SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

Vulnerability Identification and Penetration Testing (VIPT)

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

Unit 3: Penetration Testing

- Exploring Ethical Hacking, Malware Threats and their Countermeasures
- Monitoring and Capturing Data Packets using Sniffing
- Restricting the System Access – DoS Attack
- Gather Confidential Information – Social Engineering
- Vulnerability Issues: Operating System Vulnerabilities
- Application Vulnerabilities
- Vulnerability assessment for natural disaster
- Technological hazards and terrorist threats
- Implications for emergency response
- Vulnerability of critical infrastructures

Exploring Ethical Hacking

- Ethical hacking is a process of **detecting vulnerabilities** in an application, system, or organization's infrastructure that an attacker can **use to exploit an individual** or organization.
- They use this process to prevent cyberattacks and security breaches by lawfully hacking into the systems and looking for weak points.
- An ethical hacker follows the steps and thought process of a malicious attacker to gain authorized access and test the organization's strategies and network.
- In the start of international conflicts, terrorist organizations funding cybercriminals to breach security systems, either to compromise national security features or to extort huge amounts by injecting malware and denying access. Resulting in the steady rise of cybercrime. Organizations face the challenge of updating hack-preventing tactics, installing several technologies to protect the system before falling victim to the hacker.
- New worms, malware, viruses, and ransomware are primary benefit are multiplying every day and is creating a need for ethical hacking services to safeguard the networks of businesses, government agencies or defense.

Exploring Ethical Hacking

"Government agencies and business organizations today are in constant need of ethical hackers to combat the growing threat to IT security. A lot of government agencies, professionals and corporations now understand that if you want to protect a system, you cannot do it by just locking your doors"

– says Jay Bavisi, CEO of EC-Council.

Exploring Ethical Hacking

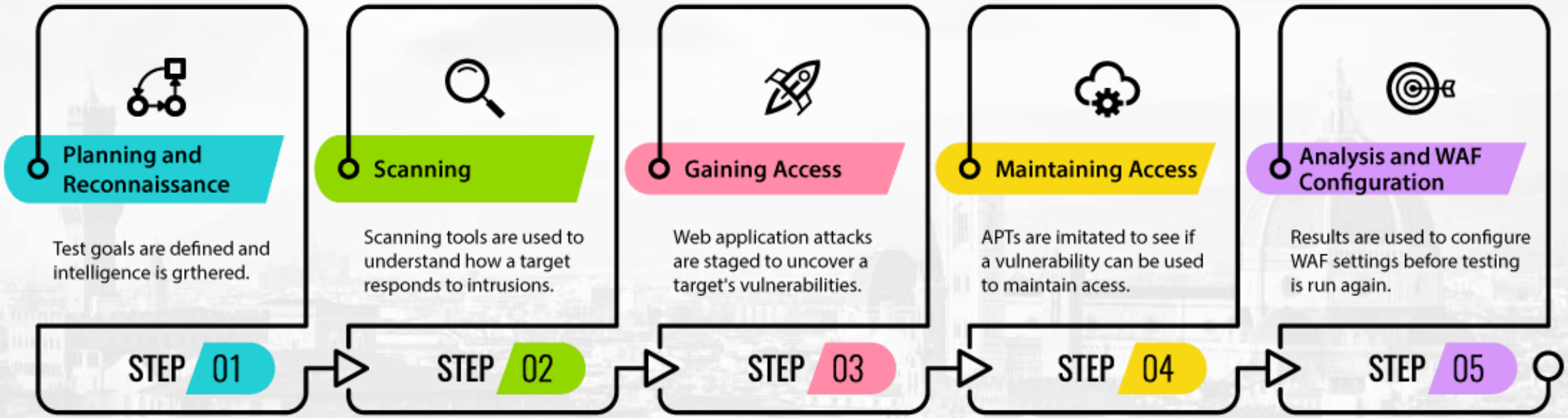
- **Benefits of Ethical Hacking**

The primary benefit of ethical hacking is to prevent data from being stolen and misused by malicious attackers, as well as:

- Discovering vulnerabilities from an attacker's PoV so that weak points can be fixed.
- Implementing a secure network that prevents security breaches.
- Defending national security by protecting data from terrorists.
- Gaining the trust of customers and investors by ensuring the security of their products and data.
- Helping protect networks with real-world assessments.

Exploring Ethical Hacking

Five Phases of Ethical Hacking



Types of Ethical Hacking

It is no big secret that any system, process, website, device, etc., can be hacked. To understand how the hack might happen and what the damage could be, ethical hackers must know how to think like malicious hackers and know the tools and techniques they are likely to use.

- Web Application Hacking
- System Hacking
- Web Server Hacking
- Hacking Wireless Networks
- Social Engineering

Hackers are of different types and are named based on their intent of the hacking system. The three types of hackers are the white hat hacker, the grey hat hacker, and the black hat hacker. The names are derived from old Spaghetti Westerns, where the good guy wears a white hat and the bad guy wears a black hat. Each type of hacker hacks for a different reason, a cause, or both. All have the required skills needed to accomplish their mission.

Malware Threats and their Countermeasures

- “Malware” is short for “malicious software” - computer programs designed to infiltrate and damage computers without the user's consent. “Malware” is the general term covering all the different types of threats to your computer safety such as viruses, spyware, worms, trojans, rootkits and so on.
- **The story of malware**
- Virus creators, or “virus writers”, started off writing viruses in the early 1980’s. Until the late 1990’s most of the viruses were just pranks made up in order to annoy users and to see how far a virus could spread.
- In the late 1990’s and early 2000’s, virus writers and hackers began to put their talents to more professional and sometimes criminal use.
- Today many experts believe the amount of malicious software being released on the web might actually surpass the release of valid software.
- The most common types of malware include viruses, keyloggers, worms, trojans, ransomware crypto-malware, logic bombs, bots/botnets, adware & spyware, and rootkits.
- You can mitigate or prevent malware attacks by developing security policies, implementing security awareness training, using app-based multi-factor authentication, installing anti-malware ; spam filters, changing default operating system policies, performing routine vulnerability assessments. It’s important to note that no system is 100% vulnerability free or “hacker-proof.”

How does malware infect a Computer Or Network

- There are several methods threat actors utilize to deploy malware into a network or system including social engineering and exploiting vulnerabilities.
- **Social Engineering**
- Malware is often deployed through phishing, vishing, or smishing, which are all types of social engineering attacks. In fact, 92% of malware is delivered by email. In short, threat actors attempt to retrieve sensitive information by manipulating people into clicking links, downloading attachments, or providing access over the phone.
- If successful, the malicious payload is delivered, and you can consider yourself breached.
- **Exploiting Vulnerabilities**

One of the easiest ways threat actors break into a system or network is by deploying a series of exploits known to work, such as Kerberoasting. This is referred to as the “trial and error” approach, however, there is a high degree of technical skill involved in this process.

Different types of malware

- **Viruses and worms – the contagious threat**
- Viruses and worms are defined by their behavior – malicious software designed to spread without the user's knowledge. A virus infects legitimate software and when this software is used by the computer owner it spreads the virus – so viruses need you to act before they can spread. Computer worms, on the other hand, spread without user action. Both viruses and worms can carry a so-called "payload" – malicious code designed to do damage.
- Viruses typically remain inactive until it has spread on to a network or a number of devices before delivering the payload.
- Worms are commonly used against email servers, web servers, and database servers. Once infected, worms spread quickly over the internet and computer networks.

Trojans and Rootkits – the masked threat

- Trojans and rootkits are grouped together as they both seek to conceal attacks on computers. Trojan Horses are malicious pieces of software pretending to be kind applications.
- Trojan horse programs are malware that is masked as legitimate software. A Trojan horse program will hide on your computer until it's called upon. When activated, Trojans can allow threat actors to spy on you, steal your sensitive data, and gain backdoor access to your system.
- Trojans are commonly downloaded through email attachments, website downloads, and instant messages. Social engineering tactics are typically deployed to trick users into loading and executing Trojans on their systems. Unlike computer viruses and worms, Trojans are not able to self-replicate.

Rootkits

- Rootkits are a back door program that allows a threat actor to maintain command and control over a computer without the user knowing. This access can potentially result in full control over the targeted system.
- The controller can then log files, spy on the owner's usage, execute files and change system configurations remotely. While traditionally deployed using Trojan horse attacks, it's becoming more common in trusted applications.
- Some antivirus software can detect rootkits, however, they are difficult to clean from a system. In most cases, it's best to remove the rootkit and rebuild the compromised system.

Malware Threats and their Countermeasures

Ransomware / Crypto-Malware

Ransomware is a type of malware designed to lock users out of their system or deny access to data until a ransom is paid. Crypto-Malware is a type of ransomware that encrypts user files and requires payment within a time frame and often through a digital currency like Bitcoin.

Logic Bombs

Logic bombs are a type of malware that will only activate when triggered, such as on a specific date/time or on the 25th logon to an account. Viruses and worms often contain logic bombs to deliver its payload (malicious code) at a pre-defined time or when another condition is met.

The damage caused by logic bombs vary from changing bytes of data to making hard drives unreadable. Antivirus software can detect the most common types of logic bombs when they're executed. However, until they do, logic bombs can lie dormant on a system for weeks, months, or years.

Malware Threats and their Countermeasures

Bots/Botnets

Botnet, short for roBOT NETwork, is a group of bots, which are any type of computer system attached to a network whose security has been compromised. They are typically controlled remotely.

The Mirai botnet was able to gain control of internet of things (IoT) connected devices like your DVR, home printer as well as smart appliances by entering the default username and password that the devices shipped with. The threat actors deployed a DDoS (distributed denial of service) attack by sending large amounts of data at a website hosting company, causing many popular websites to be taken offline.

Adware

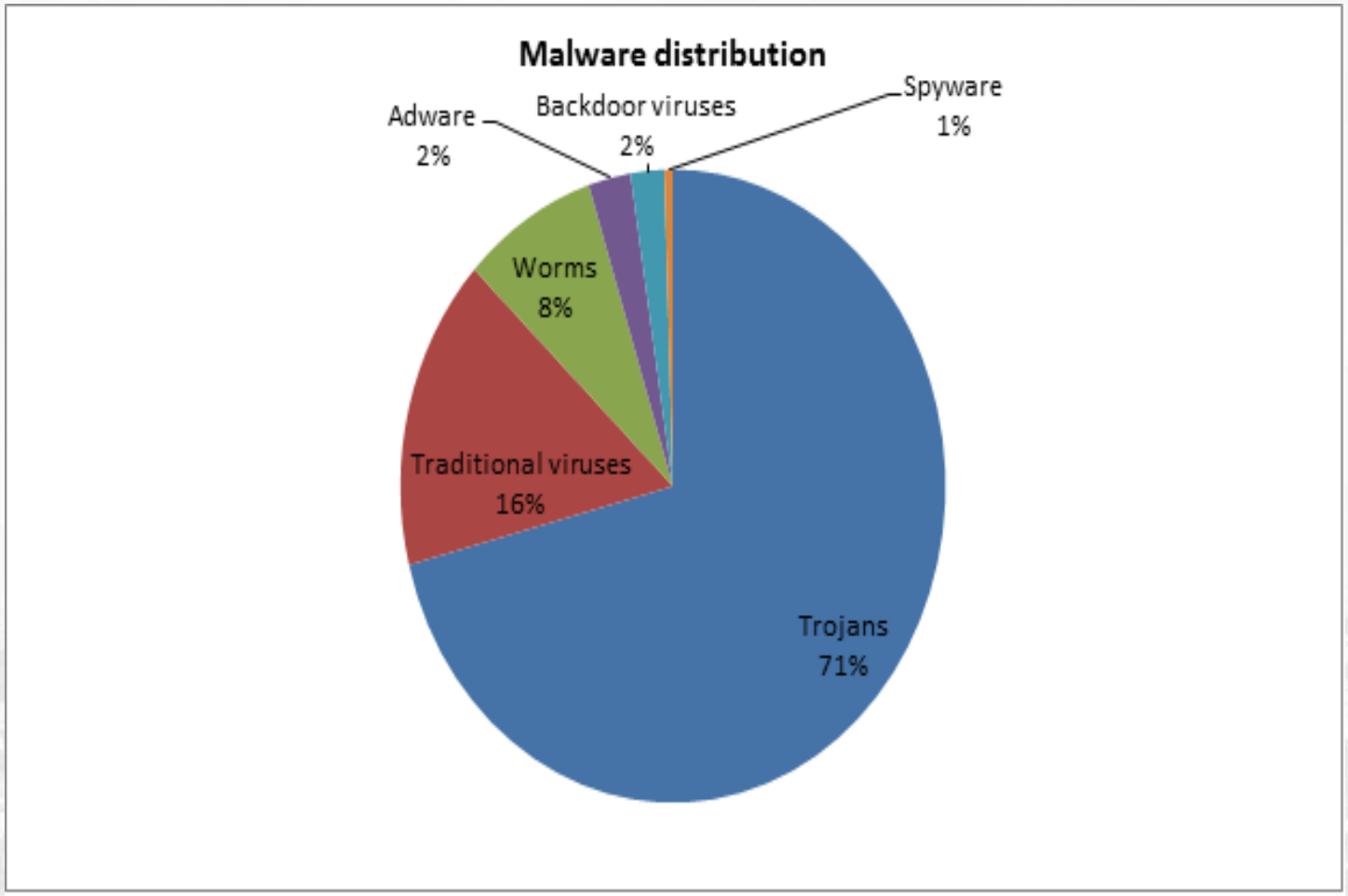
Adware and Spyware are both unwanted software. Adware is designed to serve advertisements on screens within a web browser. It's usually quietly installed in the background when downloading a program without your knowledge or permission. While harmless, adware can be annoying for the user.

Malware Threats and their Counter measures

Spyware and keyloggers – the financial threat

- Spyware and keyloggers are malware used in malicious attacks like identity theft, phishing and social engineering - threats designed to steal money from unknowing computer users, businesses and banks. Keylogging, or keyboard capturing, logs a user's keystrokes and sends data to the threat actor.
- Users are typically unaware that their actions are being monitored. While there are use cases for employers using keyloggers to track employee activity, they're mostly used to steal passwords or sensitive data. Keyloggers can be a physical wire discreetly connected to a peripheral like a keyboard, or installed by a Trojan.

Malware Threats and their Countermeasures



Malware Threats and their Countermeasures

How To Prevent Malware Attacks

- While it's not possible to be completely protected from cybercriminals, there are a number of measures companies can take to mitigate or prevent malware attacks including:
  - Developing Security Policies
  - Implementing Security Awareness Training
  - Using App-Based Multi-Factor Authentication
  - Installing Anti-Malware & Spam Filters
  - Changing Default Operating System Policies
  - Performing Routine Vulnerability Assessments

Malware Threats and their Countermeasures

- **Developing Security Policies**

  Security policies provide a road map to employees of what to do and when to do it, and who gets access to systems or information. Policies are also required for compliance, regulations, or laws. Examples of security policies that may help to prevent malware attacks include:

  - **Social Engineering Awareness Policy** – Defines guidelines to provide awareness around the threat of social engineering and defines procedures when dealing with social engineering threats.
  - **Server Malware Protection Policy** – The purpose of the Server Malware Protection Policy is to outline which server systems are required to have anti-virus and/or anti-spyware applications.
  - **Software Installation Policy** – The purpose of the Software Installation Policy is to outline the requirements around the installation of software on company computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within the Company's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.
  - **Removable Media Policy** – The purpose of the Removeable Media Policy is to minimize the risk of loss or exposure of sensitive information maintained by the company and to reduce the risk of acquiring malware infections on computers operated by the company.

Malware Threats and their Countermeasures

Implementing Security Awareness Training

- Security awareness training is an investment into the overall security of your organization. This training can save a substantial amount of money that has the potential of getting lost to cyber attacks. In addition, many compliance frameworks and audits (ISO 27001, SOC 2, CMMC, HIPAA, HITRUST, etc) require periodic security awareness training for employees. Awareness training involves developing a baseline, training users, setting up phishing campaigns, and reporting results.
- Baseline Testing – Provide baseline testing to assess the likelihood that a user falls for a phishing attack.
- Training Users – interactive modules, videos, games, posters, and newsletters designed to educate users on the latest social engineering attacks. This training is often automated with scheduled email reminders.
- Phishing Campaigns – Perform organization side and fully automated simulated phishing attacks.
- Reporting Results – Stats and graphs for both training and phishing activities to demonstrate the ROI.

The ideal way to perform security awareness is to include it in the new-hire orientation security training module and make it a mandatory requirement before granting access to critical systems.

The training should be completed at least on an annual basis and train employees not only on identifying attacks, but also to respond appropriately and report to the incident response team for proactive action. It is all about training employees to have a sense of what is considered unsafe behavior and know when to take action to protect themselves and the organization.

Malware Threats and their Countermeasures

Using App-Based Multi-Factor Authentication

- According to Microsoft, 99.9% of automated malware attacks can be prevented against windows systems just by using multi-factor authentication (MFA). Three 9s of prevention is an notable figure, however, the keyword here is “automated.” As with all things in security, MFA is simply a single layer of defense. Sophisticated threat actors deploy a number of methods outside of automated attacks to compromise a network.
- It’s also worth mentioning that SMS based MFA can easily be bypassed as the technology sends passcodes in plain text. This allows threat actors to capture the passcode, access your account, and then pass the code off to your phone without you noticing. Instead, it’s recommended that you use an app-based MFA or hardware MFA such as a YubiKey

Malware Threats and their Countermeasures

Installing Anti-Malware & Spam Filters

- Emails are the primary method for delivering malware and socially engineered attacks. While employees do have anti-virus and anti-malware software installed on their workstations, adding them to your mail servers is recommended as part of a defense in depth approach . Setting up a spam filter is a balancing act. On one hand, the network administrator wants to block all malicious traffic. On the other hand, if the filters are too aggressive then legitimate traffic gets blocked, and end-users start to complain. After 2-3 weeks of use, a baseline for the network can be established and further adjustments are made.

Malware Threats and their Countermeasures

- **Changing Default Operating System Policies**

While the default settings are good security precautions to take they can be greatly improved upon. In this example, Microsoft recommends changing the password history from 10 to 24 passwords and reducing the maximum password age from 90 days to 42 days. It's ultimately the responsibility of the network administrator to ensure that the domain, workstations, and devices are set up to adhere to security policies within the organization.

- **Perform Routine Vulnerability Assessments**

Performing routine network vulnerability scans help to identify known vulnerabilities, lack of security controls, and common misconfigurations. Scanners like Nessus are used to scan ports, analyze protocols, and map a network.

This provides network administrators with detailed information about which hosts on a network are running what services. Most scanners will display the information collected in a dashboard list.

THREATS	COUNTERMEASURES
Information gathering	Configure routers to restrict their responses to foot printing requests.
Spoofing	Filter incoming packets that appear to come from an internal IP address at your perimeter. Filter outgoing packets that appear to originate from an invalid local IP address
Sniffing	Use strong physical security and proper segmenting of the network. Encrypt communication fully, including authentication credentials.
Session hijacking	Use encrypted session negotiation. Use encrypted communication channels.
Denial of service	Use a network Intrusion Detection System (IDS) because these can automatically detect and respond to SYN attacks.
Viruses	Install Anti Virus
Foot printing	Use an IDS that can be configured to pick up foot printing patterns and reject suspicious traffic.
Password cracking	Use strong passwords for all account types.
Arbitrary code execution	Configure web server to reject URLs with "../" to prevent path traversal.
Buffer overflow;	Avoid using library files

Malware Threats and their Countermeasures

- Install a different anti-virus software on e-mail servers.
- User awareness training in identifying suspicious e-mail.
- Disable scripts when previewing or viewing e-mail.
- Block attachments at network borders.
- Prevent download of software from the Internet.
- Strict software installation policies.
- Remove removable drives to prevent unauthorized software entering a system.
- Anti-virus scanners on e-mail gateways are the only effective security measure against e-mail viruses.

Malware Threats and their Countermeasures

- **Ransomware: Facts, Threats, and Countermeasures**
- **Ransomware**
- Ransomware is a type of malware that has become a significant threat to U.S. businesses and individuals during the past two years. Most of the current ransomware variants encrypt files on the infected system/network (crypto ransomware), although a few variants are known to erase files or block access to the system using other methods (locker ransomware).
- **Infection Vectors**
- The majority of ransomware is propagated through user-initiated actions such as clicking on a malicious link in a spam e-mail or visiting a malicious or compromised website.
- **Additional Capabilities**
- In the past year, ransomware variants features have expanded to include data exfiltration, participation in distributed denial of service (DDoS) attacks, and anti-detection components.

Malware Threats and their Countermeasures

- **How to Mitigate the Risk of Ransomware Infections**
- These recommendations are not comprehensive but provide general best practices.
- **Securing Networks and Systems**
- Have an incident response plan that includes what to do during a ransomware event.
- Backups are critical. Use a backup system that allows multiple iterations of the backups to be saved, in case a copy of the backups includes encrypted or infected files. Routinely test backups for data integrity and to ensure it is operational.
- Use antivirus and anti-spam solutions. Enable regular system and network scans with antivirus programs enabled to automatically update signatures. Implement an anti-spam solution to stop phishing emails from reaching the network. Consider adding a warning banner to all emails from external sources that reminds users of the dangers of clicking on links and opening attachments.

Malware Threats and their Countermeasures

- **Disable macros scripts.** Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications.
- **Keep all systems patched,** including all hardware, including mobile devices, operating systems, software, and applications, including cloud locations and content management systems (CMS), patched and up-to-date. Use a centralized patch management system if possible. Implement application white-listing and software restriction policies (SRP) to prevent the execution of programs in common ransomware locations, such as temporary folders.
- **Restrict Internet access.** Use a proxy server for Internet access and consider ad-blocking software. Restrict access to common ransomware entry points, such as personal email accounts and social networking websites.

Malware Threats and their Countermeasures

- **Apply the principles of least privilege and network segmentation.** Categorize and separate data based on organizational value and where possible, implement virtual environments and the physical and logical separation of networks and data. Apply the principle of least privilege.
- **Vet and monitor third parties** that have remote access to the organization's network and/or your connections to third parties, to ensure they are diligent with cybersecurity best practices.
- **Participate in cybersecurity information sharing** programs and organizations, such as MS-ISAC and InfraGard.

Malware Threats and their Countermeasures

- **Securing the End User**
- **Provide social engineering and phishing training to employees.** Urge them not to open suspicious emails, not to click on links or open attachments contained in such emails, and to be cautious before visiting unknown websites.
- **Remind users to close their browser** when not in use.
- **Have a reporting plan** that ensures staff knows where and how to report suspicious activity.

Malware Threats and their Countermeasures

Responding to a Compromise/Attack

- **Immediately** disconnect the infected system from the network to prevent infection propagation.
- **Determine the affected data** as some sensitive data, such as electronic protected health information (ePHI) may require additional reporting and/or mitigation measures.
- **Determine if a decryptor is available.** Online resources such as No More Ransom! can help.
- **Restore** files from regularly maintained backups.
- **Report the infection.** It is highly recommended that SLTT government agencies report ransomware incidents to MS-ISAC. Other sectors and home users may report to infections to local Federal Bureau of Investigation (FBI) field offices or to the Internet Crime Complaint Center (IC3).

Monitoring and Capturing Data Packets using Sniffing

- An attacker or an ethical hacker follows the same five-step hacking process to breach the network or system.
- The ethical hacking process begins with looking for various ways to hack into the system, exploiting vulnerabilities, maintaining steady access to the system, and lastly, clearing one's tracks.
- In addition to providing the raw scan results, most vulnerability scanning services include an assessment report consisting of a remediation plan to resolve at risk systems. Organizations may also wish to implement a patch management program. The main purpose of patch management is to continuously identify, prioritize, remediate, and report on security vulnerabilities in systems.

Monitoring and Capturing Data Packets using Sniffing

There are two types:

- Active Sniffing:

Sniffing in the switch is active sniffing. A switch is a point to point network device. The switch regulates the flow of data between its ports by actively monitoring the MAC address on each port, which helps it pass data only to its intended target. In order to capture the traffic between target sniffers has to actively inject traffic into the LAN to enable sniffing of the traffic.

- Passive Sniffing:

This is the process of sniffing through the hub. Any traffic that is passing through the non-switched or unbridged network segment can be seen by all machines on that segment. Sniffers operate at the data link layer of the network. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called passive since sniffers placed by the attackers passively wait for the data to be sent and capture them.

Q. HUB, SWTCH, ROUTER, GATEWAY

OSI Layer wise information, attacks on each layer

Monitoring and Capturing Data Packets using Sniffing

- It’s no question that bottlenecks, downtime, and other common network performance issues can vastly affect the end-user experience and put productivity on hold, ultimately cutting into your company’s bottom line. Getting to the root cause of performance problems is a top priority for nearly every sysadmin. This is where packet sniffers, also known as network sniffers or network analyzers, come into play. With the right packet sniffer, you’ll be well-equipped to capture and analyze network traffic, helping you identify the cause of network performance problems and prevent them from recurring.

Monitoring and Capturing Data Packets using Sniffing

10 Best Packet Sniffers

1. SolarWinds Network Performance Monitor
2. Paessler PRTG Network Monitor
3. ManageEngine NetFlow Analyzer
4. Savvius Omnipeek
5. tcpdump
6. WinDump
7. Wireshark
8. Telerik Fiddler
9. NETRESEC NetworkMiner
10. Colasoft Capsa

Monitoring and Capturing Data Packets using Sniffing

- What Are Packet Sniffers?

A packet sniffer is either a software or hardware tool to intercept, log, and analyze network traffic and data. These tools aid in the identification, classification, and troubleshooting of network traffic by application type, source, and destination. There are a variety of tools on the market, most of which rely on application program interfaces (APIs) known as pcap (for Unix- like systems) or libcap (for Windows systems) to capture network traffic. The best packet sniffers then analyze this data, enabling you to both pinpoint the source of an issue and prevent it from happening in the future.

The SolarWinds Network Performance Monitor, this comprehensive software offers in-depth packet sniffing capabilities as well as a host of other cutting-edge resources at a reasonable price point.

Monitoring and Capturing Data Packets using Sniffing

Every email you send, webpage you open, and file you share is distributed across the internet as thousands of small, manageable chunks known as data packets. These packets are transmitted through a protocol stack known as the Transmission Control Protocol/Internet Protocol (TCP/IP).

The TCP/IP is broken into four layers: the application protocol layer, transmission control protocol (TCP) layer, internet protocol (IP) layer, and hardware layer.

Each packet moves through your network's application layer to the TCP layer, where it's assigned a port number. Next, the packet migrates to the IP layer and receives its destination IP address. Once a packet has a port number and IP address, it can be sent over the internet.

Monitoring and Capturing Data Packets using Sniffing

- Sending is carried out through the hardware layer, which converts packet data into network signals. When a packet arrives at its destination, the data used to route the packet (port number, IP address, etc.) is removed, and the packet moves on through the new network's protocol stack. Once it reaches the top, it's reassembled into its original form.

- **How Do Packet Sniffers Work?**

Packet sniffers work by intercepting traffic data as it passes over the wired or wireless network and copying it to a file. This is known as packet capture. While computers are generally designed to ignore the hubbub of traffic activity from other computers, packet sniffers reverse this. When you install packet sniffing software, the network interface card (NIC)—the interface between your computer and the network—must be set to unrestrained mode.

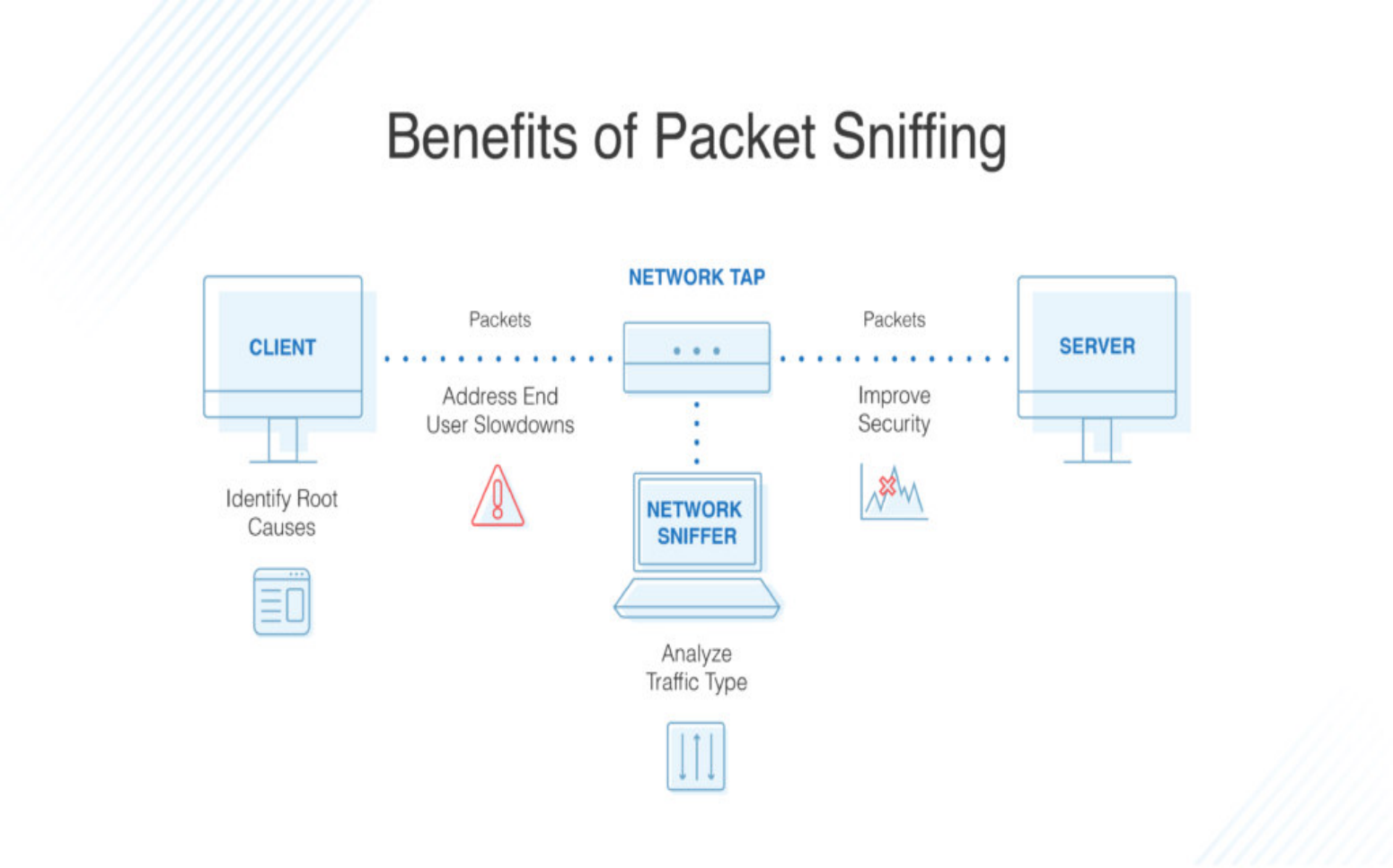
Monitoring and Capturing Data Packets using Sniffing

This commands the computer to capture and process, via the packet sniffer, everything that enters the network. What can be captured depends on the network type. For wired networks, the configuration of network switches, which are responsible for centralizing communications from multiple connected devices, determines whether the network sniffer can see traffic on the entire network or only a portion of it. For wireless networks, packet capture tools can usually only capture one channel at a time unless the host computer has multiple wireless interfaces.

The Benefits of Packet Sniffing

So, what's the point of packet analyzers, and why should you want to IP sniff? A packet sniffer can help you target new resources when expanding your network capacity, manage your bandwidth, increase efficiencies, ensure delivery of business services, enhance security, and improve end-user experience.

Monitoring and Capturing Data Packets using Sniffing



Monitoring and Capturing Data Packets using Sniffing

- **Identify the Root Cause.** For companies large and small, daily tasks can instantly be derailed by performance issues related to the network, an application, or both. To get their company back up and running, sysadmins must be able to quickly determine the root cause. Because packet sniffers view and gather information for all the traffic across the network, they can evaluate critical network pathways to help admins determine whether the application or the network is the cause of poor user experience.
- **Dig Deep into Slowdowns.** When users report slowness, admins can use PCAP analysis to measure the network response time—also known as network path latency—and determine the amount of time required for a packet to travel across a network path from sender to receiver. This enables admins to quickly determine the cause of slowdowns and identify affected applications, so they can take action.

Monitoring and Capturing Data Packets using Sniffing

- **Analyze Traffic by Type.** When evaluating network and application performance issues, having a firm grasp of the traffic on your network is paramount. With the right IP sniffer and packet analyzer, traffic is categorized into types based on destination server IP addresses, ports used, and measurement of the total and relative volumes of traffic for each type. This empowers you to identify excessive levels of non-business traffic such as social media and external web surfing) that may need to be filtered or otherwise eliminated. You can also identify traffic flowing over a network link as well as traffic to specific servers or applications for capacity management purposes.

Monitoring and Capturing Data Packets using Sniffing

- **Improve Bandwidth.** When users complain “the network is slow,” or “the internet is down,” productivity grinds to a halt, reducing ROI and jeopardizing business growth. To get back on track, you need to understand how your network bandwidth is being used and by whom. A Wi-Fi packet sniffer can retrieve performance metrics for autonomous access points, wireless controllers, and clients. Many also offer fault, performance, and network availability monitoring, cross-stack network data correlation, hop-by-hop network path analysis, and much more, to help you detect potential issues and minimize network downtime.

Monitoring and Capturing Data Packets using Sniffing

- **Improve Security.** A high volume of outbound traffic could indicate a hacker is using your applications, either to communicate externally or to transfer a large amount of data. A packet sniffer can highlight unusual spikes in traffic so you can dig deeper to determine whether a cybercriminal is at work.
- **Packet Sniffing Best Practices**

With your packet sniffer in hand and your NIC set to promiscuous mode, you'll be off and running with packet capture. But while many of the benefits of packet sniffing will fall into place, there are certain best practices to follow if you want to reap the full results and protect your company from security violations. To get the most out of your packet sniffer, ensure you:

Monitoring and Capturing Data Packets using Sniffing

- **Know the Basics**. To analyze network traffic, you must understand how networking works. Yes, some packet sniffers will break data down and offer dashboards full of insight, but knowing about the types of network traffic on a healthy network, such as the Address Resolution Protocol (ARP), for communication, and the Dynamic Host Configuration Protocol (DHCP), for network management, is key. You need to know what you want the packet sniffer to collect and have at least a general idea of what's normal and what's not. With a base-level understanding of network traffic, you can help ensure you're evaluating the right mass of packets. Equip yourself with the foundational principles and you'll be set for success.

Monitoring and Capturing Data Packets using Sniffing

- **Copy Conservatively.** Each packet contains a header identifying its source and destination as well as a payload—the term used to describe the contents of the packet. A basic packet sniffer will copy the payload and headers of all packets traveling on the network. If the packet payload isn't encrypted, members of your IT team can access sensitive business data, opening the doors to a plethora of potential security risks. To help you protect your company and avoid putting sensitive information in jeopardy, many packet sniffers can be set to copy only the header information. Most of the time, this is the only information you'll need to perform network performance analysis.

Monitoring and Capturing Data Packets using Sniffing

- **Monitor Storage Space.** Even if you're only capturing packet headers, storing every packet can consume a large amount of your disk space. If you want to glean an understanding of network usage over a set period, say a few days, it's best to copy every tenth or twentieth packet rather than copying every single one. This is known as packet sampling, and it's a practice widely used to characterize network traffic. Packet sampling works by leveraging randomness in the sampling process to prevent synchronization with any periodic patterns in the traffic. While this method of network characterization is not 100% accurate, it's a solution with quantifiable accuracy.
- **Decode the Data**. Some of the network data gathered by a packet sniffer will be encoded. To glean the full benefits of the data capture process, choose a packet sniffer able to decode this administrative information as well as extract other valuable insights, such as the varying port numbers between which the packets travel. This information will help you generate a more robust analysis of your network traffic.

Monitoring and Capturing Data Packets using Sniffing

- To protect your business from unlawful packet sniffing, it's critical to always use HTTPS (SSL encrypted sessions) when entering and sending form data. Never rely on HTTP; it's not secure and it puts your personal, sensitive information, like login credentials, in jeopardy. If you or someone in your business is using a website with HTTP, see if it will accept an HTTPS connection by typing "https://" into the browser bar before the site address. Oftentimes, a website has an SSL certificate in place but doesn't require visitors to use it. Alternatively, you can opt to skip this extra step and implement the Electronic Frontier Foundation browser add-on, known as HTTPS Everywhere, for Chrome, Firefox, and Opera.
- This add-on is designed to automatically connect every website you visit using HTTPS.

Monitoring and Capturing Data Packets using Sniffing

- Compared to other security measures, VPNs, virtual private networks, offer the most protection because they encrypt your traffic. You can also protect the metadata of your packets, such as destination addresses, by ensuring your DNS queries go through the VPN. Nevertheless, while VPNs are a security must-have, you should continue to use HTTPS even when a VPN is in place. Many sysadmins also choose to invest in intrusion detection systems, which monitor network traffic for unusual spikes in traffic—a telltale sign of an intruder. Another option is to leverage tools like AntiSniff, which detect when a network interface has been put into promiscuous mode, raising a red flag if this occurred without your knowledge.

Monitoring and Capturing Data Packets using Sniffing

How do you sniff data packets?

Wireshark is a packet sniffing tool, a network packet analyzer. Its basic operation is to take an internet connection—or any network connection really—and register the packets traveling back and forth across it. It gives you everything: packet origin and destination, contents, protocols, messages.

What is packet sniffing and how it is done? Packet sniffing is a technique whereby packet data flowing across the network is detected and observed. Network administrators use packet sniffing tools to monitor and validate network traffic, while hackers my use similar tools for nefarious purposes.

Monitoring and Capturing Data Packets using Sniffing

Which is the most commonly used tool for capturing and analyzing packets?

Wireshark Tcpdump :- Two of the most useful and quick-to-use packet capture tools are tcpdump and Wireshark. dump is a command line tool that allows the capture and display of packets on the network. Wireshark provides a graphical interface for capturing and analyzing packet data.

What are the advantages of packet sniffing?

The main advantage of such packet sniffers is that they can see; the network traffic not only from the computer, its working on but from all computers in the same network segment. The main disadvantage of such packet sniffer is that it cannot decrypt the SSL traffic without retrieving the server certificate.

Gather Confidential Information – Social Engineering

- Social engineering is the art of manipulating users of a computing system into revealing confidential information that can be used to gain unauthorized access to a computer system. The term can also include activities such as exploiting human kindness, greed, and curiosity to gain access to restricted access buildings or getting the users to installing backdoor software. Knowing the tricks used by hackers to trick users into releasing vital login information among others is fundamental in protecting computer systems.

Gather Confidential Information – Social Engineering

- **How social engineering Works?**
- **Gather Information**: This is the first stage, the learns as much as he can about the intended victim. The information is gathered from company websites, other publications and sometimes by talking to the users of the target system.
- **Plan Attack**: The attackers outline how he/she intends to execute the attack
- **Acquire Tools**: These include computer programs that an attacker will use when launching the attack.
- **Attack**: Exploit the weaknesses in the target system.
- **Use acquired knowledge**: Information gathered during the social engineering tactics such as pet names, birthdates of the organization founders, etc. is used in attacks such as password guessing.

Gather Confidential Information – Social Engineering

Common Social Engineering Techniques:

- Social engineering techniques can take many forms. The following is the list of the commonly used techniques.
- **Familiarity Exploit:** Users are less suspicious of people they are familiar with. An attacker can familiarize him/herself with the users of the target system prior to the social engineering attack. The attacker may interact with users during meals, when users are smoking he may join, on social events, etc. This makes the attacker familiar to the users. Let's suppose that the user works in a building that requires an **access code or card** to gain access; the attacker may follow the users as they enter such places. The users are most like to hold the door open for the attacker to go in as they are familiar with them. The attacker can also ask for **answers to questions** such as where you met your spouse, the name of your high school math teacher, etc. The users are most likely to reveal answers as they trust the familiar face. This information could be used to hack email accounts and other accounts that ask similar questions if one forgets their password.

Gather Confidential Information – Social Engineering

- **Intimidating Circumstances:** People tend to avoid people who intimidate others around them. Using this technique, the attacker may pretend to have a heated argument on the phone or with an accomplice in the scheme. The attacker may then ask users for information which would be used to compromise the security of the users' system. The users are most likely give the **correct answers just to avoid having a confrontation with the attacker.** This technique can also be used to avoid been checked at a security check point.
- **Phishing:** This technique uses trickery and deceit to obtain private data from users. The social engineer may try to impersonate a genuine website such as Yahoo and then ask the unsuspecting user to confirm their account name and password. This technique could also be used to get credit card information or any other valuable personal data.

Gather Confidential Information – Social Engineering

- **Tailgating:** This technique involves following users behind as they enter restricted areas. As a human courtesy, the user is most likely to let the social engineer inside the restricted area.
- **Exploiting human curiosity:** Using this technique, the social engineer may deliberately drop a virus infected flash disk in an area where the users can easily pick it up. The user will most likely plug the flash disk into the computer. The flash disk may auto run the virus, or the user may be tempted to open a file with a name such as Employees Revaluation Report 2013.docx which may actually be an infected file.
- **Exploiting human greed**: Using this technique, the social engineer may lure the user with promises of making a lot of money online by filling in a form and confirm their details using credit card details, etc.

Gather Confidential Information – Social Engineering

Social Engineering Counter Measures

Most techniques employed by social engineers involve manipulating human biases.

- **To counter the familiarity exploit**, the users must be trained to not substitute familiarity with security measures. Even the people that they are familiar with must prove that they have the authorization to access certain areas and information.
- **To counter intimidating circumstances attacks,** users must be trained to identify social engineering techniques that fish for sensitive information and politely say no.
- **To counter phishing techniques,** most sites such as Yahoo use secure connections to encrypt data and prove that they are who they claim to be. Checking the URL may help you spot fake sites. Avoid responding to emails that request you to provide personal information.
- **To counter tailgating attacks,** users must be trained not to let others use their security clearance to gain access to restricted areas. Each user must use their own access clearance.
- **To counter human curiosity,** it's better to submit picked up flash disks to system administrators who should scan them for viruses or other infection preferably on an isolated machine.

Gather Confidential Information – Social Engineering

- To counter techniques that exploit human greed, employees must be trained on the dangers of falling for such scams.
- Social engineering is the art of exploiting the human elements to gain access to un-authorized resources. Social engineers use a number of techniques to fool the users into revealing sensitive information. Organizations must have security policies that have social engineering countermeasures.

10 Common Social Engineering Techniques

Cybercriminals use several social engineering techniques to gather sensitive data or steal system access credentials. This information will often allow them to deploy well-targeted ransomware attacks or commit data theft. Here is an overview of 11 common social engineering techniques used by cybercriminals.

Gather Confidential Information – Social Engineering

1. Phishing:

- The criminal attacker may use a simple email, instant messaging, social media, or even SMS to retrieve sensitive information from the unsuspecting victim during a phishing attack. Such an attack is used to lure the victim into clicking a malicious website link.
- The message contained in the phishing campaign captures the victim's attention and calls them to action by piquing their curiosity, pulling an emotional trigger, or asking for help. The message often contains logos, text styles, or images that mirror a legitimate organisation, making it seem like a legitimate message from a colleague or company.

Gather Confidential Information – Social Engineering

- Of course, phishing messages carry a sense of urgency that leads the victim to believe they should respond to avoid negative consequences. Hackers can automate their processes and send thousands of generic emails at a time.
- When the phishing message directs victims to a counterfeit domain, that website looks legitimate. There will be minor, easily overlooked details that identify it as fake, such as using similar lettering in the URL. An example would be swapping “rn” for the letter “m.”
- The email often contains multiple legitimate links mixed in with the malicious one. Such techniques enable the malicious links and code to get past email security filters.
- One of the most common phishing tricks is exploiting the “password reset” function available on most websites. The target will receive an email urgently requesting them to click the link to reset their password as their account may have been compromised.

Gather Confidential Information – Social Engineering

2. Spear Phishing

- Spear phishing is a more sophisticated form of social engineering where messages are more targeted, well-written, and sent to a specific person or group. Criminals tailor and personalise emails to intended targets. The subject lines are distinct and will contain topics of interest to the recipients.
- It's no surprise that 91% of successful cyberattacks begin with a spear-phishing email. The messages are so well-tailored that email security filters, as well as the recipients, can miss them. The message appears legitimate and non-threatening.
- The creator of the spear-phishing email has taken the time to gather specific details about the victim. Such information is easy enough to obtain from business directories or websites like LinkedIn. From there, any social media site can yield additional personal information that the criminal can exploit to fine-tune a spear-phishing email.

Gather Confidential Information – Social Engineering

3. Whaling

- Whaling is another form of social engineering that targets specific individuals who may have elevated access to secure systems or sensitive company information and often target senior executives and network administrators.
- Because the target is highly specific, the attacker conducts meticulous research to craft a message that will prompt specific targets to respond and complete the desired action. Whaling emails are often presented as an internal critical business email sent by an employee, investor, colleague, or manager. The request requires urgent action or intervention from the victim.

Gather Confidential Information – Social Engineering

4.Vishing

- While email remains the preferred delivery method for phishing attacks, there are others. Vishing attacks, also called voice phishing, are examples because they deploy as phone calls.
- In a vishing attack, the victim receives a phone call that appears to be coming from their bank, merchant account, or some other standard service. The phone call begins as an automated call that proceeds to route the individuals to the criminals, who pose as customer service agents. The criminals use mobile apps or other technology to spoof or hide their phone numbers.
- Vishing is simply another form of social engineering that fools the target into providing personal, financial, or business information. The attacker may even claim to be an executive at your own company who works off-site. Whatever the fake reason for the call is, they will need to “verify your information” first, which is the information they intend to exploit.

Gather Confidential Information – Social Engineering

5. Smishing

- Smishing is short for SMS phishing, and it is delivered to targeted victims via mobile phone as a text message. These malicious text messages trick the user into clicking a malicious link and handing over sensitive information. The message is often disguised as something familiar like a missed delivery or some other urgent need to contact “customer support.”
- Sometimes, smishing attacks prompt the recipient to download a malicious app unknowingly. The recipient clicks a link, which sets off an automatic download for an app that deploys ransomware or other functionality that enables the hacker to control the phone remotely. Other times, the link takes the victim to a cloud-based, malicious form. The victim enters personal data, which the hacker then steals.

Gather Confidential Information – Social Engineering

6. Pretexting

- In a pretexting attack, the attacker creates a detailed, fake identity, which they use to manipulate the victim into providing private information. This more complex form of phishing or smishing is where the attacker spends more time creating the malicious alias, thus, making it all the more believable.
- For instance, the attacker may pretend to be a technician from an external IT service provider who needs the user's account details and login credentials to solve a network issue. An attacker may also pretend to be a representative from the victim's bank, stating a specific problem with the victim's account. They will then ask for the login credentials for the victim's online banking account or confirmation of the bank account number.

Gather Confidential Information – Social Engineering

7. Baiting

- Baiting is yet another social engineering technique where an attacker offers a false promise to lure a victim into a trap. The trap, of course, results in financial or personal information theft. Alternately, the goal may be to deliver malware to the user's system. The trap often arrives as a malicious attachment that has an enticing name.
- Most often, baiting tactics employ physical media to distribute malware. For instance, an attacker leaves the bait, which is a malware-infected flash drive, in a conspicuous area where a potential victim will see it. Out of curiosity, the victim inserts the flash drive into a work or BYOD computer, and malware automatically and discreetly installs on the system. An individual may receive an infected flash drive as a gift or as a reward for completing a survey, etc.
- Baiting also exists online in the form of attractive ads that lead users to malicious websites or encourage them to download malware. The ad may offer free movie or music downloads, provided they log on to a particular website.

Gather Confidential Information – Social Engineering

8. Quid Pro Quo

- A quid pro quo attack is similar to a baiting attack; instead of promising the victim something valuable, the attacker promises to perform an action that will benefit the victim. Before that happens, of course, the attacker requires a specific action from the victim first.

Gather Confidential Information – Social Engineering

9. Impersonation

- Impersonation is another social engineering tactic that cybercriminals use to trick their way into a network by using identity theft. The difference with impersonation is that it occurs in-person or over the phone rather than email or text message The cybercriminal impersonates someone the victim is likely to trust and, more specifically, obey. They are convincing enough to fool the victim into permitting access to their office, personal information, or information systems.
- This social engineering tactic plays on the human tendency to believe that a person is whom they say they are. Thus, they follow instructions when a perceived authority figure asks. It also involves constant manipulation to get the victim to release information without realising that they are participating in a security breach.

Gather Confidential Information – Social Engineering

10. Tailgating

- For physical access, an attacker will employ tailgating to gain entry to a restricted area. For the attack to be successful, that access point must be unattended or controlled by electronic access. This way, the attacker can walk in behind someone who has legitimate access. If your organisation has more than one access door or a secondary exit, say, to the parking lot, tailgating is a constant threat.
- It's common for an impersonator to be dressed like a delivery driver waiting outside the building. When an employee opens the door, the attacker either slips in behind them or asks them to hold the door. Most people naturally oblige, thereby enabling the attacker to gain access to the facility.
- Tailgating won't work in corporate settings where security is more restricted. Anyone entering the building is required to swipe a card. However, the attacker will often strike up a casual conversation with employees in mid-sized and smaller companies to establish familiarity. Eventually, they will tailgate their way into the building.

Gather Confidential Information – Social Engineering

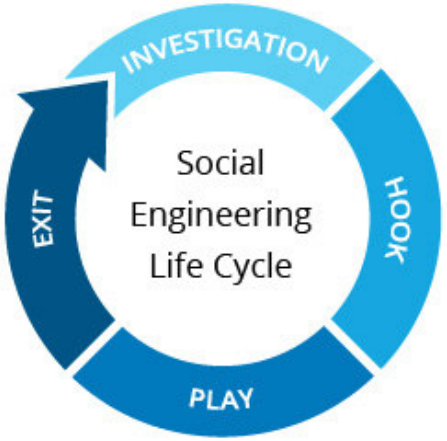
Conclusion:

- Any of these social engineering techniques exploit fundamental human decision-making and cognitive biases. We are all human and will make mistakes in judgment now and again. Considering how many decisions we need to make daily, it's only a matter of time before our guard slips.
- Cybercriminals who engage in social engineering campaigns understand psychological weak points and waste no time exploiting them. Unfortunately, such attacks can significantly impact your organisation, especially if the result is significant data theft or a ransomware attack.
- Recognising these common social engineering techniques is a first step in fortifying your security systems and preventing data breaches. Be sure to train your employees on how to handle potential threats to ensure you are employing the best defence possible.

Gather Confidential Information – Social Engineering

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).



Deceiving the victim(s) to gain a foothold:

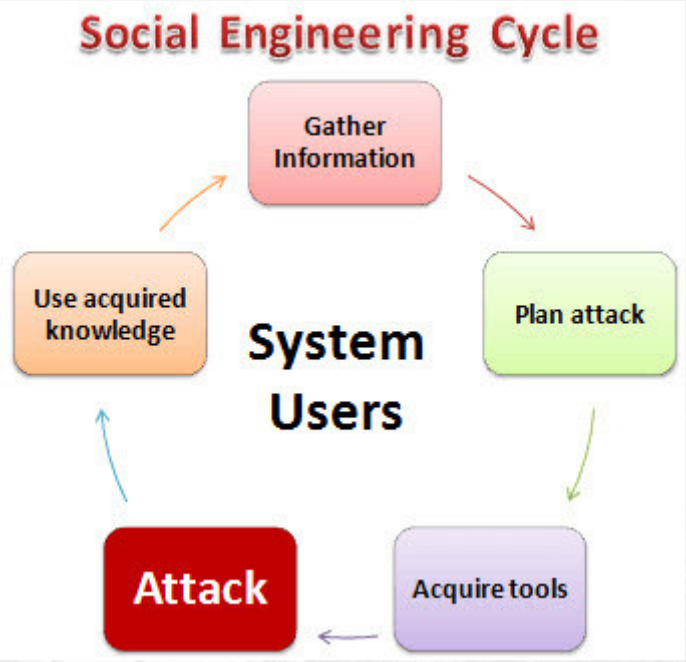
- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction,
ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.



Gather Confidential Information – Social Engineering

- **Which social engineering method is used to see a persons private confidential information?**
- **Pretexting**
  In a pretexting attack, the attacker creates a detailed, fake identity, which they use to manipulate the victim into providing private information.
- **How do social engineers gain access to information in person?**
- So, **when employees call for help the individual asks them for their passwords and IDs** thereby gaining the ability to access the company's private information. Another example of social engineering would be that the hacker contacts the target on a social networking site and starts a conversation with the target.

Gather Confidential Information – Social Engineering

- **What methods does a social engineering hacker use to gain information?**
- Social engineering is the art of manipulating, influencing, or deceiving you in order to gain control over your computer system. The hacker might use **the phone, email, snail mail or direct contact** to gain illegal access. Phishing, spear phishing, and CEO Fraud are all examples.
- **What is the most common form of social engineering used by hackers?**
- **phishing**
- The most common form of social engineering attack is **phishing**. Phishing attacks exploit human error to harvest credentials or spread malware, usually via infected email attachments or links to malicious websites.

Restricting the System Access – DoS Attack

- A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.
- Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

Restricting the System Access – DoS Attack

There are two general methods of DoS attacks: **flooding services or crashing services**.

- Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:
- **Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle.
- **ICMP flood** – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or **ping of death.**
- **SYN flood** – A SYN Flood attack exploits the Transmission Control Protocol (TCP) handshake – a method used for the TCP network to create a connection with a local host/client/server. Unfortunately, the handshake is left incomplete, leaving the connected host in an occupied status and unavailable to take further requests. Attackers will double down on the requests, saturating all open ports and preventing anyone from connecting to the network.
- **Teardrop** - In a teardrop attack, IP data packet fragments are sent to the target network. The network then reassembles the fragments into the original packet. The process of reassembling these fragments exhausts the system and it ends up crashing. It crashes because the fragments are designed to confuse the system so it can never be put back together.

Restricting the System Access – DoS Attack

Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system, so that it can't be accessed or used.

- **Volume-based attacks:** These use large amounts of fake traffic to overwhelm an online resource, like a server or website. The volume of the attack is measured in bits per second.
- **Protocol or network-layer attacks:** These send large numbers of packets to network infrastructure and infrastructure management tools. Their size is measured in packets per second (PPS) and include Smurf DDoS attacks (network-layer attacks designed to flood a targeted server with error messages) and SYN floods (which tie up networks with half-opened connection requests).
- **Application-layer attacks:** These are similar to volume-based attacks but are conducted by flooding applications with malicious requests. Their size is measured in requests per second (RPS).

- An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once.

Restricting the System Access – DoS Attack

- The distribution of hosts that defines a DDoS provide the attacker multiple advantages:

  He can leverage the greater volume of machine to execute a seriously disruptive attack

  The location of the attack is difficult to detect due to the random distribution of attacking systems (often worldwide)

  It is more difficult to shut down multiple machines than one

  The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems

  Modern security technologies have developed mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS, it is still regarded as an elevated threat and is of higher concern to organizations that fear being targeted by such an attack.

  A denial-of-service attack can disrupt an organization's website and network, resulting in a loss of business and other costs without the right prevention tactics.

Restricting the System Access – DoS Attack

Symptoms by ecommerce site-

- Inability of users (you) to access the website
- Slow network performance
- Failing to load site pages
- Loss of connectivity across devices on the same network

Restricting the System Access – DoS Attack

- **DoS Attack Prevention and Protection**
- As the Cybersecurity and Infrastructure Security Agency (CISA), run by the U.S. Department of Homeland Security, notes, “the symptoms of a DoS attack can resemble non-malicious availability issues, such as technical problems with a particular network or a system administrator performing maintenance.” However, CISA adds, “unusually slow network performance and unavailability of a particular website can be strong signs of a DoS attack.”

Restricting the System Access – DoS Attack

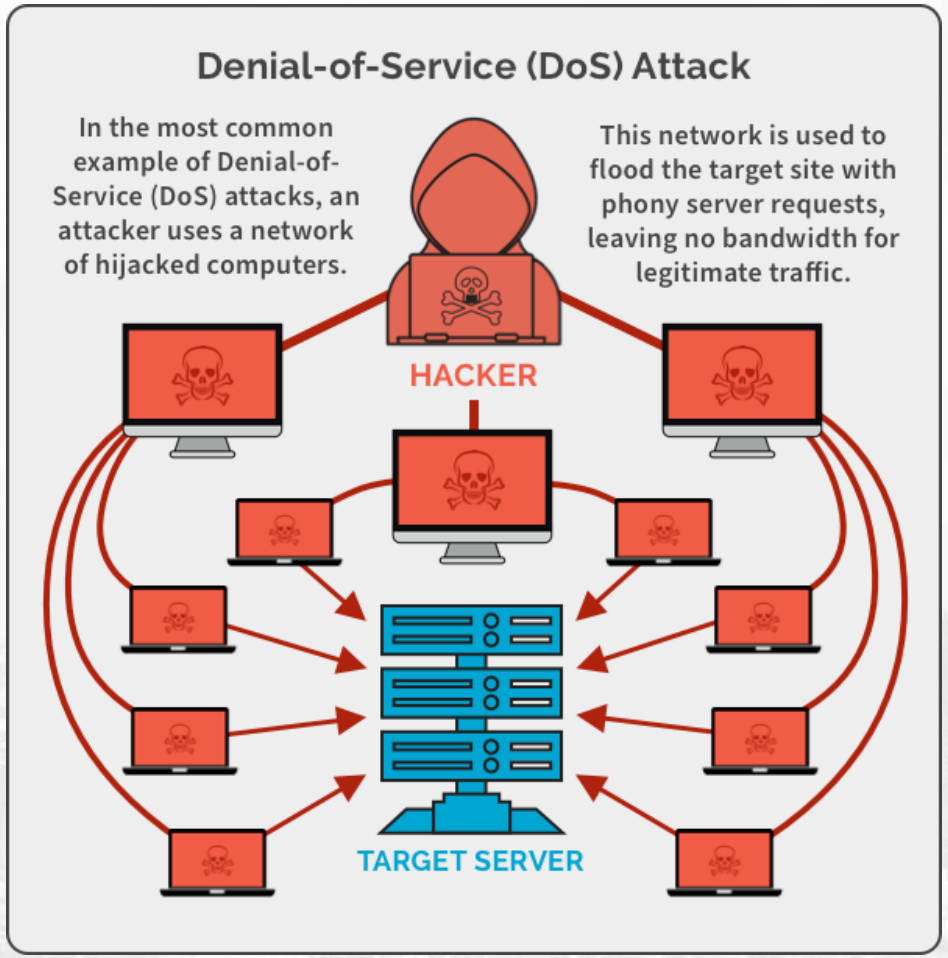
Organizations can take the following actions toward denial-of-service attack protection and prevention:

- **Monitor and analyze network traffic:** Network traffic can be supervised via a firewall or intrusion detection system. Administrators can set up rules that create alerts for unusual traffic, identify traffic sources or drop network packets that meet a certain criteria.
- **Strengthen their security posture:** This includes fortifying all internet-facing devices to prevent compromise, installing and maintaining antivirus software, establishing firewalls configured to protect against DoS attacks and following robust security practices to monitor and manage unwanted traffic.
- **Monitor traffic:** Organizations can enrol in a service that detects or redirects the abnormal traffic flows typically associated with a DoS attack, while allowing normal traffic to proceed on the network.
- **Establish a DoS attack response plan:** The key is to create and also practice a disaster recovery plan for DoS attack that covers communication, mitigation and recovery.

The Difference Between DoS and DDoS

- DoS and DDoS are two different names for the same attack. DDoS has been incredibly effective as a threat and is considered one of the top cybersecurity trends from 2020.

Restricting the System Access – DoS Attack



Restricting the System Access – DoS Attack

The Real Motivation Behind DoS Attacks

- A deer hunter uses a decoy to pull the deer in close. With the deer focused on the decoy, hunters get better opportunities for a good shot. Similarly, a DoS attack is the decoy, the hacker is the hunter, and guess who the deer is?
- That's right. You!
- Businesses are often fearful that DoS attacks will impact sales, but they should be just as concerned, if not more concerned, about data theft. Peel through the surface and you will find that DoS and DDoS attacks are used to draw attention away in order for hackers to launch secondary attacks elsewhere on your network.
- A staggering 92 percent of companies that have experienced just one DDoS attack also reported some form of data theft.

Restricting the System Access – DoS Attack

Protect Your Business Against DoS Attacks

There are two approaches you can take to protect your business against DoS attacks:

- **Pre-emptive Measure**
- Identify DoS attacks before they cause harm by using network monitoring. Also, test run DoS attacks to see how you will fare against an actual attack so you can refine your overall strategy.
- **Post-Attack Response**
- Create a Disaster Recovery Plan to ensure proper communication, mitigation and recovery of data. A good plan can be the difference between an inconvenient attack or a devastating one.
- Spanning protects your organization's critical data from loss caused by a DoS attack and other cyberthreats. It allows administrators to quickly find and restore data to its original state in just a few clicks. This ensures business continuity even during an ongoing DoS/DDoS attack.

Restricting the System Access – DoS Attack

- **What is a DDoS attack and how can it be prevented?**
- A distributed denial-of-service (DDoS) is a type of DoS attack where the traffic used to overwhelm the target is coming from many distributed sources. This method means the attack **can't be stopped just by blocking the source of traffic**. Botnets are often employed for DDoS attacks.
- **What is DoS and DDoS attack?**
- A DoS attack **tries to make a web resource unavailable to its users by flooding** the target URL with more requests than the server can handle. A Distributed Denial of Service (DDoS) attack is a DoS attack that comes from more than one source at the same time.

Restricting the System Access – DoS Attack

- **Why it is difficult to prevent a DDoS attack?**
- These attacks are also extremely difficult to defend against **because of their distributed nature**. It is difficult to differentiate legitimate Web traffic from requests that are part of the DDoS attack. There are some countermeasures you can take to help prevent a successful DDoS attack.

Points of Difference	DoS	DDoS
Source	A single computer and IP address is used to launch an attack.	The source of the attack comes from multiple locations that include compromised computers, webcams and IoT devices.
Tools	DoS attacks are initiated using scripts or tools like Low Orbit Ion Cannon.	DDoS attacks are initiated with botnets.
Delivery Speed	DoS attacks are slower to execute.	DDoS attacks are faster to execute.
Blocking Attack	Easier to block.	More difficult to block due to the volume of machines used to execute the attack.
Traceability	Easier to trace since only single device is in play.	Tracing the true party is challenging since they can hide behind various compromised systems.
Attack Types	Buffer Overflow, Ping of Death, Teardrop	Volumetric, Fragmentation, Application Layer

Vulnerability Issues: Operating System Vulnerabilities

- Cybercriminals are constantly seeking to take advantage of your computer security vulnerabilities.
- While the goals of these cybercriminals may vary from one to the next (political motives, monetary gain, or just for kicks/prestige) they pose a significant threat to your organization.

- What is a Vulnerability in Computer Security?
- To put it in the most basic terms, a computer system vulnerability is a flaw or weakness in a system or network that could be exploited to cause damage, or allow an attacker to manipulate the system in some way.
- The way that a computer vulnerability is exploited depends on the nature of the vulnerability and the motives of the attacker.

Vulnerability Issues: Operating System Vulnerabilities

- **What is a vulnerability issue?**

In cybersecurity, a vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting a vulnerability, a cyberattack can run malicious code, install malware and even steal sensitive data.

- **What are the operating system vulnerabilities?**

A vulnerability is **effectively an error in the code or the logic of operation within the OS or the application software**. Because today's OSs and applications are very complex and include a lot of functionality, it's difficult for a vendor's development team to create software that contains no errors.

Security Vulnerability Types

- **Network Vulnerabilities.** These are issues with a network's hardware or software that expose it to possible intrusion by an outside party. Examples include insecure Wi-Fi access points and poorly-configured firewalls.
- **Operating System Vulnerabilities.** These are vulnerabilities within a particular operating system that hackers may exploit to gain access to an asset the OS is installed on—or to cause damage. Examples include default superuser accounts that may exist in some OS installs and hidden backdoor programs.
- **Human Vulnerabilities.** The weakest link in many cybersecurity architectures is the human element. User errors can easily expose sensitive data, create exploitable access points for attackers, or disrupt systems.
- **Process Vulnerabilities.** Can be created by specific process controls (or a lack thereof)-- Use of weak passwords (which may also fall under human vulnerabilities).

Vulnerability Issues: Operating System Vulnerabilities

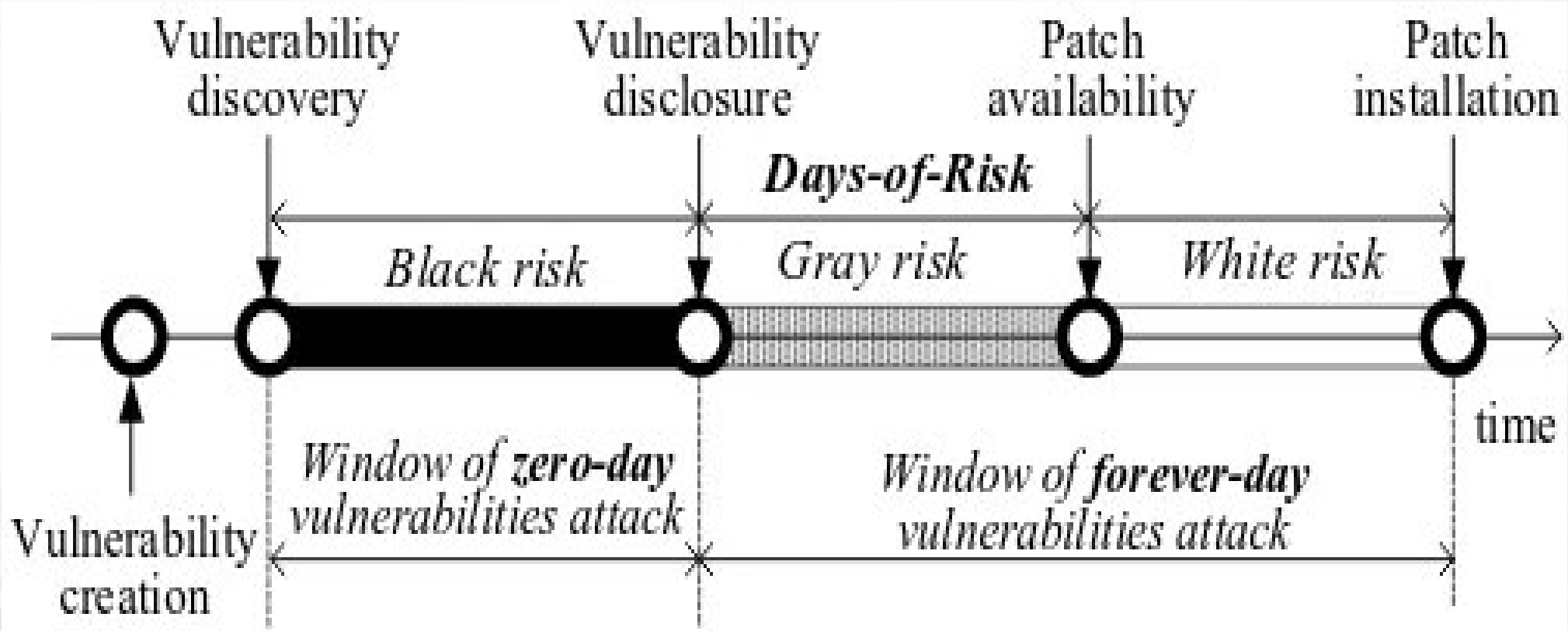
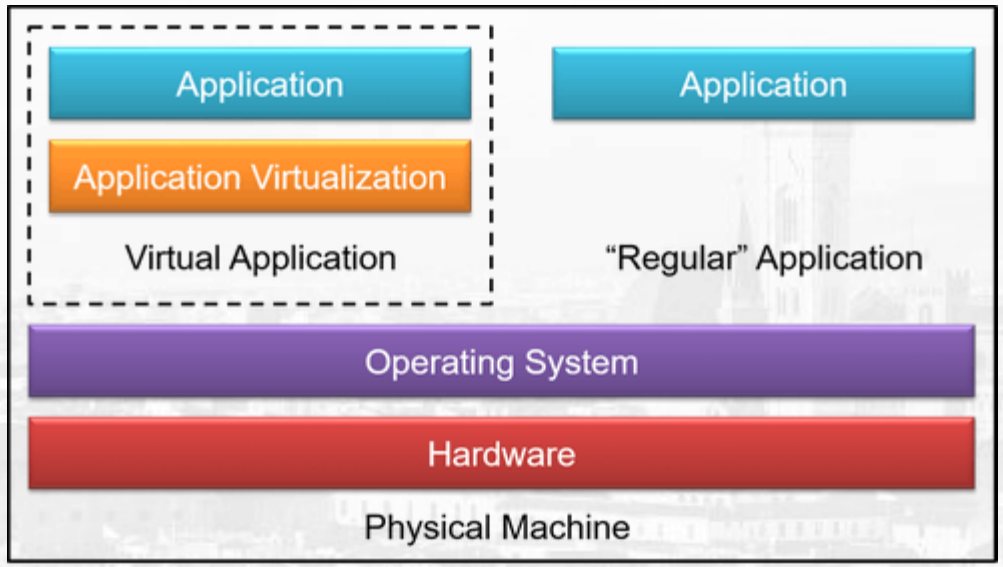


Fig. 1. Vulnerability lifecycle.

How to Find Security Vulnerabilities

- Audit Your Network Assets
- Penetration Testing
- Creating a Threat Intelligence Framework



Examples of security vulnerabilities

- Hidden Backdoor Programs
- Superuser or Admin Account Privileges
- Automated Running of Scripts without Malware/Virus Checks
- Unknown Security Bugs in Software or Programming Interfaces
- Unencrypted Data on the Network

Application Vulnerabilities

- Application vulnerabilities are flaws or weaknesses in an application that can lead to exploitation or a security breach. With the enormous global reach of the Internet, web applications are particularly susceptible to attack, and these can come from many different locations across many attack vectors.
- Sometimes you don't know what you don't know, but the good news is that there is guidance for organizations who wish to find the vulnerabilities in their applications before the attacker does.
- In response to escalating cybersecurity attacks, we pioneered the forensic practice in 2010. In our work helping organizations secure their applications across the tech stack, we have gained technical information about the vulnerabilities identified in applications and the respective best practices in cybersecurity that help mitigate the vulnerabilities.

Application Vulnerabilities

- For the past several months, however, we have investigated our forensic data for application security with a new urgency, for it seems to us that the new ways of working have opened new attack vectors to cybercriminals.
- Based on years of our collective forensic data from over 1000 investigations, this blog post will help you understand where vulnerabilities could arise in the applications and give you a basic idea of how to “think like a hacker” when testing the security posture of applications. In addition, we try to inject the development and testing teams with a healthy dose of paranoia by offering best practices for application security that are essential for QA managers, testing experts, tech leads and information security managers.

Application Vulnerabilities

Application Vulnerabilities

1. Structured Query Language (SQL)/Database Queries

This is the **most common area of application vulnerability** specifically due to the use of multiple databases in conjunction with multiple applications. SQL Injection attacks take place due to a flaw in the code of applications where the attacker successfully retrieves, alters, deletes data, executes SQL commands, or alters server configurations. In the reconnaissance stage, the hacker looks for spots in the application where they can inject undesired values to SQL commands.

- For example, the attacker may use a string value for server queries to inject an escape sequence. The following is a potential SQL query for searching customers in a database:

SELECT * FROM customer WHERE name='" + strName + "'; DROP TABLE customer;"

If the above SQL string input is not validated, it can execute a command to delete the customer table with the string name.

Application Vulnerabilities

- **How to secure applications from SQL Injection attacks?**

This specific application vulnerability has a lot in relation with SQL being natural-language oriented, or better put, human-oriented programming language. Therefore, it is important that anything passed to the SQL server is sanitized to prevent such attacks. It is best done by looking for areas of the application where it connects to a database and passing unusual values as a part of the application security testing program. Moreover, testing experts must always try to make sure that parameterized queries are used, and least privileges are given to applications for reading or inserting data to databases.

Additionally, robust testing tools can be used for dynamic analysis and static analysis that help in discovering application vulnerabilities at the code level.

Application Vulnerabilities

2. Broken Authentication

- URL rewriting, application timeout not set properly, passwords not properly salted and hashed, or predictable login credentials are just a few causes of a broken authentication, in most cases of breaches at least. The prevalence of broken authentication in application (in)security is widespread. It is due to the weak implementation of identity and access controls. Certainly, session management forms the bedrock of the modern-day applications, but they are also not positioned well for many applications.

Application Vulnerabilities

- The landscape of broken authentication in applications as we see it
- The logic behind this approach is uncomplicated and best illustrated with an example. Most authentication-based attacks take place due to the consistent use of plain passwords as the only credentials for an application. Once considered a best practice for application security, password complexity requirements and regular rotation have become obsolete for the new age cyberattacks
- Fortunately, the PCI DSS standard (and other similar regulatory standards) have mandated the use of multi-factor authentication as an application security control.
- Application security team action

Application Vulnerabilities

- To think like a hacker, the testing teams must understand that “what password the user knows” or “who the user is” isn’t enough for the authentication of applications. “Where the user is located” and “what the user is performing” are relevant for the authentication too. Identification of personal patterns including contextual evaluations of user behaviour, geolocations, biometrics and tokens are equally important. Risk-based authentication is relevant

Application Vulnerabilities

Some of the **application security best practices** for testing broken authentication are:

- Check the existence of multi-factor authentication for credential stuffing, brute force, etc.
- Admin users are allocated specific deployment credentials.
- Check that credential recovery and API pathways are hardened.
- Limit the number of failed login credentials.
- Session IDs are not recorded or stored in public interfaces.

Application Vulnerabilities

3. Cross-Site Scripting (CSS)

- Cross-site scripting, CSS, or commonly abbreviated XSS, is the concept that gives attackers the ability to push malicious scripts into dynamic webpages. In many cases, these malicious programs inserted by hackers are disguised as legitimate data. Part of the problem is that the validity of scripts is not checked before execution – and can be programmed to steam passwords or reformat databases.
- Particularly, it is a concern for many banking and financial services applications as they are accessed on web browsers. In a hypothetical example, an attacker may send a trojan URL with client-side scripts that if, clicked by a user, gives the data back to the client

Application Vulnerabilities

4. Modular Program and Container Security

- Hopefully, all the core functions of applications – logic and programming, will stay within the bounds of the applications. However, with the wide adoption of containerization and orchestration technologies such as Docker, Kubernetes, OpenShift and PCF, modular code is empowered at scale, propelling application programs and functions out of the testing boundaries.
- The next wave of application vulnerabilities in containerization

Application Vulnerabilities

5. Checking Networking and Communication Streams

- For an application security tester, all outgoing and incoming network communications are to be treated as vulnerable. For instance, an application code may establish an FTP connection to retrieve an important file. The presence of tainted data can allow an attacker to modify listening server processes and intrude.
- The above example is a small but potential vulnerability in applications. Modern enterprises work on ephemeral computing environments that are very dynamic in nature and are equally vulnerable to cyberthreats. Say an ecommerce company is preparing for the Black Friday and has opted for auto-scaling using Azure Autoscale.
- The trigger can result in the automatic installation of multiple resources such as VPCs, API Management service, Load Balancer, Azure Data Explorer Clusters, Logic Apps with auto provisioned Azure VMs, making it an overextended network infrastructure. Although such automation and auto-scaling of networking elements are the cornerstone of application agility, they require new approaches of application security testing.

Application Vulnerabilities

How to test network security for applications?

- Secure APIs by evaluating the sensitive data and resources they're exposing – Amazon API Gateway implements Client-Side SSL Certificates for authentication by the backend.
- Ensure appropriate in-app permissions – Azure Active Directory provides authentication capabilities for applications.
- Gate admin access based on real-time data – ensure that devices and users are not trusted only on internal networks.
- Ensure all internal communications are encrypted for applications.
- Employ microsegmentation for application network security.
- Hardening and endpoint protection for applications are managed in tandem with changing network environments.

Application Vulnerabilities

What sort of vulnerabilities affects applications?

- **Common Web Application Vulnerabilities Explained**
- Broken access control.
- Broken authentication.
- Carriage Return and Line Feed (CRLF) Injection.
- Cipher transformation insecure.
- Components with known vulnerabilities.
- Cross-Origin Resource Sharing (CORS) Policy.
- Credentials management.
- Cross-site request forgery (CSRF)

Application Vulnerabilities

What are the web application vulnerabilities?

- Web application vulnerabilities involve a system flaw or weakness in a web-based application. They have been around for years, largely due to not validating or sanitizing form inputs, misconfigured web servers, and application design flaws, and they can be exploited to compromise the application's security.

What is application vulnerability testing?

- Vulnerability testing is an assessment used to evaluate application security by identifying, diagnosing, and triaging application vulnerabilities. The entire process requires application security (AppSec) teams to plan vulnerability tests and analyze result

Application Vulnerabilities

How can a web application vulnerability affect an organization?

- Attackers leverage vulnerabilities such as **outdated software or plugins**, as in this attack, to gain access to your application and system. Organizations like the Open Web Application Security Project (OWASP) give companies and users information about the latest vulnerabilities.

Vulnerability Assessment for Natural Disaster

- **A hazard vulnerability assessment (HVA)** systematically evaluates the damage that could be caused by a potential disaster, the severity of the impact, and the available medical resources during a disaster to reduce population vulnerability and increase the capacity to cope with disasters.
- **Hazard Identification and Vulnerability Assessment**

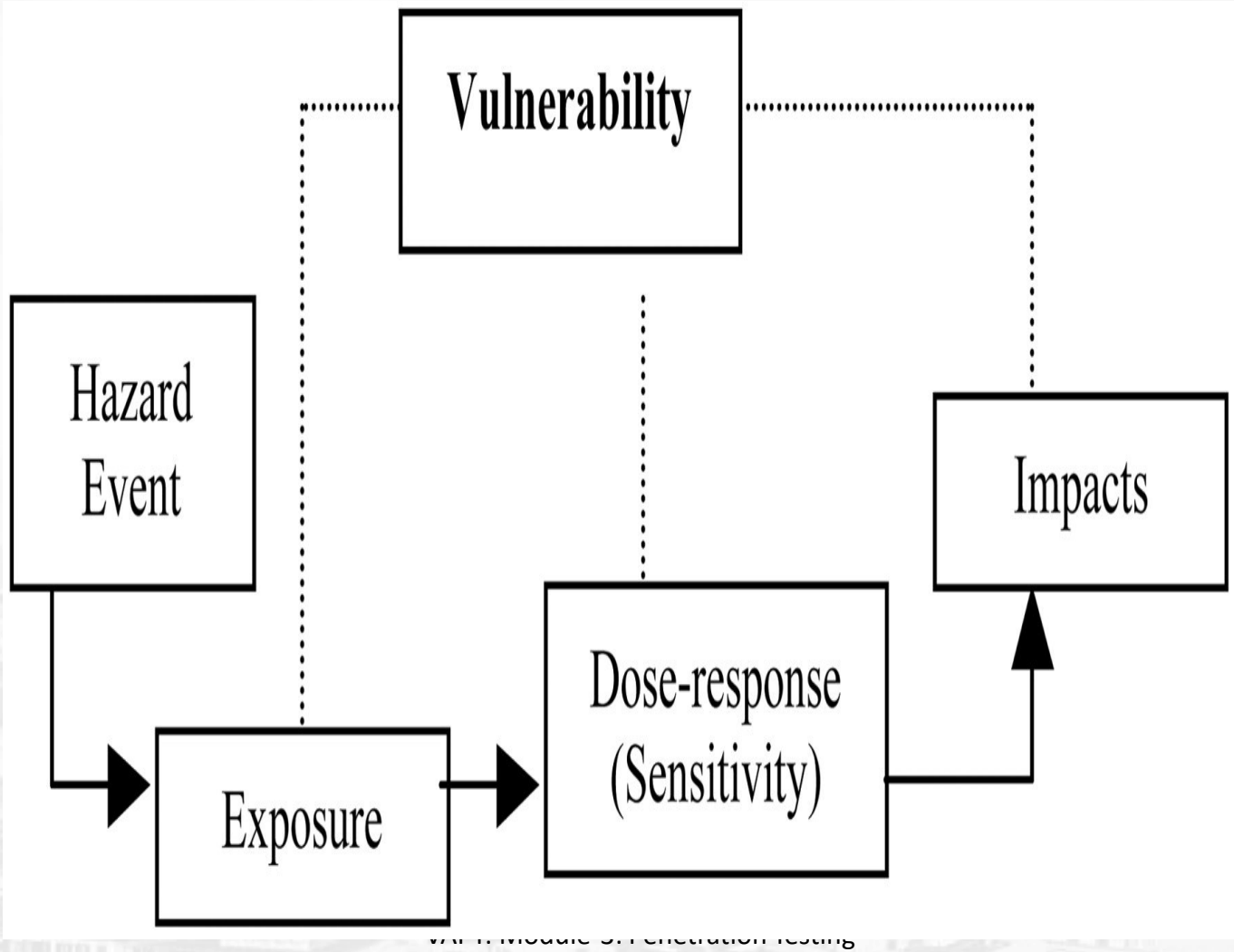
Conducting a Hazard Identification and Vulnerability Assessment (HIVA) is the initial step supporting the emergency management process of hazard preparedness, response, recovery, and mitigation. Hazard identification refers to the systematic use of all available information to determine which types of hazards might affect a community, along with their driving forces ,typical effects. Vulnerability assessment refers to the estimation of scale and severity these hazards may have on the people, property, environment, economy of a community.

Vulnerability Assessment for Natural Disaster

How do we measure vulnerability in disaster?

- **Prevalent Vulnerability Index (PVI)** that measures three tangible social-related vulnerability aspects: hazard exposure and physical susceptibility, socioeconomic fragility, and resilience.
- Risk Management Index (RMI) that measures institutional and community performance on disaster risk management.

Vulnerability Assessment for Natural Disaster



Technological hazards and terrorist threats

- **Manmade or technological** disasters are unpredictable, can spread across geographical boundaries, may be unpreventable, and may have limited physical damage but long-term effects.
- Some disasters in this class are entirely manmade, such as terrorism.
- Other technological disasters occur because industrial sites are located in communities affected by natural disasters, equipment failures occur, or workers have inadequate training or fatigue and make errors.
- The threat of terrorism is categorized as a potential technological disaster and includes bioterrorism, bombings, civil and political disorders, and economic emergencies.

Technological hazards and terrorist threats…

What are five major hazards of terrorism?

- Acts of terrorism include threats of terrorism; assassinations; kidnappings; hijackings; bomb scares and bomb blast ; cyber-attacks (computer-based attacks); and the use of chemical, biological, nuclear, and radiological weapons.

What are the examples of technological hazards?

Examples of technological hazards include industrial pollution, nuclear radiation, toxic wastes, dam failures, transport accidents, factory explosions, fires, and chemical spills.

Implications for emergency response…

What are the appropriate responses to emergency management?

- Prevention, mitigation, preparedness, response and recovery are the five steps of Emergency Management.
- Prevention. Actions taken to avoid an incident. ...
- Mitigation. ...
- Preparedness. ...
- Response. ...
- Recovery.

Implications for emergency response…

vulnerability of critical infrastructures

Critical Infrastructure Vulnerabilities

- **This means that the physical location of critical infrastructures and assets are in sufficient proximity to each other. This also means that they are vulnerable to disruption of the same.**

What is critical infrastructure problem?

- There are two classes of threats to critical infrastructures:
  - Natural - earthquakes, tsunamis, land shifting, volcanic eruptions, extreme weather (hurricanes, floods, draught), fires.
  - Human-Caused - terrorism, product tampering, explosions and bomb blast, theft, financial crimes, economic espionage.