Introduction to Management Information Systems

Information Assurance & Security: Attacks

Network Systems

networks - security

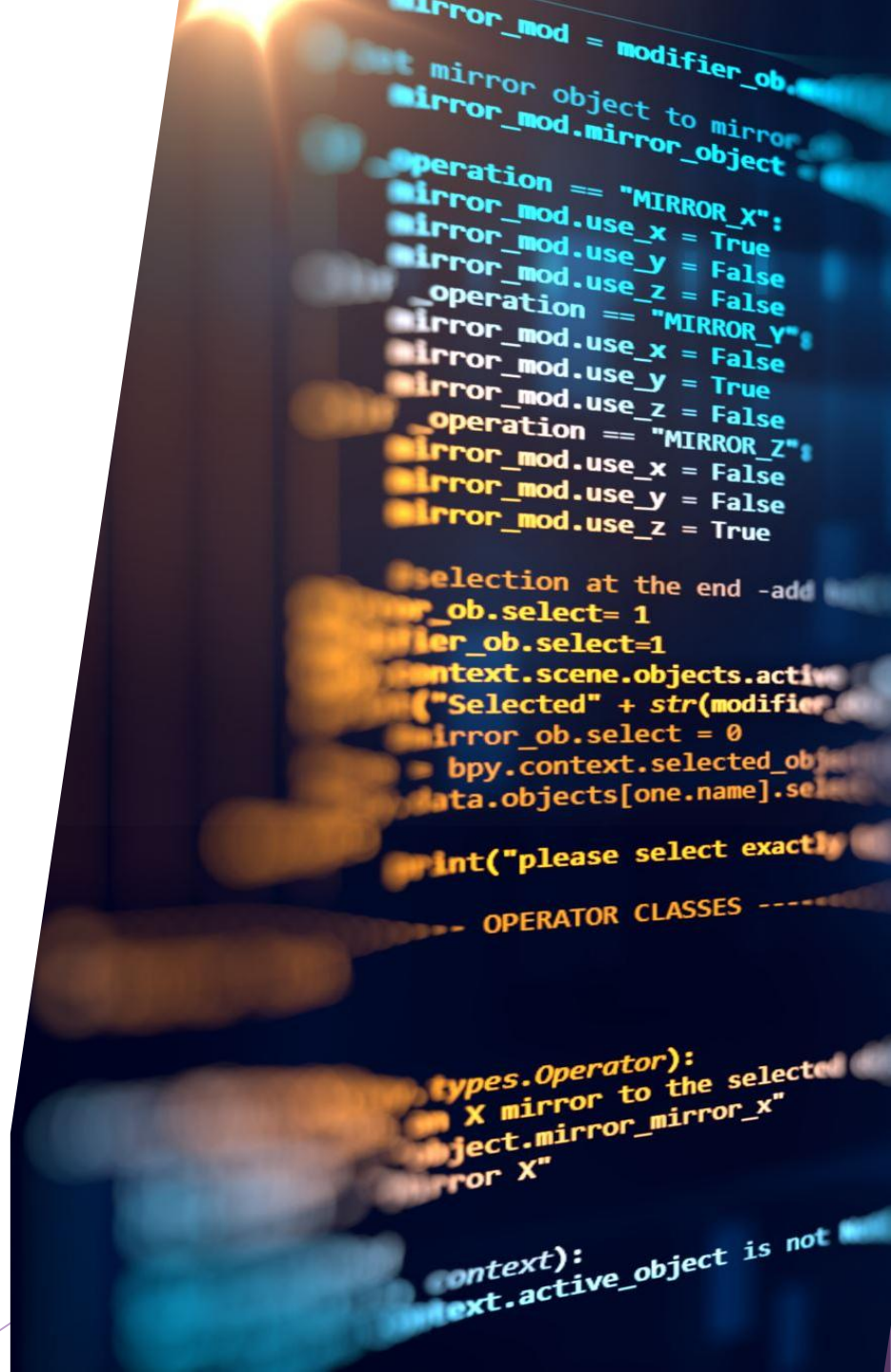
What are the issues?

malware (e.g. viruses)

hackers

malware

- Viruses: Self-replicating code that attaches to files.
- Worms: Standalone malware that replicates across networks.
- Trojans: Malicious software disguised as legitimate applications.
- Spyware: Software that collects user information without consent.
- Adware: Software that displays unwanted advertisements.
- Ransomware: Malware that encrypts files and demands payment for decryption.
- Rootkits (Backdoors)



Hacking Stages

Reconnaissance (Footprinting)
Gathering information about the target system or network.

Scanning
Using tools to discover open ports, services, and vulnerabilities.

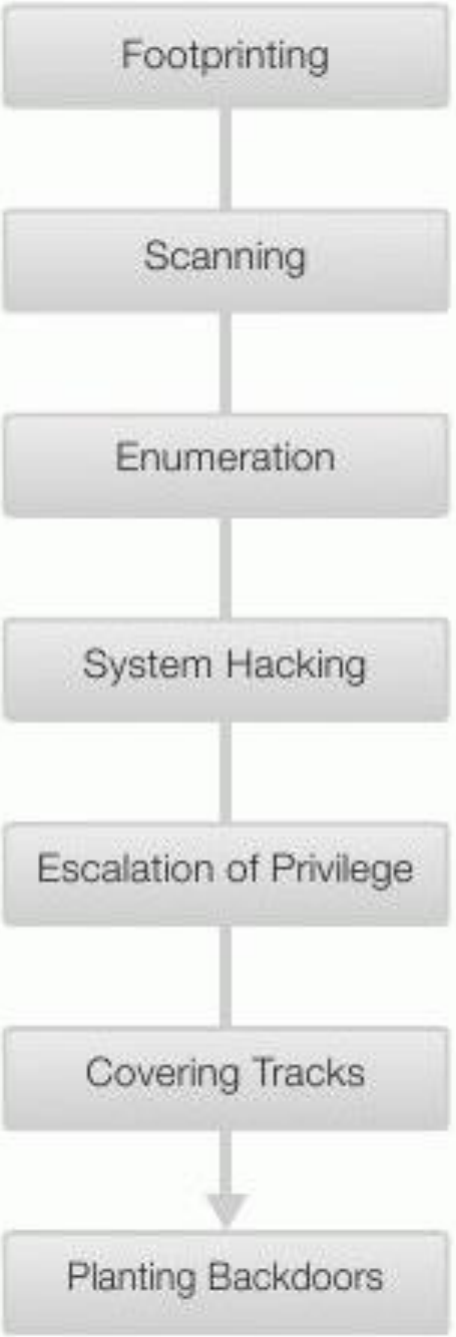
Enumeration
Actively probing for detailed information about the system, such as user accounts, network shares, and services.

Gaining Access
Exploiting vulnerabilities to breach the target system and establish control.

Escalation of Privileges
Increasing access rights to obtain administrative or root-level control.

Covering Tracks
Hide the intrusion by deleting logs, hiding files, and erasing evidence.

Maintaining Access
Installing backdoors, rootkits, or other tools to ensure continued access.



Attacks - malware

types of malware

malware

"Software that performs any action or activity without the knowledge of the system's owner"

- Inherently hostile, intrusive, or annoying
- Often resides on systems without detection
- Before – a prank, annoying
- Now – criminal

enforced new laws

US laws introduced include:

- The Computer Fraud and Abuse Act 1986
  - relates to federal, Government and financial matters
- The Patriot Act
  - is the collective damage over $5000?
  - up to 10 years, 20 years second offense

targets

- credit card data
- passwords
- inside information
- data storage – illegal / undesirable content
  - e.g. financial data, child pornography

categories of malware

Viruses

- term often used for all types of Malware
- A piece of code or software
- spreads by attaching itself to other files
- when the file is accessed, the virus is activated
- the code carries out the attack or action

Viruses

Creeper Virus 1971

- find new system, replicate and delete the old copy
- “I’m the creeper, catch me if you can.” message
- Reaper code used to remove the Creeper

- mid-70s Wabbit virus – replicated until the system crashed
- ‘82 ElkCloner – now infect inserted media
- ‘86 PC-virus – boot sector virus
- ‘87 logic bomb – Jerusalem virus (Friday 13th)

Types of Viruses

- Logic bombs
  - waits for an event before it “goes off”
  - commonly destroys data or systems
- Polymorphic viruses
  - can hide from anti-virus software
  - can change upon execution
  - 2 main types:
    1. polymorphic engines: change design not payload
    2. encryption

Types of Viruses

Multipartite viruses

- multiple targets e.g. boot infector, file infector
- can reside in multiple locations
- if any part remains it can re-infect

Macro viruses

- built into application e.g. Office VBA
- Macros used to automate tasks
- infects on opening apps
- can disable

Virus Prevention

Education

- don’t …. e.g. download, install, share
- inform IT
- ban / limit use of flash drives
- permissions

Antivirus

- keep up-to-date
- database of signatures
- can detect more than viruses
- monitor behavior / dictionary-based

Worms

- self-replicating software
- no user action is required
- self-contained, does not require a host
- infects over networks
- causes big damage
  - Slammer about $1billion in the first 5 days
- quickly
  - Slammer doubled every 8.5 seconds

Worms

- can carry a virus
- can transmit information from a victim system
- locates a vulnerability
- infects
- uses the system to spread to other systems
- can be designed to locate vulnerabilities
- signs include a slowdown as resources are consumed
- “cryptoviral extortion” – extorts money for the encryption key

Worms

- Operating systems (OS) with unpatched vulnerabilities
- OS vendors try to improve the product and supply patches
- need to apply patches immediately

- Zero-day exploit – vulnerabilities come with the software so can be exploited immediately

Worms - protection

- Education e.g. ILOVEYOU! – no it doesn’t!
- up-to-date anti-virus / anti-spyware
- built in firewalls

Spyware

- Software designed to collect and report information without the owner’s consent and knowledge
- Example of information:
  - browsing habits
  - keystrokes
  - software usage
  - general computer usage
- Target ads, steal personal information, can download other malware

Adware

- often used with spyware
- bombarded with ads
- software versions
  - free – with ads
  - not free – ad free
  - users pay not to have ads

Scareware

- malware tricks users to purchase or download dangerous software
- hide as anti-virus software,
- states there is a virus problem
- user clicks to solve the problem
- user unknowingly downloads infected files
- also
  - extortion –e.g. ransomware

Trojans

- A Trojan, or Trojan horse, is an old form of malware
- designed to give an attacker access to a victim’s system
- a program that carries something of hidden intent
- dangerous because they hide from detection
- usually used to open a backdoor

Trojans

- usually used to open a backdoor
- backdoors are openings that bypass normal security measures
- they allow undetected, unauthorized remote access

Trojan - Keystroke logging

- ‘Feds out-hack Russian hackers’
- hackers stole thousands of US credit card numbers
- hackers & server in Russia
- FBI created software to steal their username & password
- $100 software called ‘WinWhatWhere’ investigator
- software used is now called ‘keystroke logging’
- hackers entered their usernames & passwords
- all keystrokes were passed back to FBI

Trojan symptoms

- slow operation is the most common symptom
- unusual network traffic
- frequent crashes
- unusual changes in files
- changes in the screen or screensaver
- CD draw opens and closes
- mouse pointer moves unusually or disappears
- many others, ..,

Backdoors

- provide access despite security countermeasures
- provide undetectable access
- provide easy access, minimal effort and time
- common backdoors include:
  - password-cracking backdoors
  - Rootkits
  - services backdoor
  - process hiding backdoor

Backdoors

Rootkits

- attackers replicate existing files
- can replicate key system files
- then they have the ability to alter the system's behaviour

services backdoor

- use network services
- use open ports when used by these services

Backdoors

Covert

- unless you are looking for the hidden information you will not find it
- covert storage channels
  - writing to a location by one service
  - reading from the location by another service
- covert timing channels
  - manipulates the system's resources
  - e.g. CPU time or memory usage
  - a second service interprets these responses

Protection Software

Antivirus - looks for infections

Anti-spyware - looks for unusual behaviour

Firewalls - block attacks

Updates

Education

malware

- Delivery Methods
  - Phishing emails, malicious downloads, and compromised websites.

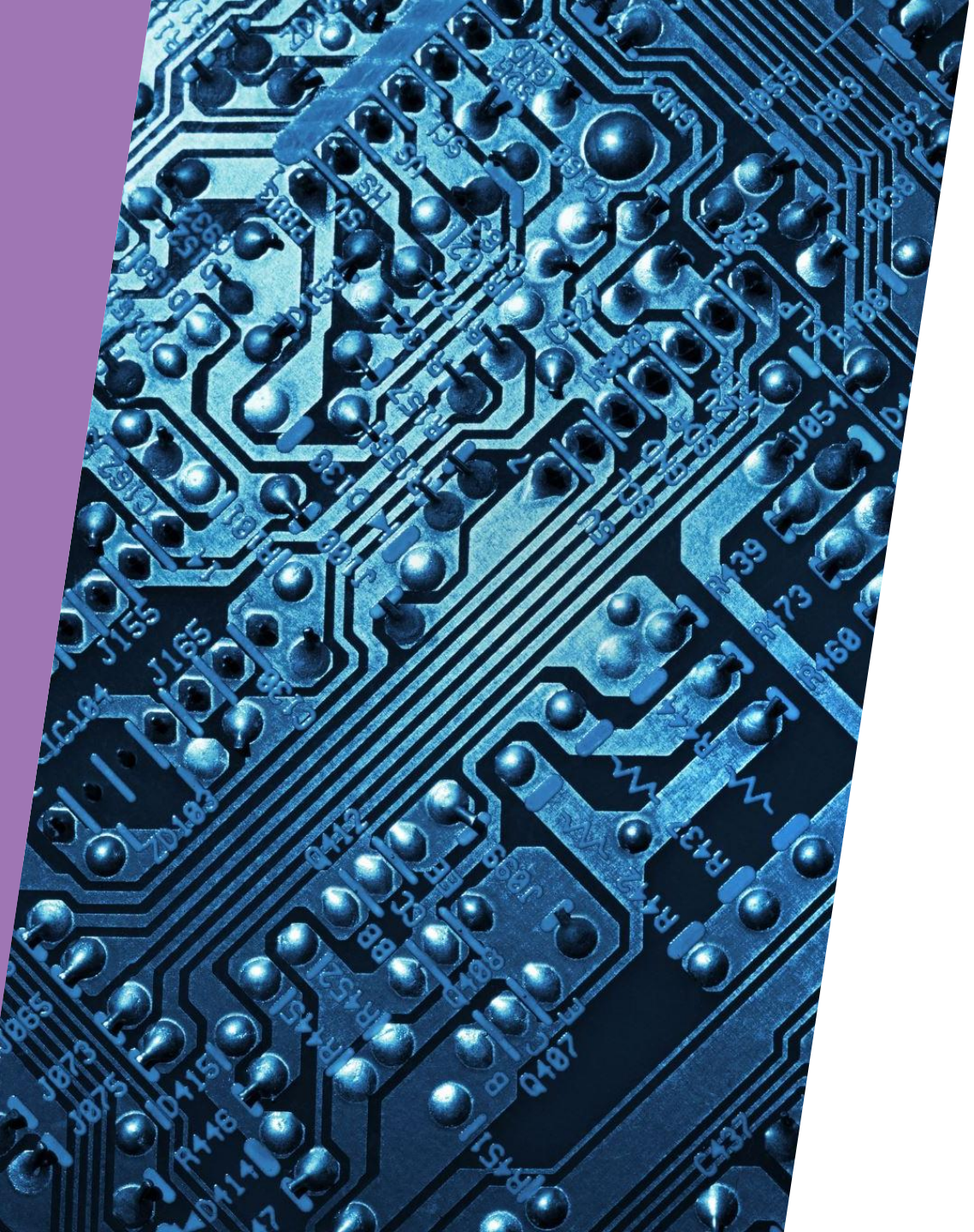
- Exploitation Techniques
  - Zero-day vulnerabilities and unpatched software as entry points for attacks.

- Advanced Techniques
  - Use of encryption to hide communication between malware and command-and-control servers.
  - Evasion tactics such as polymorphism and metamorphism.

Attacks - hacking

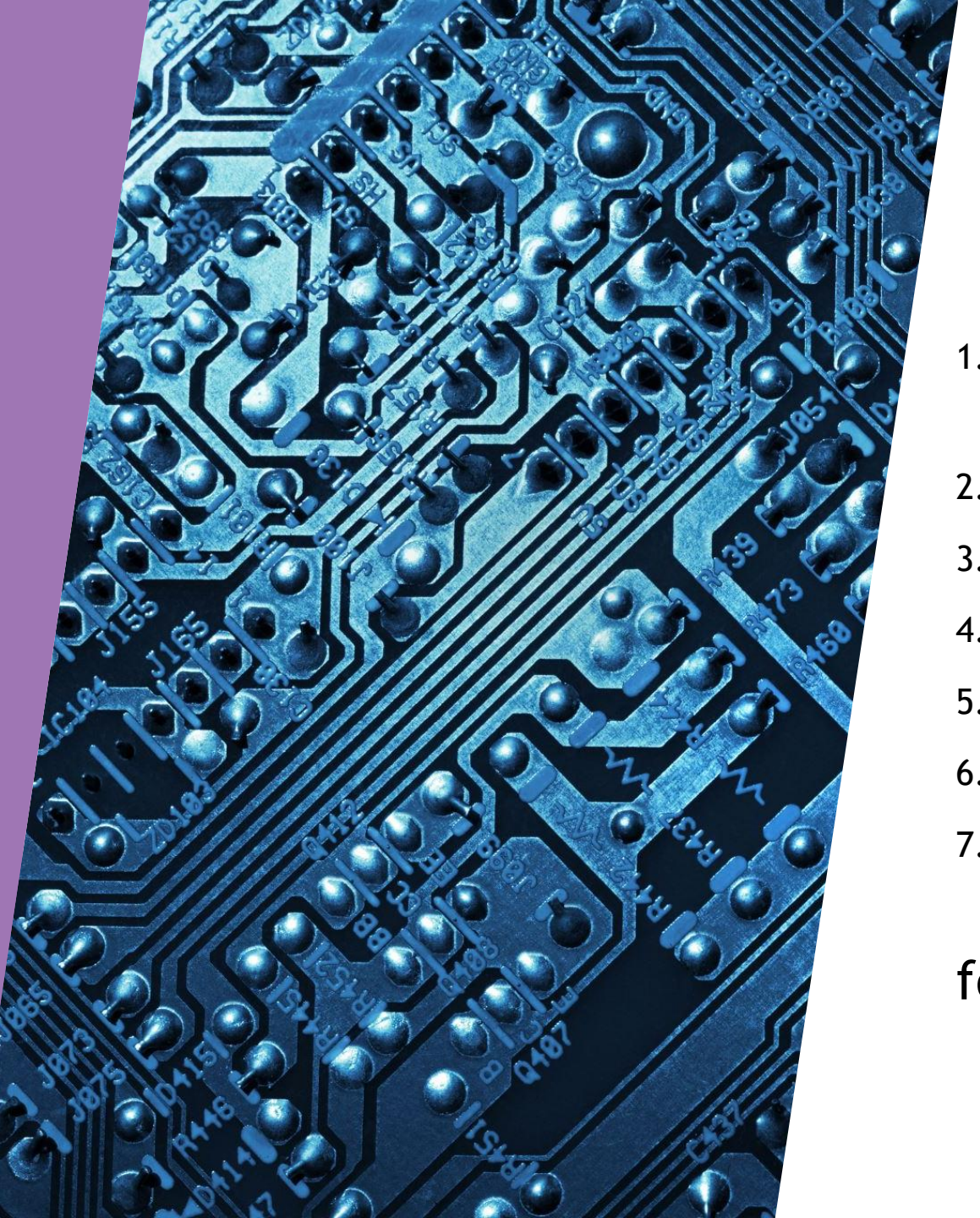
phrases of hacking

Footprinting, Scanning, and Enumeration



Footprinting

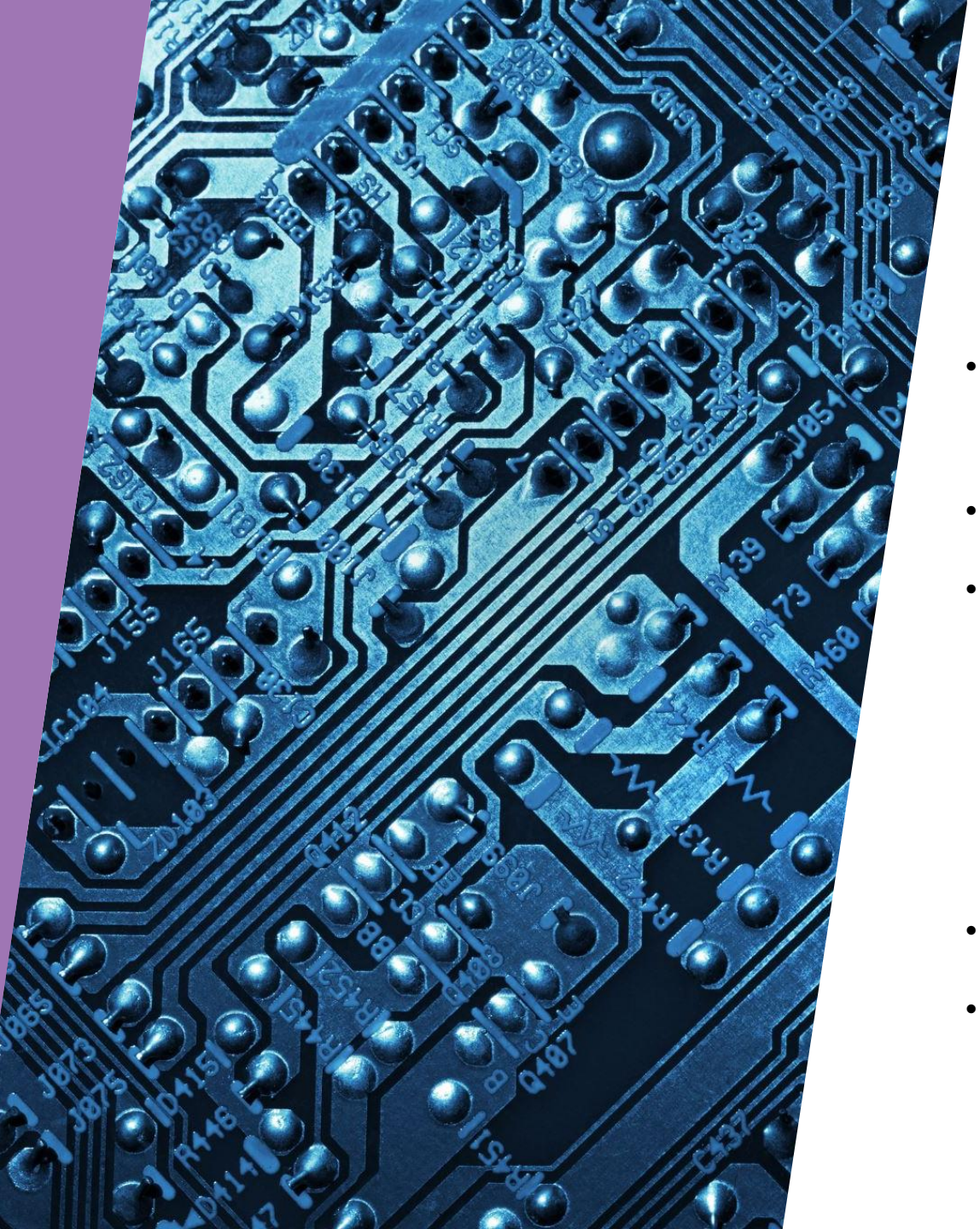
- effective hacking takes place in phases
- the first phase is the footprinting phase
- used extensively by profit-driven attacks
- process to passively gain information such as:
  - locations, network range
  - financial information
  - employee information (names & titles)
  - equipment & technologies used



Information Gathering

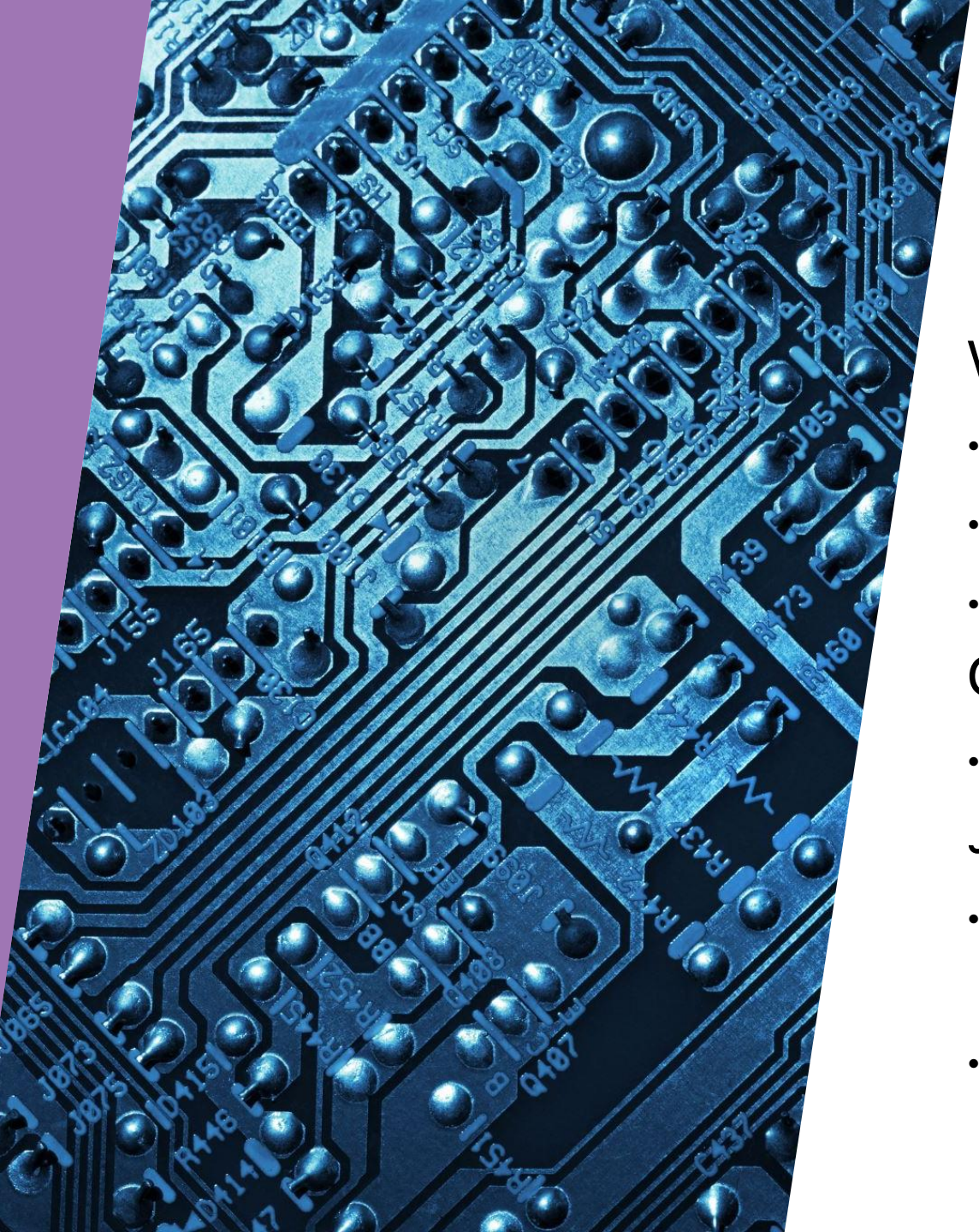
1. victim details e.g. assets, technologies, etc.
2. determine the network range
3. id target machines
4. find open ports & access points
5. id operating systems
6. using fingerprinting services
7. mapping the network

footprinting is a passive phase



Domain Information Leakage

- several sources of domain information
- Nslookup, traceroute, RIR, etc.
- Internet Assigned Numbers Authority (IANA) is responsible for the coordination of the DNS root, IP addressing and other web protocols
- use the root zone database
- Whois contains the network range



Countermeasures

Web site

- remove sensitive information
- restrict the use of contact details
- don’t give out system details

Google Hacking

- sanitize information

Job listings

- be generic or use third-party companies
- don’t list versions of applications

Port Scanning

- Footprinting gets a detailed picture of the victim
- What's next? answer: port scanning
- to identify open and closed ports
- to identify systems services that are running
- where and what course of action
- followed by mapping the network and
- looking for vulnerabilities

Pinging

- used to determine if a system is present, online
- an ICMP message
- reply is a ping reply or echo
- measure speed with TTL
- often blocked or switched off
- can scan multiple IP addresses (hence sweep)
- can scan entire network quickly
- will be picked up by a IPS or IDS

Mapping Open Ports

many tools can map open ports & identify network services

Nmap – most widely used & security requires Nmap knowledge

can use many switches to perform different scans

ports are open, closed or filtered

half open scanning does not complete the connection

Techniques & Tools

OS fingerprinting

- open ports do not mean vulnerabilities
- identifying the operating system allows an attack to be focused
- this is called OS fingerprinting (active or passive)
- OS have unique characteristics and use different responses

Fingerprinting

Active OS fingerprinting

- send specially crafted packets to the target system
- can use *fuzzy signature matching* – perform a series of tests to identify the operating system
- Nmap can be used for active OS fingerprinting

Fingerprinting

Passive OS fingerprinting

- monitors network traffic
- analyzes patterns to identify the OS (matches OS signatures)
- harder to detect
- takes longer, more traffic

Results analysis

- understand potential vulnerabilities and potential points of entry
- e.g. unsecure access points, unpatched web servers
  - analyze services
  - explore vulnerabilities
  - research potential exploits
- research potential exploits on the OS
- web pages list OS vulnerabilities
- have the information to plan an effective & devastating attack

Enumeration

- so far the processes show what the system look like
- but not what it has to offer
- enumeration takes the information gathered & attempts to extract information about the nature of the system
- involves interaction with the system
- usernames, group information, share names & other details
- enumeration is followed by system hacking (later)

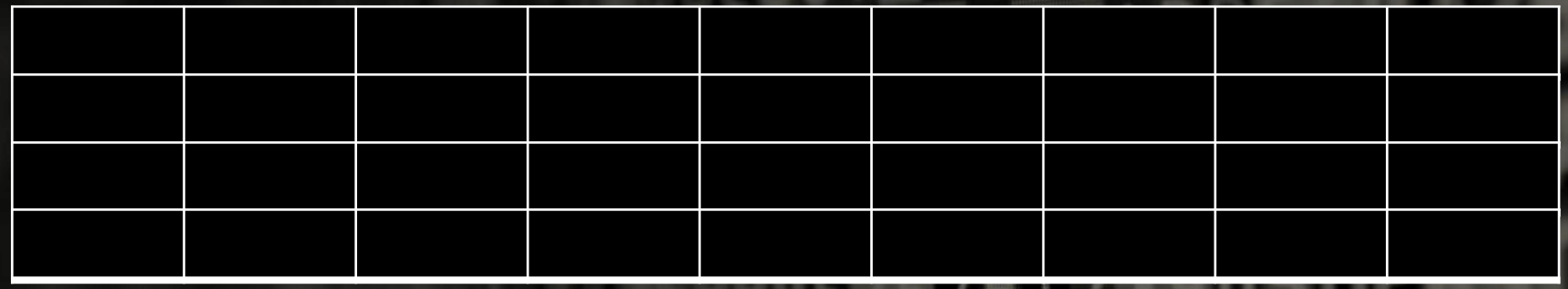
Windows?

Windows Security Account Manager (SAM)

where are all the ‘safely’ stored passwords on windows?

CVE-2021-36934, allowed local users to read the SAM file under certain conditions, exposing password hashes and enabling privilege escalation attacks

32-digit password



32-digit password (split into 4 = 4 * 8-digit password)

password

any number / digit (e.g. 0, 1, 2 to 9)

a) 32 character password
b) now split these into 4 x 8 character password

a) Time to crack a single 32-digit password: Approximately 3.17×10^{15} (1,000,000,000,000,000) years
b) Time to crack four 8-digit passwords concurrently: Approximately 0.1 seconds

password - digits

- 32 character password
- any letters, numbers or characters like punctuation (e.g. 100)
- takes 10^{61} years

- now split these into 4 x 8 character password
- any letters, numbers or characters like punctuation (e.g. 100)
- takes 284 days

types of hacking

network threats

network threats

sniffers e.g. Wireshark	• observing network traffic
session hijacking	• taking over the session
denial of service (DoS)	• shut down or deny use of a service • distributed DoS (DDoS) more than a single computer attacking the system, large-scale may involve a botnet

sniffers

passive sniffing

network with a hub

all traffic can be seen by all network devices

active sniffing

networks with a switch

not sent to the device therefore can’t be observed using passive sniffing

active sniffing

used to see traffic not directed towards the device

- e.g. network switch in use
- introduces network traffic
- therefore can be detected

MAC flooding (media access control)

- ARP poisoning (address resolution protocol)

MAC flooding

- switches have a lookup table
- stored in memory
  - content addressable memory (CAM)
- but the CAM is limited
- when flooded with MAC addresses the switch will fail-open
- a fail-open switch is effectively a hub
- now passive sniffing will observe all traffic
- there are several tools / methods used to perform flooding

ARP poisoning

- ARP used to resolve IP address / MAC address
- host broadcasts an ARP request
- so ARP resolves the logical address to the physical address for an interface (link)
- ARP packets can be spoofed to redirect traffic
- therefore ARP poisoning can intercept and redirect traffic to another device

ARP poisoning

- send ARP broadcast with a given IP address and the attacker's MAC address
- victim initiates communication
- traffic is forwarded to the given MAC address
- attacker forwards traffic back to the router / real destination

Session Hijacking

- active attack
- advances sniffing to take over the communication
- actively inject packets into the network to take over an existing session
- an existing session will have already passed the authentication phase

sniffing Defense

Encryption

- SSL
- IPSec

Port security (configure switches to static MACs)

Static ARP entries (difficult)

not all traffic needs protecting

network efficiency / speed a consideration

Denial of Service (DoS) Attacks

- older type of attack
- threat against availability
- simple so used by script kiddies
- was irritating but now serious
- adjusted to be used by criminals for extortion
- essentially DoS denies a service by overloading its resources

Bandwidth Use

Smurf

- uses ICMP, broadcast spoofed packets, sheer number of replies floods the network

Fraggle

- similar to Smurf except it uses UDP packets

Chargen

- protocol designed to test & evaluate networks
- can flood by creating traffic quickly

Bandwidth Use

SYN flood

- uses forged packets with the SYN flag set
- system connection resources overwhelmed

ICMP flood

- Smurf attack
  - give the victim as the return address source, all hosts respond to the victim & overwhelm
- Ping flood
  - send large amount of ping requests
  - attacker needs more bandwidth than the victim

Distributed Denial of Service (DDoS) Attacks

- DoS involving many compromised machines
- can be hundreds or thousands of devices
- impact increased over DoS multiplying strength & power
- primary victim – recipient of the attack
- secondary victim – used to launch the attack
- difficult to track back because of sheer numbers involved
- defense is difficult – router configuration can block same-address traffic for only a small number of attacks

A large, well planned and executed DDoS is nearly impossible to stop

Botnets

- systems infected with software used in DDoS attacks
- A ‘bot’ is a type of malware that allows the attacker to take control over an affected computer.
- Bots normally are part of a network of many bots (botnets) that can be worldwide
- used for
  - DDoS
  - spam
  - stealing information
  - click on ads – generates revenue

types of hacking

system hacking

system hacking

- Hacking initially involves footprinting, scanning and enumeration – we have seen
- with this information the hacker can attack the system
- the hacker has details about user accounts and groups
- these provide points on the target of the system to concentrate efforts
- now the weaknesses are exploited

passwords

- have information on user accounts
- to gain access the attack just needs the password
- passwords are usually easy to remember so can be
  - only letters or only numbers
  - only lower case or upper case
  - use proper names
  - use dictionary words
  - short (8 characters or less)

passwords

passive online attacks

active online attacks

offline attacks

nontechnical attacks

passwords – active online

- brute force
  - all possible combinations are attempted
  - successful with time
- dictionary attacks
  - restricts selections to a predefined list
  - attempts words in reverse form, character changes and additional characters appended
- generally stopped by limiting users password attempts

passwords – offline

- rely on weaknesses on how passwords are stored
- not encrypted – where is it?
- encrypted or protected – how is it encrypted or protected?
- can use brute force, dictionary and a hybrid of the two
- dictionary attacks look for the hashes of the list values
- a question of complexity and time
- countermeasures include salting
  - add on characters before hashing passwords

Techniques & Tools

Using password cracking

- cracked passwords normally have low level access
- if so then the next stage is privilege escalation
- passwords are stored, therefore identify a high level access account and change it’s password
- several utilities available to do this
  - e.g. Active@ Password Changer

Techniques & Tools

Planting Backdoors

- escalating privileges is followed by planting a backdoor to allow future access
  - place a rootkit
  - execute a Trojan
- if an attacker has a high level access account (Administrator) this is simple
- run an application remotely
- several tools available e.g. PsTools

Techniques & Tools

Rootkits

- made popular by Sony (s/w prevented music copying)
- alters system files and utilities
- ability to hide
- benefits from the scope of access gained (root access)
- attacker effectively ‘owns’ the system
- even the administrator may not be able to detect the rootkit
- is an application & can be run remotely

Techniques & Tools

Rootkits allow:

- install a virus
- place a Trojan
- install spyware e.g. keylogger
- hide an attack controls the system's behaviour
- maintain (long term) access
- monitor network traffic install a sniffer
- block the logging of certain events
- redirect output

Techniques & Tools

Covering Tracks

- attacks can be detected
- hackers cover their tracks
- all evidence of the attack is removed

Disabling Auditing

- best not to have any tracks to cover
- disable auditing
- can be done remotely or via several tools
- IDS systems detect audit policy changes

Techniques & Tools

Covering Tracks – hiding data

- hide the relevant system files
- OS provides services to hide files
- file attributes can be changes to hide files
- Windows HTFS features can be used to hide files
- these files are not detected by normal system processes
- simple
- hidden well and easy to restore (for the attacker)
- there are tools to locate these files
  - if you know you are looking for them

System Hacking Conclusion

- Sniffers capture (sniff) network traffic
- Session Hijacking advances sniffing to take over the communication
- A denial of service (DoS) shuts down or denies use of a service
- System hacking includes password cracking
- such as passive or active online attacks, offline attacks or nontechnical attacks

nontechnical attacks

- use the user not the system
- shoulder surfing
  - observe a person entering a password (read the post-it!)
- keyboard sniffing
  - use keylogging software
- social engineering
  - trick the user to giving out the password

Human Attacks

- Piggybacking and shoulder surfing
- Dumpster diving
- Installing unauthorized hardware and software
- Access by non-employees
- Social engineering
- Reverse social engineering

Reverse Social Engineering

- An alternate approach to social engineering is called reverse social engineering.
- Here, the attacker hopes to convince the target to initiate the contact.
  - The attack may be successful because the target initiates the contact.
  - Attackers may not have to convince the target of their authenticity.

types of hacking

wireless, web & database security

Techniques & Tools

rogue APs

- ignorance e.g. unauthorized AP installation
- on purpose e.g. evil twin
- Promiscuous Client
  - may use strong signal to attract victims
  - e.g. Las Vegas

Web Servers - risks

- poor web design
  - information in the comments
  - hidden fields holding information
    - e.g. item price – attacker can change

Web Servers - risks

- buffer overflow
  - when an application attempts to put more data in a buffer than it can hold
  - created in the code (unrestricted buffer)
  - causes corruption, lost integrity

Techniques & Tools

Web Servers - risks

- SQL injection
  - SQL engine processes unintended commands
  - can reveal information
  - attack ‘injects’ code
  - unauthorized access
  - alter data

Techniques & Tools

SQL Injection

- countermeasures
  - input validation
    - whitelist – safe characters
    - blacklist – unsafe characters

Techniques & Tools

Web page - defacement

- Cross-site Scripting (XSS)
  - attacks the user
  - uses a scripting language
  - inject code
  - example
    - email to victim
    - victim goes to web site
    - web site runs the script on the victim

Techniques & Tools

Databases

- heart of many web applications
- contain password, configuration, web page content, and personal information
- can be hidden e.g. within an application bundle
- need to find these databases
  - identify databases
  - *can be used to crack passwords*

case studies

Stanley Mark Rifkin (1978)

- In 1978, when Stanley Mark Rifkin stole $10.2 million from the Security Pacific Bank in Los Angeles:
  - He was working as a computer consultant for the bank.
  - He learned details on how money could easily be transferred to accounts anywhere in the United States.
  - He transferred the money to another account in Switzerland under a different name.
- The crime might have gone undetected if he had not boasted of his exploits to an individual.

WannaCry Ransomware Attack

- occurred in May 2017
- exploited a vulnerability in Microsoft Windows known as EternalBlue,
  - which was developed by the NSA.
  - that allowed users to gain access to any number of computers connected to a network
- WannaCry encrypted user files and demanded payment in Bitcoin for decryption keys.
- It spread rapidly due to its worm-like capabilities, allowing it to propagate across networks without user intervention.
- It infected over 230,000 computers across 150 countries,
- affecting critical services such as the UK's National Health Service (NHS), causing significant disruptions.

NotPetya Attack

- NotPetya emerged in June 2017
- initially appearing as ransomware but was later identified as a destructive malware designed to cause damage rather than generate profit
- It primarily targeted Ukraine but quickly spread globally, affecting major corporations like Maersk and Merck, leading to billions in damages.
- NotPetya utilized similar exploits as WannaCry but also leveraged legitimate software tools to spread within networks.

Equifax Data Breach

- In September 2017, Equifax announced a massive data breach that exposed sensitive information of approximately 147 million individuals.
- The breach was attributed to an unpatched vulnerability in Apache Struts, a web application framework.
- Attackers exploited this vulnerability to gain access to Equifax's systems over several months before detection.
- The breach included names, Social Security numbers, birth dates, addresses, and in some cases, driver’s license numbers.

Thank you!

any questions?