CYBER SECURITY
SURVEILLANCE CAMERA
SECURE PAYMENT
GLOBAL SECURE SHIELD
COMPUTER SECURITY
FINGERPRINT

Presentation on IT Fundamentals of Cyber Security

- Introduction to cybersecurity tools and cyber attack
- Cybersecurity roles, processes and operating system security
- Cybersecurity compliance, Framework and system administration
- Network security and Database

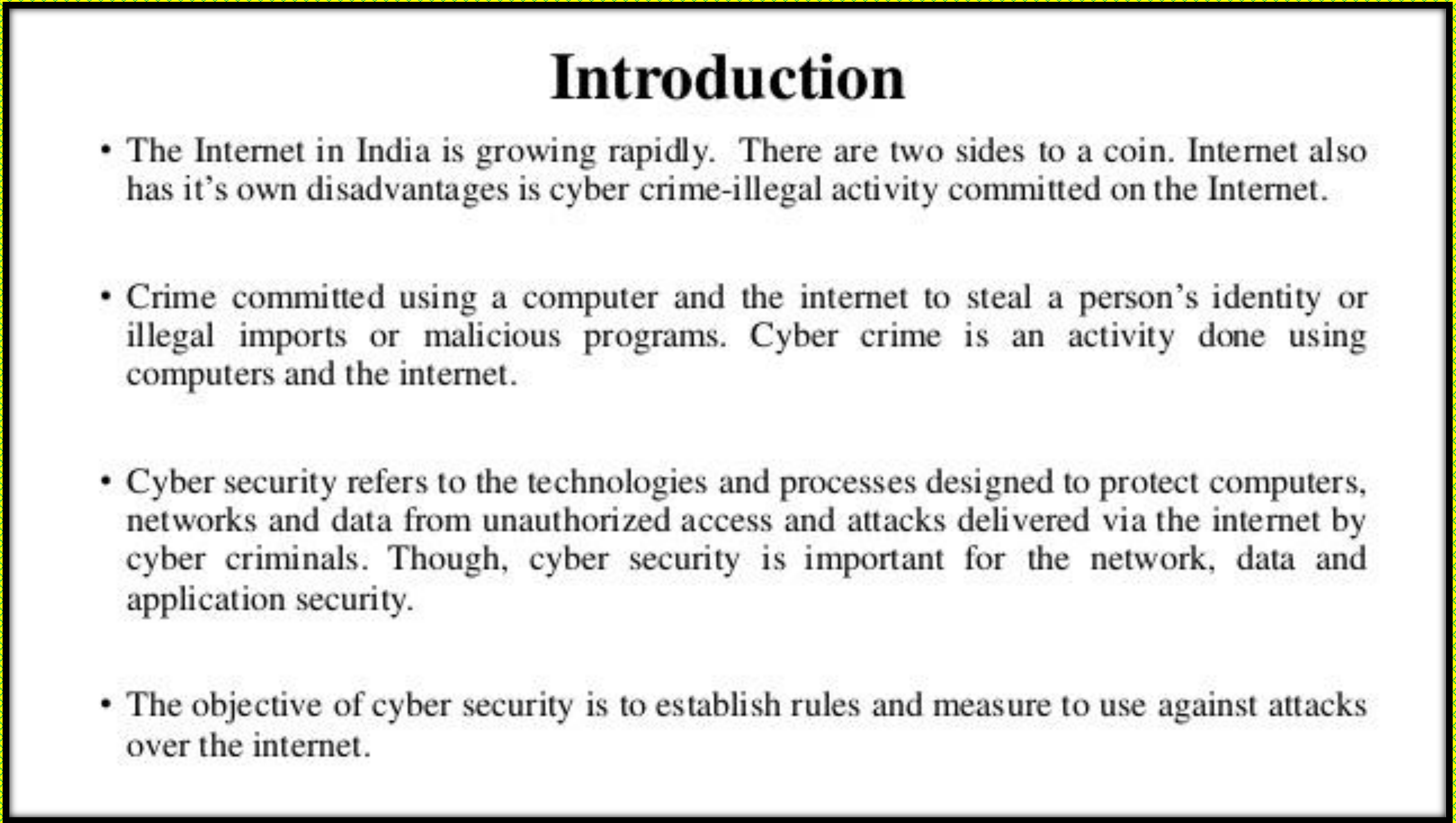
(Duration:-71 hours(Beginners level))

(Submitted by:-Tanishk Jharwal)

Submitted to:-Mrs. Kavita Jain

Content

- Introduction
- Categories of Cyber crime
- Types of Cyber crime
- Types of Security tools
- Advantage of Cybersecurity
- Safety tips to Cyber crime
- References



Introduction

- The Internet in India is growing rapidly. There are two sides to a coin. Internet also has it's own disadvantages is cyber crime-illegal activity committed on the Internet.

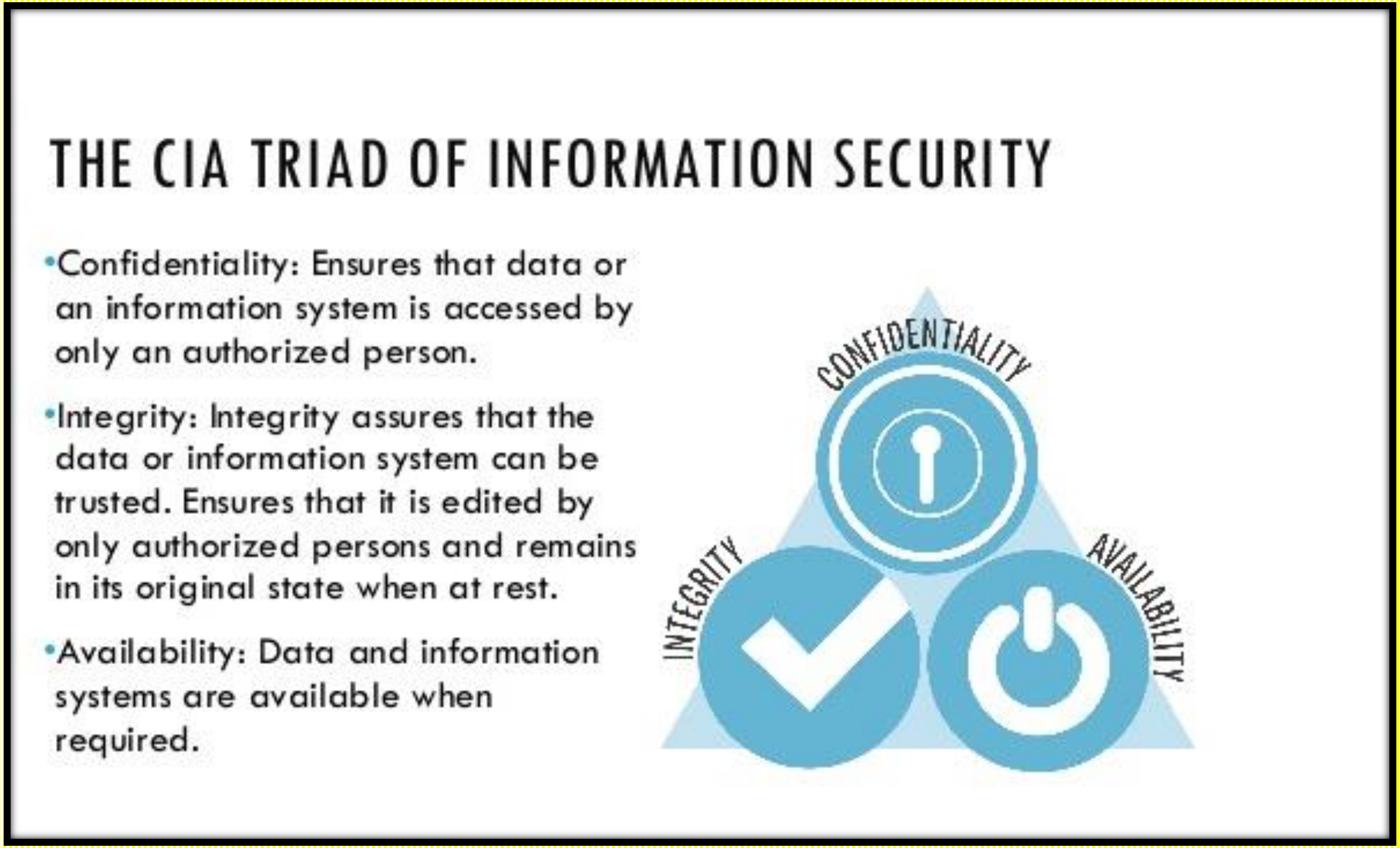
- Crime committed using a computer and the internet to steal a person's identity or illegal imports or malicious programs. Cyber crime is an activity done using computers and the internet.

- Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access and attacks delivered via the internet by cyber criminals. Though, cyber security is important for the network, data and application security.

- The objective of cyber security is to establish rules and measure to use against attacks over the internet.

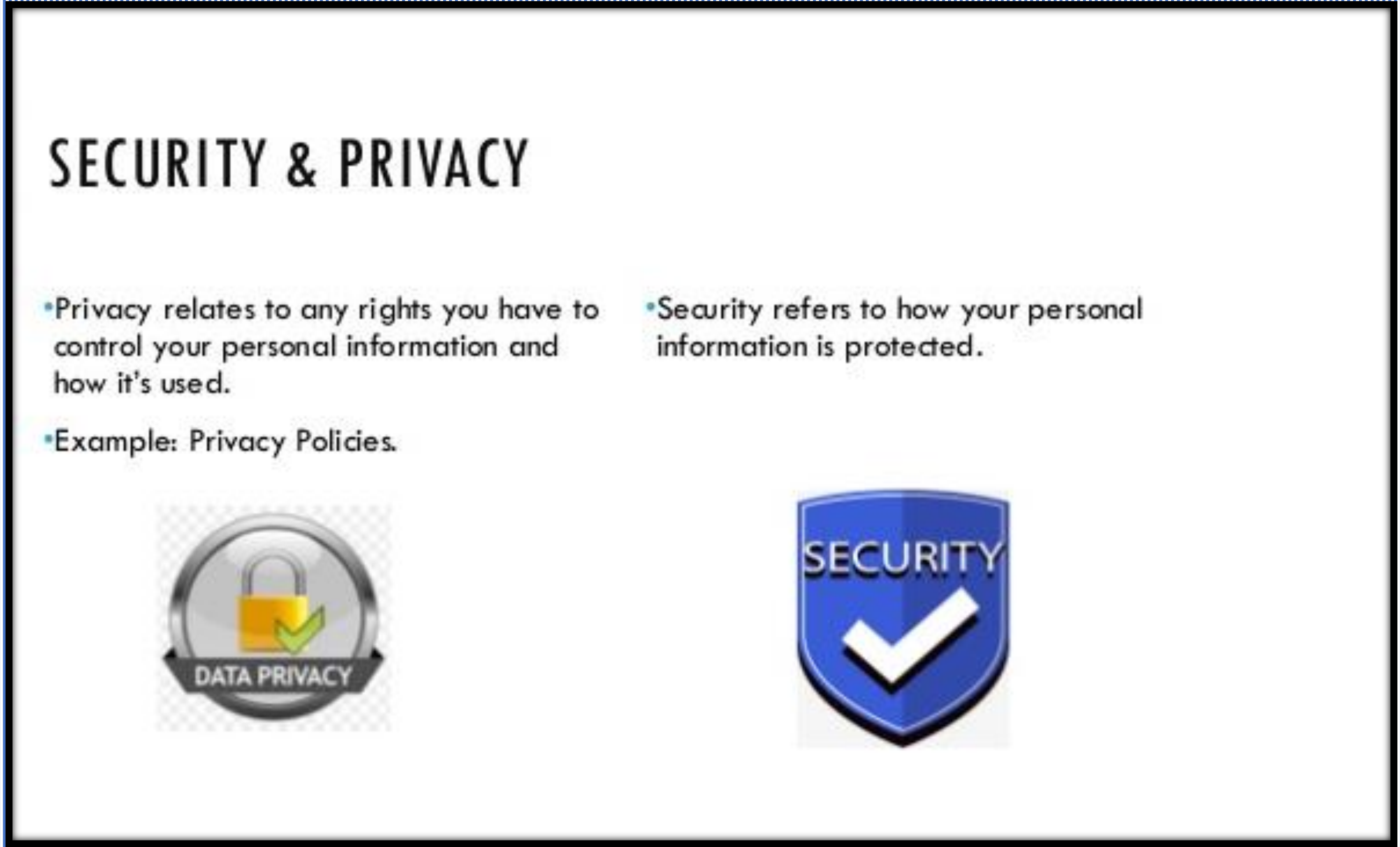
WHAT IS CYBER SECURITY?

- Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks.
- In a computing context, security comprises cybersecurity and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems.
- Information security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cybersecurity.



THE CIA TRIAD OF INFORMATION SECURITY

- Confidentiality: Ensures that data or an information system is accessed by only an authorized person.
- Integrity: Integrity assures that the data or information system can be trusted. Ensures that it is edited by only authorized persons and remains in its original state when at rest.
- Availability: Data and information systems are available when required.



SECURITY & PRIVACY

- Privacy relates to any rights you have to control your personal information and how it's used.
- Example: Privacy Policies.

- Security refers to how your personal information is protected.

DATA PRIVACY
SECURITY

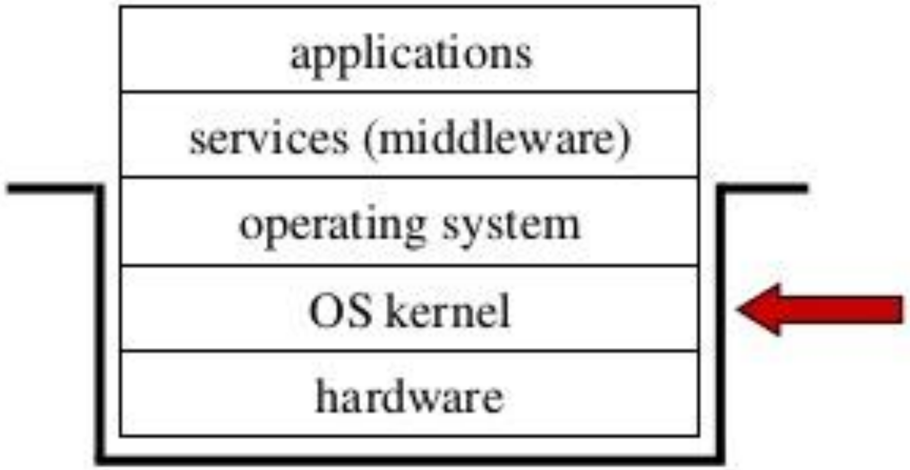
Categories of Cyber Crime

We can categorize cyber crime in two ways:-

The computer as a target: Using a computer to attacks other computer e.g. Hacking, Virus/Worms attacks, DoS attack etc.

The computer as a weapon: Using a computer to commit real world crime e.g. credit card fraud etc.

Principles of Computer Security



applications

services (middleware)

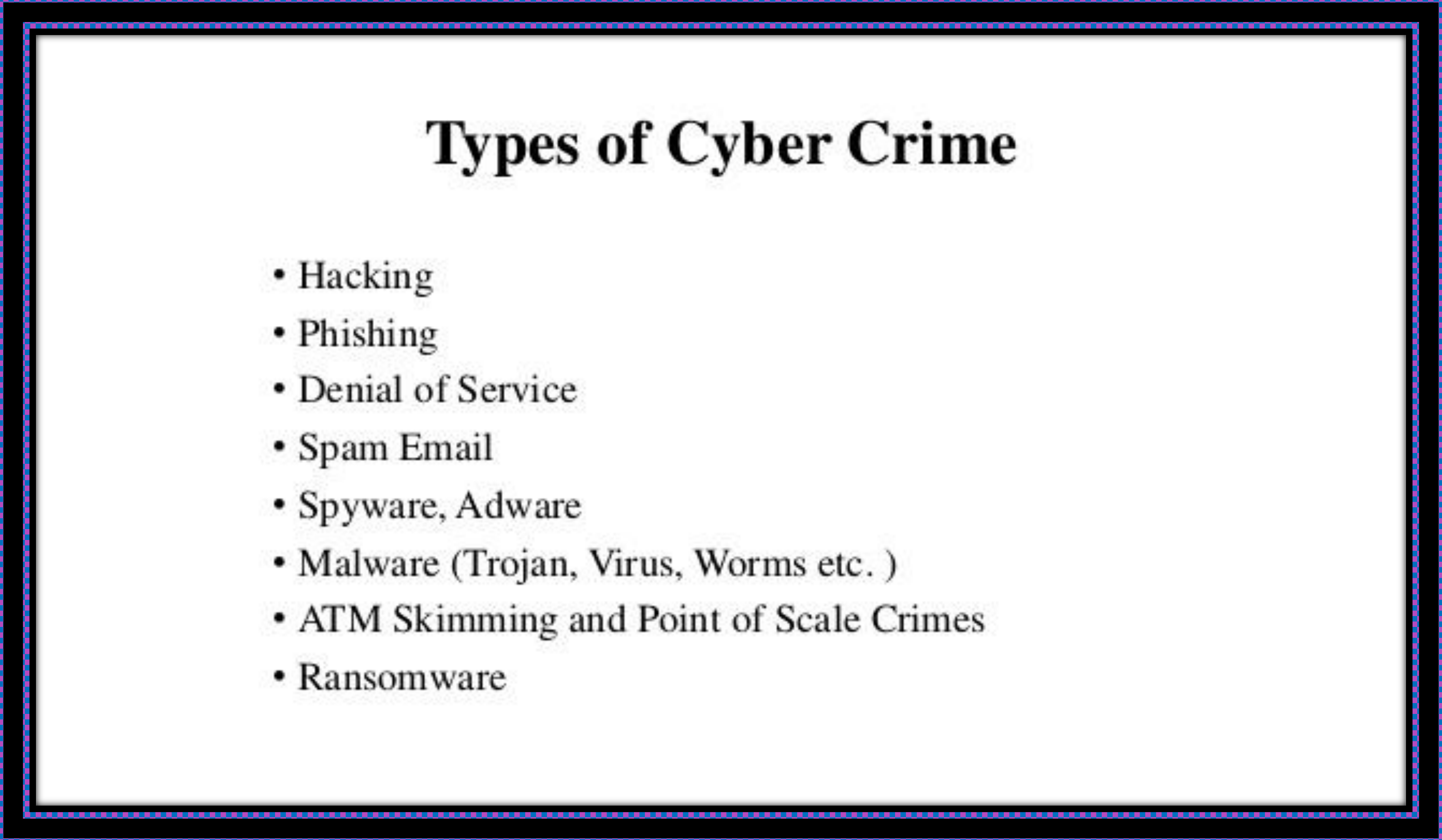
operating system

OS kernel

hardware

Hackers attack at level below security perimeter

- How do you stop an attacker from getting access to a layer below your protection mechanism?
- Every protection mechanism defines a security perimeter (boundary). Attackers try to bypass protection mechanisms.

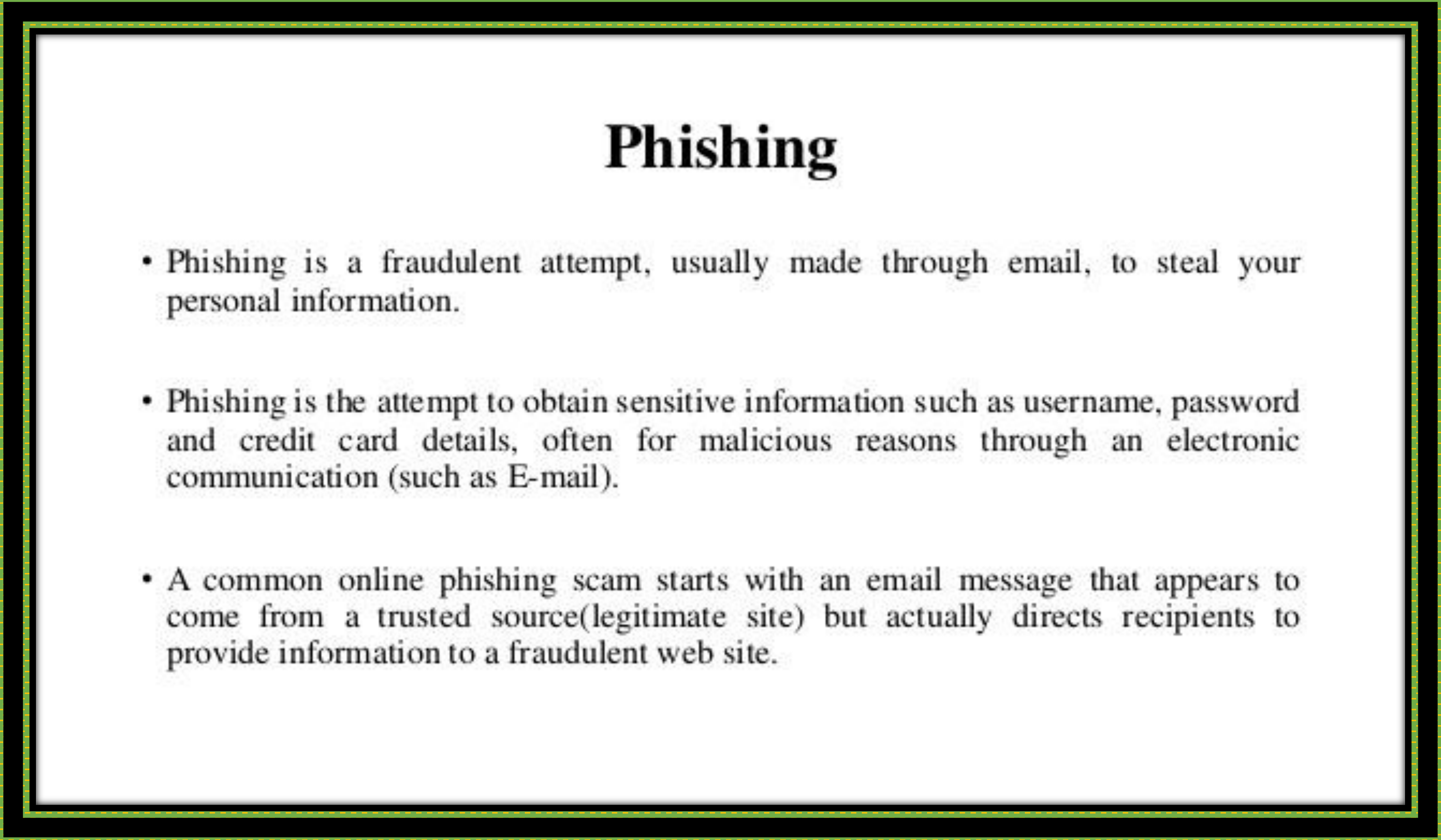


Types of Cyber Crime

- Hacking
- Phishing
- Denial of Service
- Spam Email
- Spyware, Adware
- Malware (Trojan, Virus, Worms etc.)
- ATM Skimming and Point of Scale Crimes
- Ransomware

Hacking

- Hacking in simple terms means an illegal intrusion into a computer system and/or network.
- It is also known as cracking. Government websites are the hot targets of the hackers due to the press coverage, it receives.

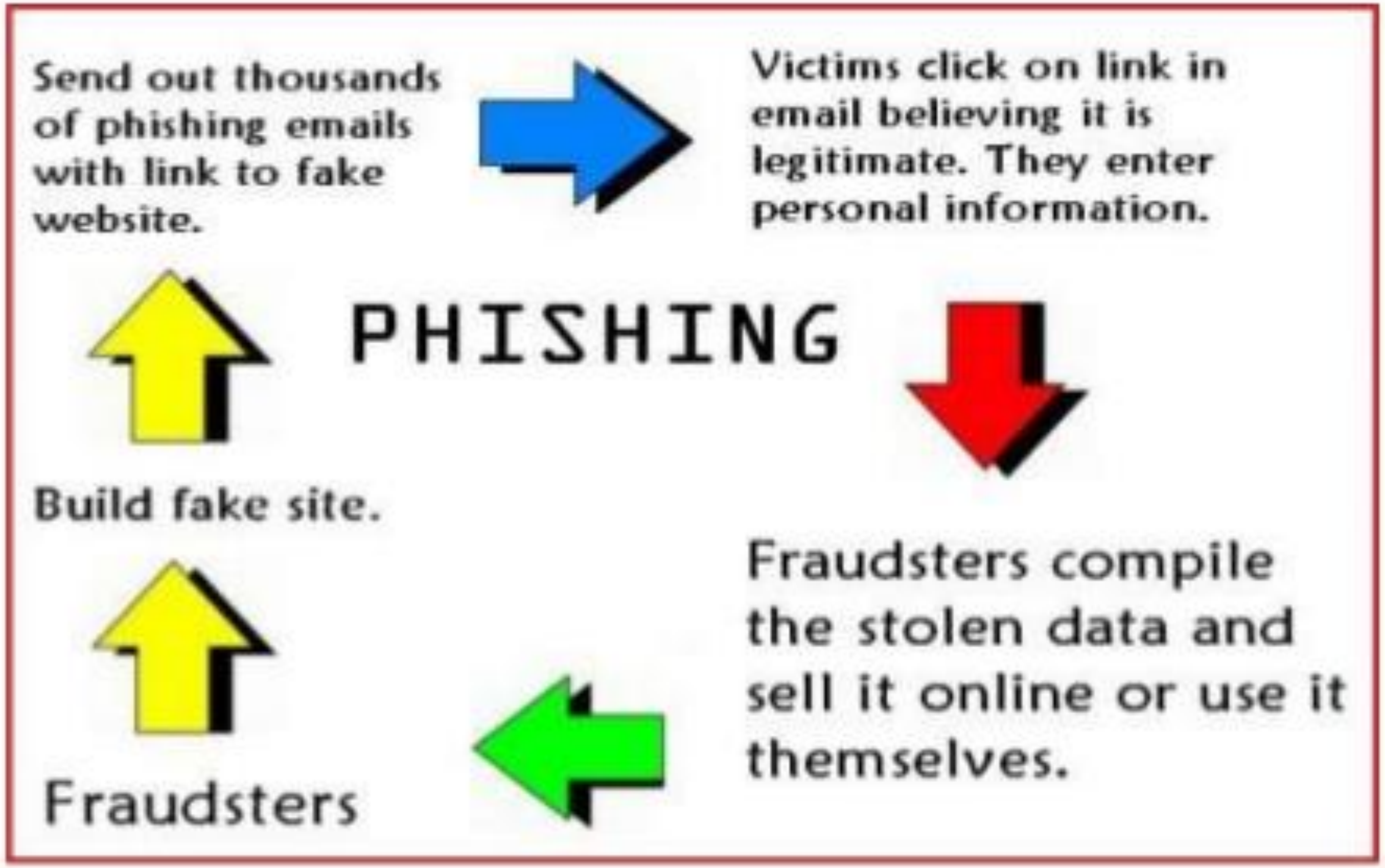


Phishing

- Phishing is a fraudulent attempt, usually made through email, to steal your personal information.

- Phishing is the attempt to obtain sensitive information such as username, password and credit card details, often for malicious reasons through an electronic communication (such as E-mail).

- A common online phishing scam starts with an email message that appears to come from a trusted source(legitimate site) but actually directs recipients to provide information to a fraudulent web site.



Send out thousands of phishing emails with link to fake website.

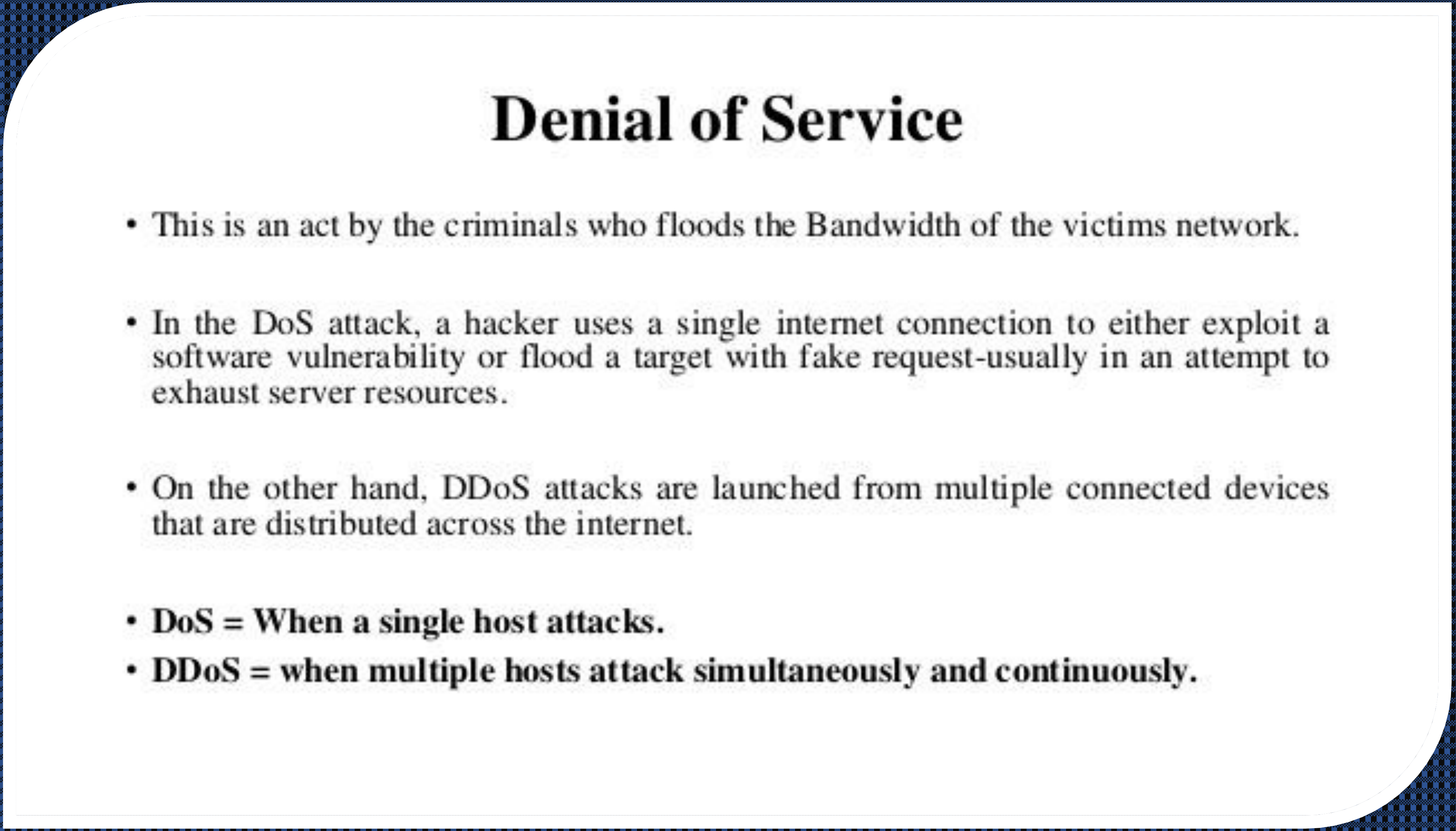
Victims click on link in email believing it is legitimate. They enter personal information.

PHISHING

Build fake site.

Fraudsters compile the stolen data and sell it online or use it themselves.

Fraudsters



Denial of Service

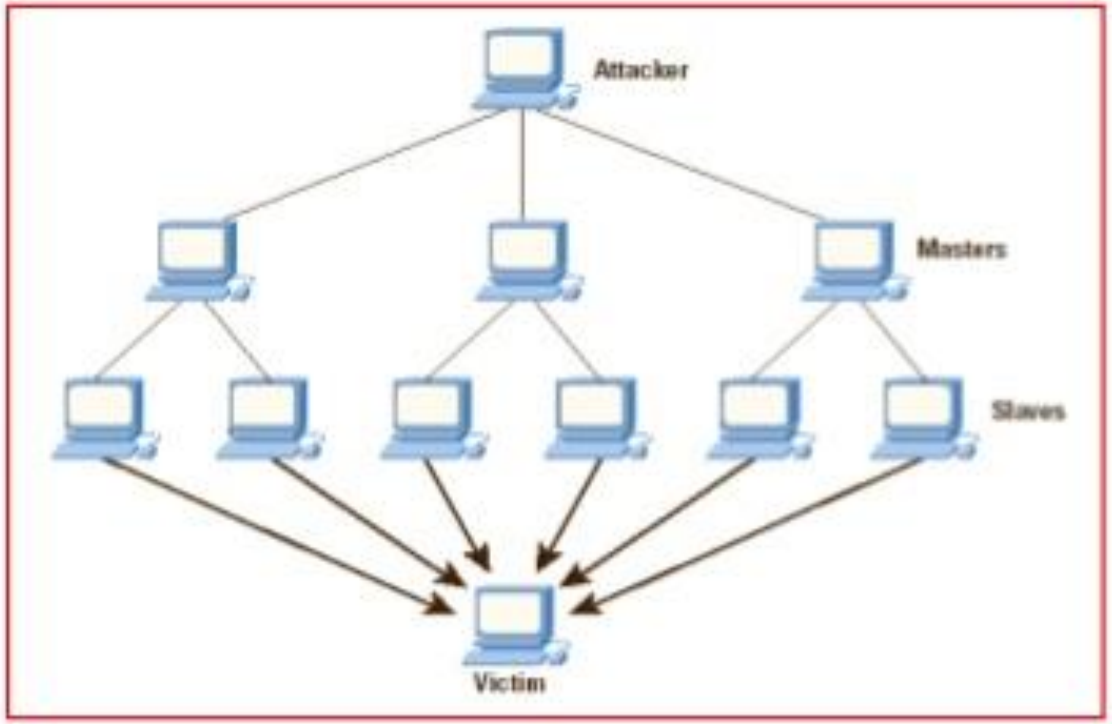
- This is an act by the criminals who floods the Bandwidth of the victims network.

- In the DoS attack, a hacker uses a single internet connection to either exploit a software vulnerability or flood a target with fake request-usually in an attempt to exhaust server resources.

- On the other hand, DDoS attacks are launched from multiple connected devices that are distributed across the internet.

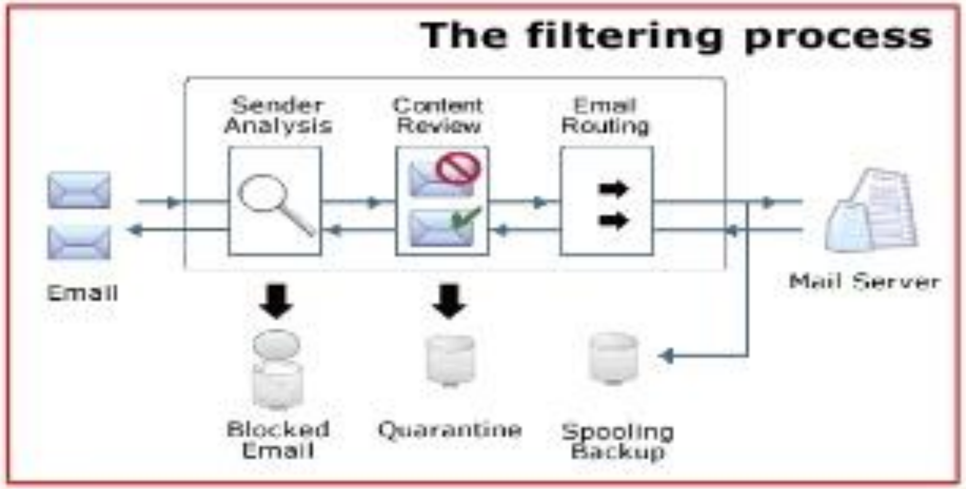
- **DoS = When a single host attacks.**
- **DDoS = when multiple hosts attack simultaneously and continuously.**

Figure of DDoS attack:



Spam Email

- **Email Spam** is the electronic version of junk **mail**. It involves sending unwanted messages, often unsolicited advertising, to a large number of recipients. **Spam** is a serious security concern as it can be used to deliver Trojan horses, viruses, worms, spyware, and targeted phishing attacks.

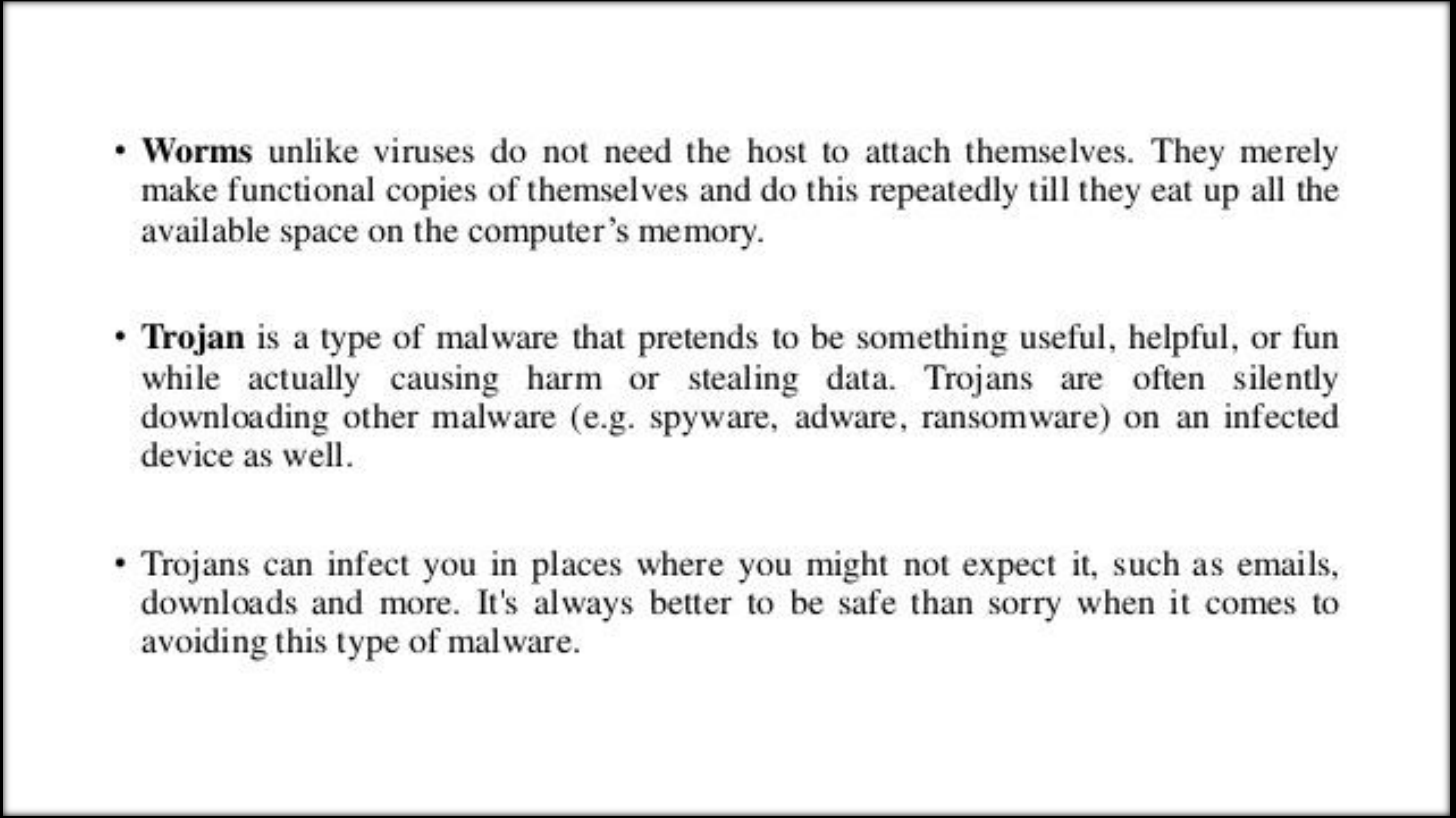


Malware

- It’s malicious software (such as Virus ,Worms & Trojan) , which specifically designed to disrupt or damage computer system or mobile device.

- Hackers use malware for any number of reasons such as, extracting personal information or passwords, stealing money, or preventing owners from accessing their device.

- **Viruses** are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer and mobile device either by altering or deleting it.



- **Worms** unlike viruses do not need the host to attach themselves. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on the computer's memory.

- **Trojan** is a type of malware that pretends to be something useful, helpful, or fun while actually causing harm or stealing data. Trojans are often silently downloading other malware (e.g. spyware, adware, ransomware) on an infected device as well.

- Trojans can infect you in places where you might not expect it, such as emails, downloads and more. It's always better to be safe than sorry when it comes to avoiding this type of malware.

Overview

- **Objective:**
- **Create a web-based cybersecurity tool that offers:-**
- **Malicious file detection (PDF/TXT)- URL threat classification**
- **Password strength analysis**

Malicious Files Detection

- Malicious Files Detection Feature:- Upload and analyze PDF or TXT files. Functionality:- Scan uploaded documents for malicious patterns, viruses, or embedded threats.

- Technologies Used:- Machine Learning models-
- Antivirus signature libraries

URL Threat Detection

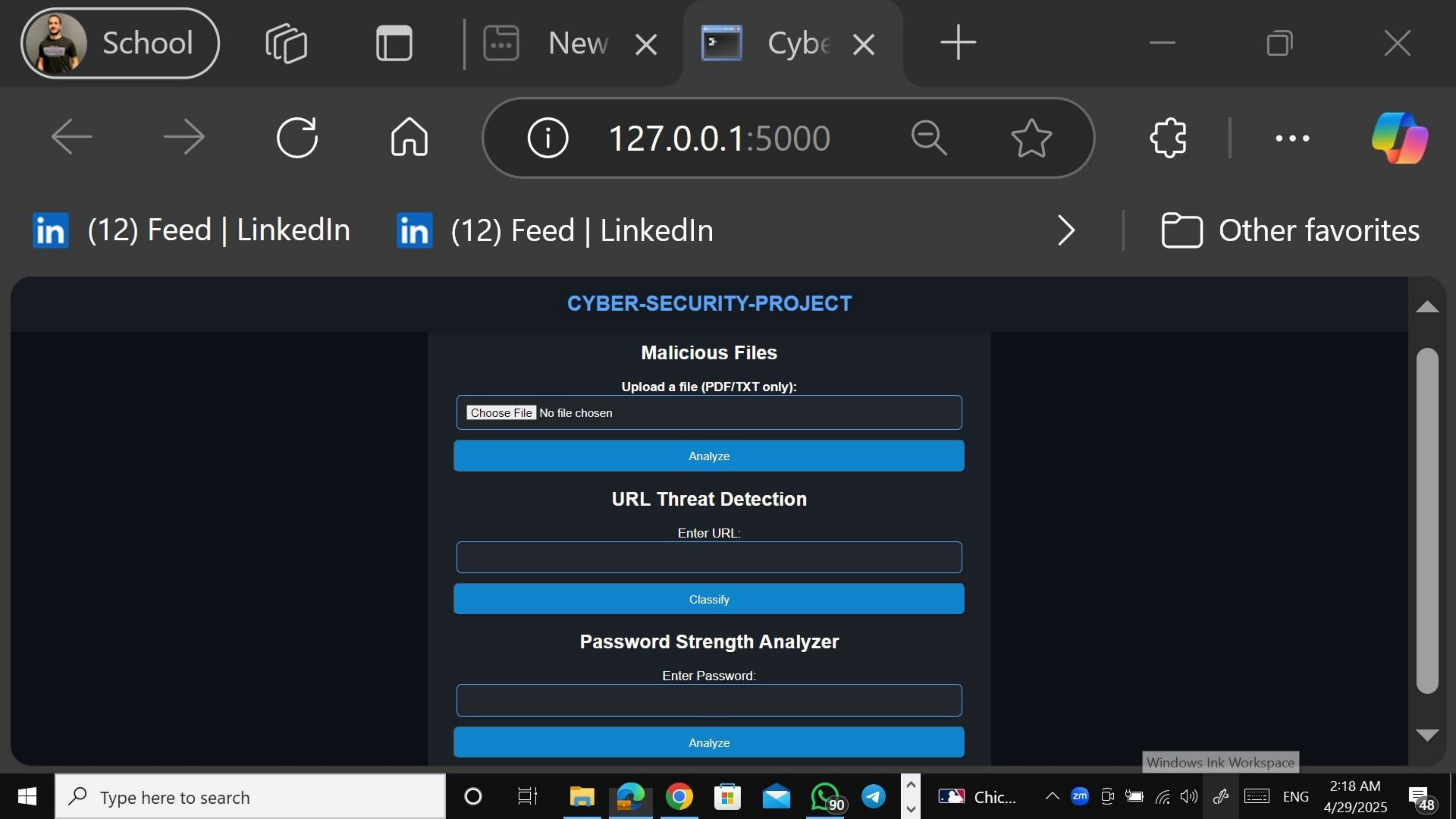
- URL Threat Detection Feature:- Input a URL to check its safety. Functionality:- Classify URLs as safe or dangerous using a threat detection model. Technologies Used:- URL scanning APIs- ML classifiers for malicious link detection

Password Strength Analyzer

- Password Strength Analyzer Feature:- Analyze the strength of any password entered. Functionality:- Measure password complexity and provide strength feedback (Weak/Moderate/Strong). Technologies Used: Cyber Security Project Presentation- Regular Expressions (Regex)- Entropy-based password strength metrics

User Interface

- User Interface
- Tools Used:-
- Backend: Flask (Python)-
- Frontend: HTML/CSS
- Design Philosophy:- Simple- Intuitive- User-focused



CYBER-SECURITY-PROJECT

Malicious Files

Upload a file (PDF/TXT only):

No file chosen

URL Threat Detection

Enter URL:

Password Strength Analyzer

Enter Password:

Spyware

- Spyware is a type of malware that hackers use to spy on you in order to gain access to your personal information, banking details, or online activity. We should protect ourselves by an anti-spyware tool.

Adware

- Adware is a type of malware that bombards you with endless ads and pop-up windows that could potentially be dangerous for your device. The best way to remove adware is to use an adware removal tool.

Ransomware

- Ransomware is as scary as it sounds. Hackers use this technique to lock you out of your devices and demand a ransom in return for access. Ransomware puts you in a sticky situation, so it's best to know how to avoid it.

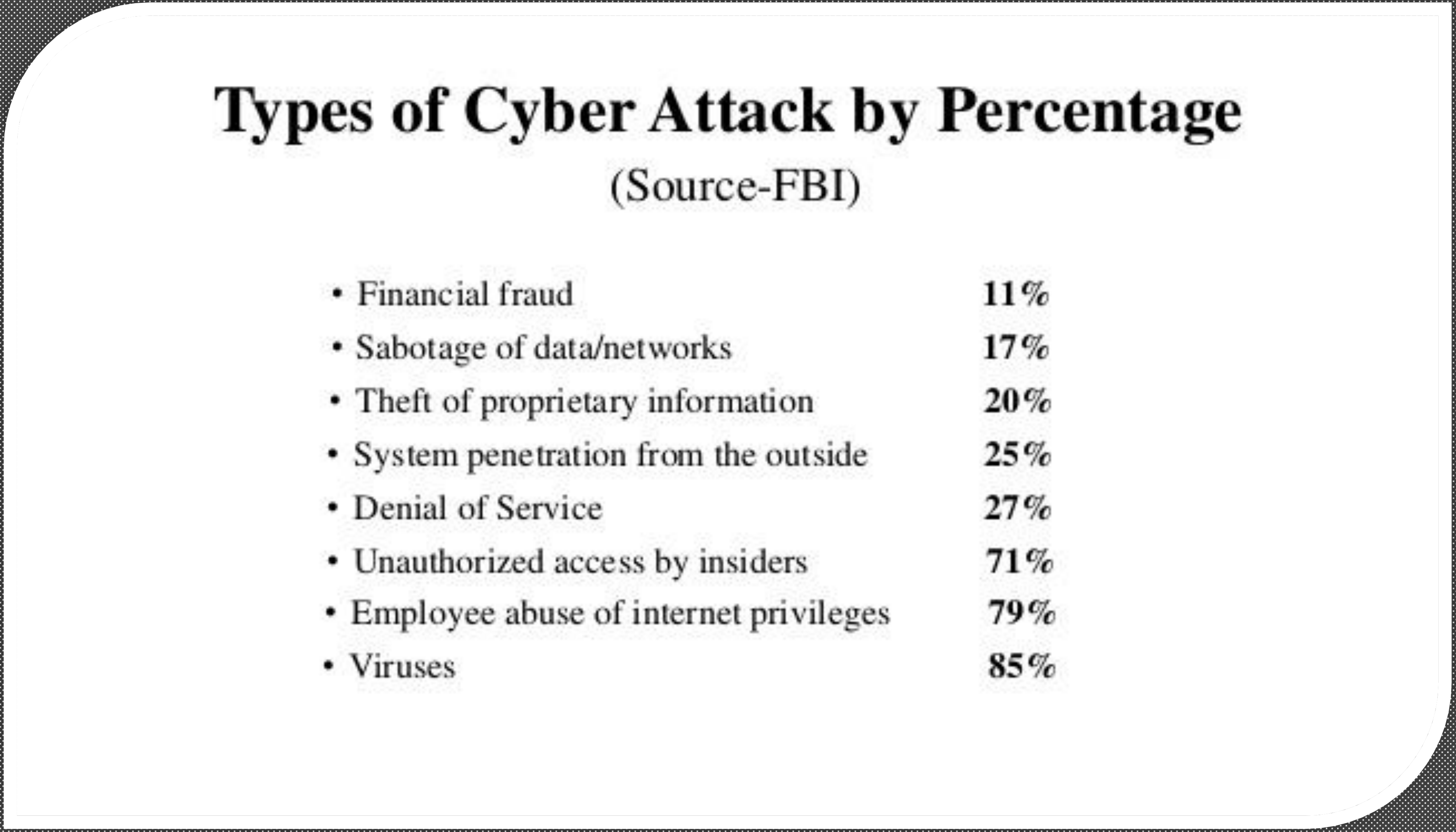
- Ransomware (a.k.a. rogueware or scareware) restricts access to your computer system and demands that a ransom is paid in order for the restriction to be removed. The most dangerous ransomware attacks are caused by Wannacry, Petya, Cerber and Locky ransomware. The money which suppose to be paid to remove ransomware from your system which is called ransom money.

- Current affairs : eg. WannaCrypt , Petya Variant

ATM Skimming and Point of Scale Crimes

- It is a technique of compromising the ATM machine by installing a skimming device a top the machine keypad to appear as a genuine keypad or a device made to be affixed to the card reader to look like a part of the machine.

- Additionally, malware that steals credit card data directly can also be installed on these devices. Successful implementation of skimmers cause in ATM machine to collect card numbers and personal identification number codes that are later replicated to carry out fraudulent transaction.

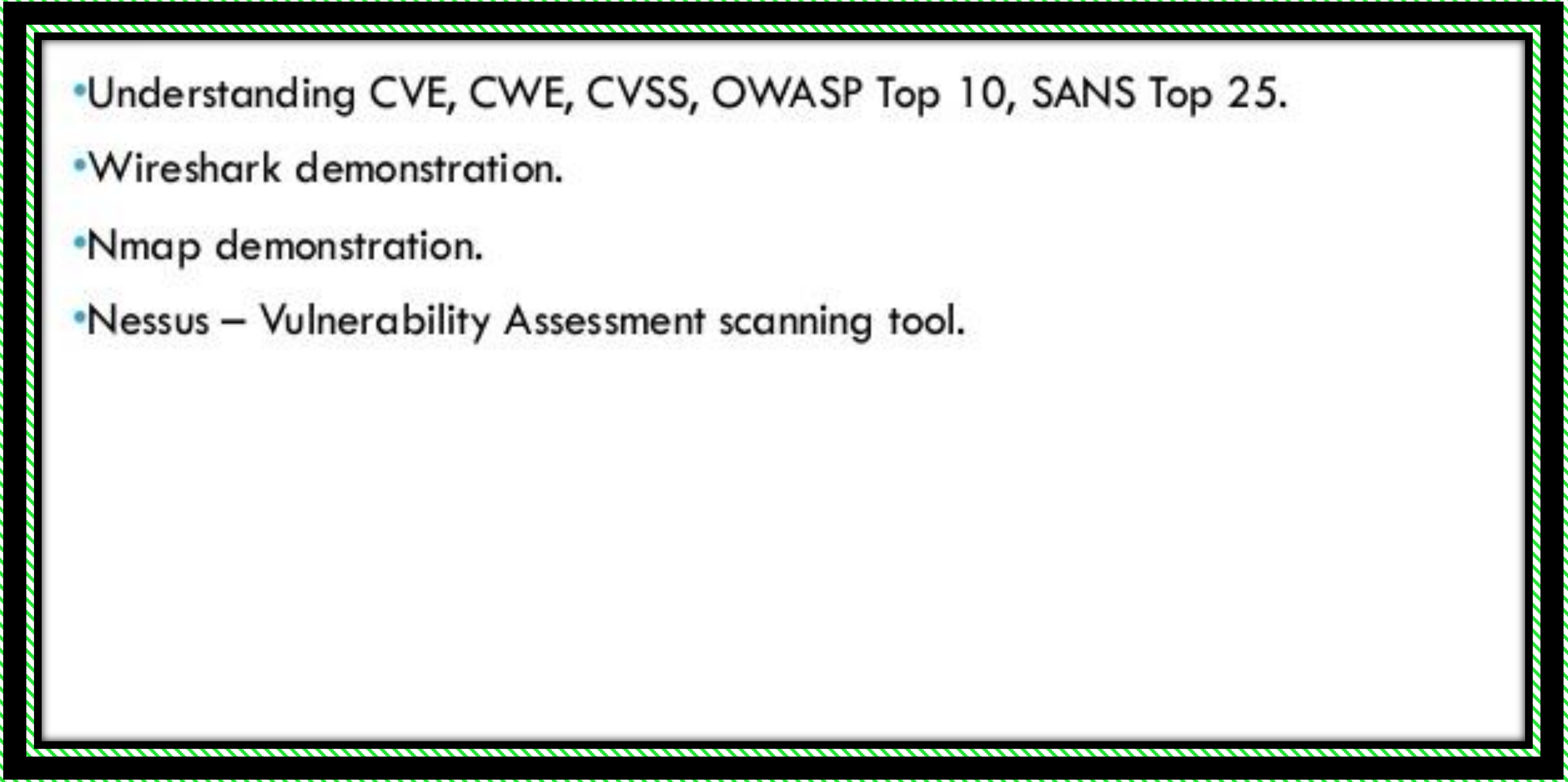


Types of Cyber Attack by Percentage

(Source-FBI)

• Financial fraud	**11%**
• Sabotage of data/networks	**17%**
• Theft of proprietary information	**20%**
• System penetration from the outside	**25%**
• Denial of Service	**27%**
• Unauthorized access by insiders	**71%**
• Employee abuse of internet privileges	**79%**
• Viruses	**85%**

OVERVIEW



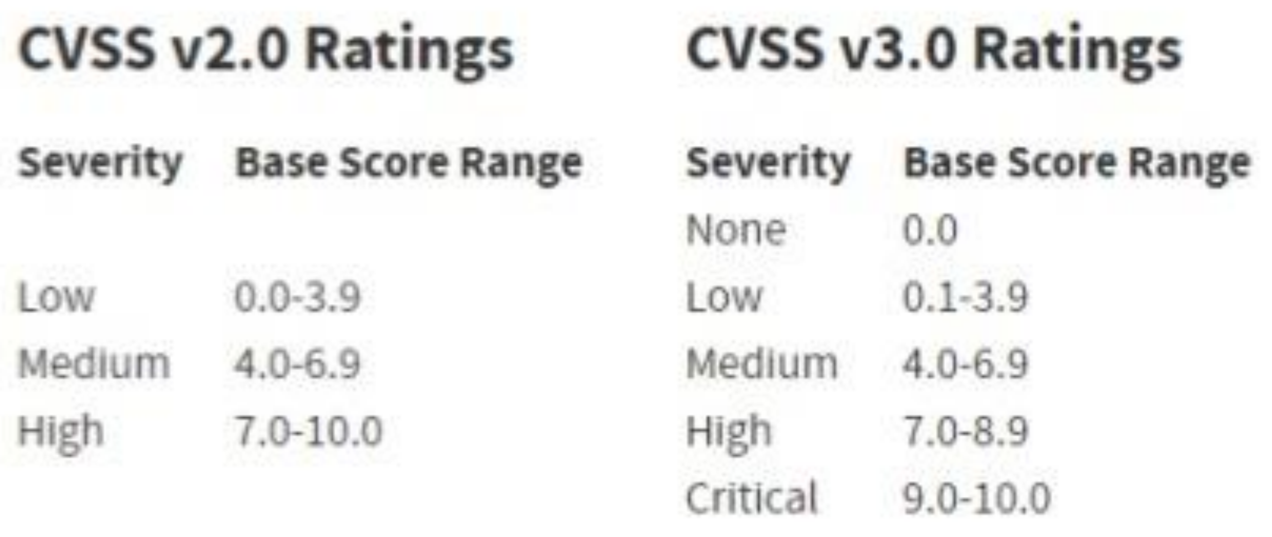
- Understanding CVE, CWE, CVSS, OWASP Top 10, SANS Top 25.
- Wireshark demonstration.
- Nmap demonstration.
- Nessus – Vulnerability Assessment scanning tool.

WHAT IS CVE, CWE, CVSS, OWASP TOP 10, SANS TOP 25

- Common Vulnerabilities and Exposures (**CVE**) is a catalog of known security threats. The catalog is sponsored by the United States Department of Homeland Security (DHS), and threats are divided into two categories: vulnerabilities and exposures.

- CVE Databases:
  - The National Institute of Standards and Technology (NIST)
  - The MITRE Corporation

- The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities.



CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

- Common Weakness Enumeration (CWE) is a list of software weaknesses.

- **CWE Database:**

  The MITRE Corporation

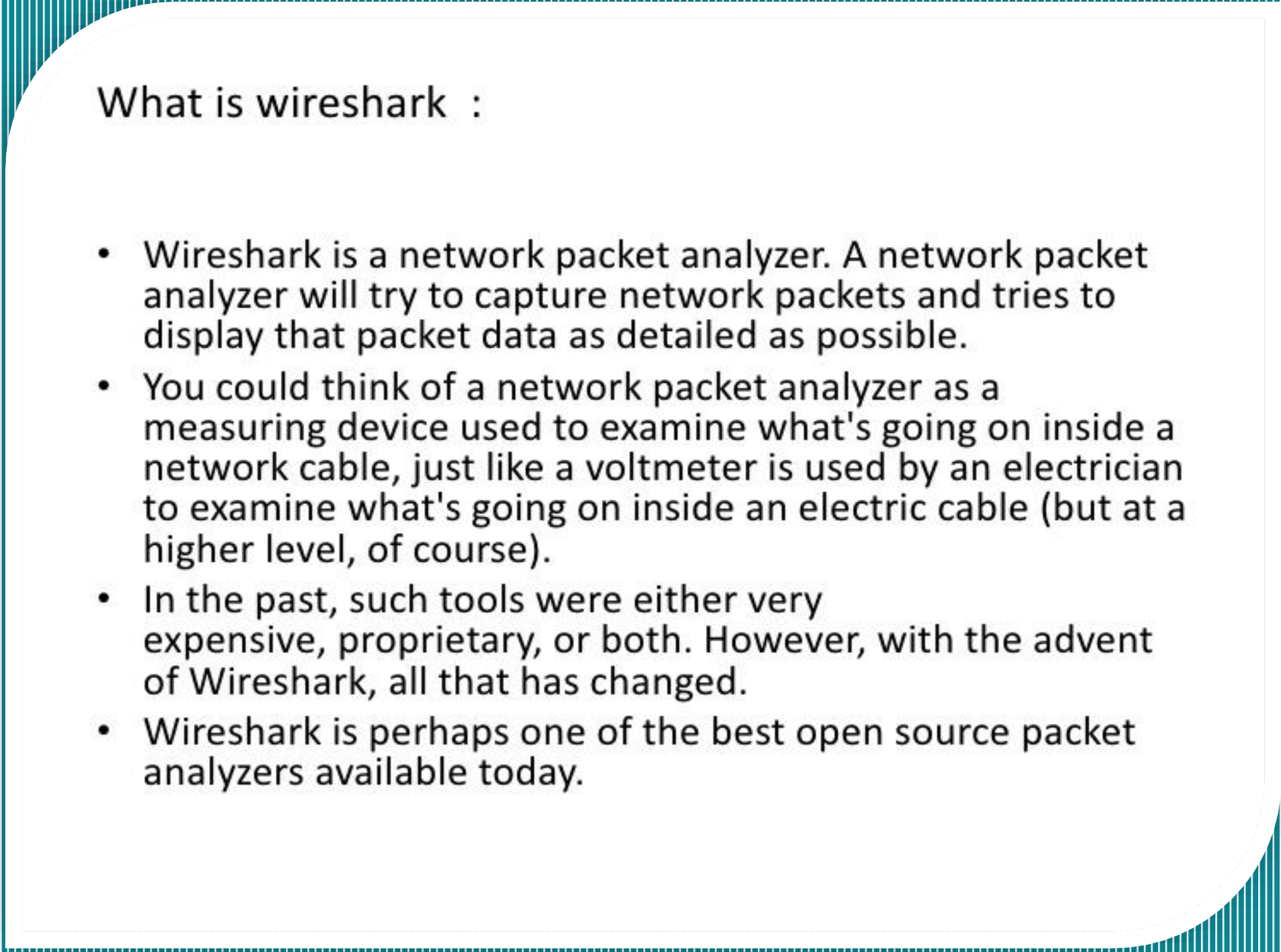
- **Total number of CWE's:** 808

- CWE/SANS Top 25 Most Dangerous Software Errors is a list of the most widespread and critical errors that can lead to serious vulnerabilities in software.
- They are often easy to find, and easy to exploit.
- They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all.

- The **OWASP Top 10** is a powerful awareness document for web application security.
- It represents a broad consensus about the most critical security risks to web applications.
- The OWASP Top 10 list consists of the 10 most seen application vulnerabilities:
- Injection
- Broken Authentication
- Sensitive data exposure
- XML External Entities (XXE)

- Broken Access control
- Security misconfigurations
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Using Components with known vulnerabilities
- Insufficient logging and monitoring

Wireshark

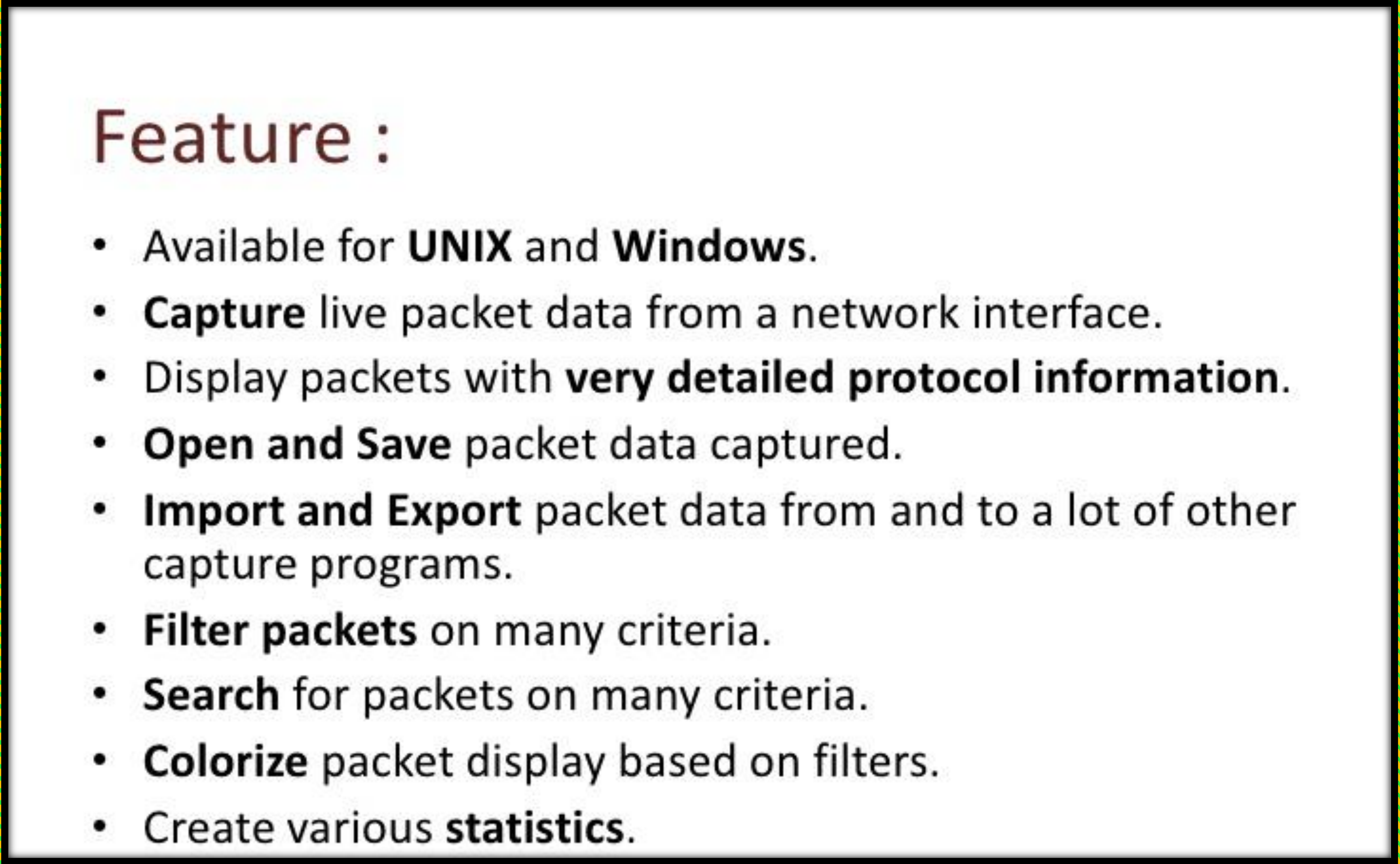


What is wireshark :

- Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.
- You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).
- In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed.
- Wireshark is perhaps one of the best open source packet analyzers available today.

people use Wireshark for :

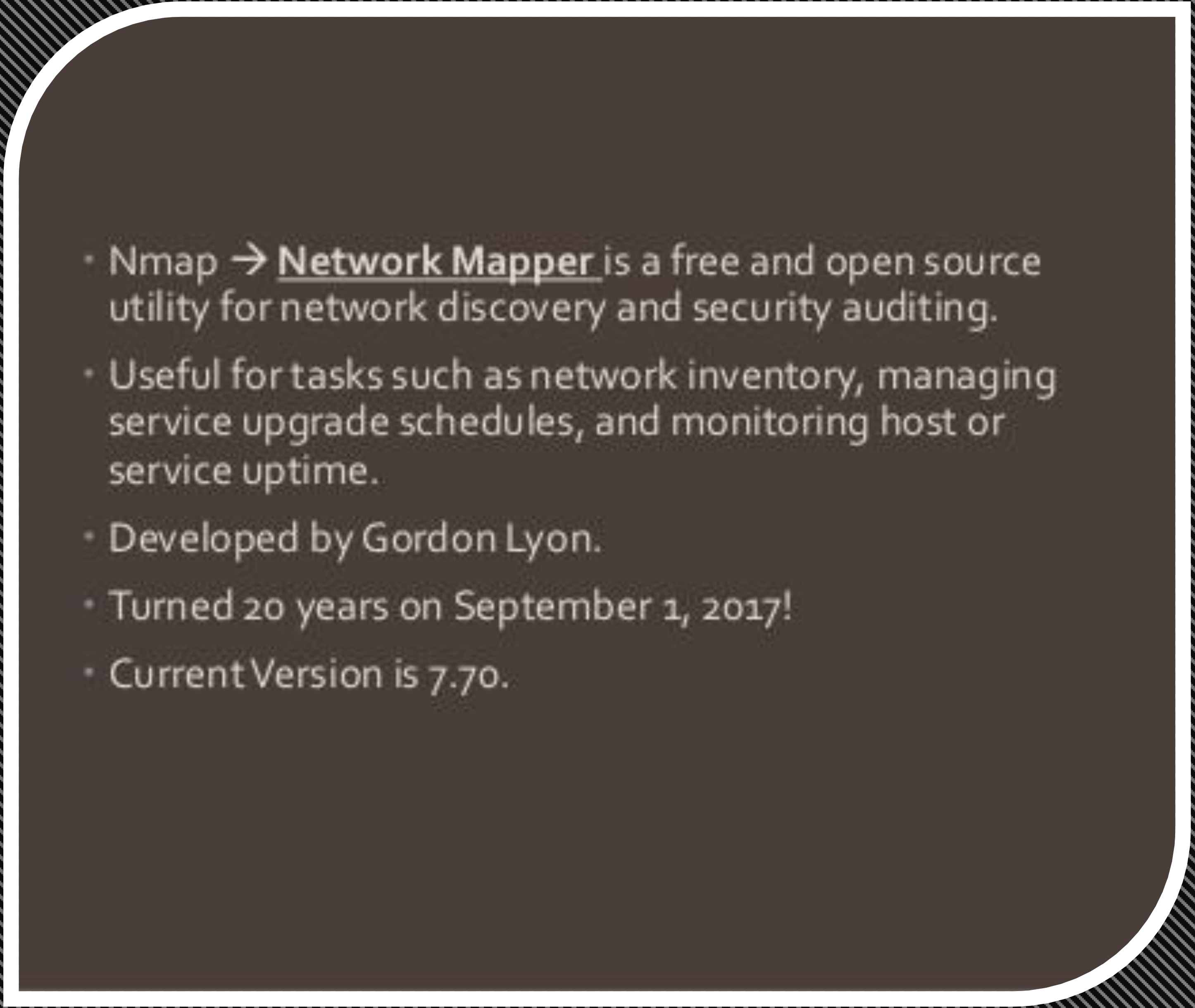
- network administrators use it to **troubleshoot network problems**
- network security engineers use it to **examine security problems**
- developers use it to **debug protocol implementations**
- people use it to **learn network protocol** internals
- Beside these examples, Wireshark can be helpful in many other situations too.



Feature :

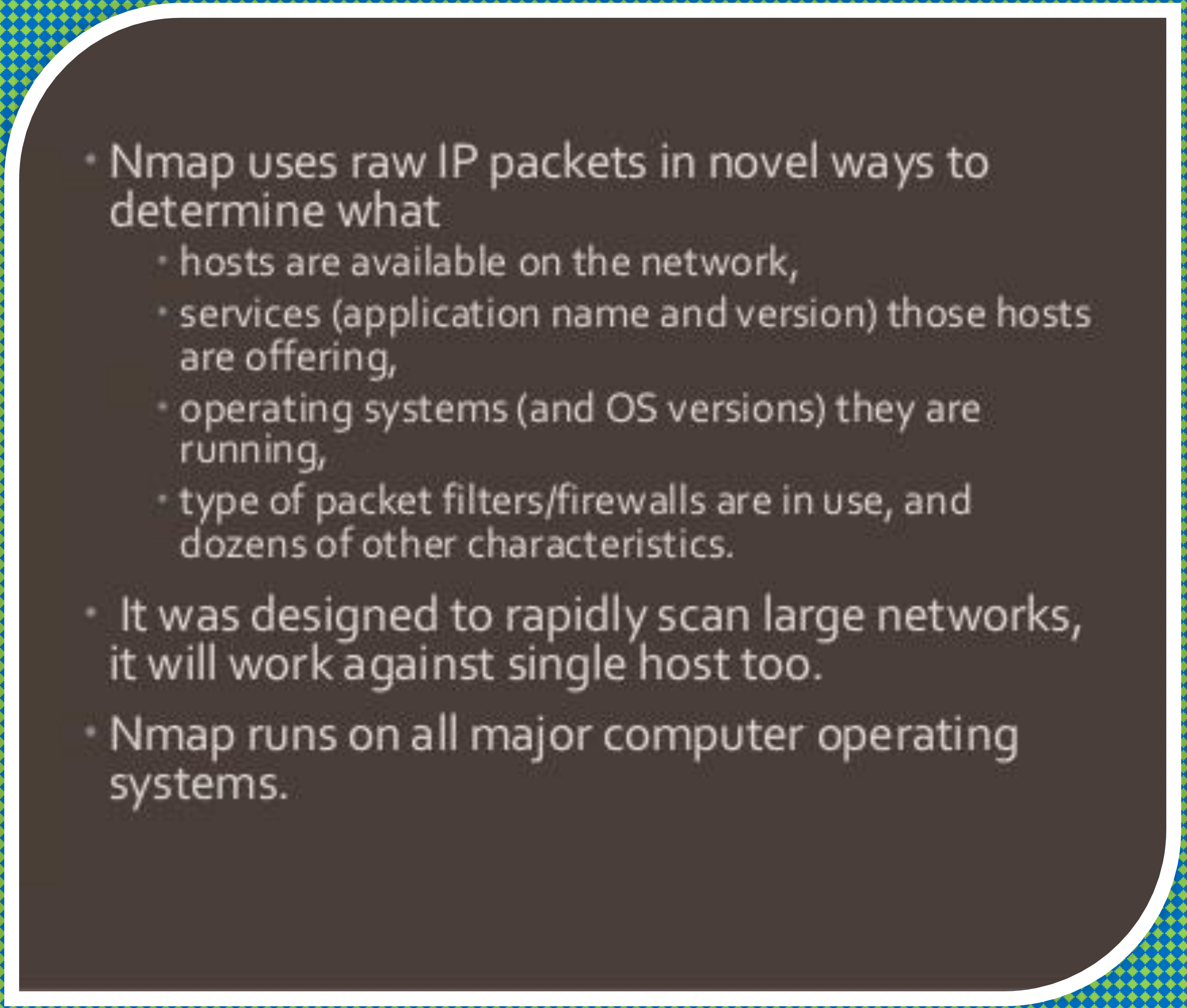
- Available for **UNIX** and **Windows**.
- **Capture** live packet data from a network interface.
- Display packets with **very detailed protocol information**.
- **Open and Save** packet data captured.
- **Import and Export** packet data from and to a lot of other capture programs.
- **Filter packets** on many criteria.
- **Search** for packets on many criteria.
- **Colorize** packet display based on filters.
- Create various **statistics**.

N-Map

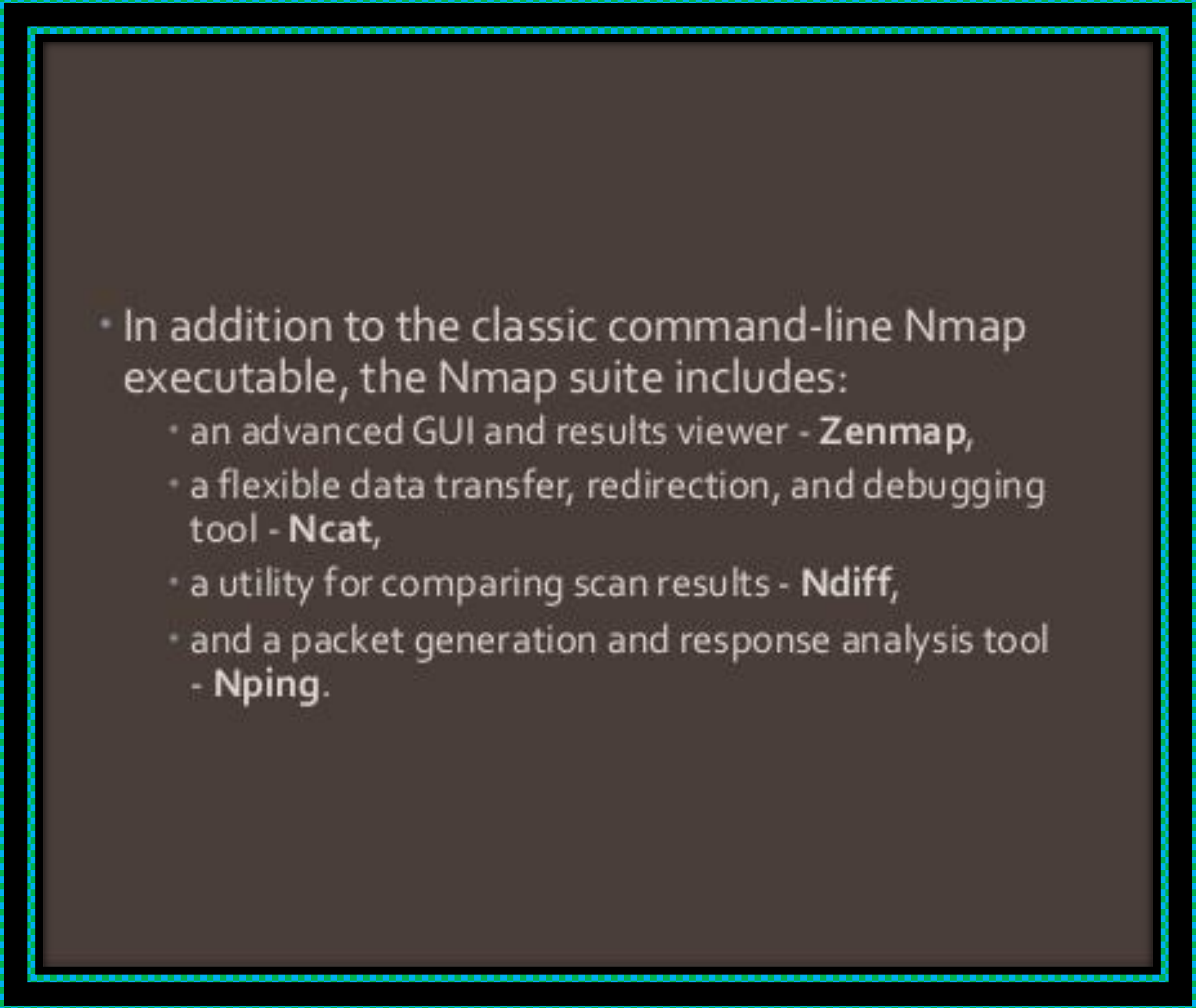


- Nmap → **Network Mapper** is a free and open source utility for network discovery and security auditing.
- Useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- Developed by Gordon Lyon.
- Turned 20 years on September 1, 2017!
- Current Version is 7.70.

Features

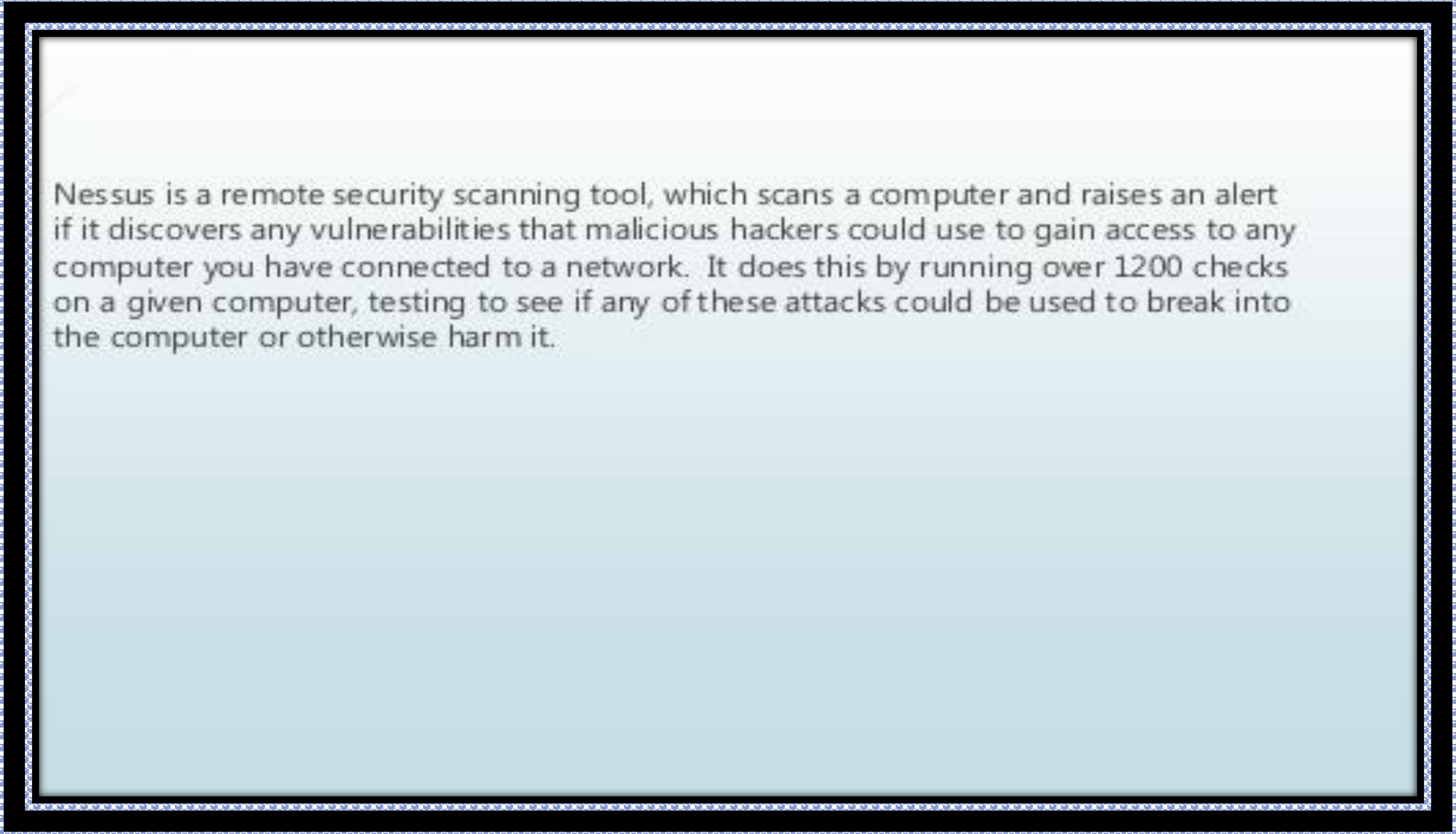


- Nmap uses raw IP packets in novel ways to determine what
  - hosts are available on the network,
  - services (application name and version) those hosts are offering,
  - operating systems (and OS versions) they are running,
  - type of packet filters/firewalls are in use, and dozens of other characteristics.
- It was designed to rapidly scan large networks, it will work against single host too.
- Nmap runs on all major computer operating systems.



- In addition to the classic command-line Nmap executable, the Nmap suite includes:
  - an advanced GUI and results viewer - **Zenmap**,
  - a flexible data transfer, redirection, and debugging tool - **Ncat**,
  - a utility for comparing scan results - **Ndiff**,
  - and a packet generation and response analysis tool - **Nping**.

Nessus

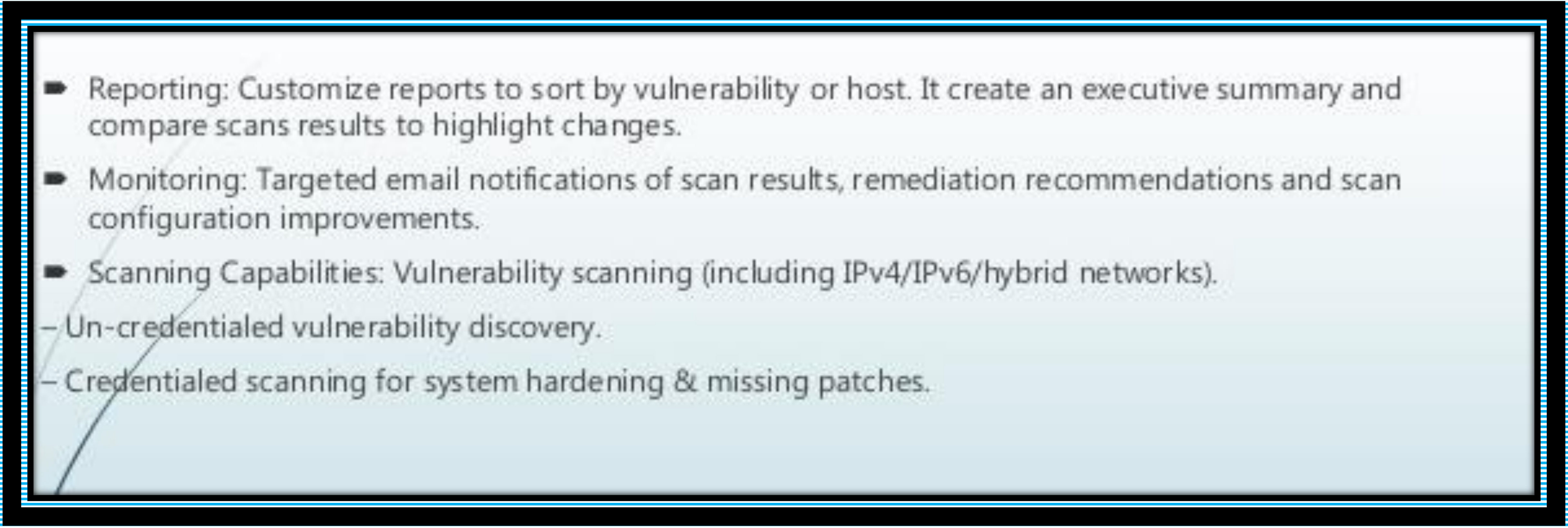


Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

FUNCTIONALITIES

- Basic Network Scan
- Malware Scan
- Mobile Device Scan
- Host Discovery
- Policy Auditing
- Drown Detection
- PCI External Scan

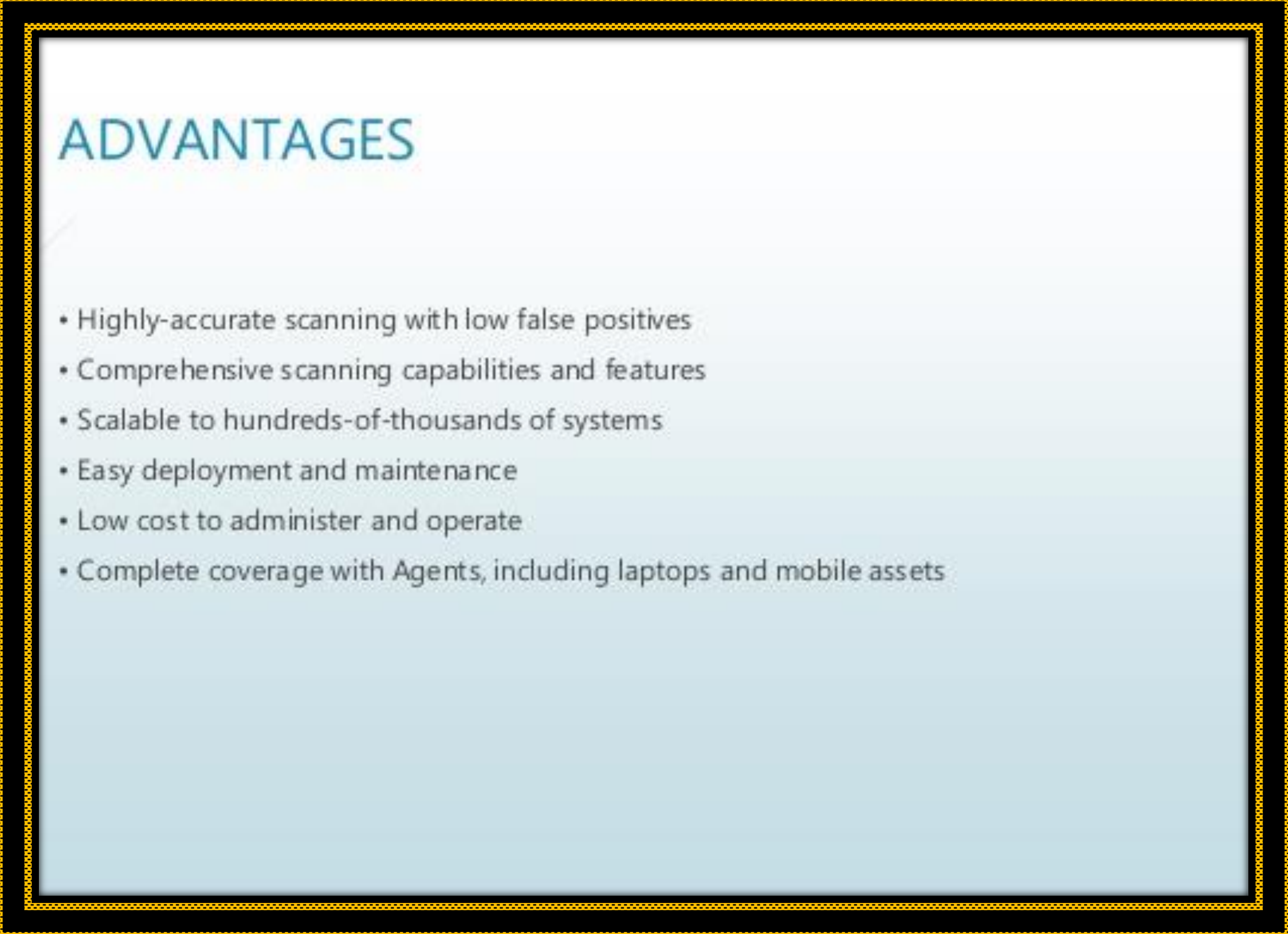
Features



- Reporting: Customize reports to sort by vulnerability or host. It create an executive summary and compare scans results to highlight changes.
- Monitoring: Targeted email notifications of scan results, remediation recommendations and scan configuration improvements.
- Scanning Capabilities: Vulnerability scanning (including IPv4/IPv6/hybrid networks).

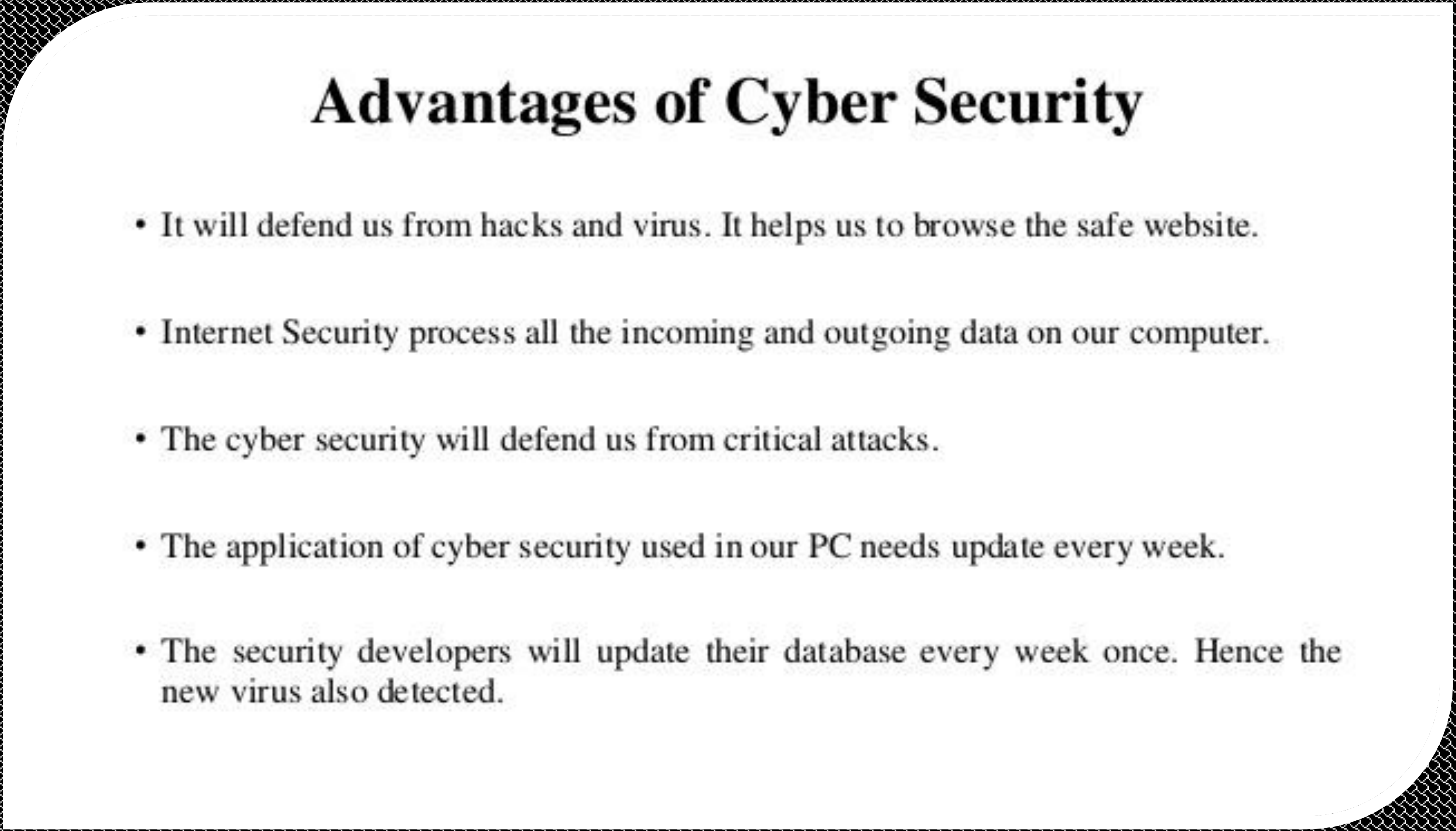
– Un-credentialed vulnerability discovery.

– Credentialed scanning for system hardening & missing patches.



ADVANTAGES

- Highly-accurate scanning with low false positives
- Comprehensive scanning capabilities and features
- Scalable to hundreds-of-thousands of systems
- Easy deployment and maintenance
- Low cost to administer and operate
- Complete coverage with Agents, including laptops and mobile assets



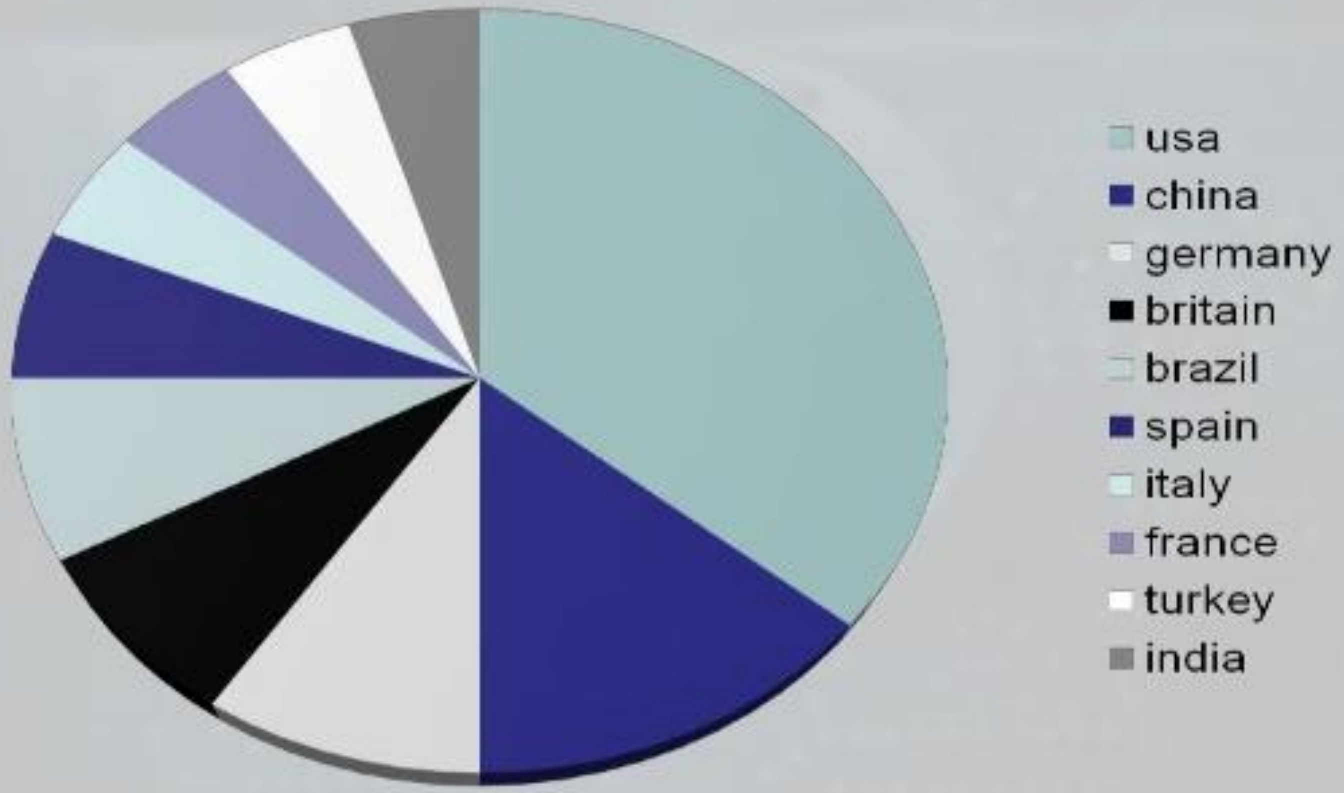
Advantages of Cyber Security

- It will defend us from hacks and virus. It helps us to browse the safe website.
- Internet Security process all the incoming and outgoing data on our computer.
- The cyber security will defend us from critical attacks.
- The application of cyber security used in our PC needs update every week.
- The security developers will update their database every week once. Hence the new virus also detected.

Safety Tips to Cyber Crime

- Use Antivirus Software.
- Insert Firewalls.
- Uninstall unnecessary software.
- Maintain backup.
- Check security settings.
- Never give your full name or address to strangers.
- Learn more about the internet privacy.

India stands 10th in the cyber crime in the world



References

- www.Wikipedia.org
- www.avtest.org
- www.billmullins.blogspot.com
- www.digit/forum.com
- www.antivirusnews.com

Thank you