



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Hacking



*Advanced Cybersecurity
(ACCB6000)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



Previous sessions...

- *Understanding Information Security, Risks involved, assessing, managing and monitoring Risks, Cyber risk resilience*
- *Purpose and role of Hackers, Penetration Testing, Various Laws and Standards*
- *Understanding Footprinting and Reconnaissance Concepts, Methodology.*
- *Using various Tools, Taking Countermeasures*

So far, we discussed about Information security, the threats and attack vectors. In continuation to that, I hope you all have understood the hacking concepts and the reasons to stay ethical. Add more insight, we also discussed various security laws and standards. To conclude, we covered various “Risk” concepts like risk factors, cyber risk resilience in the process of enhancing security.

In continuation, we discussed Footprinting concepts focusing on different methodologies like Search Engines, Google Hacking Techniques etc. giving a walkthrough on Website Footprinting, Email Footprinting, Competitive Intelligence, Network Footprinting etc.

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*



Previous sessions...

Scanning and Enumeration

- Network Scanning, Tools and Techniques
- Banner Grabbing
- Scanning – PenTesting

Enumeration

- Concepts, Techniques
- Countermeasures

Understanding and Assessing Vulnerabilities

- What is Vulnerability? How is it classified?
- Assessing Vulnerabilities.
- Managing Vulnerabilities

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

Continuing the earlier lectures, we discussed on Network Scanning, different tools and methodologies used like Banner Grabbing and mitigation methods etc. following that enumeration concepts, its different tools and techniques were discussed. we continued focusing on assessing vulnerabilities within a network (either it is our target to attack or defend), different tools used to assess and techniques

During the tutorials, under isolated lab environment you might have practiced different Footprinting, scanning, enumerating methods using various tools and assessed the vulnerabilities.

Lab/ Tutorials

- Activity 1: Download and Setup your Lab.
- Coursework Description.
- Activity 2 Information Gathering
- Activity 3 Vulnerability Assessment
- Activity 4 – Methods to Exploit Vulnerabilities



Gaining access and escalating privileges

- *Hacking Methodology (Based on CEH)*
- *Understanding techniques to gain access to the system*
- *Techniques to escalate privileges*

Lab/Tutorials

- *Activity 4 – Methods to Exploit Vulnerabilities*

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

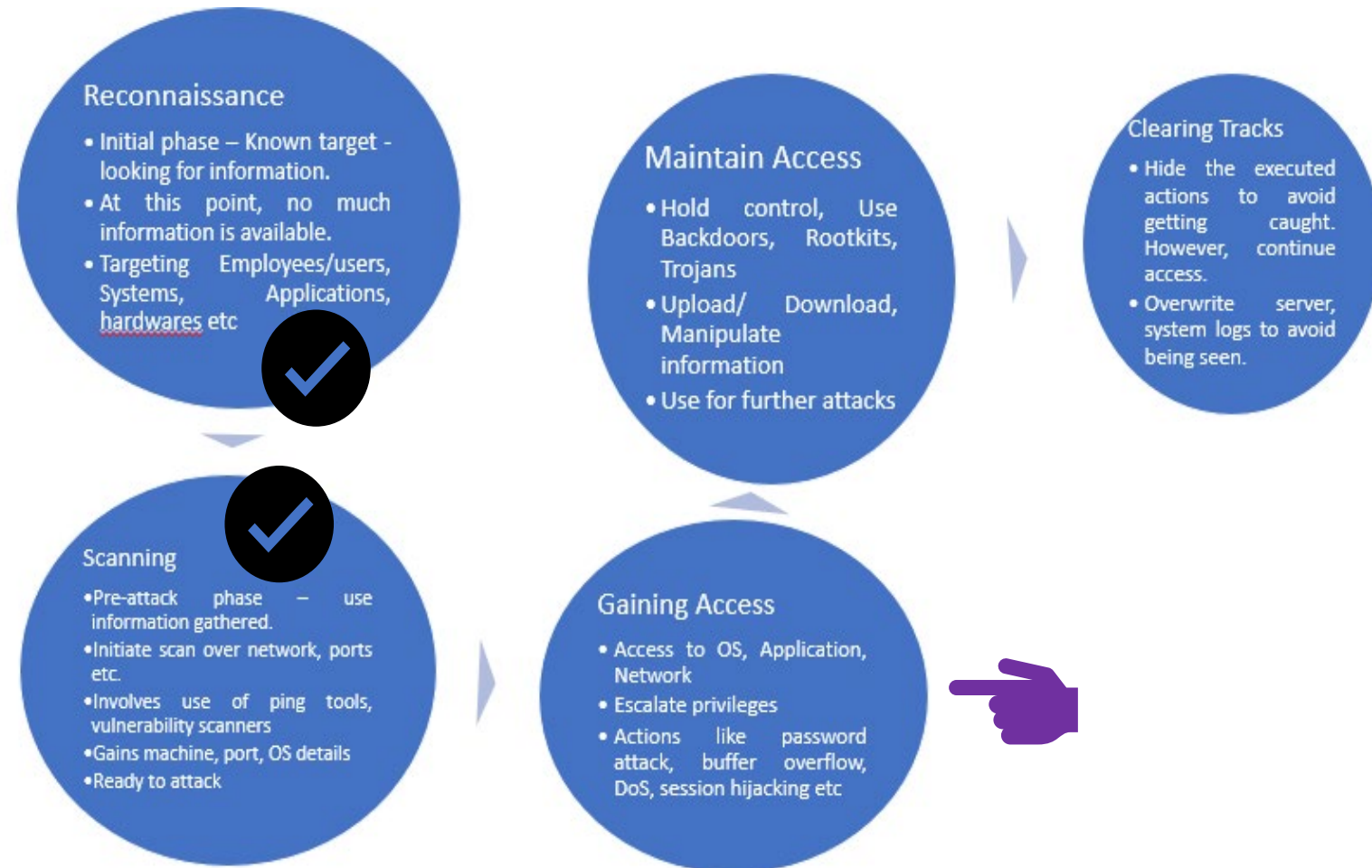
During this week, with applied knowledge and understanding on Footprinting, Network Scanning, Enumerating the target, and assessing vulnerabilities, we shall move forward focusing on the hacking methodology. We shall understand various techniques to gain access, escalate privileges, create and maintain remote access to the target.

During the tutorials, under isolated lab environment you will be using different techniques to gain access and escalate privileges.

Hacking - Methodology

○ Do you remember the process?

- ✓ Footprinting and Reconnaissance
- ✓ Scanning
- ✓ Enumeration
- ✓ Vulnerability Analysis
- Gaining Access
- Maintaining Access
- Clearing Logs



Hacking - Methodology

- Do you remember the process?
 - ✓ Footprinting and Reconnaissance
 - ✓ Scanning
 - ✓ Enumeration
 - ✓ Vulnerability Analysis
 - Gaining Access
 - Maintaining Access
 - Clearing Logs

Gaining Access

Cracking Passwords



Escalate Privileges

Maintaining Access

Executing Applications



Hiding Files

Clearing Logs

Cover your tracks



Hacking - Methodology

- Gaining Access
 - To bypass the access control systems and gain access into the target system
 - Techniques like Password cracking, Social Engineering helps to gain access
- Privilege Escalation
 - To get rights of a legitimate user or administrator
 - Techniques like vulnerability exploitation helps to escalate privileges
- Execute Application
 - To create and maintain remote access to the target system
 - Trojans, Spywares, Backdoors, Keyloggers help to execute applications
- Hiding Files
 - To hide your presence in the target system
 - To hide the attackers' malicious activities and data theft
 - Rootkits, Steganography helps to hide files
- Covering Tracks
 - To hide the evidences
 - Clearing the logs

Gaining Access – Password Cracking

- Gaining Access

- To bypass the access control systems and gain access into the target system
- Techniques like Password cracking, Social Engineering helps to gain access
- The primary intention of cracking passwords is to recover them. However, it could be used on a wrong intention to gain unauthorized access to the target system
- Password Cracking won't be always successful. It depends on the strength and nature of passwords been placed on a system

- Types

- ✓ Non – Electronic Attacks
- ✓ Online Attacks
 - ✓ Active
 - ✓ Passive
- ✓ Offline Attacks

Gaining Access – Password Cracking

- **Non – Electronic Attacks**
 - Social Engineering Attacks
 - Shoulder Surfing
 - Dumpster Diving

- **Active Online Attacks**
 - **Default Passwords**
 - Password Guessing
 - Trojans, Spyware, Keylogger
 - LLMNR/NBT-NS Poisoning

Default Passwords

Search Passwords

531 vendors, 2117 passwords

[@passdb on Twitter](#) / [Firefox Search](#)

1. Fortinet - FortiGate	
Method	Serial Console
User ID	maintainer
Password	pbcpbn(add-serial-number)
Level	Administrator
Doc	
Notes	You must have physical access to the system.

2. Fortinet - FortiGate	
Method	Serial Console
Password	bcpb(serial number of the firewall)
Level	Administrator

[Home](#) > [Brocade](#) > Fabric OS - All

🔍 Brocade - Fabric OS - All

Default username, password, ip...

	User name	Password	Description
🙄	root	show me!	- Gigabit SAN (by Nicolas Gregoire)n- Admin access (Multi)

Username root

Password fivranne

Notice - Gigabit SAN (by Nicolas Gregoire)n- Admin access (Multi)

👍 Its working!

👎 Not working

Gaining Access – Password Cracking

- **Non – Electronic Attacks**

- Social Engineering Attacks
- Shoulder Surfing
- Dumpster Diving

- **Active Online Attacks**

- Default Passwords
- **Password Guessing**
- Trojans, Spyware, Keylogger
- LLMNR/NBT-NS Poisoning



More time required.
Probability of success
is very less.



Target a User

Create a list of passwords

Rank the passwords

Test the password

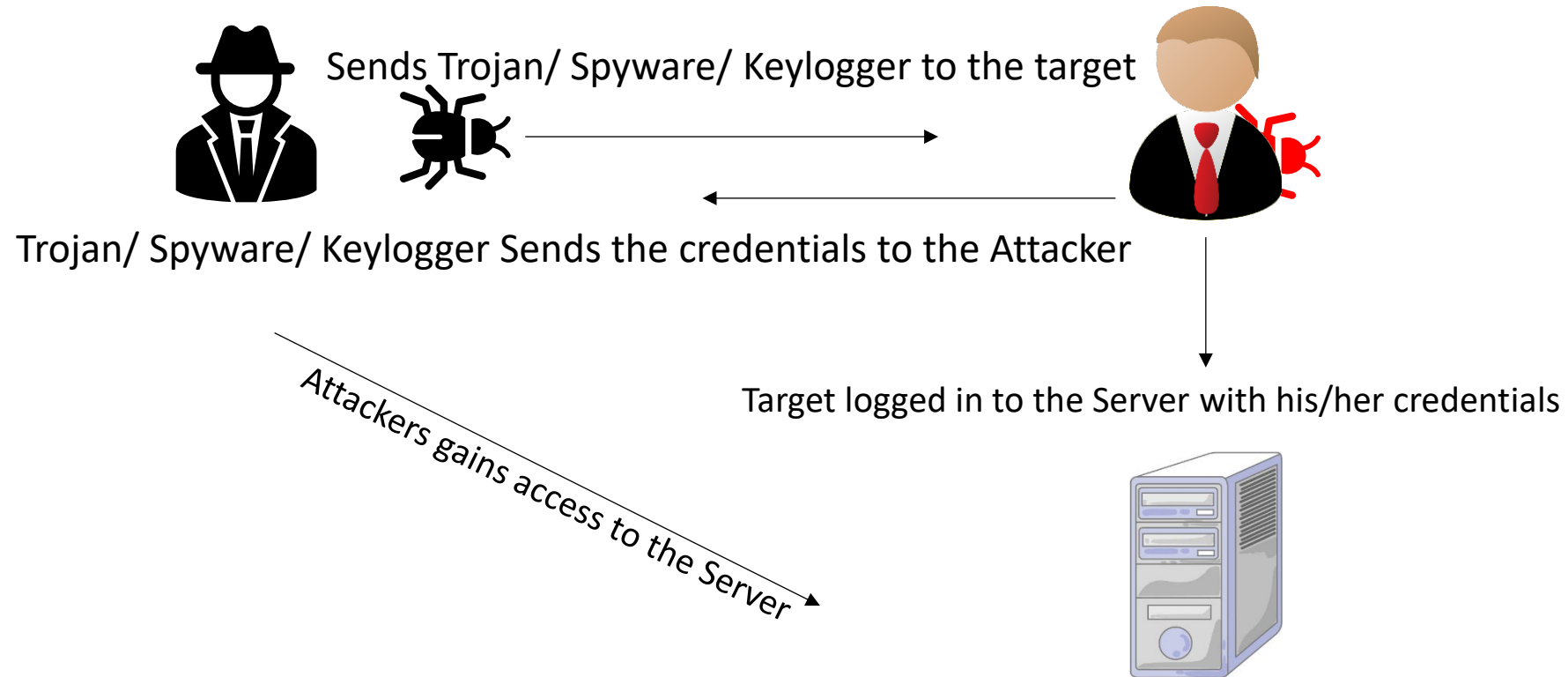
Gaining Access – TSK

- **Non – Electronic Attacks**

- Social Engineering Attacks
- Shoulder Surfing
- Dumpster Diving

- **Active Online Attacks**

- Default Passwords
- Password Guessing
- **Trojans, Spyware, Keylogger**
- LLMNR/NBT-NS Poisoning



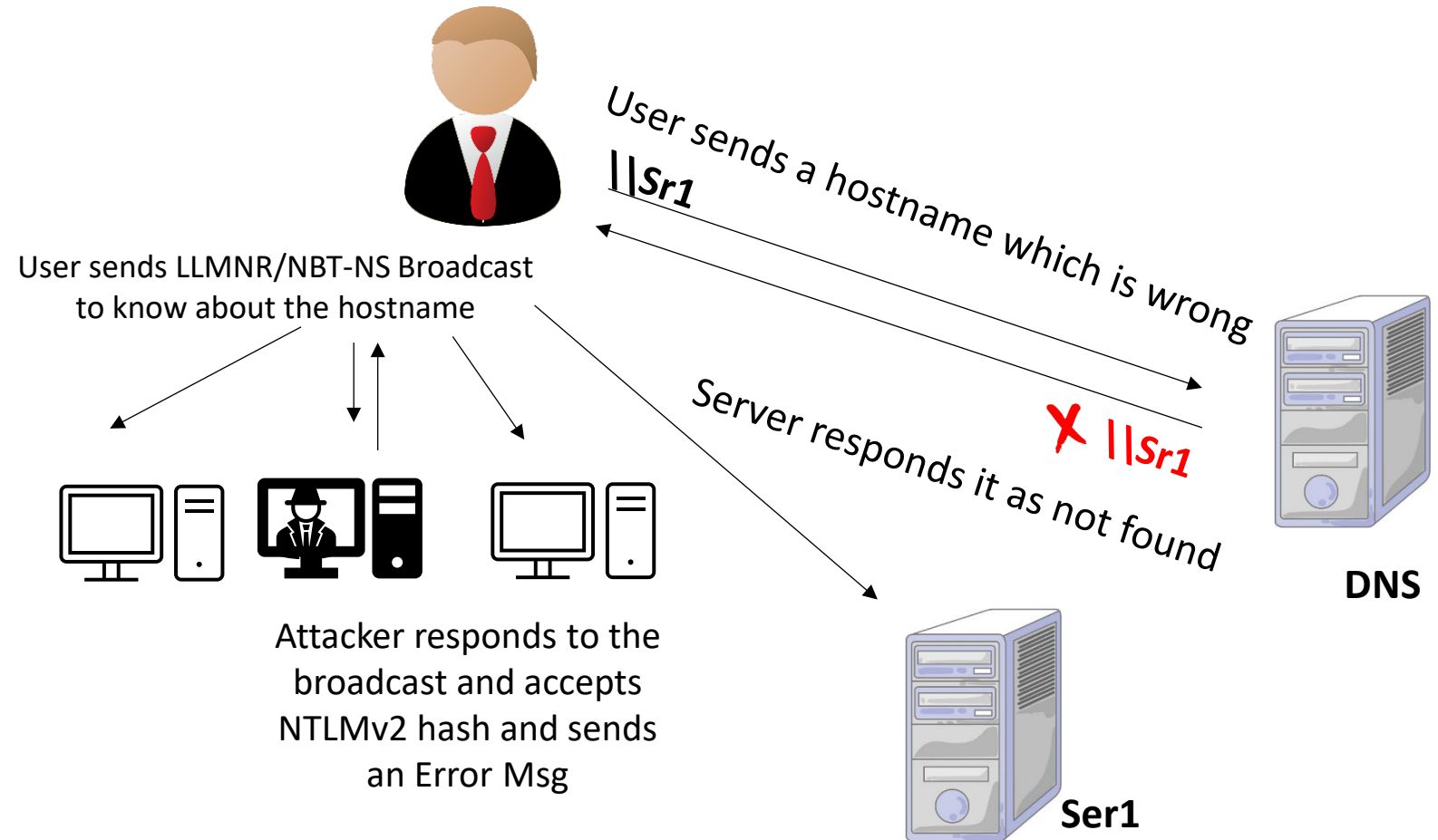
Gaining Access – Name Resolution Services

- **Non – Electronic Attacks**

- Social Engineering Attacks
- Shoulder Surfing
- Dumpster Diving

- **Active Online Attacks**

- Default Passwords
- Password Guessing
- Trojans, Spyware, Keylogger
- **LLMNR/NBT-NS Poisoning**



Gaining Access – Passive Attacks

- **Non – Electronic Attacks**

- Social Engineering Attacks
- Shoulder Surfing
- Dumpster Diving

- **Active Online Attacks**

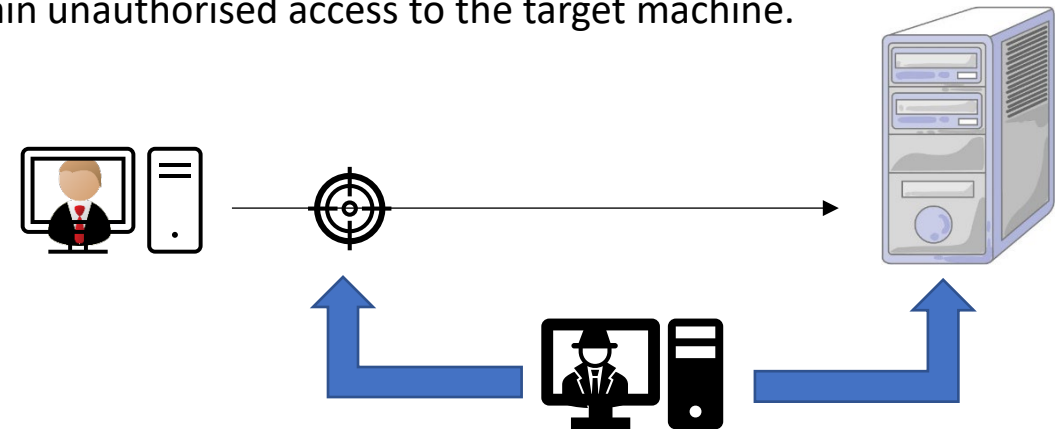
- Default Passwords
- Password Guessing
- Trojans, Spyware, Keylogger
- LLMNR/NBT-NS Poisoning

- **Passive Online Attacks**

- **Wire Sniffing**
- **Man-in-the-Middle and Replay Attack**



- ❑ Attacker uses packet sniffing tools to gain access and observe the traffic within the network.
- ❑ Sensitive data traffic (FTPs, rlogins, passwords etc) are later used to gain unauthorised access to the target machine.



- ❑ Attacker gains access to the communication channels between victim and target server to gather information.
- ❑ With gathered information, a replay attack may be initiated using the tokens to gain access to the network.

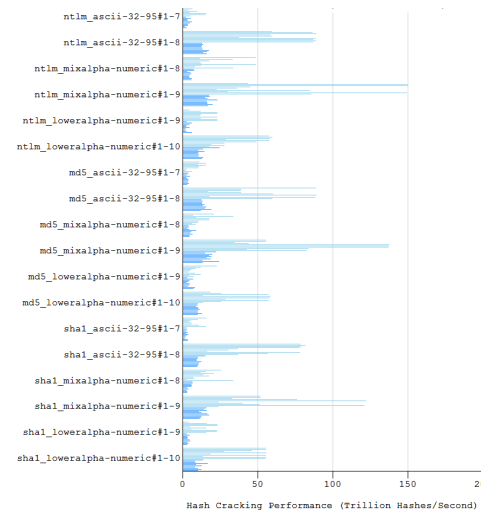
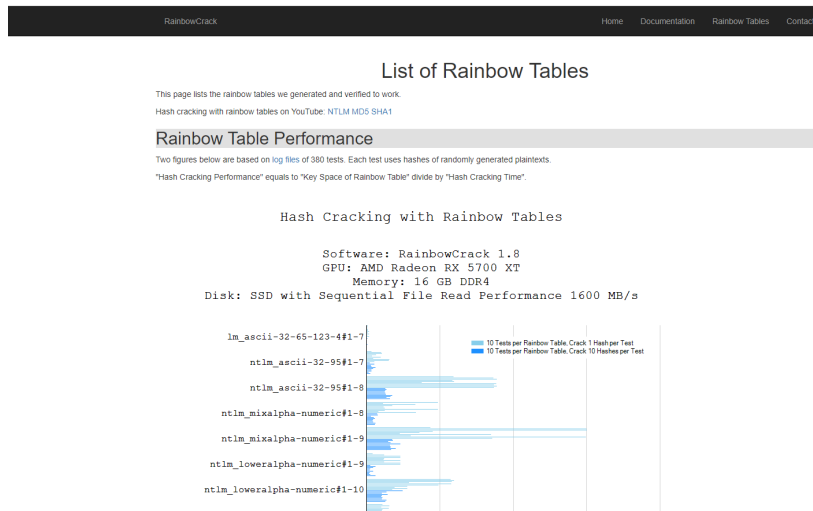
Gaining Access – Offline Attacks

- **Rainbow Table Attack**

- Using the pre-computed hash table values, compare the hash values of passwords that are gathered during the earlier phases and match the password.

- **Distributed Network Attack**

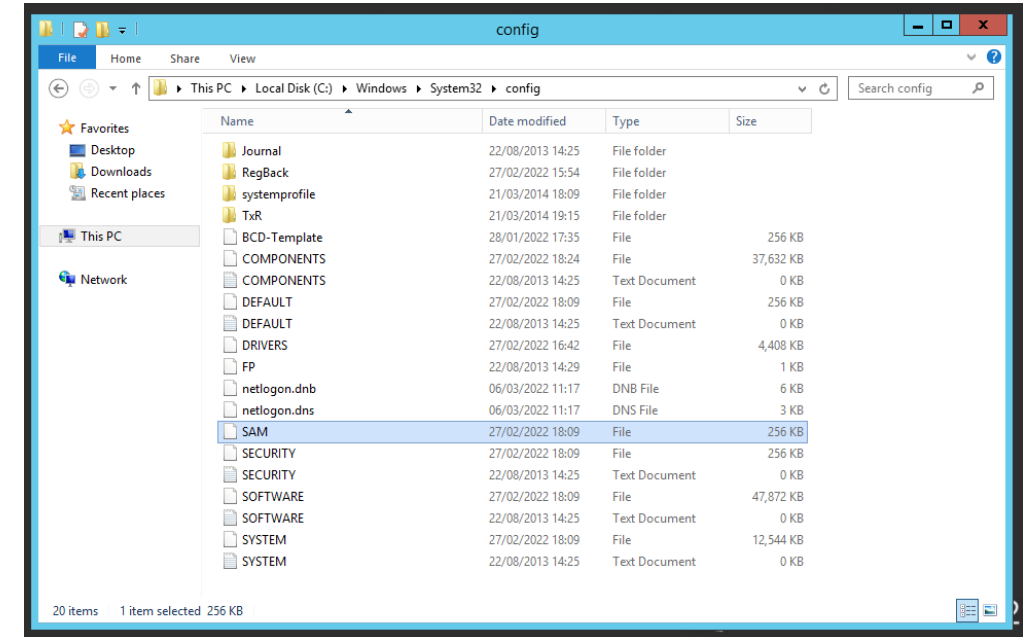
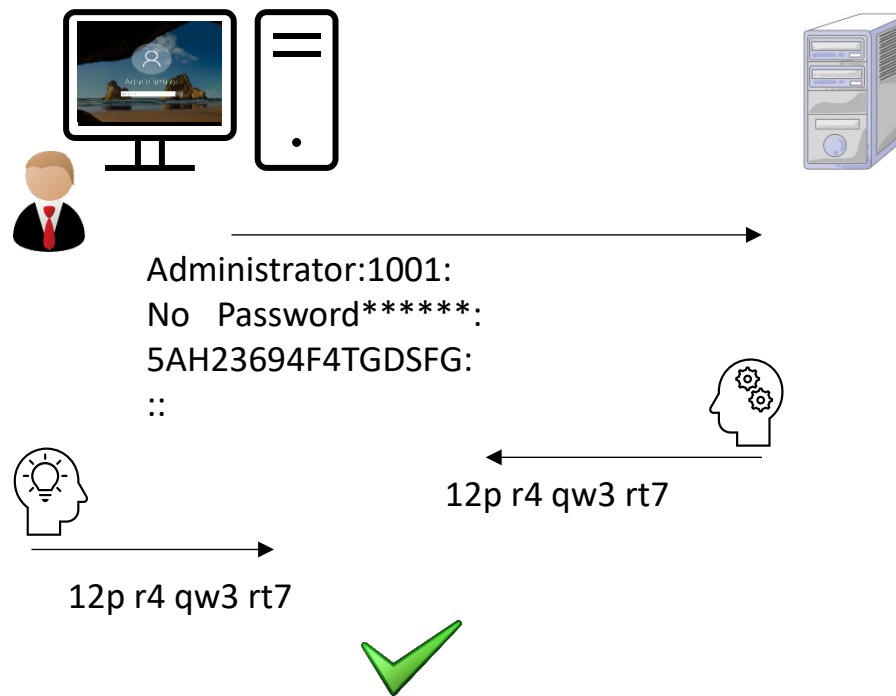
- A technique used to recover passwords from hashes and (or) password protected files.
- This technique uses the unused processing power of machines across the network to decrypt the passwords.



Gaining Access – Authentication Mechanism

- Security Accounts Manager (SAM) Database: *It has Username, User ID, LM Hash, NTLM Hash.*

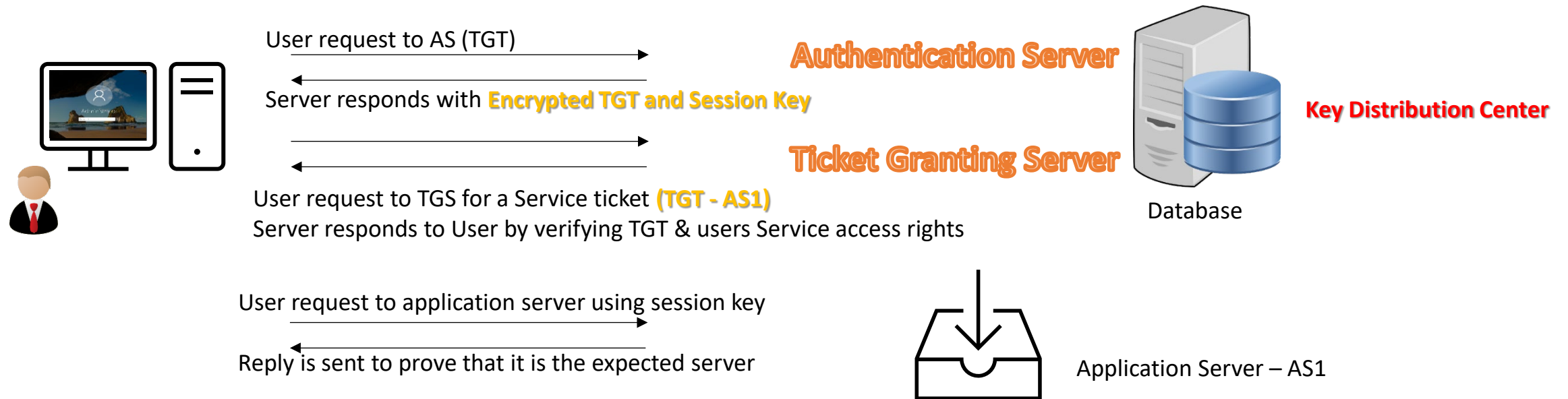
- NTLM Authentication



- Kerberos Authentication: Windows has made Kerberos as its default authentication protocol.

Gaining Access – Authentication Mechanism

- Kerberos Authentication: Windows has made Kerberos as its default authentication protocol.



Gaining Access – Salting

- It is a technique where random string of characters are added to the password before calculating the hash.
- This makes reverse hashing more complex.
- This could overcome pre-computed hash attacks.

Gaining Access – Defending Password Cracking

- **How to defend against password cracking?**

- With reference to our lecture so far.... Could you state ways to defend against password cracking?

- **Disable LMBNR, NBT-NS**

- Turn off multicast name resolution

- Disable NetBIOS over TCP/IP

Privilege Escalation

- Escalating privileges

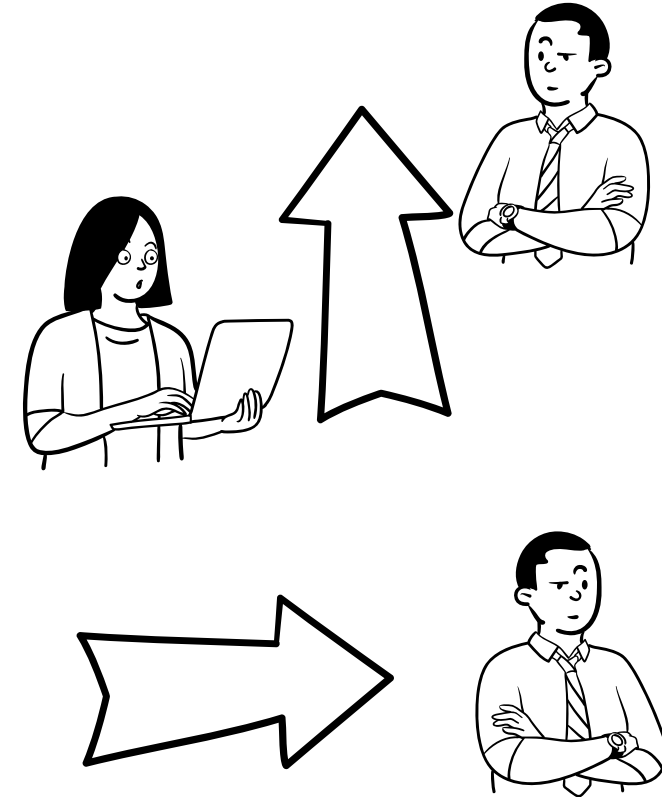
- After gaining access to the network, the attacker would need to have privileges to execute the intended tasks.
- To acquire the privileges, the attacker looks for **design flaws, configuration errors, code weaknesses** etc in Operating Systems and available Software Applications.

- Types



✓ Vertical Privilege Escalation

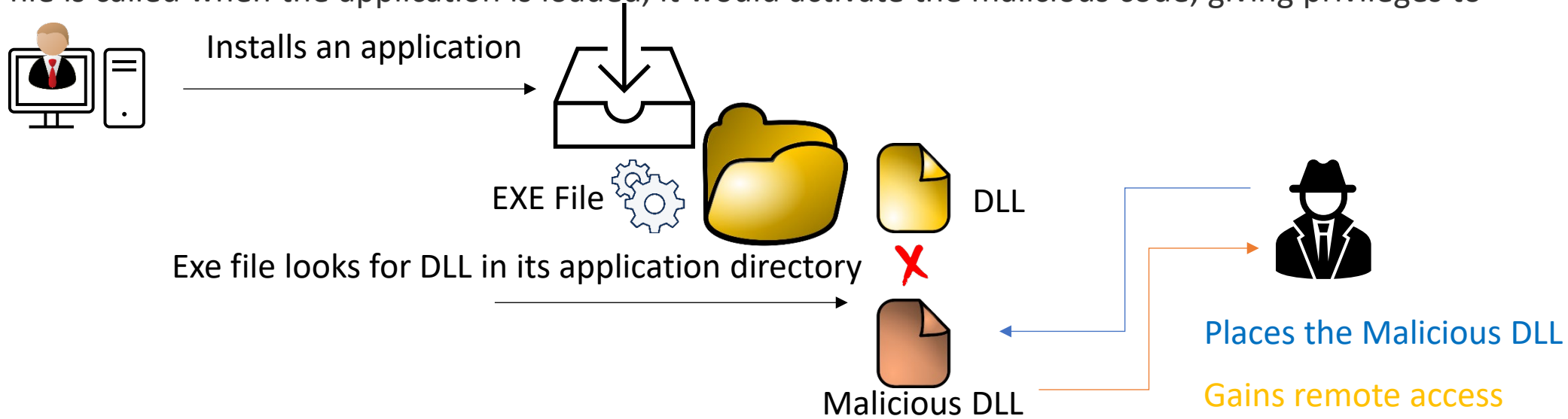
✓ Horizontal Privilege Escalation



Privilege Escalation – Methods

○ DLL Hijacking

- By injecting malicious code in the form of DLL file into an application, DLL Hijacking could be executed.
- Once the DLL file is called when the application is loaded, it would activate the malicious code, giving privileges to the attacker.



○ Dylib Hijacking

- In Apple Computers, OS X, it searches for dylib in multiple directories.
- Attacker can inject a malicious Dylib in its directories. Once the Dylib file is called when the application is loaded, it would activate the malicious code, giving privileges to the attacker.

Privilege Escalation – Methods

- Attackers exploit software vulnerabilities using its flaws in the program code, services, even in Kernel.
- Then, execute malicious code.
- They find out the exploit using various web sources.
- Exploiting software applications helps attackers to execute commands or binary to gain higher privileges.
- They desperately need to escalate privileges to bypass security and achieve their goals.

Privilege Escalation – Vulnerabilities

- **Spectre Vulnerability**

- **Using SV**

- ✓ Attackers *read adjacent memory locations of a process and access information for which they are not authorized.*
 - ✓ Attackers can read the kernel memory or perform a web-based attack using JavaScript

- **Meltdown Vulnerability**

- **Using MV**

- ✓ Attackers escalate privileges by *forcing an unprivileged process to read other adjacent memory locations* such as kernel memory and physical memory.
 - ✓ Attackers can access system's critical information like credentials, private keys etc.

- **Access Token Manipulation, Application Shimming, File System Permissions Weakness, Path Interception, Scheduled Tasks, Launch Daemon, Plist Modification, Setuid and Setgid, Web Shell etc are similar kind of Privilege escalation techniques**

Privilege Escalation – Defending them

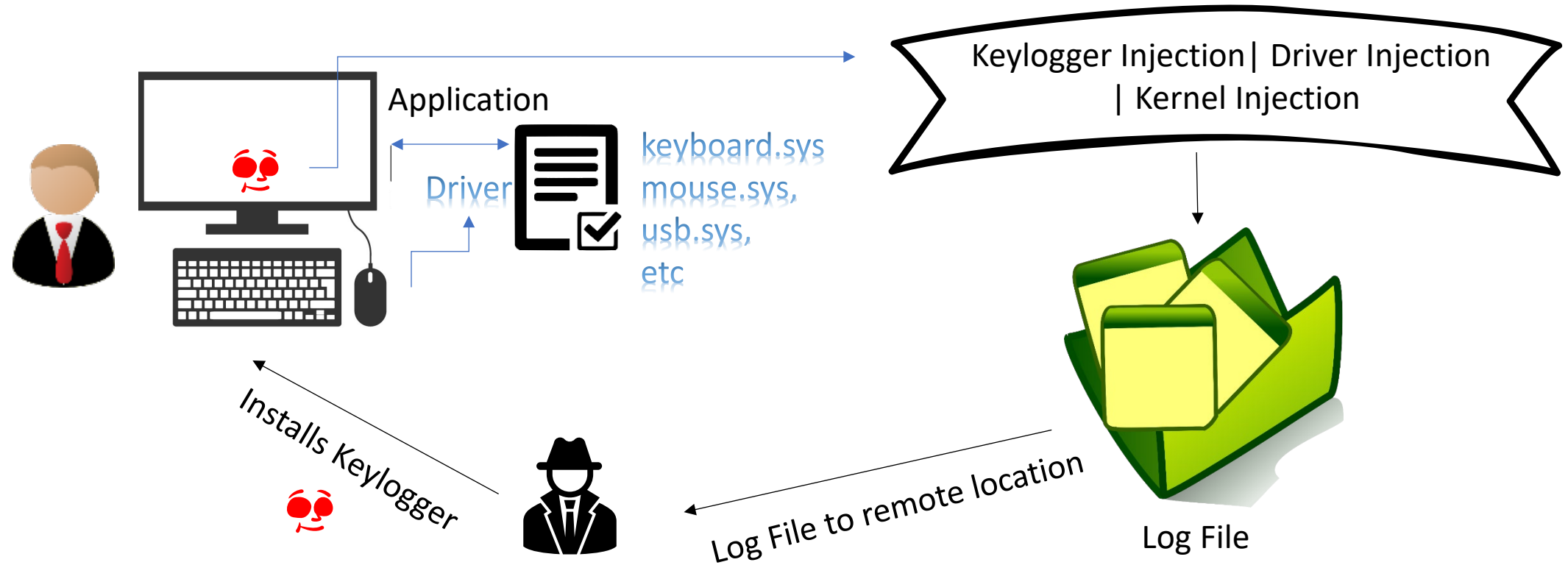
- Restrict **Privileges**
- **Encrypt** Sensitive data
- Implement **MFA** and **Authorization**
- Run services as **unprivileged accounts**
- **Test** for coding errors and bugs
- Implement a **privilege separation methodology** to limit the scope of programming errors and bugs
- **Patch and Update** regularly
- Restrict **users**
- Continuously **monitor file system permissions** using auditing tools
- Reduce the privileges of users and groups, so that **only legitimate administrators can make service changes**
- Use **whitelisting tools** to identify and block malicious software.
- Use **fully qualified paths** in all the windows applications
- **Block** unwanted system utilities or software

Executing Applications

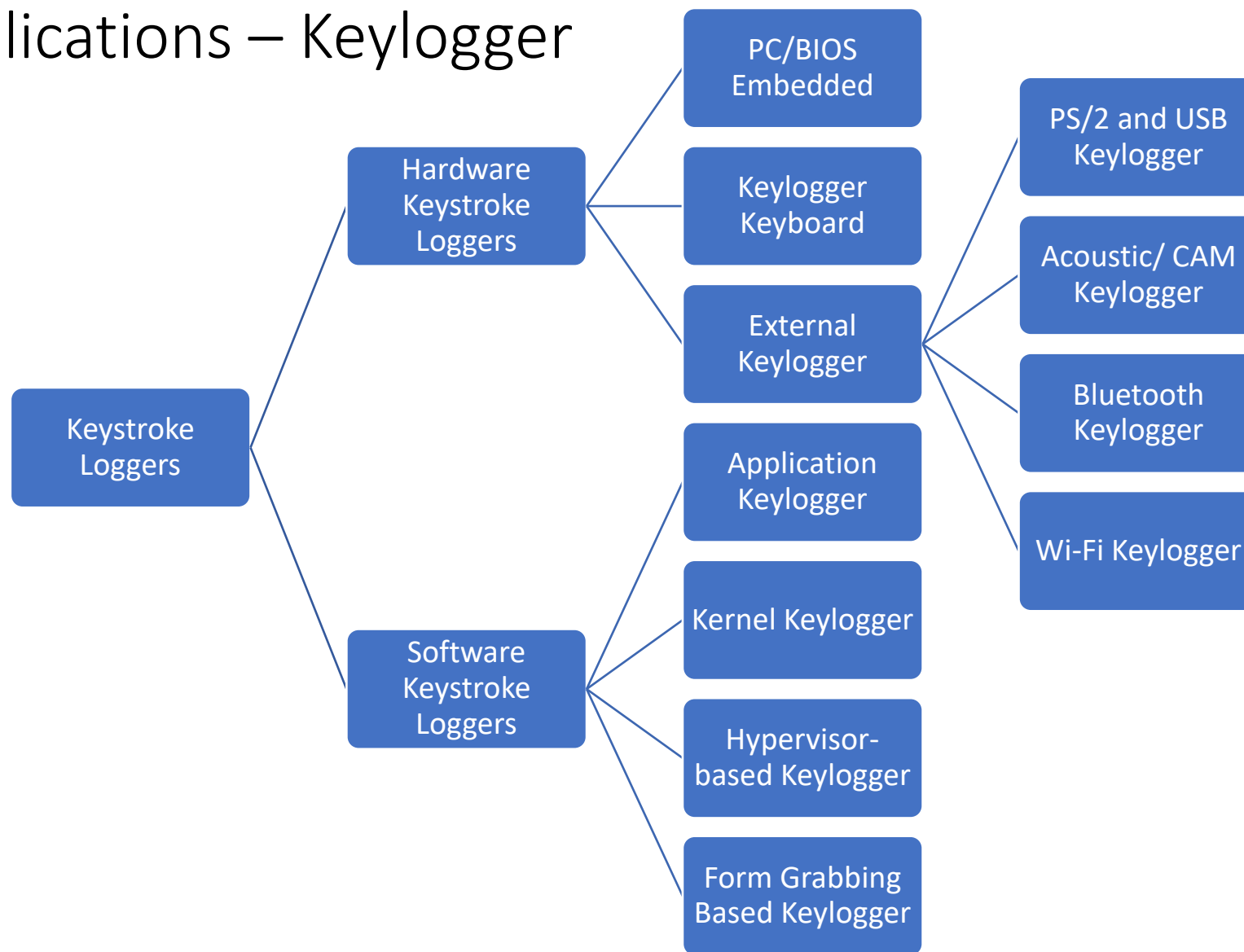
- Once privileges are escalated, attackers are now able to execute malicious applications.
- The malicious programs are remotely executed by the attackers. This enables the attacker to breakdown the privacy by looking at the information, screen captures etc and to install backdoors to maintain easy access.
- Types
 - Keyloggers
 - Backdoors
 - Spyware
 - Crackers

Executing Applications – Keylogger

- Keylogger (Keystroke Logger is a software/ hardware that observes the key stroke).
- The purpose of Keylogger is to monitor computer activities based on organizational policies/ children's activities etc.
- However, it allows attackers to spy on the target.

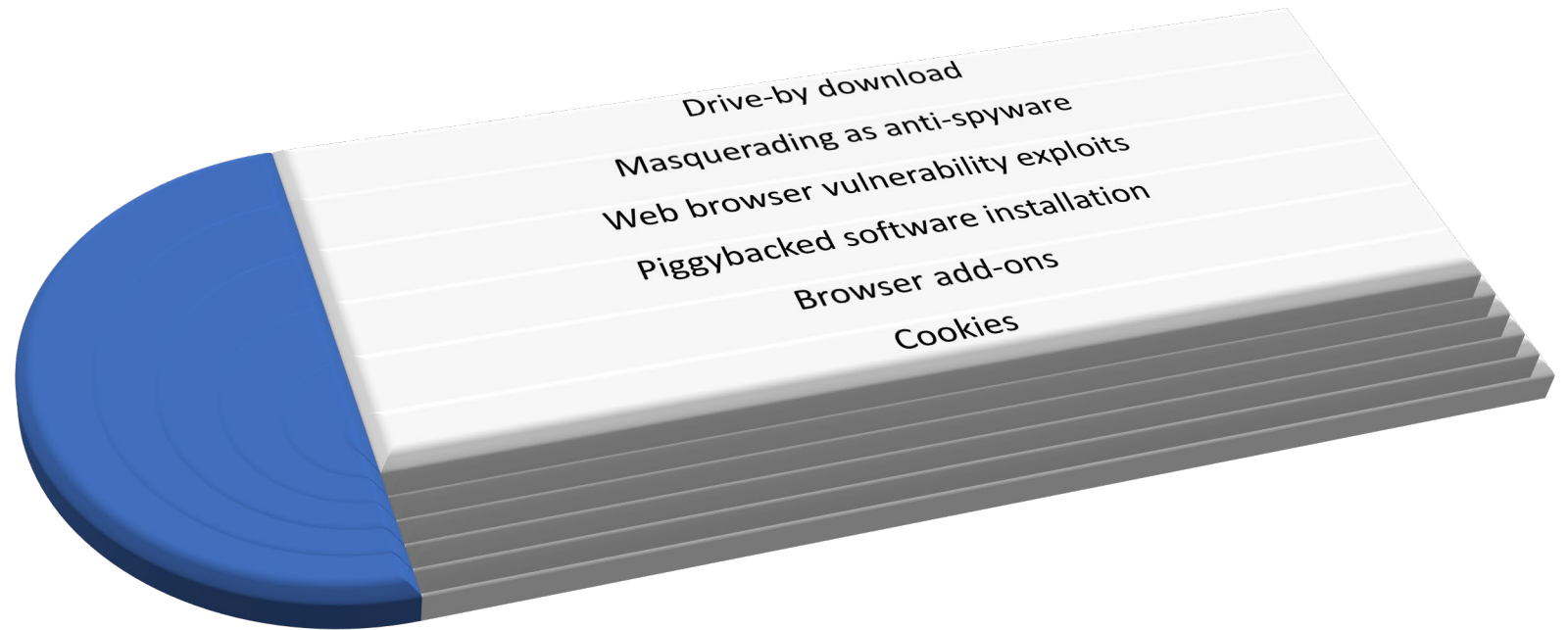


Executing Applications – Keylogger



Executing Applications – Spyware

- It is a stealthy program that hides its process, files and other objects from being detected.
- It records user interaction with the computer and internet without the user's knowledge and sends them to the remote attackers.



Spyware Propagation



Defending

- **Against Keyloggers**

- ✓ **Anti-spyware/antivirus programs, Host-based IDS, Firewalls, Anti-logging software's with updated signature**
- ✓ **Keystroke interference software**
- ✓ **Use registry editor or process explorer to check for the keystroke loggers**
- ✓ **Restrict Physical access**
- ✓ **Use encryption between keyboard and its driver**
- ✓ **Use anti-keylogger**

Defending

- **Against Spywares**

- ✓ **Anti-spyware/antivirus programs, Host-based IDS, Firewalls, Anti-logging software's with updated signature**
- ✓ **Set Browser security settings**
- ✓ **Check task manager report and MS configuration manager report**
- ✓ **Create Awareness – Be aware when downloading files, Pop-ups etc**
- ✓ **Use anti-spyware**

Hiding Files

Once, gaining access (using various methods – we have discussed so far)

- Attackers may place files to grant access to the target and execute malicious tasks.
- These files may be hidden from being identified.
- These programs are called as **Rootkits**.
- Rootkits mainly focus on replacing some OS system calls and utilities with a modified version.
- Rootkits generally are Backdoor programs, DDoS programs, Packet Sniffers, BOTS etc.

Objectives of Rootkit

- *Gain* backdoor *access*.
- *Store malicious programs*.
- *Hide tracks* and *malicious applications*.
- *Gather restricted data*.

Hiding Files

Types of Rootkit

- **Hypervisor Level Rootkit.**
- **Hardware/ Firmware Rootkit.**
- **Kernel Level Rootkit.**
- **Boot Loader Level Rootkit.**
- **Application-Level Rootkit.**
- **Library Level Rootkit.**

✓ Rectangle Table Discussion

- ✓ **Sony's Rootkit Scandal**
- ✓ **New FudModule Rootkit**
- ✓ **What is MosaicRegressor?**
 - ✓ Collaborate as a Team (2-3 Members) – Not more
 - ✓ Do a detailed research on the above rootkits
 - ✓ Document your Team's collected information and initiate a discussion.
 - ✓ Discuss/ Debate with other teams via our Rectangle Table Discussion.

Process (Original)

- Code section...
- Call FindNextFile
- Import data section
- FindNextFile: 0x87651234
- Kernel32.dll
- 0x87651234: FindNextFile code

Process (Hooked)

- Code section...
- Call FindNextFile
- Import data section
- FindNextFile: 0x87651234
- Kernel32.dll
- **0x98752**1234: FindNextFile code
- Rootkit Code: **0x98752**1234: FindNextFile

Detecting and Defending Rootkits

Detecting Rootkit

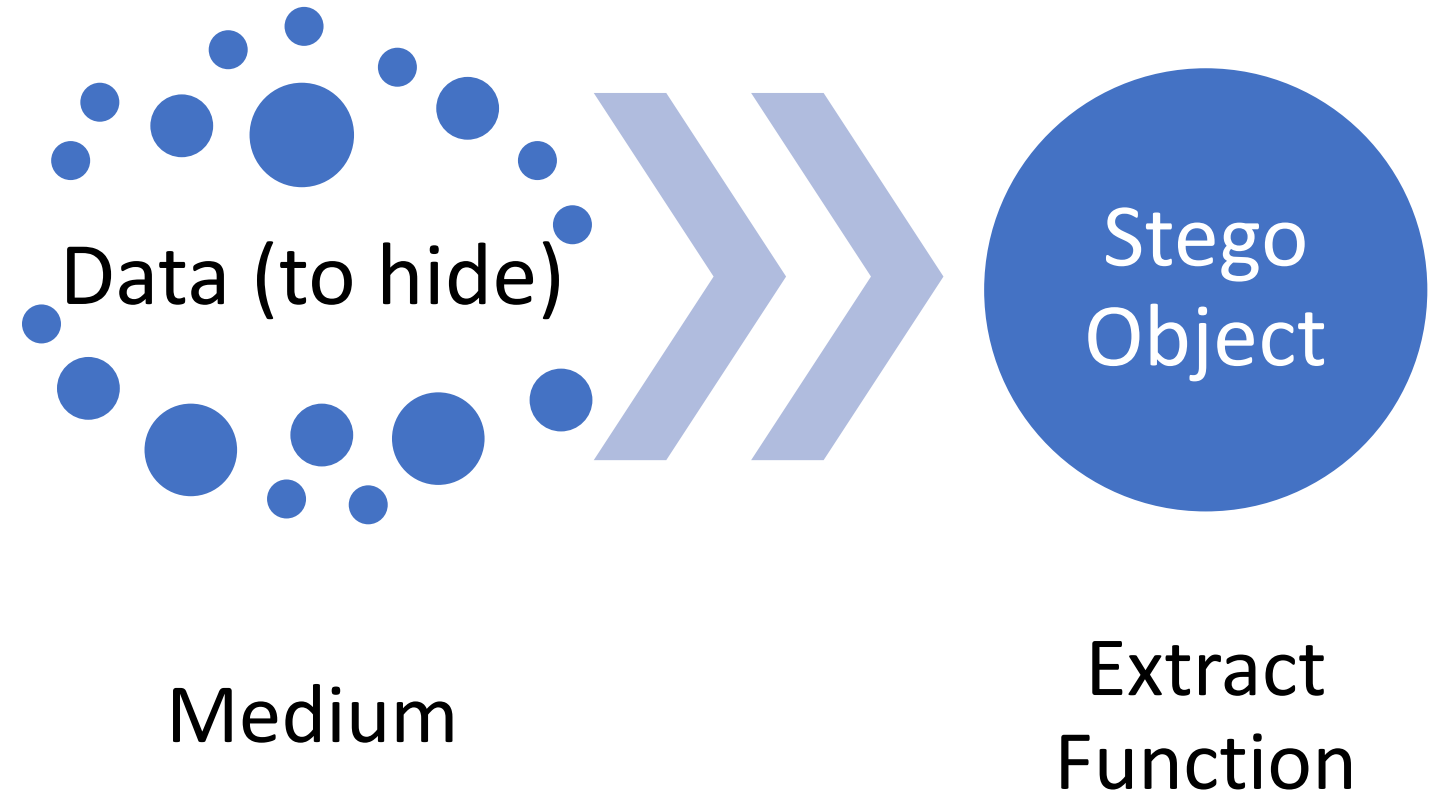
- *Integrity-Based detection*
- *Signature-Based detection*
- *Heuristic/Behavior-Based detection*
- *Runtime Execution Path Profiling*
- *Cross View-Based detection*

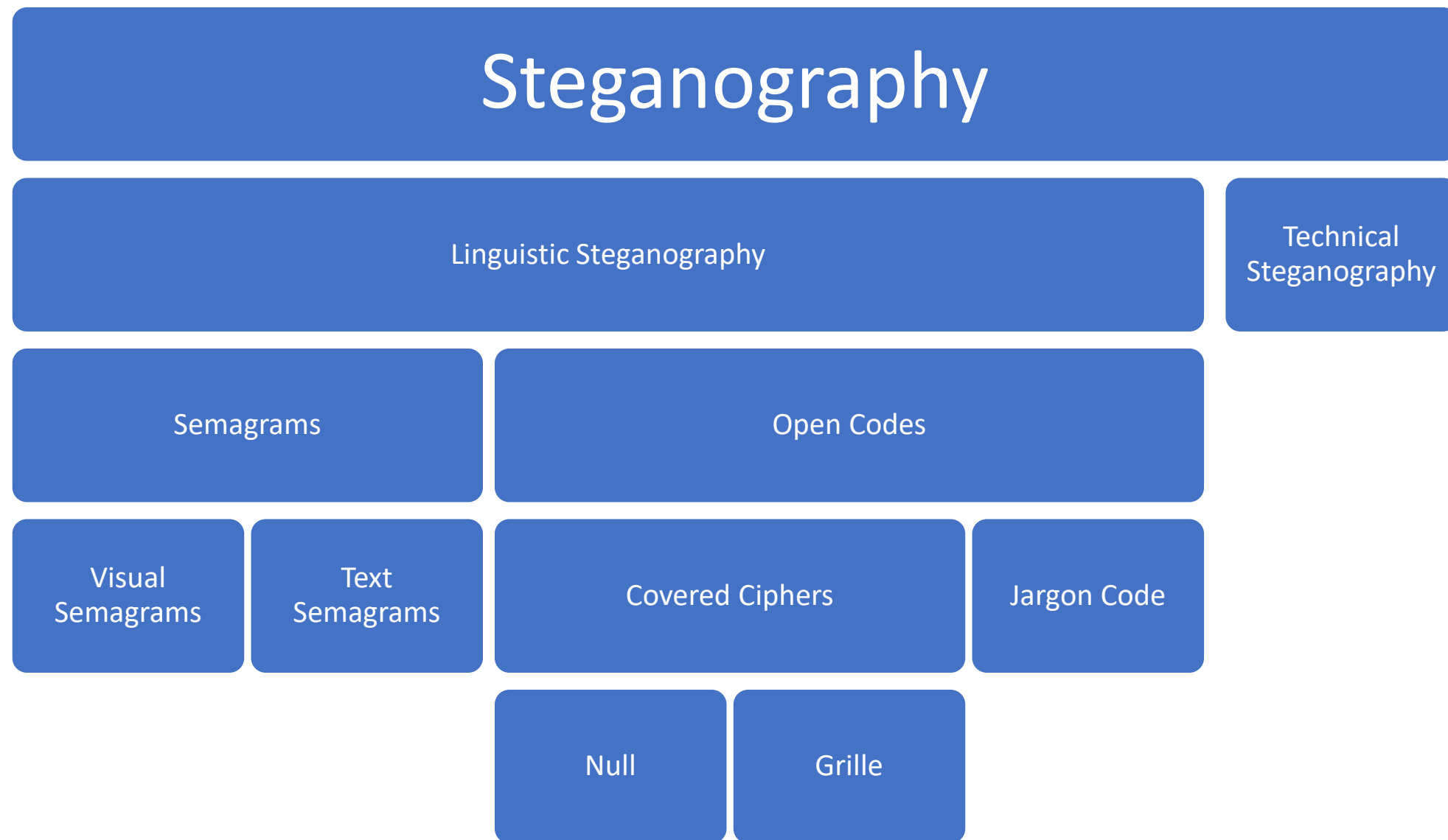
Defending Rootkit

- *Reinstall OS/ Applications*
- *Update and Patch OS/ Applications*
- *Verify the integrity of the system files regularly*
- *Update anti-virus/ anti-spyware software*
- *Prevent installation of unnecessary applications*

Steganography

- Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data.
- Attackers use steganography to hide messages.



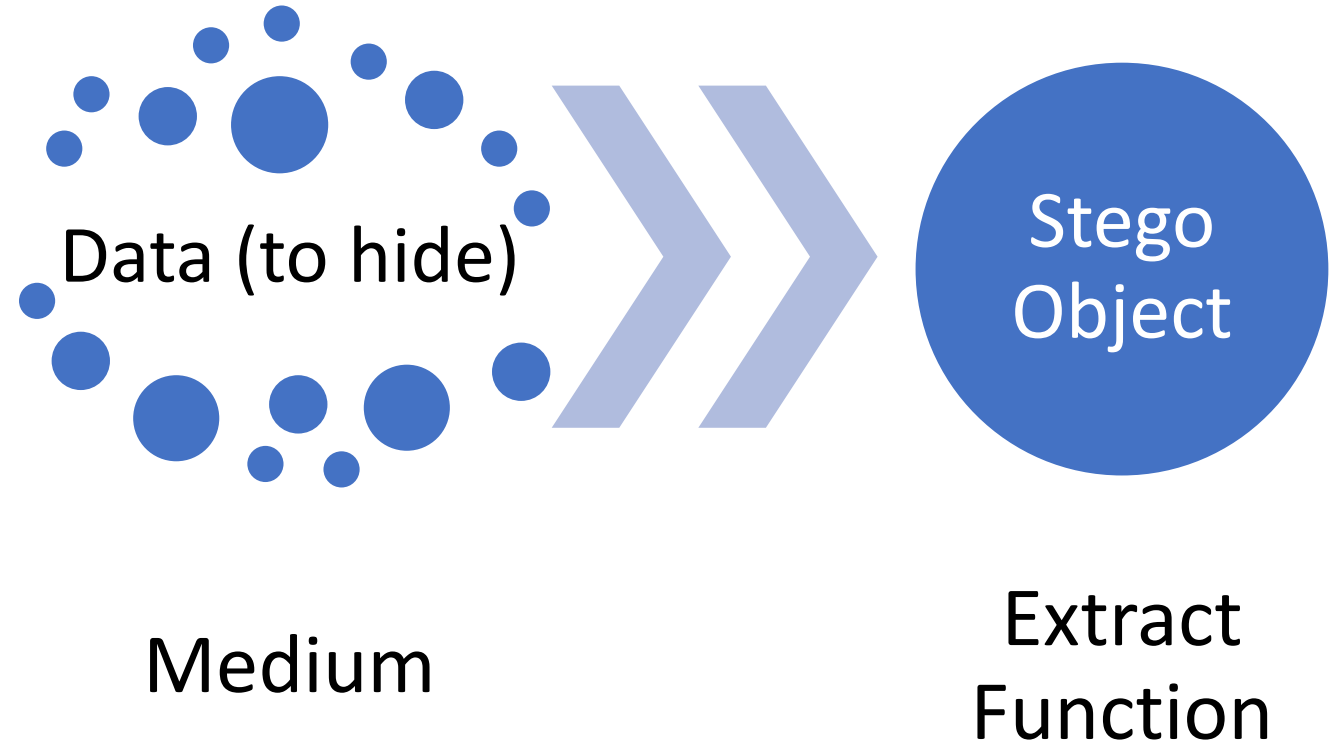


Steganalysis

- Reverse process of Steganography.
- Art of discovering and rendering covert messages using Steganography.
- Detects the hidden messages embedded in images, text, audio, video etc.

Methods

- *Stego-Only*
- *Known-stego*
- *Known-message*
- *Known-cover*
- *Chosen-message*
- *Chosen-stego*



Detecting Steganography

- **Text File**

Modifications are done based on Character Positions

Observe the text patterns, disturbances, language used, blank spaces etc to detect

- **Image File**

Observe the Size, file format, timestamp modification, colour palette.

Statistical Analysis method could be used for scanning images

- **Audio File**

Modifications are done based on LSB. Detect data existence based on Odd distortions/ Patterns

Statistical Analysis method could be used for audio files. Scan inaudible frequencies.

- **Video File**

✓ Combination of Image and Audio file detection shall be used to detect data in video files

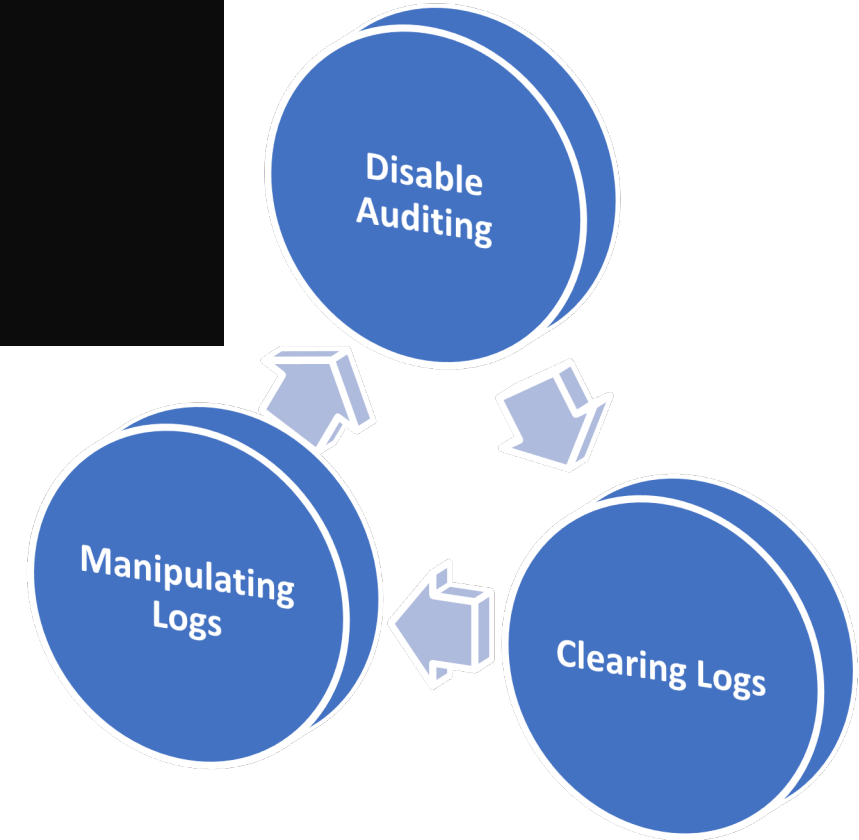
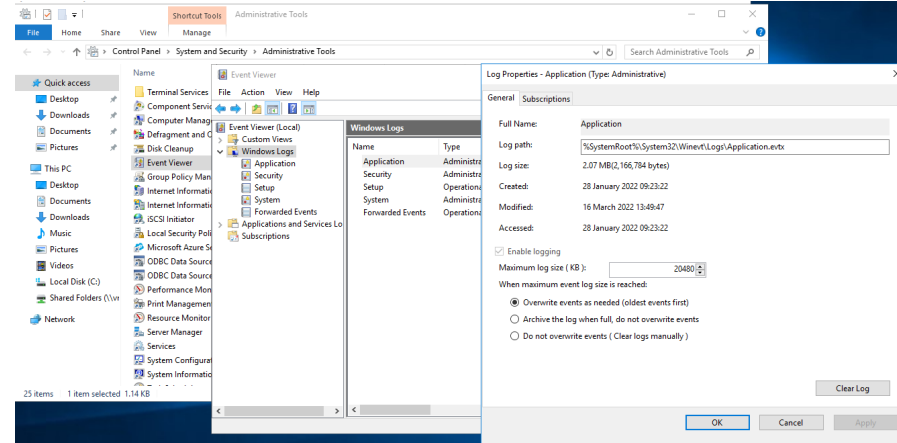
Clearing Logs

- Disables Auditing features
- Clear or delete the system log entries
- Clear Event Logs Manually
- Delete the MRU, cookies, cache etc
- Turnoff Autocomplete
- Clear Toolbar data from browsers
- Clear the Bash History
- Use Reverse HTTP Shells
- Use Reverse ICMP Tunnels
- Use DNS Tunneling
- Use TCP Parameters

```
Use AuditPol <command> /? for details on each command

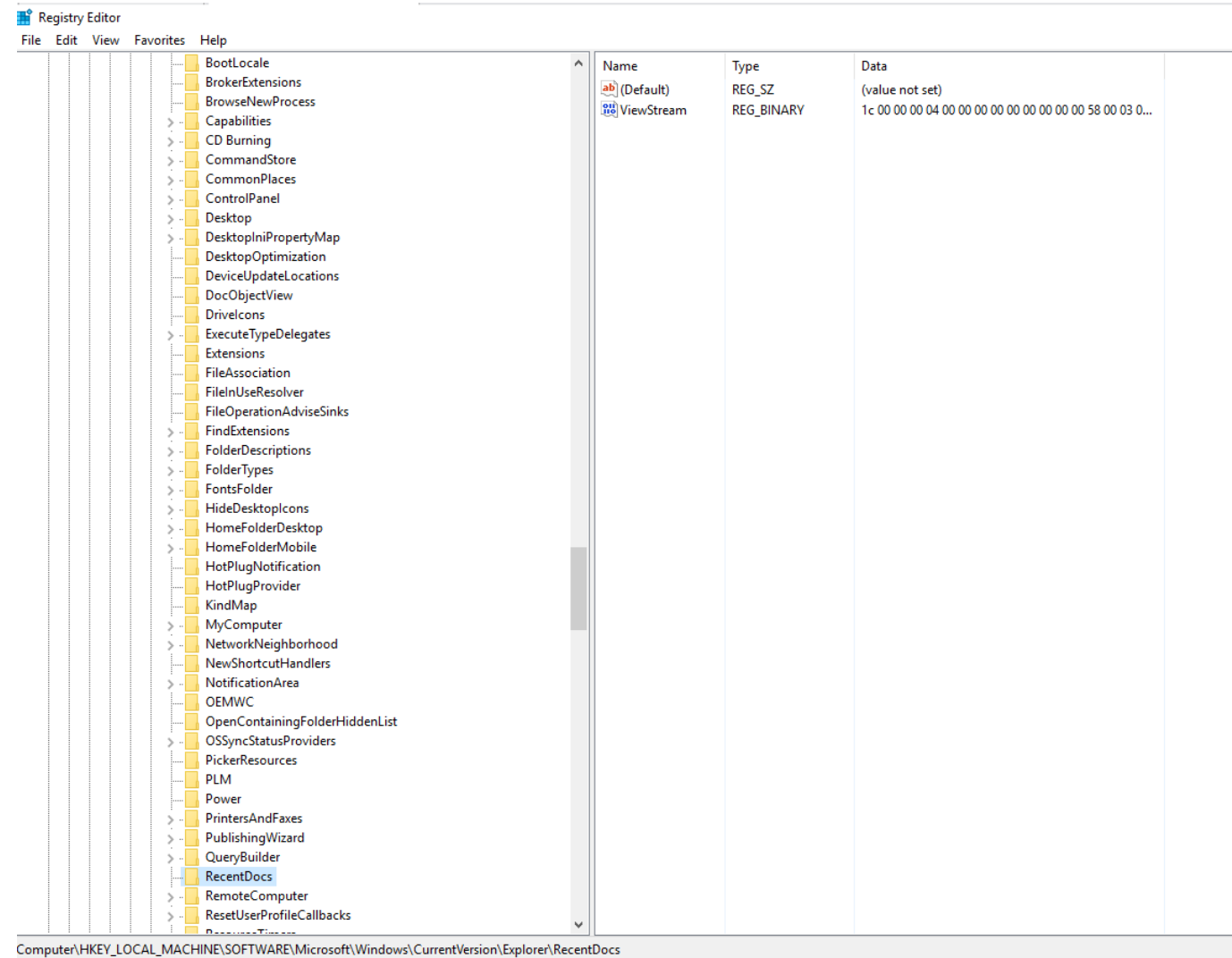
C:\windows\system32>Auditpol.exe /get /category:"Logon/Logoff"
System audit policy
Category/Subcategory          Setting
Logon/Logoff
  Logon                        Success and Failure
  Logoff                       Success
  Account Lockout              Success
  IPsec Main Mode              No Auditing
  IPsec Quick Mode             No Auditing
  IPsec Extended Mode          No Auditing
  Special Logon                Success
  Other Logon/Logoff Events     No Auditing
  Network Policy Server        Success and Failure
  User / Device Claims         No Auditing
  Group Membership             No Auditing

C:\windows\system32>
```



Clearing Logs

- **Disables Auditing features**
- **Clear or delete the system log entries**
- **Clear Event Logs Manually**
- **Delete the MRU, cookies, cache etc**
- **Turnoff Autocomplete**
- **Clear Toolbar data from browsers**
- **Clear the Bash History**
- **Use Reverse HTTP Shells**
- **Use Reverse ICMP Tunnels**
- **Use DNS Tunneling**
- **Use TCP Parameters**



Pen Test

Identify Password Protected Systems: Do you have access to the password? Yes → Check the Password Complexity | No, → Go to next step

Perform Social Engineering, Shoulder Surfing, Dumpster Diving, Dictionary Attack, Brute Force Attack, Rule Based Attack, Guess the Password: Do you have access to the password? Yes → Good | No → Go to next step

Place Keyloggers/ Trojan/ Spyware, Hash Injection Attacks, Wire Sniffing, MiTM, Replay Attack, Rainbow Table Attack, Distributed Network Attack: Do you have access to the password? Yes → Escalate Privilege | No → Try Again (Go Home!!! Not your day)

Pen Test

Login using enumerated username and cracked passwords: Check your Privilege. Need more privilege? Yes → Go to next step

Perform DLL Hijacking, Exploit Vulnerabilities, Dylib Hijacking.

Privilege Escalated? Yes → Go to next step | No: Try other PE Techniques.

Check Firewall Status, Antivirus Status, Anti-Keylogging Software Status, Physical Security Status, Use Keyloggers, Spyware.

Application Executed? Yes → Go to next step | No: Try Remote tools to execute applications.



Pen Test

Install Rootkits in the target system: Perform Integrity Based Detection Technique, Signature Based Detection Technique, Cross View Based Detection Technique, Heuristic Detection Technique

Files Hidden? No → Go to next step | Yes: Great

Check Antivirus and Antispyware Software's, OS Patched and Updated: Use Windows hidden Stream to inject Malicious code, Steganography to hide secret message, Perform Steganalysis Techniques

Files Hidden? Yes → Go to next step | No: Try other Techniques.

Cover your Tracks: Remove Web activity tracks, Disable Auditing, Tamper Log files, Clear BASH Shell tracks, Clear Network Tracks, Close remote connections, Close opened ports



Pen Test

Report

- A structured report that details the findings of the penetration tests that are conducted for a client.
- It is recorded by the involved pen testers
- It is a one-to-one correspondence exists between the documentation and the testing process.

Goal of the Penetration Testing Report

- Help **executive management** make decisions about implementing security controls in the organization.
- Help those **responsible for information system security** implement security controls and patch any flaw discovered during pen testing.
- Assure the organization that the testing team sincerely wishes to **improve the organization's security posture**.

Pen Test

Objectives it to:

- List the security flaws, vulnerabilities, security misconfigurations, and other exploitable resources found during the testing.
- Analyze the options available to mitigate the vulnerability.
- Suggest solutions for security risks.
- Clarify prioritization of corrections for the client's assets
- Recommend actions to prevent possible future cyberattacks.

Pen Test

Objectives it to:

- List the security flaws, vulnerabilities, security misconfigurations, and other exploitable resources found during the testing.
- Analyze the options available to mitigate the vulnerability.
- Suggest solutions for security risks.
- Clarify prioritization of corrections for the client's assets
- Recommend actions to prevent possible future cyberattacks.

Deliverables:

- Detailed analysis of the methodologies used in the testing.
- Detailed information about all the activities performed and their results in a clear standard format.
- Evidence of successful tests of the organizational resources in the form of pictures, videos, and documents.
- Detailed information about the affected resources, cyberattacks performed, tools used, etc..
- Documents that corroborate the test findings. *(Include information on the availability of updates, data from the compromised servers, details of the compromised accounts, etc)*
- Documents containing tips for remediating the security flaws, eliminating vulnerabilities, and strengthening the security of the tested components

Pen Test

Types of Report

- **Executive report:**
 - Complete testing process
 - Includes details of the tested components, vulnerabilities, misconfigurations, updates required, and other details that can help the authorities make decisions for securing the target.
- **Host report:**
 - Information about the hosts tested, vulnerabilities found, exploited hosts, etc.
- **Client-side test report:**
 - Details of the client-side test such as phishing, spear-phishing, spam, and social engineering attacks used during the testing.
 - Detailed information about compromised client-side systems.

Pen Test

Types of Report

- **User report:**

- Information of users who were identified and targeted during the testing process along with the tasks performed by them.

- **Vulnerability report:**

- Detailed information about all the vulnerabilities found during the pen testing process.
- It is recommended that the report lists the components with vulnerabilities and also offers solutions to eliminate the vulnerabilities.

- **Activity report:**

- Activities that the testing team had performed across the organization
- Can also include various documents to support the claims.

Pen Test

A good pen-test report should be:

- Written in simple language that everyone can easily understand.
- Written in a professional manner using formal language.
- Comprehensible to both technical and nontechnical personnel such as security admins and stakeholders.
- Clearly explain the purpose of the penetration test as well as that of writing the report.
- Provide complete information to the reader in a clear format and not contain unnecessary information.
- Grammatically correct, punctuated appropriately, and free of typographical errors.
- Provide accurate information and support it with proper evidence, such as screenshots of the test results and stolen credentials.
- Contain information sorted according to the security risks, with the highest risks being prioritized.
- Structured logically.
- The style of presentation and the usage of words should be attractive to readers.
- Should contain unbiased recommendations and suggestions based on the analysis by the pen testers

Pen Test

A good pen-test report structure

- Final report delivery date
- Cover letter
- Executive summary:
 - Organization synopsis: This section includes a brief description of the organization and its network.
 - Purpose for the evaluation: This section defines the reason for undertaking penetration testing.
 - System description: This section includes a brief description of the systems used across the client organization.
 - Scope of the project: This section includes the total number of IP addresses, apps, devices, hosts, and other network resources that the organization had mentioned in the contract.
 - Summary of evaluation: This section should contain a summary of the tests performed by the pen testers and the results obtained.

Pen Test

A good pen-test report structure

- Final report delivery date
- Cover letter
- Executive summary:
 - Assumptions/Timeline: This section should specify all the assumptions made during the testing process and include all the commencement and completion dates for each test.
 - Major findings and recommendations: This section should include a summary of the major findings and any issues that could lead to future cyberattacks. The testers should also mention any recommended actions to mitigate the vulnerabilities.
 - Testing methodology: This section specifies the standard frameworks and techniques followed to perform penetration testing.
 - Planning: This section includes the details of the planned penetration testing process and how the actual process was performed
 - Exploitation: This section includes all the detailed exploitation processes followed during the penetration test.
 - Conclusions: This is the concluding section of the report. These conclusions include any further suggestions from the testing team.

Pen Test

Common Mistakes by Organisations/ you might come across

- Not understanding the scope of the pen testing service
- Not asking for a retest
- Not asking for a letter of attestation
- Using a vendor without creating and signing a contract
- Not receiving guidance on the type of test to conduct
- Not asking for a detailed debrief or report walkthrough
- Not asking for a report with detailed steps and reproducible results
- Using vendors and tools that provide reports with hundreds or thousands of vulnerabilities that are mostly not critical
- Employing an inexperienced pen tester who creates reports using automated tools



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Any Questions?

*Advanced Cybersecurity
(ACCB6000)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

References

- EC-Council CEH
- Cisco Networking Academy
- Certified Ethical Hacker (CEH) Version 10 Cert Guide, 3rd edition
- Wikipedia
- Other website sources given in this presentation
- * The intension of usage is for Educational Purpose Only

Advanced Cybersecurity
(ACCB6000)

Applied Computing - WISA

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk