time to analyse false data provided by the decoy.
- This increases the time the attacker is under watch and provides useful intelligence on their objectives.

What is Anti-Forensics?

- Approach used by criminal hackers to make it harder for investigation agencies to find them and even harder to prove the crime links to the hacker.
  - Data hiding: Encryption, steganography, hardware/software based concealment
  - Artifact hiding/erasing: Disk cleaning utilities (Cyber scrub, CyberCide, KillDisk), File wiping utilities (BC wipe, Eraser Cyber scrub)
  - Trail obfuscation: Log cleaners, timestamp modification, misinformation, spoofing, trojan command
  - Tunnelling
  - Onion routing
  - IP and MAC spoofing
  - Counter forensic tools

Understand Trust Boundaries

innovate achieve lead

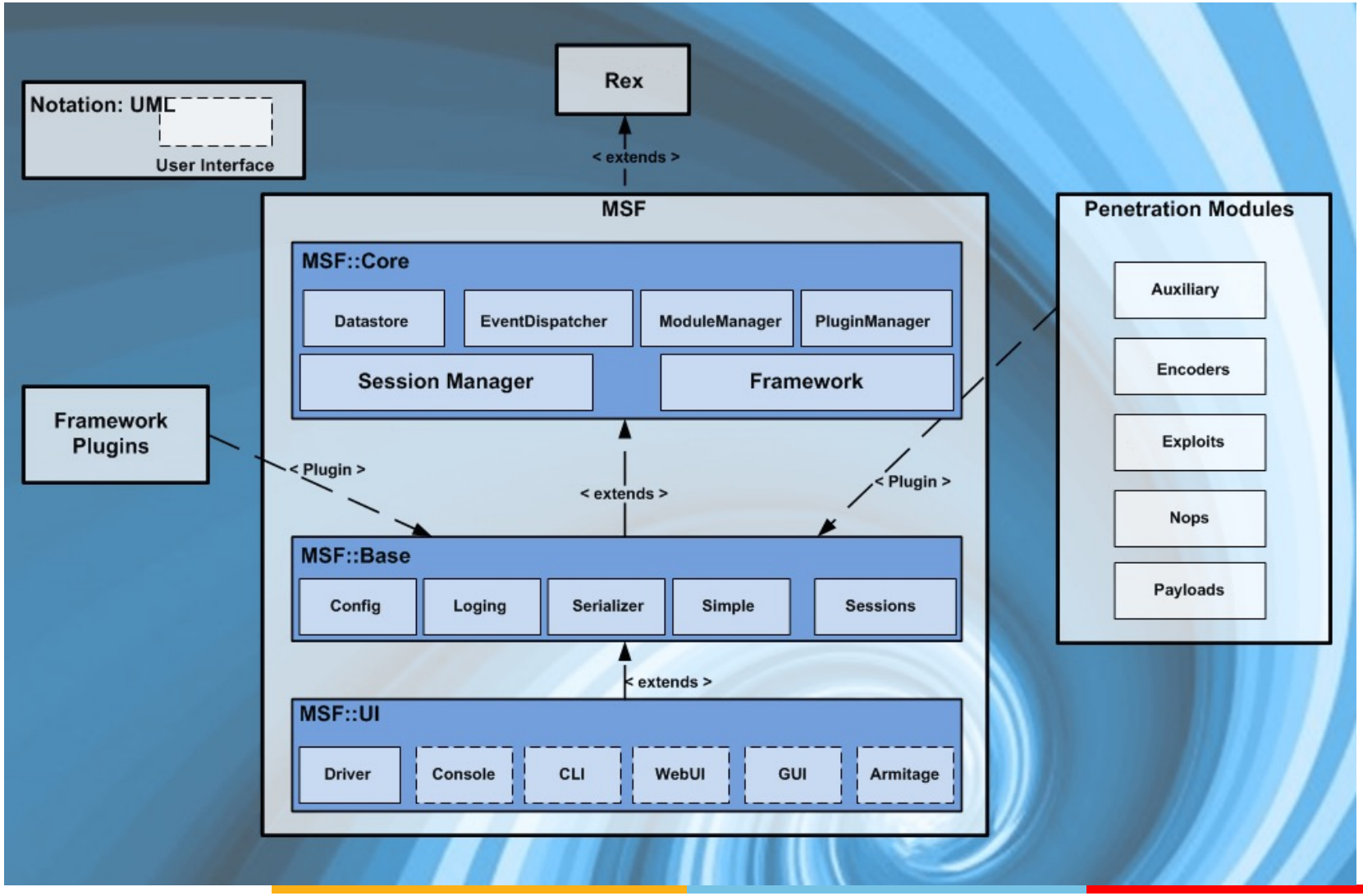
- **BetterCAP:** BetterCAP is a powerful, flexible and portable tool to perform various types of MITM attacks against:
  - A network,
  - Manipulate HTTP, HTTPS and TCP traffic in real-time
  - Sniff credentials and other important information.

Metasploit Framework Overview

What is Metasploit Framework (MSF)?

- Collection of several tools and mainly used for Penetration Testing, Research, Creating and Testing new exploits
- Provides infrastructure to automate mundane and complex tasks
- Created by HD Moore in 2003 in Perl
- Many contributing developers worldwide
- Metasploit 2.0 in 2004 and Metasploit 3.0 in 2007
- Acquired by security firm Rapid7 in 2009
  - Paid (Metasploit Pro and Metasploit Express) & Community versions
- Website: http://www.metasploit.com/
- Reference: https://www.offensive-security.com/metasploit-unleashed/introduction/

Metasploit Architecture



Metasploit Framework: Core

- MSF Core consists of various subsystems such as module management, session management, event dispatching, and others.
- MSF Core provides an interface to the modules and plugins with the framework.
- Following the object-oriented approach of the entire architecture, MSF Core itself is a class, which can be instanced and used as any other object.
- MSF Core consists of:
  - Datastore
  - Event Notifications
  - Framework Managers

Metasploit Framework: Base

- MSF Base is built on top of the MSF Core and provides interfaces to make it easier to deal with the core.
- Some of these are:
  - **Configuration:** Maintains a persistent configuration and obtains information about the structure of an installation, such as the root directory of the installation, and other attributes.
  - **Logging:** Provides extensive and flexible logging support.
  - **Sessions** Maintains information about and controls the behaviour of user sessions.

Metasploit Framework: UI

- The framework User Interfaces allow the user to interact with the framework.
- Following interfaces are provided:
  - Console: Main console of Metasploit
  - CLI: Command Line Interface
  - WebUI: Web based UI
  - GUI: GUI client
  - Armitage: Attack management tool that automates MSF in a graphical way
  - APIs (Drivers) – REST APIs

REX

- Rex stands for Ruby Extension Library
- Rex is a collection of classes and modules that can be used by developers to develop projects or tools around the MSF
  - The basic library for most tasks
  - Handles sockets, protocols, text transformations, and others
  - SSL, SMB, HTTP, XOR, Base64, Unicode

Plugins

- New concept with the MSF 3.0 version
- Plugins enhance the utility of the framework as a security tool development platform.
- Plugins work directly with the API.
  - Plugins manipulate the framework as a whole
  - Plugins hook into the event subsystem
  - Plugins automate specific tasks that would be tedious to do manually
- Plugins only work in the msfconsole.
  - Plugins can add new console commands
  - They extend the overall Framework functionality

Penetration Modules

- Encoders
  - Encoders are used to evade the anti-virus tools and firewall
  - Encoders have no effect on the functionality of exploit
  - Popular encoders are: shikata_ga_nai, base64, Powershell_base64
- NOPS
  - NOP is short for No Operation
  - NOPs keep the payload sizes consistent ensuring that validly executable by the processor
  - Used to make payload stable
- Auxiliary
  - Provides additional functionality like scanning, fuzzing, Information gathering etc.
  - An exploit without a payload

Penetration Modules: Exploits

- An exploit is the means by which an attacker takes advantage of a vulnerability within a system. Exploits examples are buffer overflows, web application vulnerabilities (such as SQL injection), and configuration errors.
- There are two types of exploits in Metasploit: Active & Passive
- Active exploits will exploit a specific host, run until completion, and then exit.
  - Brute-force modules will exit when a shell opens from the victim.
  - Module execution stops if an error is encountered.
  - Exploits can run in background (using '-j' to exploit command)
- Passive exploits wait for incoming hosts and exploit them as they connect.
  - Passive exploits almost always focus on clients such as web browsers, FTP clients, etc.
  - Can be used in conjunction with email exploits, waiting for connections.
  - Passive exploits report shells as they happen can be enumerated by passing '-l' to the sessions command. Passing '-i' will interact with a shell.

Penetration Modules: Payloads

- A payload is a custom code that attacker wants the system to execute and that is delivered by the Framework. For example, a reverse shell is a payload that creates a connection from the target machine back to the attacker.
- There are three types of payload modules: **Singles**, **Stagers** & **Stages**
  - **Singles** payloads are self-contained and completely standalone.
  - **Stagers** setup a network connection between the attacker and victim and are small and reliable.
  - **Stages** are payload components that are downloaded by Stagers modules.
- Others: Meterpreter, PassiveX, NonX, Ord, IPV6, Reflective DLL Injection etc
- Two common payload used are **shellcodes or shell payloads**
  - Provide the attacker an interactive shell to control the system remotely
  - **Bind Shells:** A socket is created, a port is bound to it and when a connection is established to it, it will spawn a shell.
  - **Reverse Shells**: A connection is created to a predefined IP and Port and a shell is then shoveled to the Attacker.

Generating Payloads

- Payloads can be generated from within the MSFConsole.
- When a particular payload is used, Metasploit adds the **generate**, **pry**, and **reload** commands.
  - Generate: generates a payload
  - Pry: Opens a pry session on current module
  - Reload: Reloads the current module from disk
- Can create payloads in C, Python, Java, Ruby etc
- Msfvenom process steps:
  - Create a malicious file
  - Start the payload handler
  - Get victim to run the malicious file

MSF File System and Libraries

- **data**: editable files used by Metasploit
- **documentation**: provides documentation for the framework
- **external**: source code and third-party libraries
- **lib:** core of the framework code base
- **modules**: actual MSF modules
- **plugins**: plugins that can be loaded at run-time
- **scripts**: Meterpreter and other scripts
- **tools**: various useful command-line utilities

Google Dorks Commands

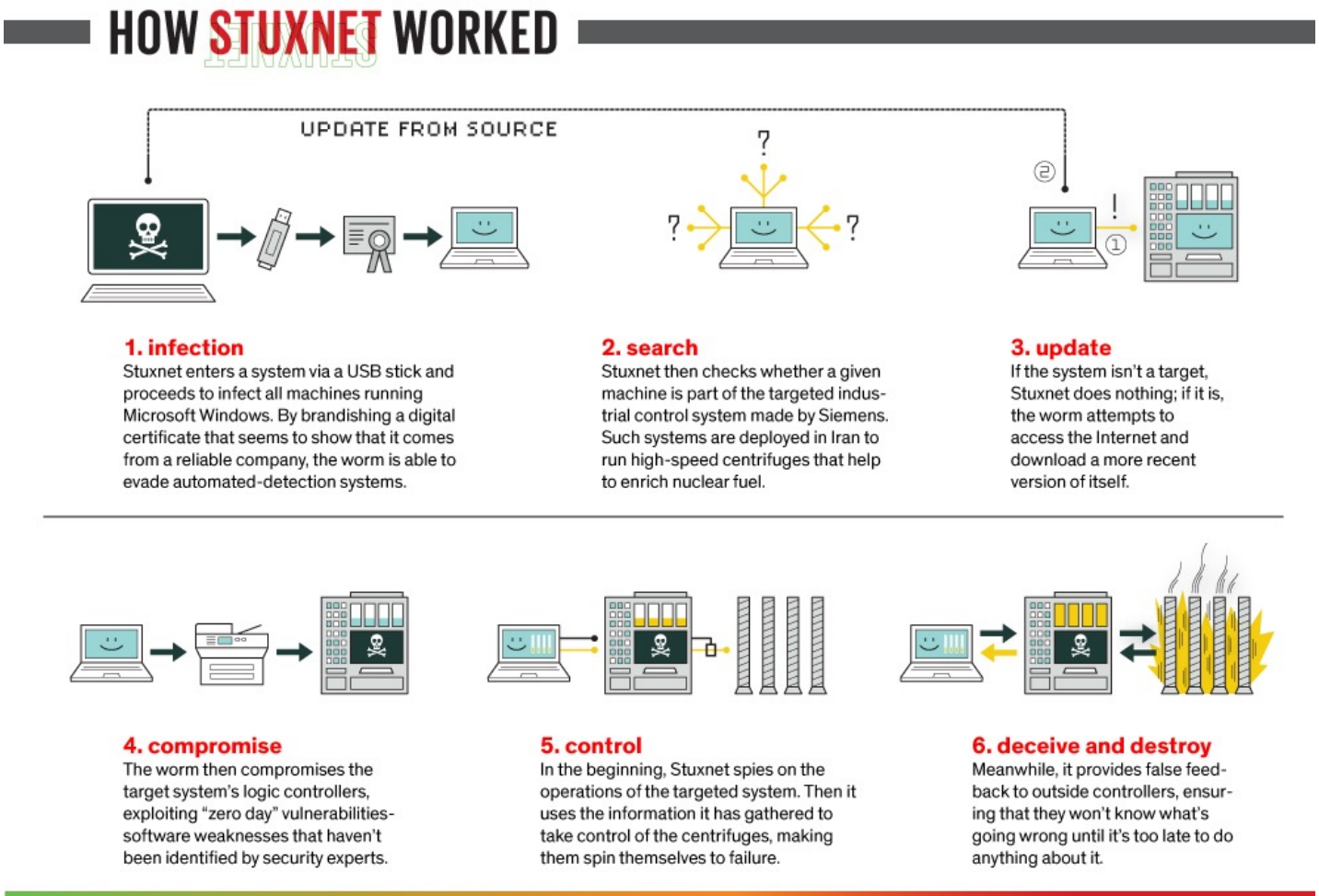
- Popular Google Dorks Commands:
  - Find the text "admin.password" in the Pastebin website (site used by hackers to publish sensitive leaked information): **site:pastebin.com intext:admin.password**
  - Find the text “admin-password” in exposed files of the following types: TXT, LOG, CFG:
    - **"admin_password" ext:txt | ext:log | ext:cfg**
  - filetype:sql intext:wp_users phpmyadmin
  - filetype:env intext:password
  - Zoom meetings: inurl:zoom.us/j and intext:scheduled for
  - Live camera view: inurl:"view.shtml" "Network Camera"
  - Intitle:”WebcamXP 5”
  - allintext:username filetype:log
  - allintext:password filetype:log after:2020
  - DB_USERNAME filetype:env
  - Inurl:top.htm inurl:currenttime — live camera
  - Intitle:”index of” inurl:ftp — publicly exposed ftp sites
  - Intitle:”index of” inurl:http after 2020 — sites still using HTTP
  - Intitle: “forums” inurl:http after 2020 — forums/blogs using HTTP
  - “Inurl:.gov/index.php?id=”
  - Cache:websitetime.com — when the page was last crawled

Shodan Commands

- https://www.shodan.io
- Searches internet connected devices
  - Search ‘Cisco’
  - Search “Cisco” and “New York City”
  - Search Cisco city:”New York”
- Some basic search filters you can use:
  - **city:** find devices in a particular city.
  - **country:** find devices in a particular country.
  - **geo:** search for specific GPS coordinates.
  - **hostname:** find values that match the hostname.
  - **product:** search the name of the software or product identified in the banner.
  - **os:** search based on operating system.
  - **port:** find particular ports that are open.
  - **before/after:** find results within a timeframe.

- **Ref:** https://help.shodan.io/the-basics/search-query-fundamentals

Stuxnet: Rootkit for Industrial Control Systems



Stuxnet: Rootkit for Industrial Control Systems

- Stuxnet: Destroyed Iranian nuclear facility

  http://virus.wikidot.com/stuxnet

- What is a root kit

  https://www.varonis.com/blog/rootkit/

Assignment for next class: Nmap

- Use of Nmap command for hacking activities
  - What is Nmap command?
  - What are various command line arguments for Nmap command?
  - How Nmap can be used for hacking purpose?

Thank You