



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

Hacking Ethically!!!



Advanced Cybersecurity - Continuation (ACCB6000)

Applied Computing - WISA



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

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

VM Download

\\192.168.135.200\ACCB6000\$

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**
- **Network Scanning, Tools and Techniques**
- **Banner Grabbing**
- **Scanning – PenTesting**
- **Enumeration Concepts, Techniques, 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.



Previous sessions...

Understanding and Assessing Vulnerabilities

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

Social Engineering

- **Understand Social Engineering Concepts, Techniques**
- **Understanding Threats, Impersonation**
- **Countermeasures**

Lab/ Tutorials

- **Activity 1 Getting Ready**
- **Activity 2 Information Gathering**
- **Activity 3 Scanning and Enumeration**
- **Activity 4- Vulnerability Assessment**
- **Activity 5 – Social Engineering**

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.

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 6 – Exploiting and Testing***

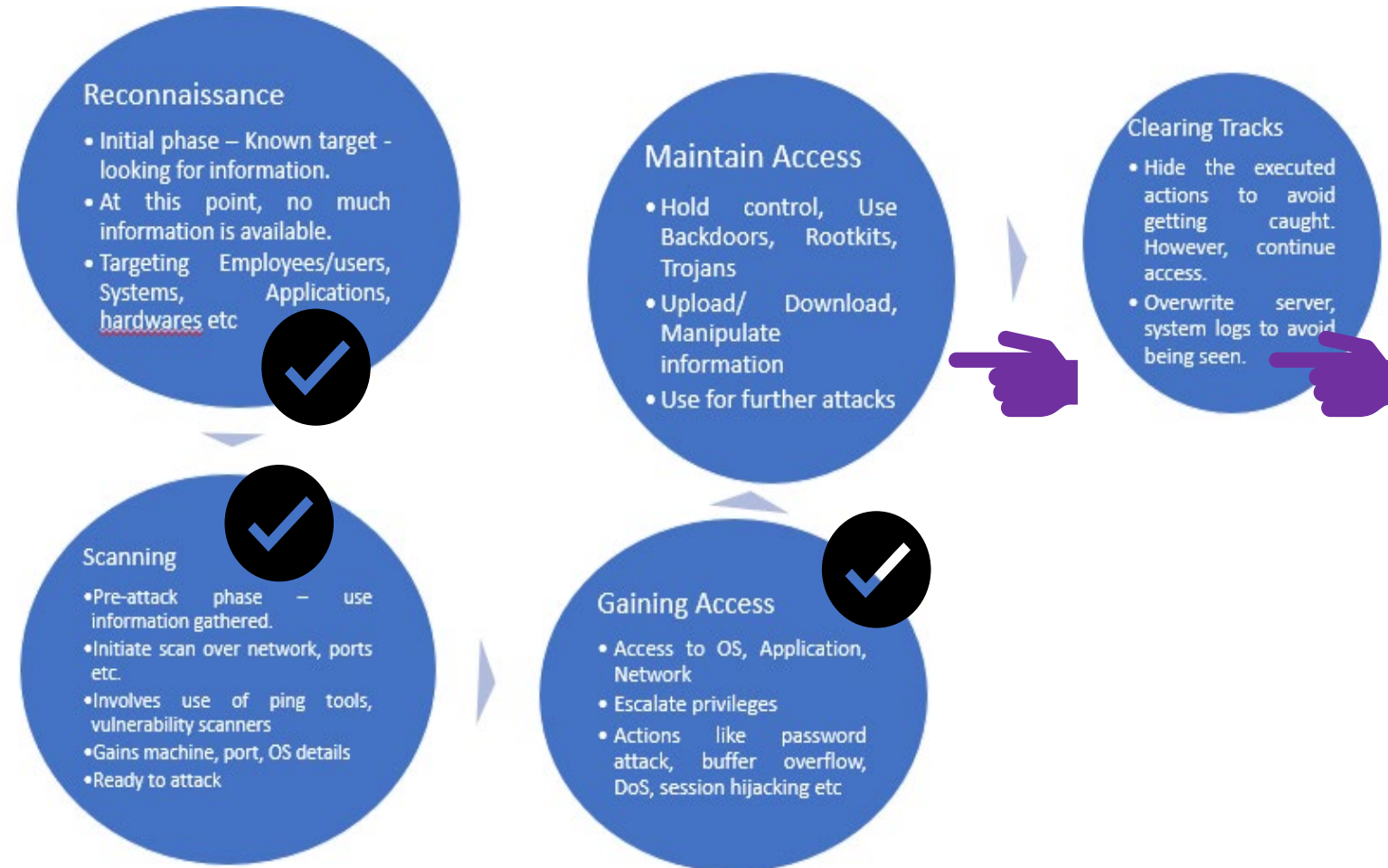
During this week, with applied knowledge and understanding on Footprinting, Network Scanning, Enumerating the target, and assessing vulnerabilities, we shall move forward focusing on the hacking methodology. We shall understand various techniques to gain access, escalate privileges, create and maintain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

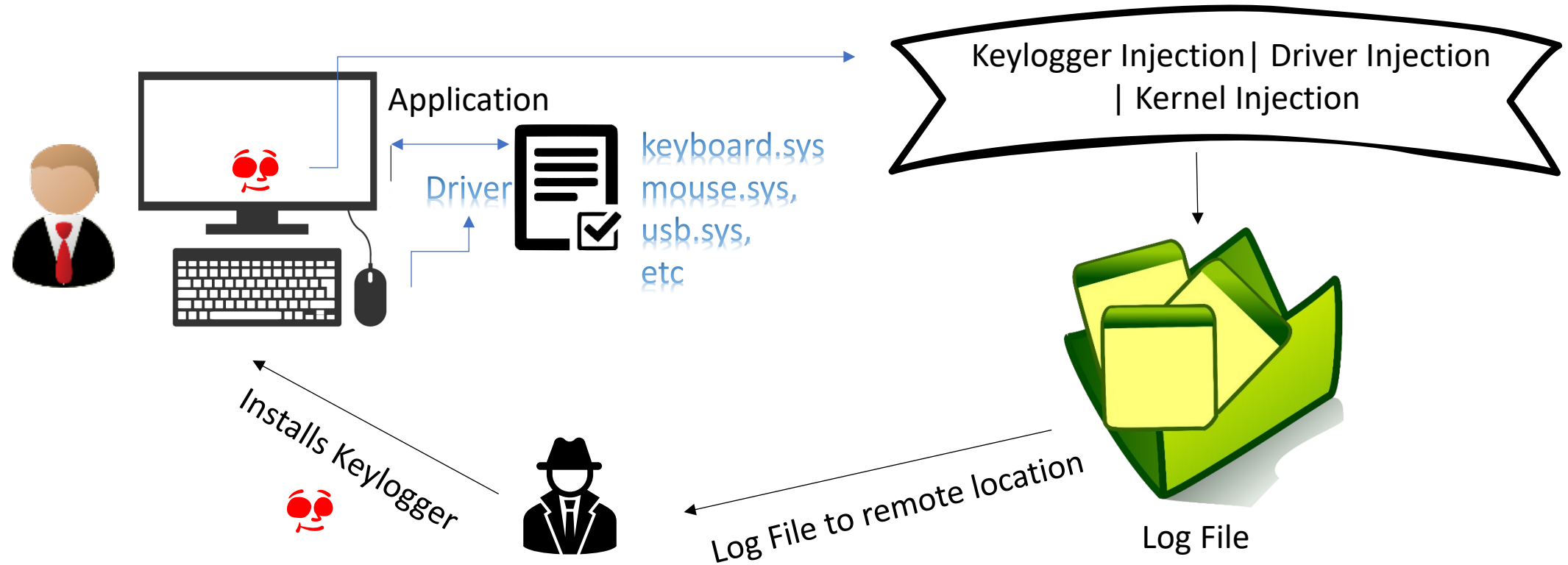
- Gaining Access
 - To bypass the access control systems and gain access into the target system
 - Techniques like Password cracking, Social Engineering helps to gain access
- Privilege Escalation
 - To get rights of a legitimate user or administrator
 - Techniques like vulnerability exploitation helps 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

Executing Applications

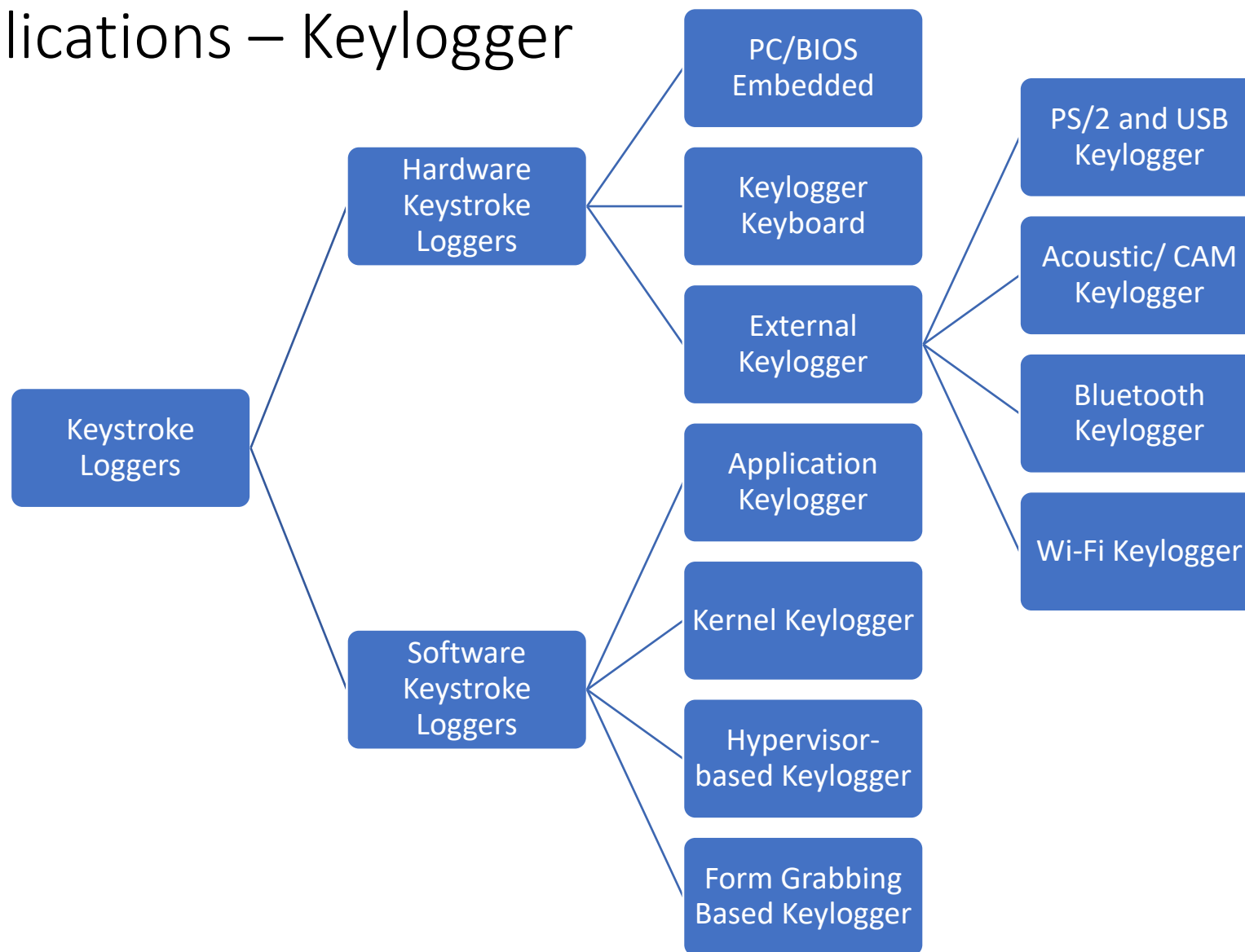
- Once privileges are escalated, attackers are now able to execute malicious applications.
- The malicious programs are remotely executed by the attackers. This enables the attacker to breakdown the privacy by looking at the information, screen captures etc and to install backdoors to maintain easy access.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

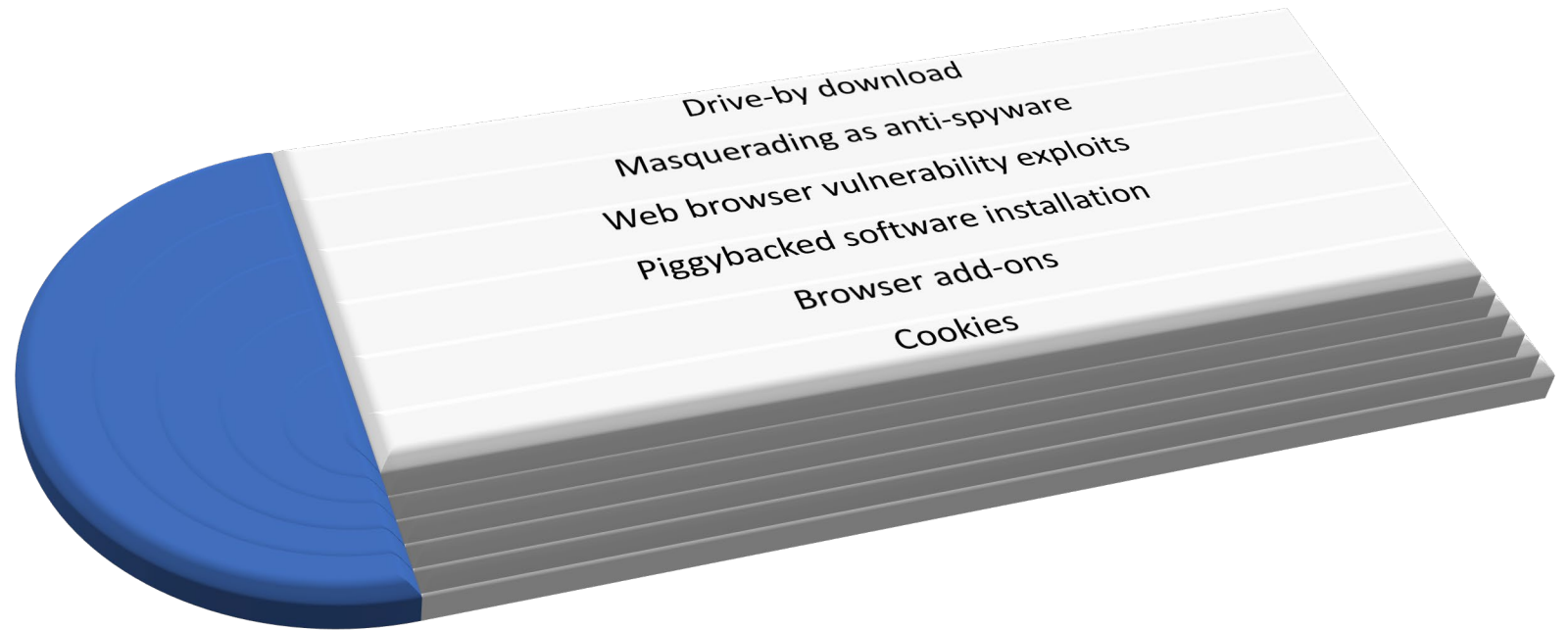


Executing Applications – Keylogger



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

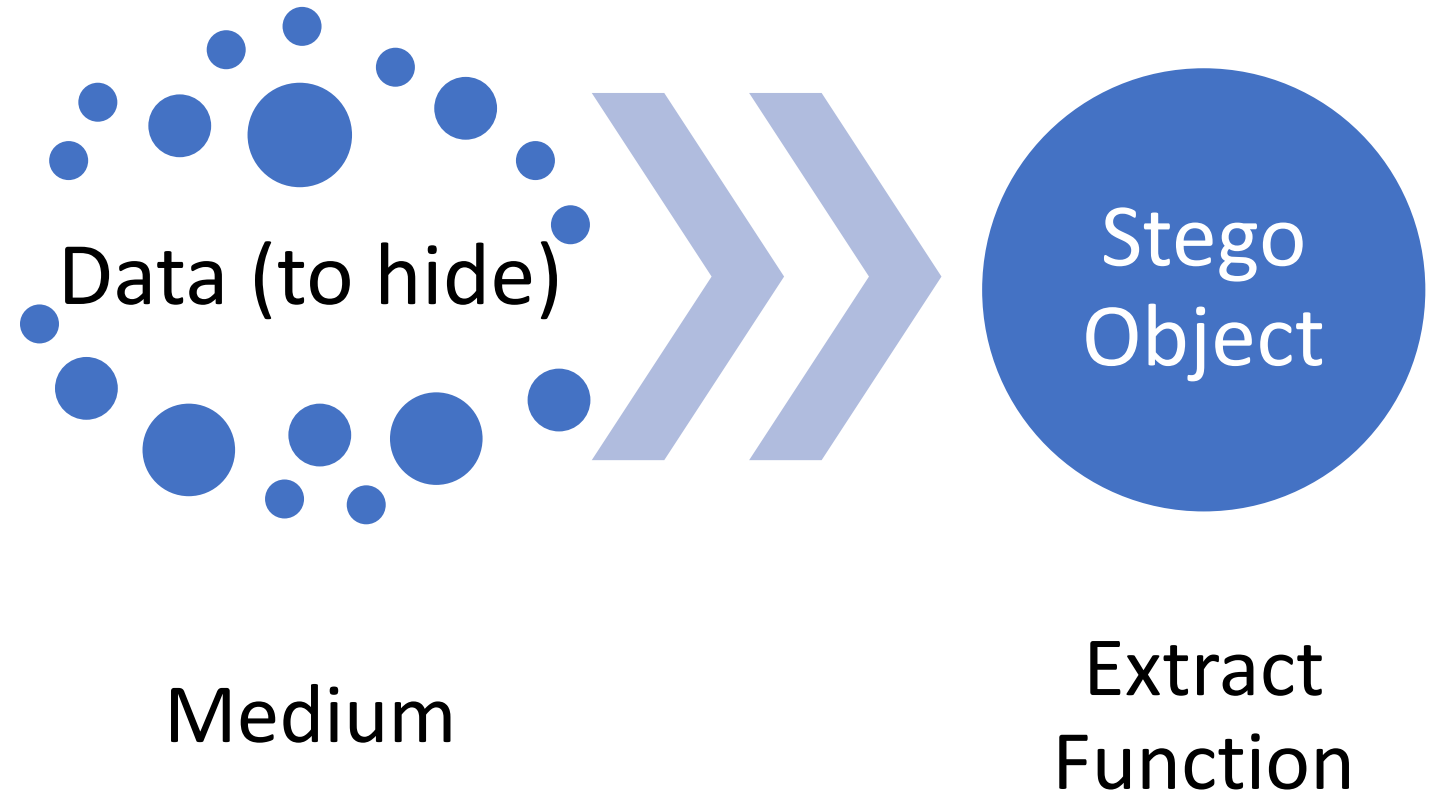
- *Integrity-Based detection*
- *Signature-Based detection*
- *Heuristic/Behavior-Based detection*
- *Runtime Execution Path Profiling*
- *Cross View-Based detection*

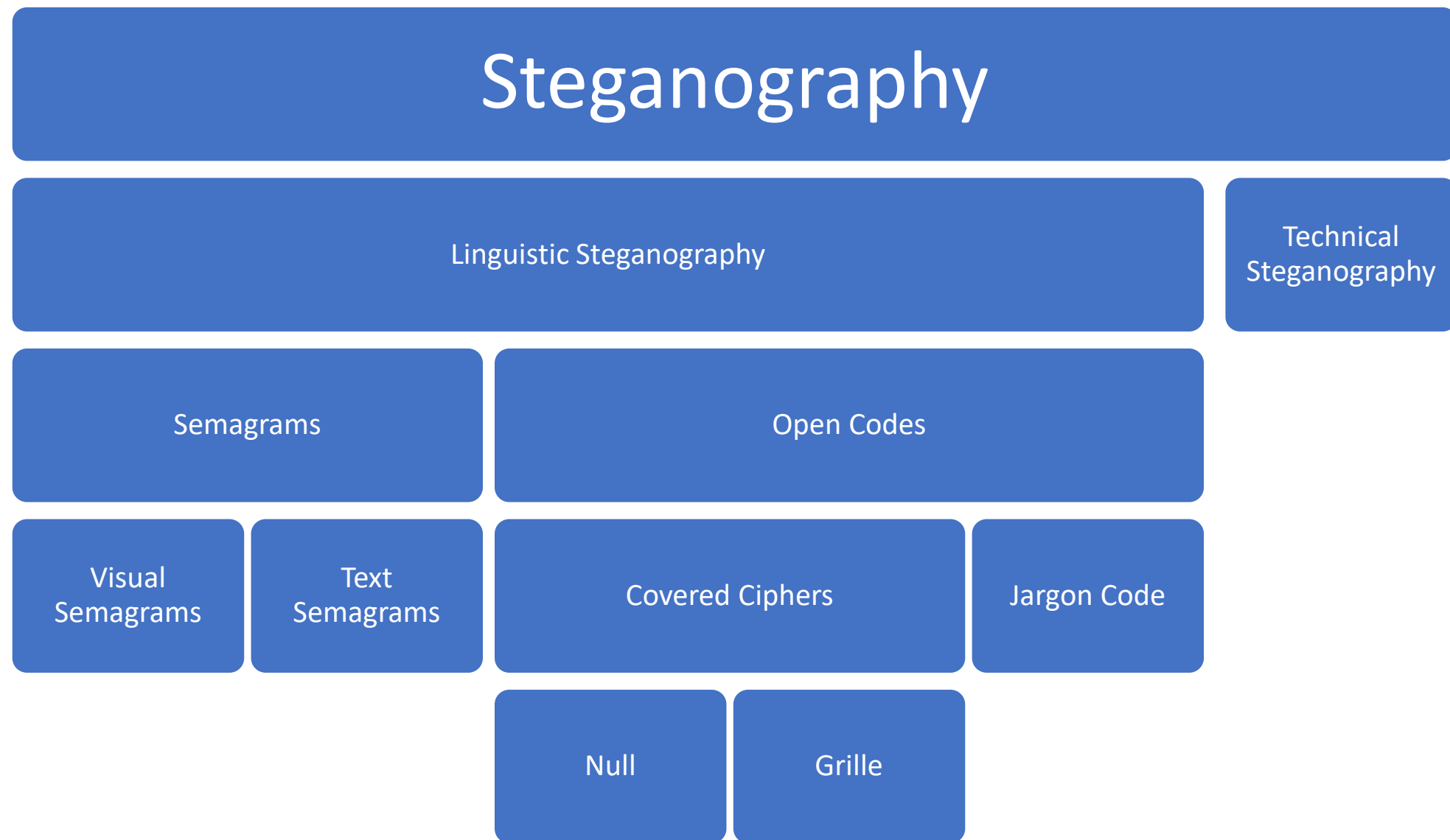
Defending Rootkit

- *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.



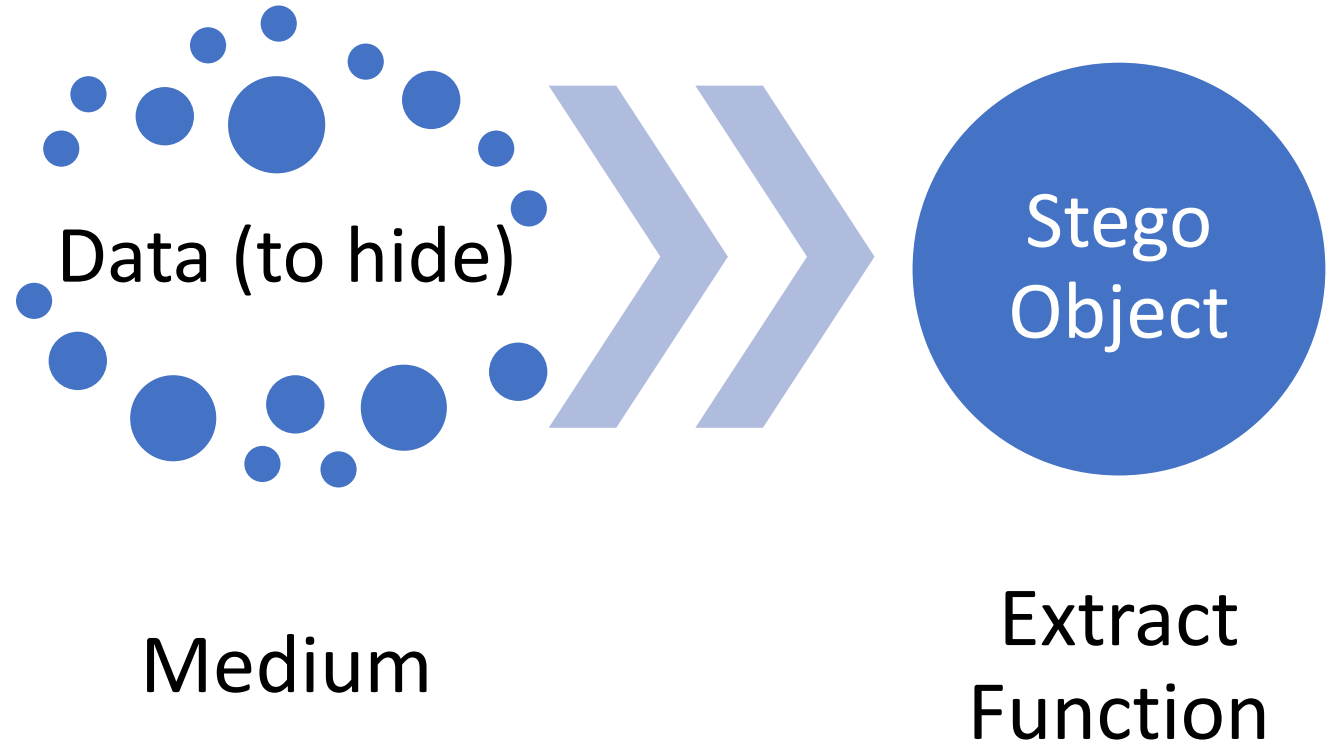


Steganalysis

- 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

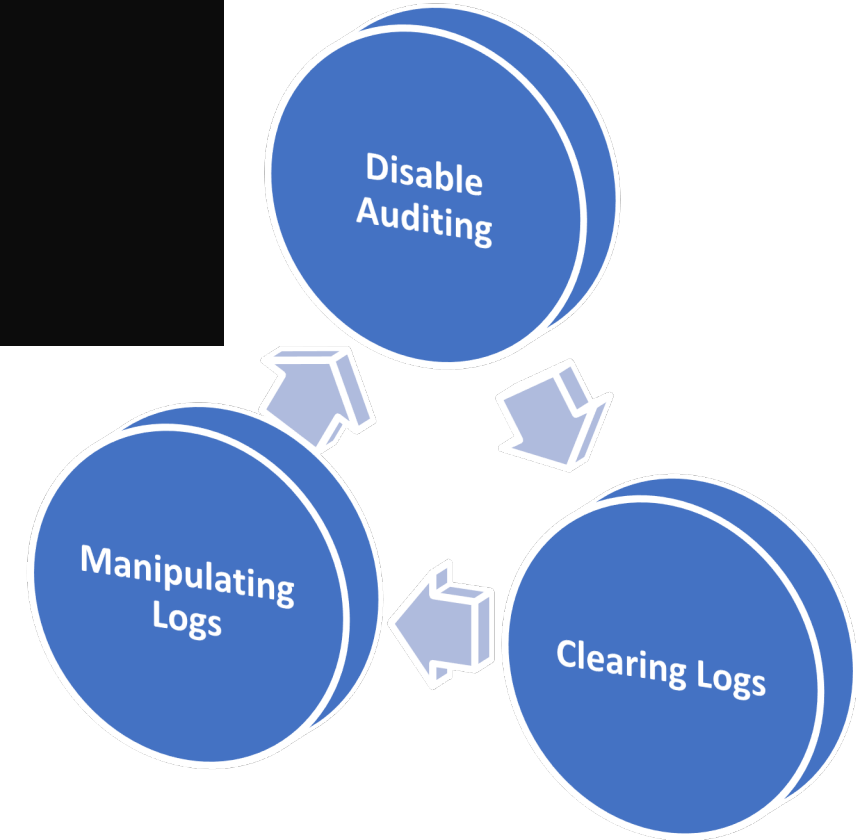
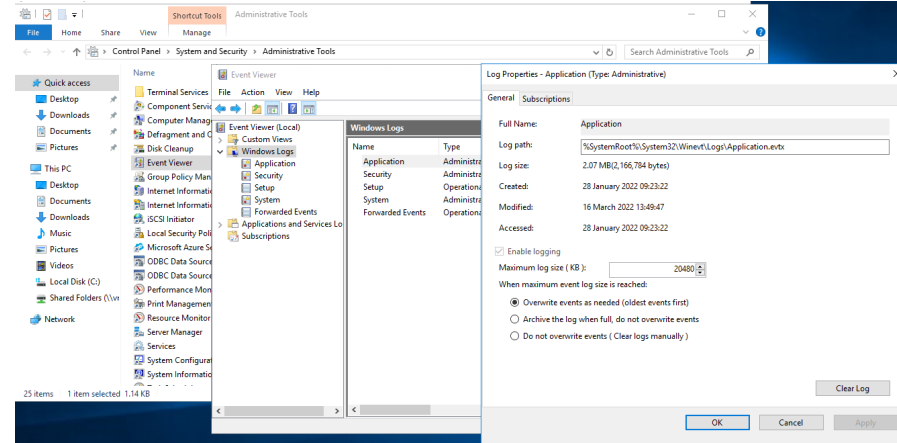
Clearing Logs

- 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

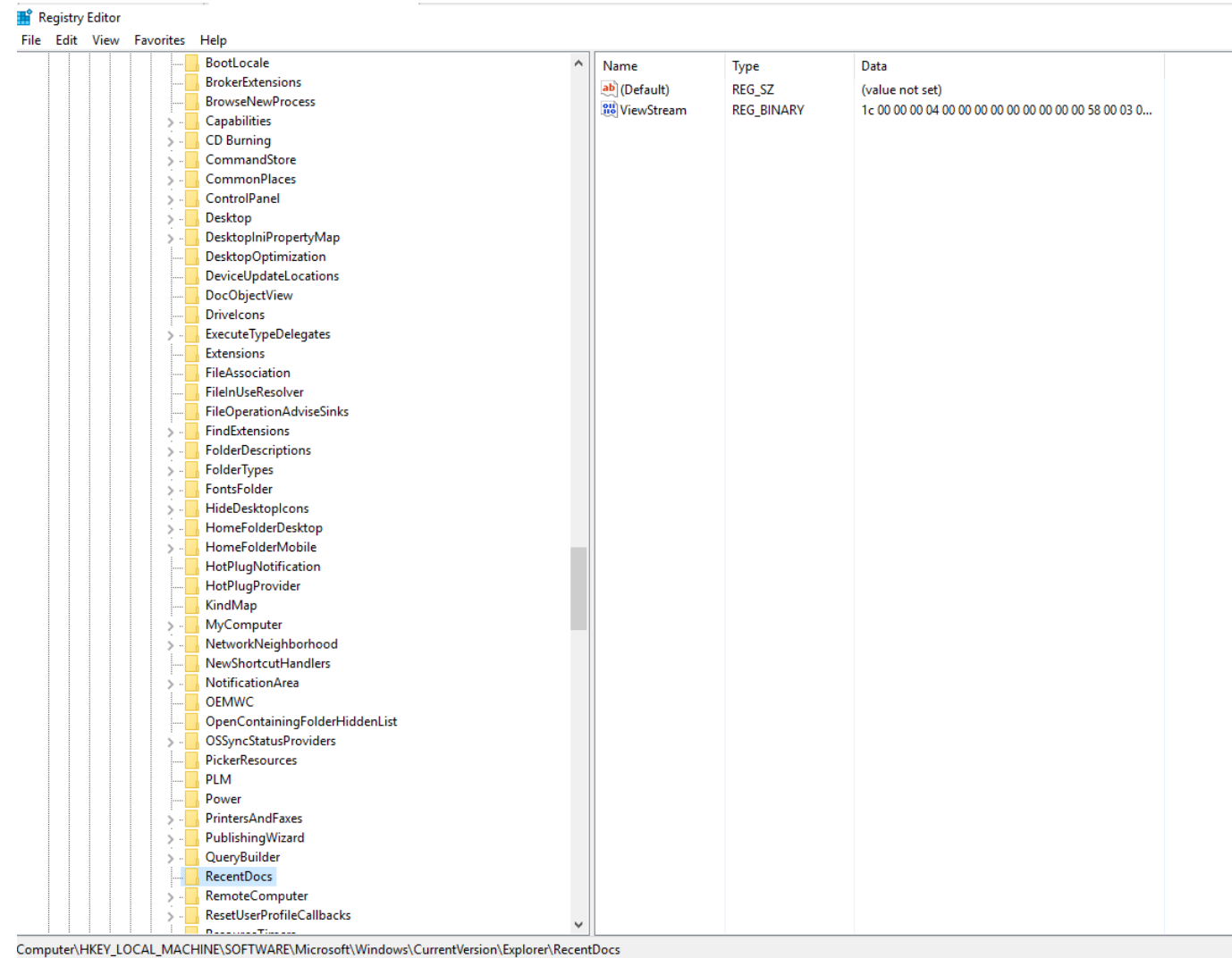
C:\windows\system32>Auditpol.exe /get /category:"Logon/Logoff"
System audit policy
Category/Subcategory          Setting
Logon/Logoff
  Logon                        Success and Failure
  Logoff                       Success
  Account Lockout              Success
  IPsec Main Mode              No Auditing
  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**



Any Questions?

References

- **EC-Council CEH**
- **Cisco Networking Academy**
- **Tevel Cyber Corps**
- **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**