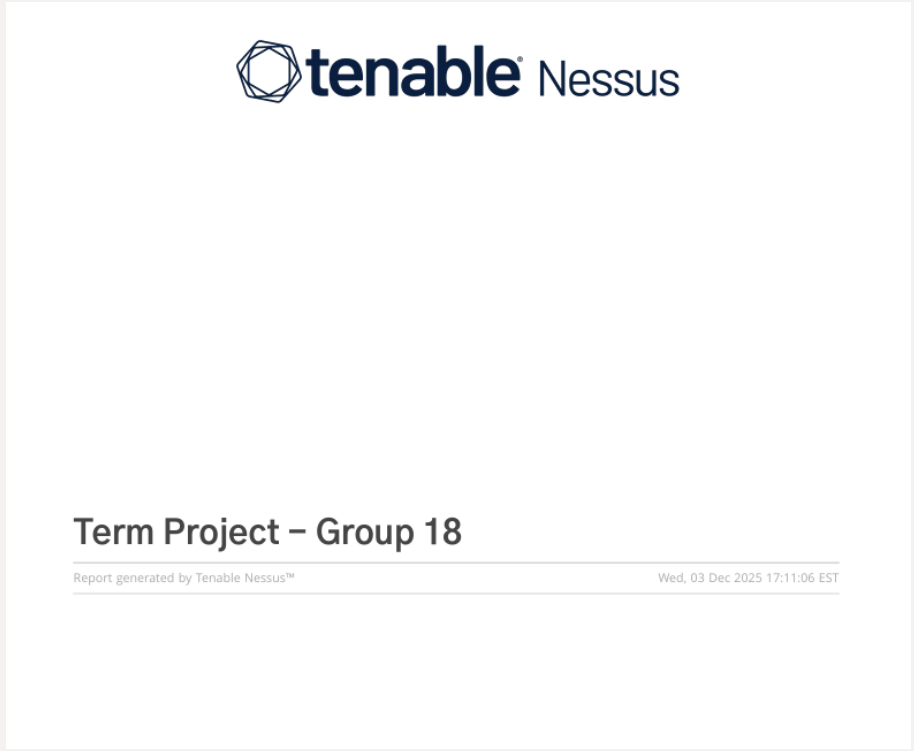
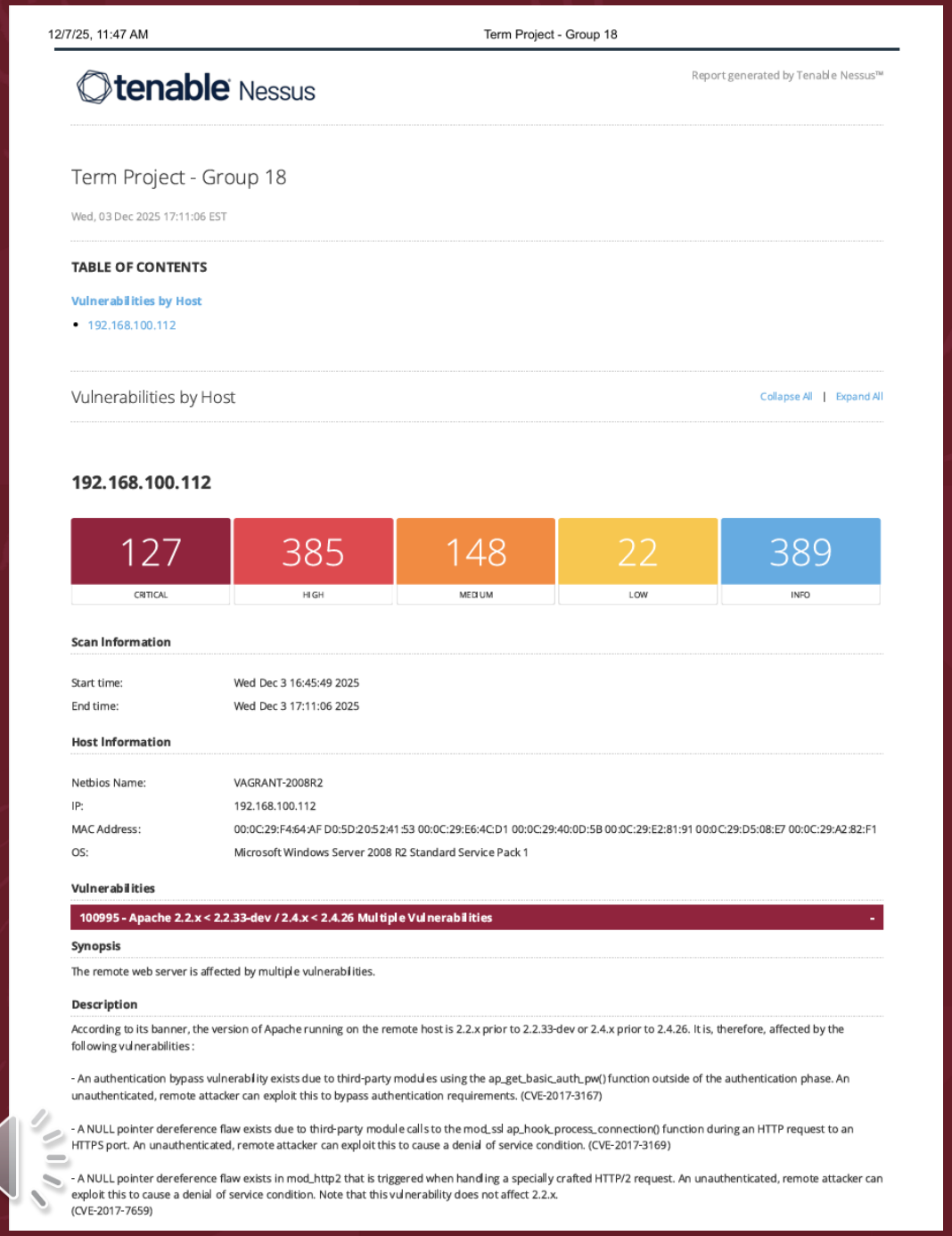
Title: SEC555 Term Project: Offensive & Defensive Operations

- **Subtitle:** The "Lockdown Browser" Incident
- **Group Name:** Group 18
- **Member:** Saket Chahal (SOC Analyst)
- **Date:** December 8, 2025

Vulnerability Report

- **1. Tools Used in Kali Linux**
- To generate the report, the following tool was used within your virtual environment (Kali Linux):
- **Tool: Tenable Nessus Essentials** (Vulnerability Scanner).
- **Platform:** Installed and configured on the **Kali Linux** VM.
- **Target: Metasploitable3** (Windows Server 2008 R2).
- **Usage:** The scanner was used to perform a credentialed scan against the target IP (192.168.100.112) to identify security weaknesses, missing patches, and configuration issues.





12/7/25, 11:47 AM Term Project - Group 18

tenable Nessus

Report generated by Tenable Nessus™

Term Project - Group 18

Wed, 03 Dec 2025 17:11:06 EST

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.100.112

Vulnerabilities by Host

Collapse All | Expand All

192.168.100.112

127	385	148	22	389
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Dec 3 16:45:49 2025

End time: Wed Dec 3 17:11:06 2025

Host Information

Netbios Name: VAGRANT-2008R2

IP: 192.168.100.112

MAC Address: 00:0C:29:F4:64:AF D0:5D:20:52:41:53 00:0C:29:E6:4C:D1 00:0C:29:40:0D:5B 00:0C:29:E2:81:91 00:0C:29:D5:08:E7 00:0C:29:A2:82:F1

OS: Microsoft Windows Server 2008 R2 Standard Service Pack 1

Vulnerabilities

100995 - Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities -

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.33-dev or 2.4.x prior to 2.4.26. It is, therefore, affected by the following vulnerabilities :

- An authentication bypass vulnerability exists due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167)

- A NULL pointer dereference flaw exists due to third-party module calls to the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-3169)

- A NULL pointer dereference flaw exists in mod_http2 that is triggered when handling a specially crafted HTTP/2 request. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. Note that this vulnerability does not affect 2.2.x.
(CVE-2017-7659)

2. Vulnerability Scan Report Details (Task 5a & 5b)

Target System: Metasploitable3 VM

IP Address: 192.168.100.112

MAC Address: 00:0C:29:F4:64:AF

Operating System: Microsoft Windows Server 2008 R2 Standard Service Pack 1

Scan Date/Time: Wed, 03 Dec 2025 from 16:45:49 to 17:11:06 EST

NetBIOS Name: VAGRANT-2008R2

SOC Member Analysis (Task 2a & 2a.i)

I will focus on the **Critical** findings that pose the most immediate risk to the organization. Here are the top critical vulnerabilities identified in the scan and how to fix them.

- **Critical Vulnerability 1: Unsupported Operating System (End of Life)**
- The Issue: The target is running Windows Server 2008 R2, which is End of Life (EOL) and no longer supported by Microsoft. This means no new security patches are released for new threats.

- **Impact:** Critical. The system is vulnerable to unpatched exploits (like BlueKeep) and cannot be secured effectively in its current state.

- **How to Fix:**
- **Immediate Action:** Upgrade the operating system to a currently supported version (e.g., Windows Server 2019 or 2022).
- **Mitigation:** If immediate upgrade is impossible, isolate the machine from the network and strictly limit access.

Critical Vulnerability 2: BlueKeep (CVE-2019-0708) - Remote Desktop Services RCE

- **The Issue:** A remote code execution vulnerability exists in Remote Desktop Services. An unauthenticated attacker can connect via RDP and send specially crafted requests to execute arbitrary code.
- **Impact:** Critical. This is "wormable," meaning it can spread automatically from computer to computer without user interaction.
- **How to Fix:**
- **Patch:** Apply the Microsoft security update for CVE-2019-0708 immediately.
- **Mitigation:** Enable Network Level Authentication (NLA) for RDP, which forces authentication before the vulnerability can be triggered, or block TCP port 3389 at the perimeter firewall.

Critical Vulnerability 3: Apache Struts Remote Code Execution (S2-045 / S2-046)

- **The Issue:** The web application uses a vulnerable version of Apache Struts. An attacker can execute arbitrary code by sending a malicious Content-Type header in an HTTP request.

- **Impact:** Critical. This specific vulnerability (S2-045) is famous for being the cause of major data breaches (e.g., Equifax) because it is easy to exploit remotely.

- **How to Fix:**
- **Patch:** Upgrade Apache Struts to version 2.3.32 or 2.5.10.1 or later.
- **Mitigation:** If patching is delayed, implement a Web Application Firewall (WAF) rule to filter out malicious Content-Type headers.

Critical Vulnerability 4: SMB Server Vulnerabilities (MS11-020)

- **The Issue:** The SMB (Server Message Block) server has a vulnerability that allows an attacker to execute arbitrary code by sending specially crafted packets.

- **Impact:** Critical. Allows attackers to take full control of the system via the network file sharing service.

- **How to Fix:**
- **Patch:** Install the Microsoft security update MS11-020 (KB2508429).
- **Mitigation:** Disable SMBv1 on the host and ensure port 445 is not exposed to the internet.

Critical Vulnerability 5: Apache Log4j Unsupported Version

- **The Issue:** The system is running Apache Log4j 1.x, which is End of Life and contains multiple known vulnerabilities.
- **Impact:** High/Critical. Unsupported logging libraries can be exploited to execute code or cause denial of service.
- **How to Fix:**
- **Patch:** Upgrade to the latest supported version of Apache Log4j 2.x (e.g., 2.17.1 or later). Note that 1.x cannot be simply patched; it must be replaced.

- Our environment is critically exposed due to the use of an End-of-Life operating system (Windows Server 2008 R2). This has left us vulnerable to high-profile exploits like **BlueKeep** and **Apache Struts RCE**. Our immediate remediation plan involves upgrading the OS, patching the specific RCE vulnerabilities in our web applications, and disabling legacy protocols like SMBv1.

Summary of Vulnerability Report

Lab Environment Configuration for SOC Project

VM Name	Role	IP Address	Credentials (User/Pass)	Network Config
VyOS Router	Network Gateway	**192.168.100.1**	`vyos` / `vyos`	**GW:** N/A
Kali Linux	Attacker (C2 Server)	**192.168.100.20**	`student` / `student` *(Root: `kali`)*	**GW:** 192.168.100.1 **DNS:** 192.168.254.1
Windows 10	Victim Workstation	**192.168.100.50**	`student` / `student`	**GW:** 192.168.100.1 **DNS:** 192.168.254.1
Security Onion	SOC / Analyst	**192.168.100.10**	`student` / `student`	**GW:** 192.168.100.1 **DNS:** 192.168.254.1
Metasploitable 3	Vulnerable Target	**192.168.100.112**	`vagrant` / `vagrant`	**GW:** 192.168.100.1 **DNS:** 192.168.254.1

C2 Framework Selection Selected Tool: PowerShell Empire (GUI: Starkiller)

Why we chose it:

•Verified: Listed on the C2 Matrix (Gold Standard for C2 tools).

•Capability: Provides native PowerShell integration for seamless Remote Code Execution (RCE) on Windows environments.

•Differentiation: Distinct from "Sliver" (used in course labs), satisfying the project requirement to explore new tools.

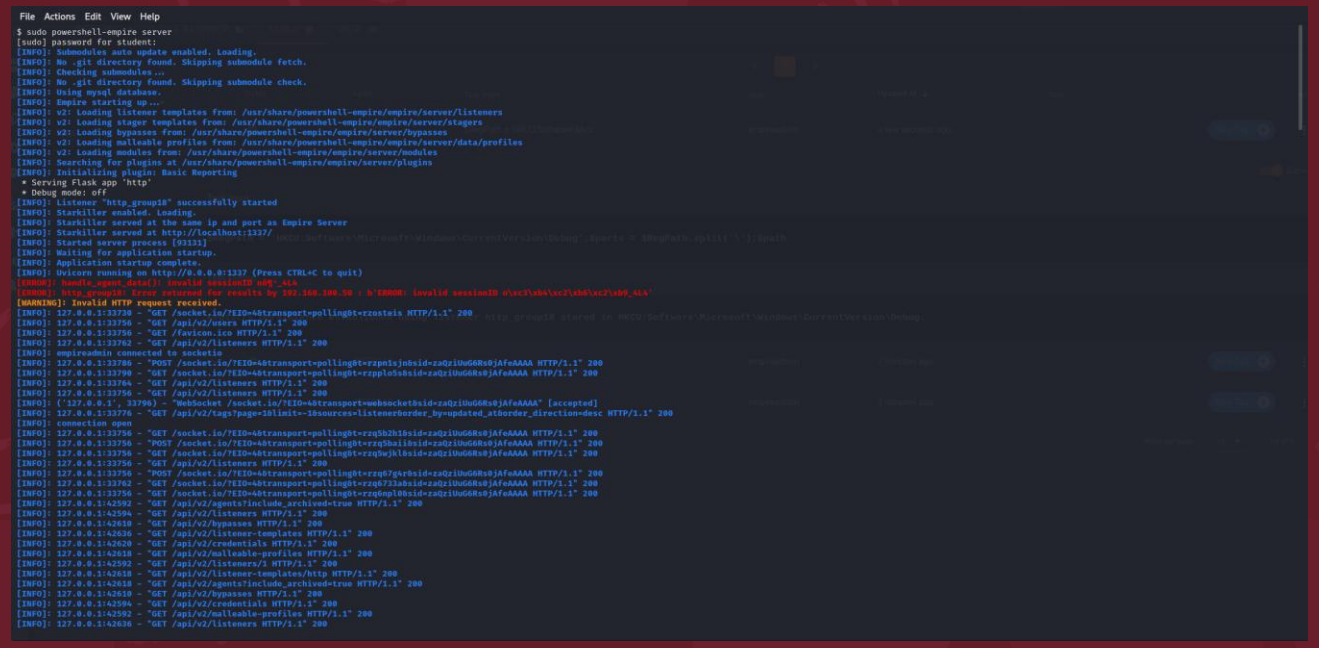
Architecture:

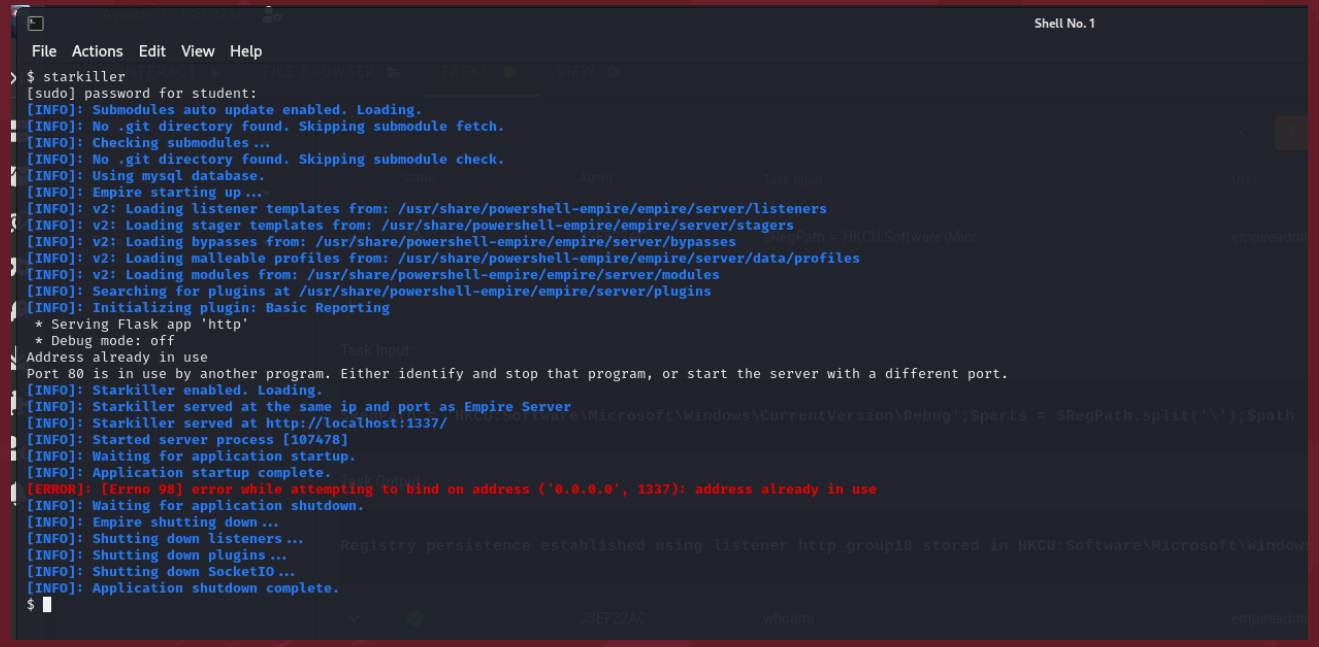
•Server (Attacker): Kali Linux (IP: 192.168.100.20) running the Empire Server.

•Agent (Victim): PowerShell Empire HTTP Agent running on Windows 10.

•Listener: Configured on Port 80 (HTTP) to blend malicious traffic with normal web browsing activity.

Turning On Powershell and Starkiller

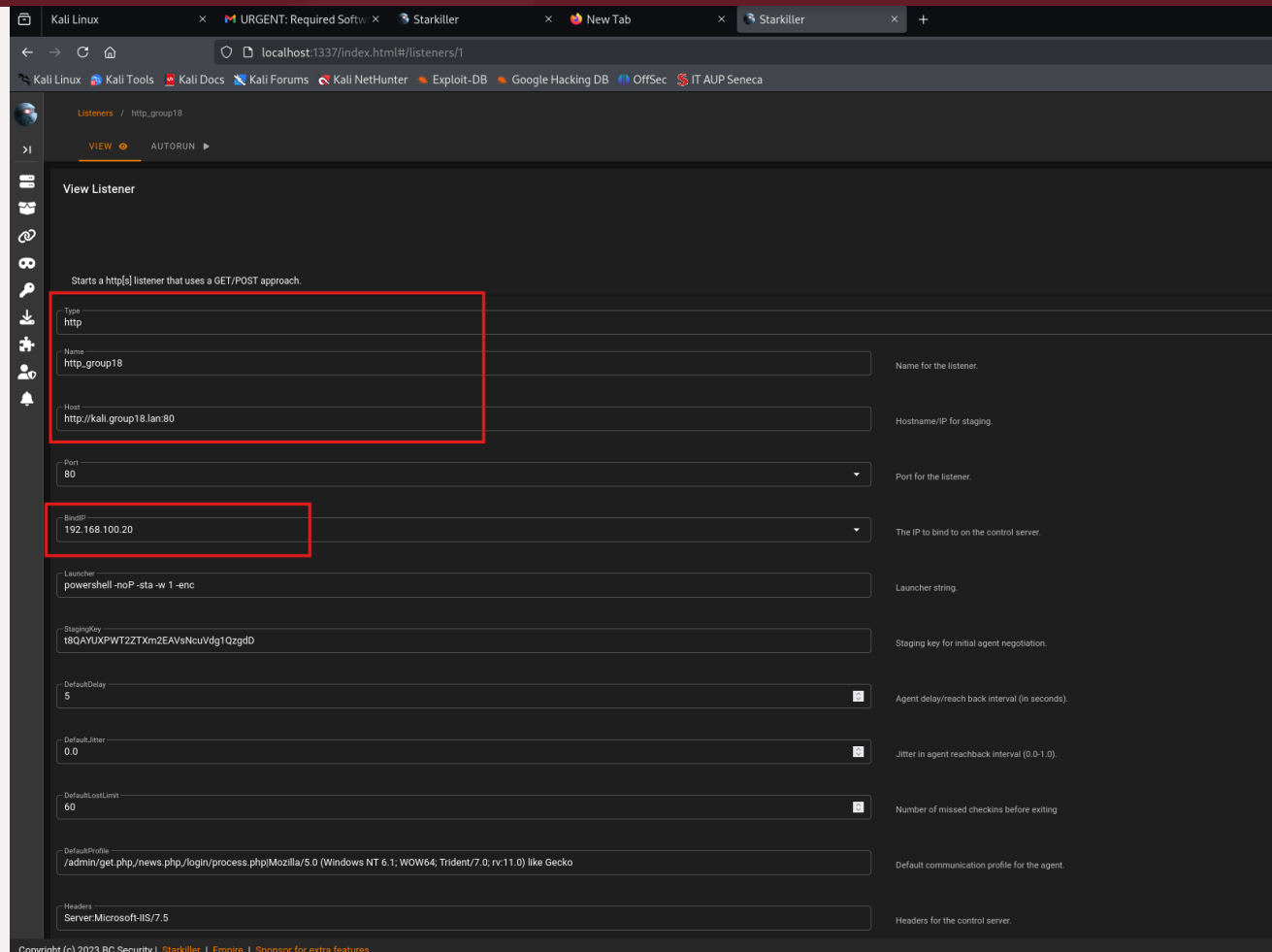




Setting up the Infrastructure (The Listener)

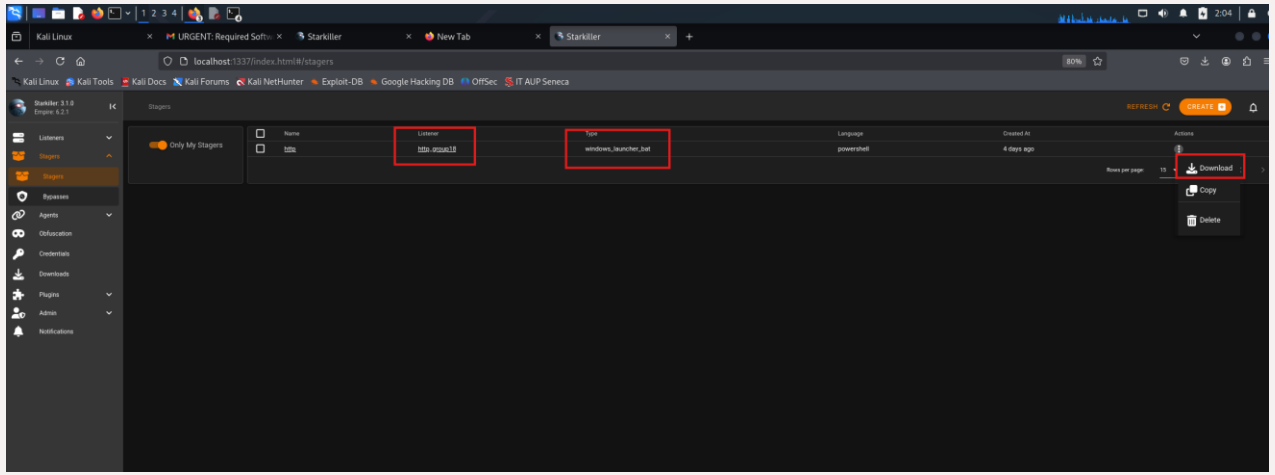
- To establish a communication channel between the attacker and the victim, we configured an HTTP Listener in PowerShell Empire.

  - **Name:** http_group18
  - **Host:** http://kaligroup18.lan (Simulating a legitimate-looking domain)
  - **Bind IP:** 192.168.100.20 (Our Kali Linux Attacker IP)
  - **Port:** 80
  - **Why Port 80?** We deliberately chose the standard HTTP port to blend our malicious traffic in with normal internet browsing, making it harder for firewalls to detect."



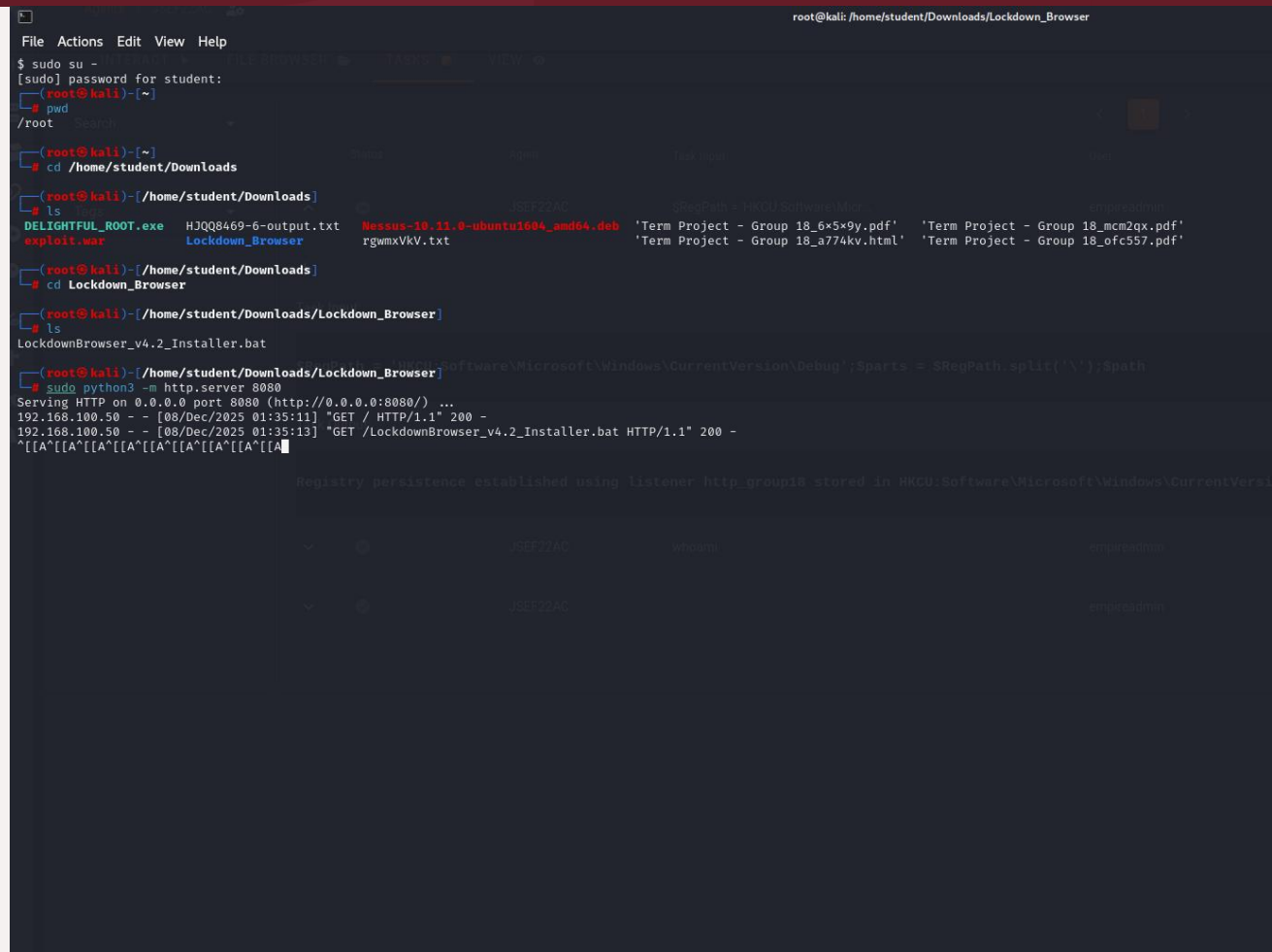
Weaponization (Creating the Payload)

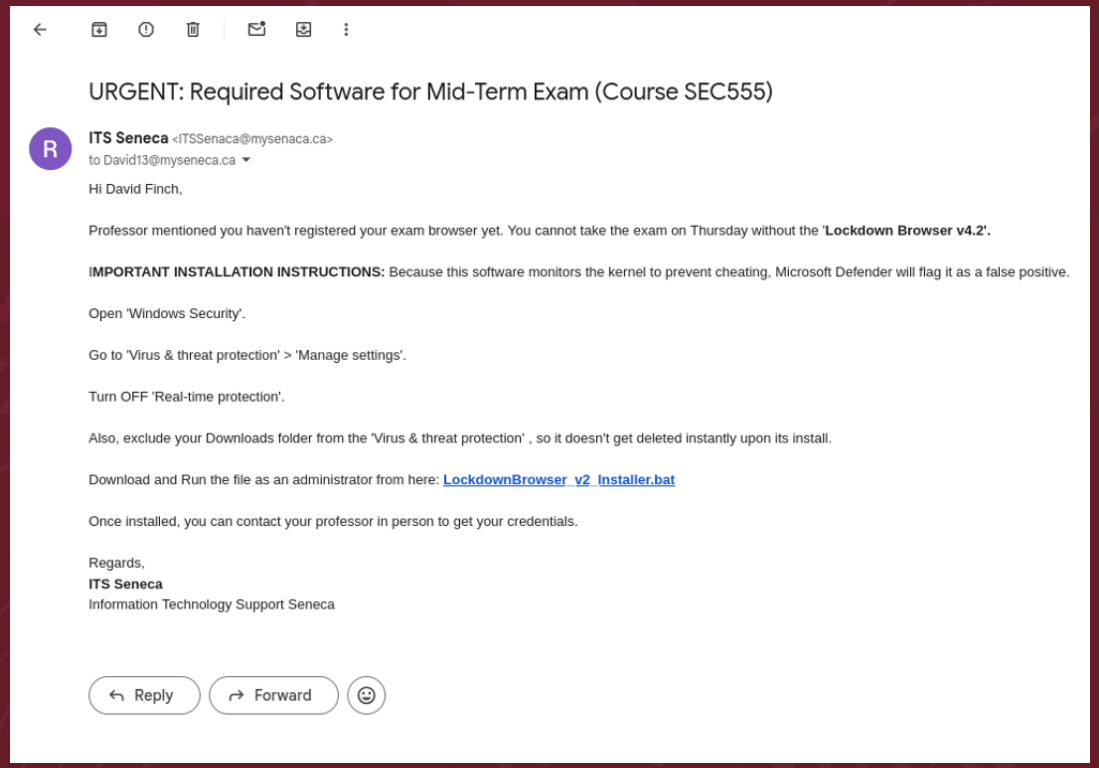
- We generated a Batch File Stager that links back to our active listener.
- **Name:** LockdownBrowser_v4.2_Installer.bat
- **Stager Type:** windows/launcher_bat
- Listener Selected: http_group18 (The one configured in the previous step)
- **The Technique:** This batch file contains a base64-encoded PowerShell command. When executed, it doesn't install software; instead, it forces the victim's computer to reach out to **http://kaligroup18.lan** on port 80 and download the full agent into memory.



Hosting the Payload (Creating the Malicious Link)

- To deliver the payload effectively, we needed a credible download link for our phishing email.
- **Staging:** We moved the LockdownBrowser_Installer.bat into a dedicated hosting directory Lockdown_Browser on our attacker machine.
- **Hosting:** We opened a file-serving port (e.g., Port 8000) to make the directory accessible over the network.
- **The Resulting Link:** This created the URL http://192.168.100.20:8000/LockdownBrowser_Installer.bat, which we embedded in the email. This mimics a legitimate software repository download."





URGENT: Required Software for Mid-Term Exam (Course SEC555)

ITS Seneca <ITSSenaca@mysenaca.ca>
to David13@myseneca.ca

Hi David Finch,

Professor mentioned you haven't registered your exam browser yet. You cannot take the exam on Thursday without the '**Lockdown Browser v4.2'.**

IMPORTANT INSTALLATION INSTRUCTIONS: Because this software monitors the kernel to prevent cheating, Microsoft Defender will flag it as a false positive.

Open 'Windows Security'.

Go to 'Virus & threat protection' > 'Manage settings'.

Turn OFF 'Real-time protection'.

Also, exclude your Downloads folder from the 'Virus & threat protection' , so it doesn't get deleted instantly upon its install.

Download and Run the file as an administrator from here: LockdownBrowser_v2_Installer.bat

Once installed, you can contact your professor in person to get your credentials.

Regards,
ITS Seneca
Information Technology Support Seneca

Reply Forward

The Attack Scenario (Narrative)

Social Engineering Vector: "The Midterm Panic"

The Context:

- It is midterm exam week. Stress levels are high.
- The victim (Student) receives an urgent email claiming they are missing mandatory proctoring software ("Lockdown Monitor v4.2") required to take their exam.

The Pretext (The Lie, Phising):

- The email appears to come from “ITS Support”, telling the student to download the school’s latest lockdown browser version for the exam on Thursday.
- It explicitly instructs the user to disable Windows Defender Real-Time Protection to avoid "false positives" during the installation of the anti-cheat kernel driver.

The Payload:

- File: LockdownBrowser_v2_Installer.bat
- Type: A malicious batch file that executes a hidden PowerShell script.
- Technique: Invokes PowerShell Empire stager to establish a Command and Control (C2) connection.

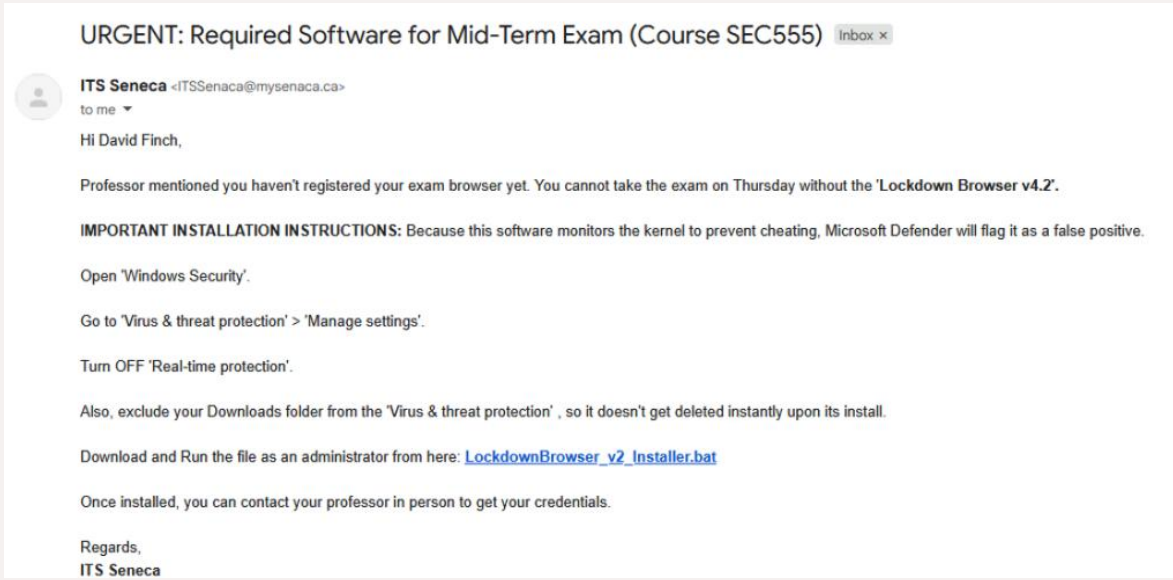
Attack Execution Flow

Delivery: Victim receives the phishing email with a link to the "installer" hosted on the attacker's server (Kali HTTP port 8080).

Compliance: Trusting the authority of "ITS Support," the victim navigates to Windows Security > Virus & threat protection and manually toggles "Real-time protection" to OFF.

Infection: The victim downloads LockdownBrowser_v2_Installer.bat and runs it as Administrator.

Compromise: The batch file executes, connecting back to the C2 server (192.168.100.20) on port 80.



URGENT: Required Software for Mid-Term Exam (Course SEC555) Inbox ×

ITS Seneca <ITSSenaca@mysenaca.ca>
to me

Hi David Finch,

Professor mentioned you haven't registered your exam browser yet. You cannot take the exam on Thursday without the **'Lockdown Browser v4.2'.**

IMPORTANT INSTALLATION INSTRUCTIONS: Because this software monitors the kernel to prevent cheating, Microsoft Defender will flag it as a false positive.

Open 'Windows Security'.

Go to 'Virus & threat protection' > 'Manage settings'.

Turn OFF 'Real-time protection'.

Also, exclude your Downloads folder from the 'Virus & threat protection' , so it doesn't get deleted instantly upon its install.

Download and Run the file as an administrator from here: LockdownBrowser_v2_Installer.bat

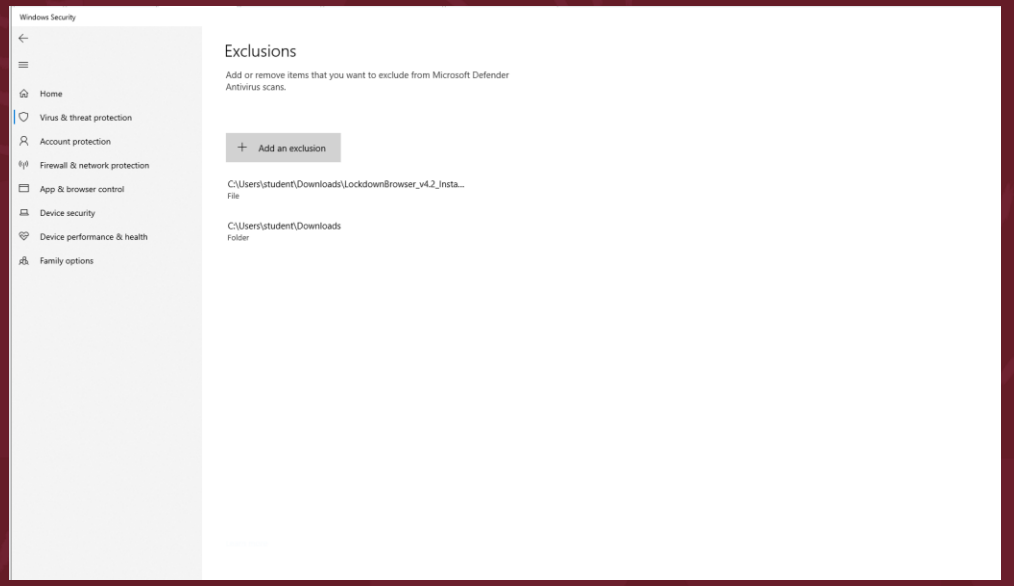
Once installed, you can contact your professor in person to get your credentials.

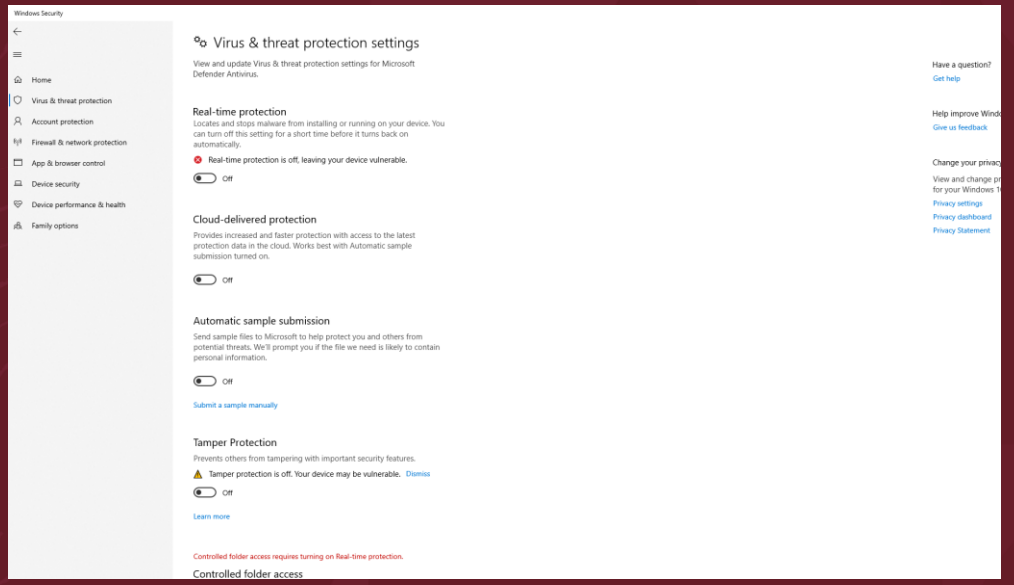
Regards,
ITS Seneca

Social Engineering & User Compliance

- **The Phish:**
- The user received the spoofed email instructing them to disable security to "fix" the installation.

- **The Bypass (Crucial Step):**
- Following the instructions, the student manually added an Exclusion for the Downloads folder in Windows Defender, blinding the antivirus to our malware in that location.

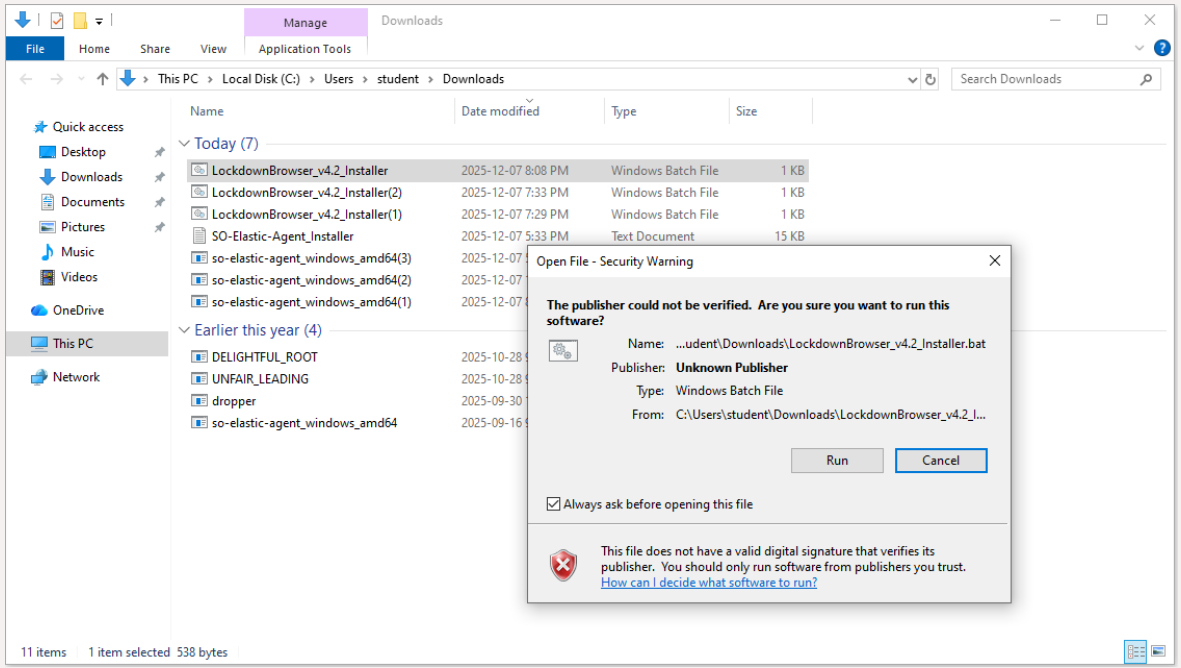




Malicious File Execution

- **The Execution:**
- The user located the LockdownBrowser_v4.2_Installer.bat file in the excluded folder.
- Believing it required high privileges to install the "Anti-Cheat Driver," the user right-clicked and selected "Run as Administrator."

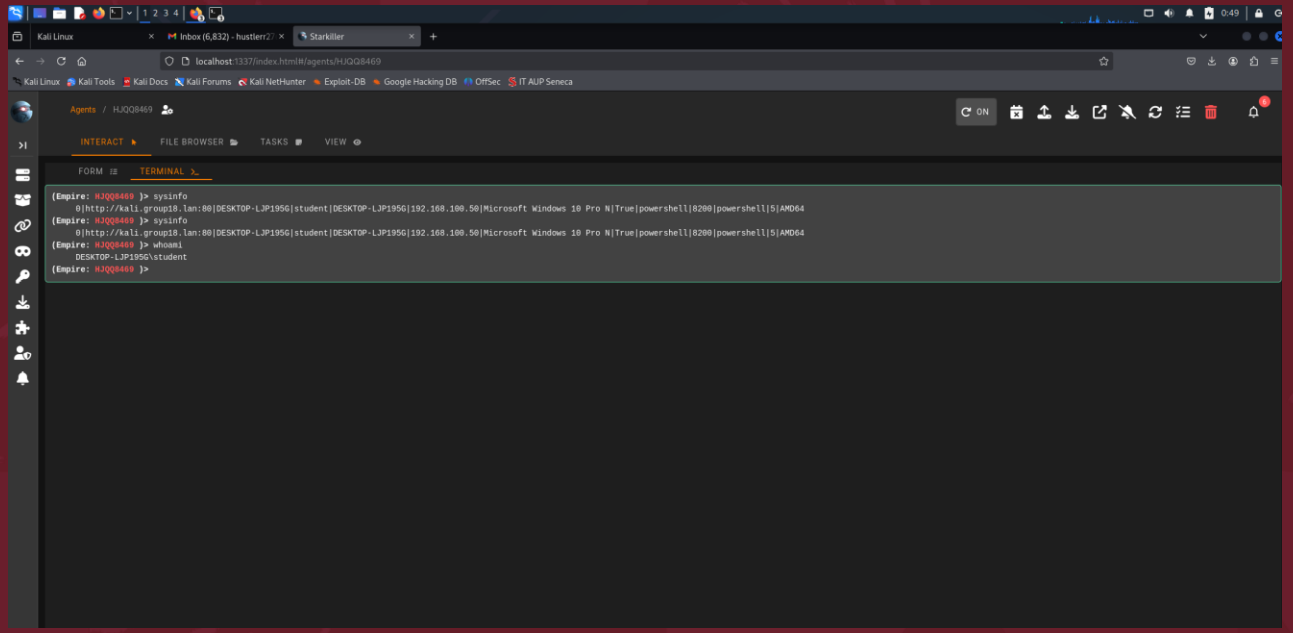
- **The Result:**
- This action granted our payload full administrative rights on the system, bypassing UAC (User Account Control) and establishing a high-privilege C2 session.

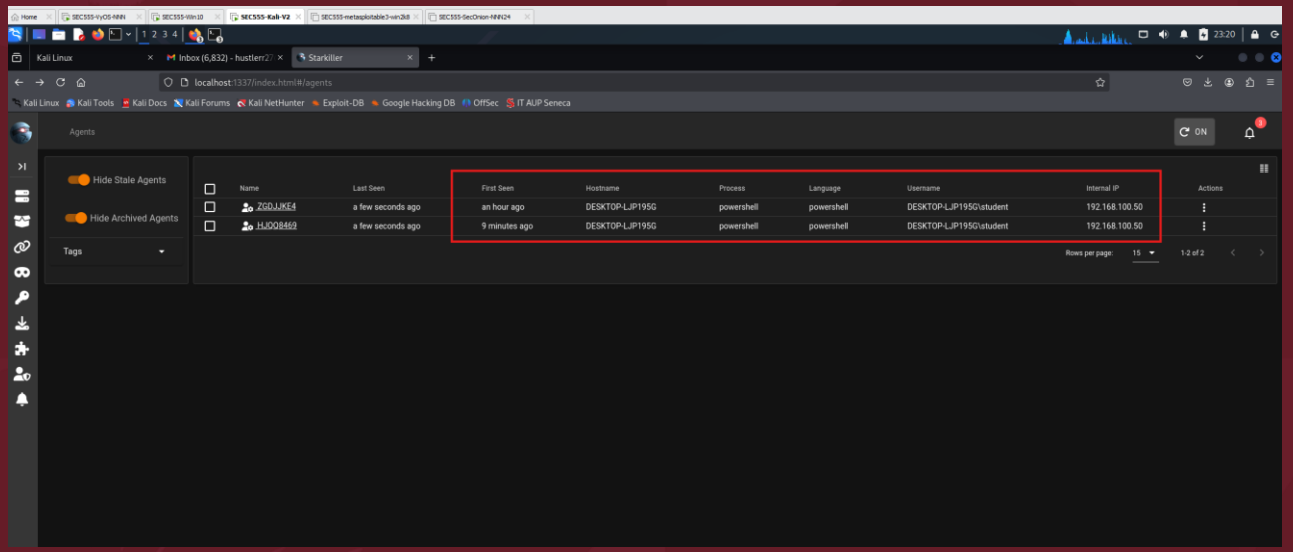


Agents activated and Remote Code Execution

- **Initial Access:**
- Immediately after the user ran the batch file, we received a callback on our Empire listener.

- **Enumeration & Control:**
- We interacted with the agent to verify our level of access.
- executed whoami to confirm we were running as the user student.
- Executed sysinfo to pull the IP address (192.168.100.50) and Hostname (DESKTOP-LJP195G).





Establishing Persistence (Rubric 2.c.i)

The Technique:

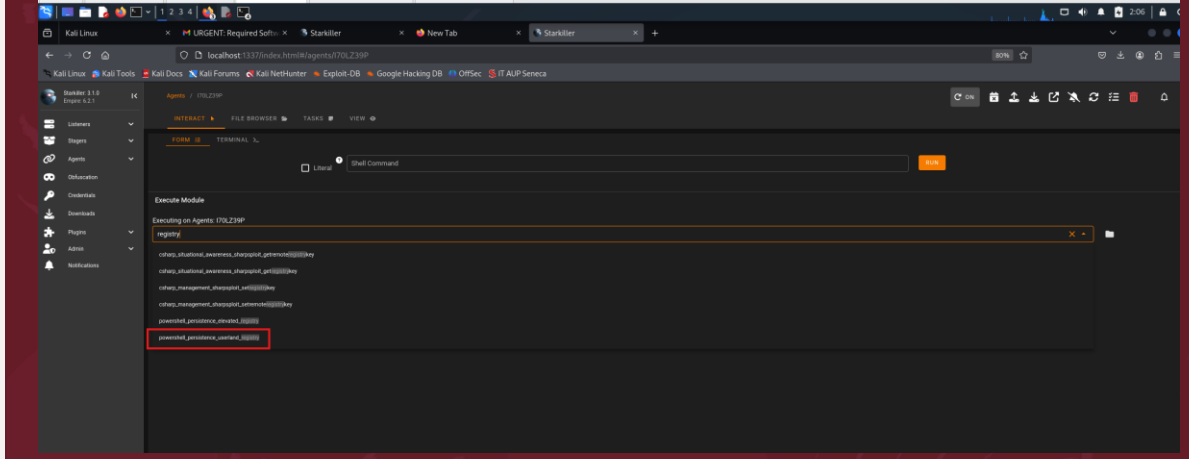
- To ensure we retained access after the student turned off their computer, we used the Registry Run Key technique.
- We configured the Empire persistence/userland/registry module to implant a hidden trigger.

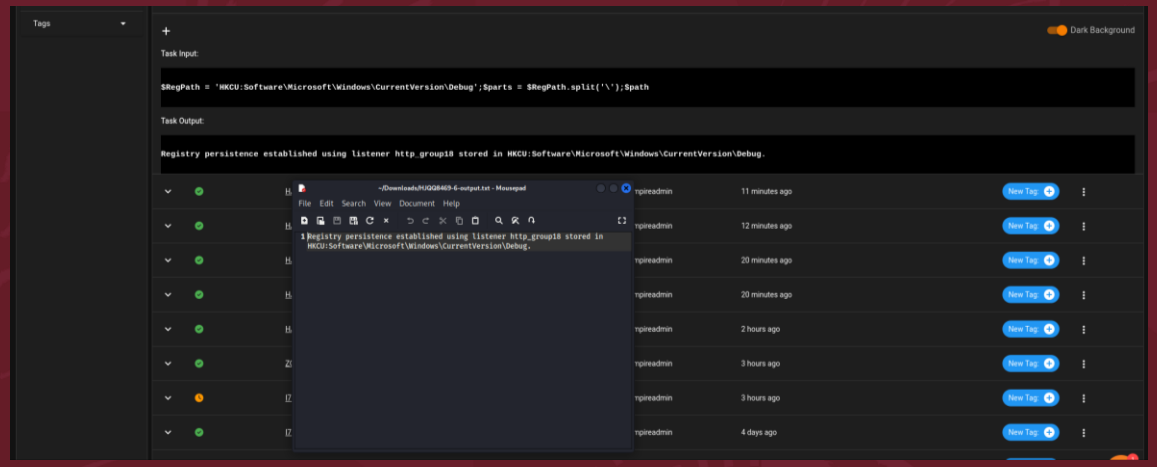
Execution:

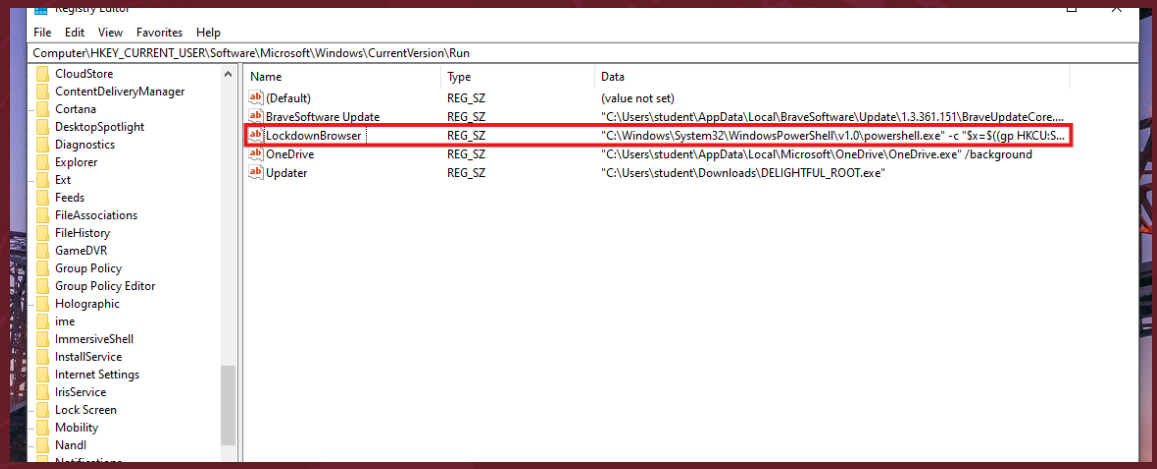
- The module edited the Windows Registry to add a key named "LockdownBrowser"

Success Verification:

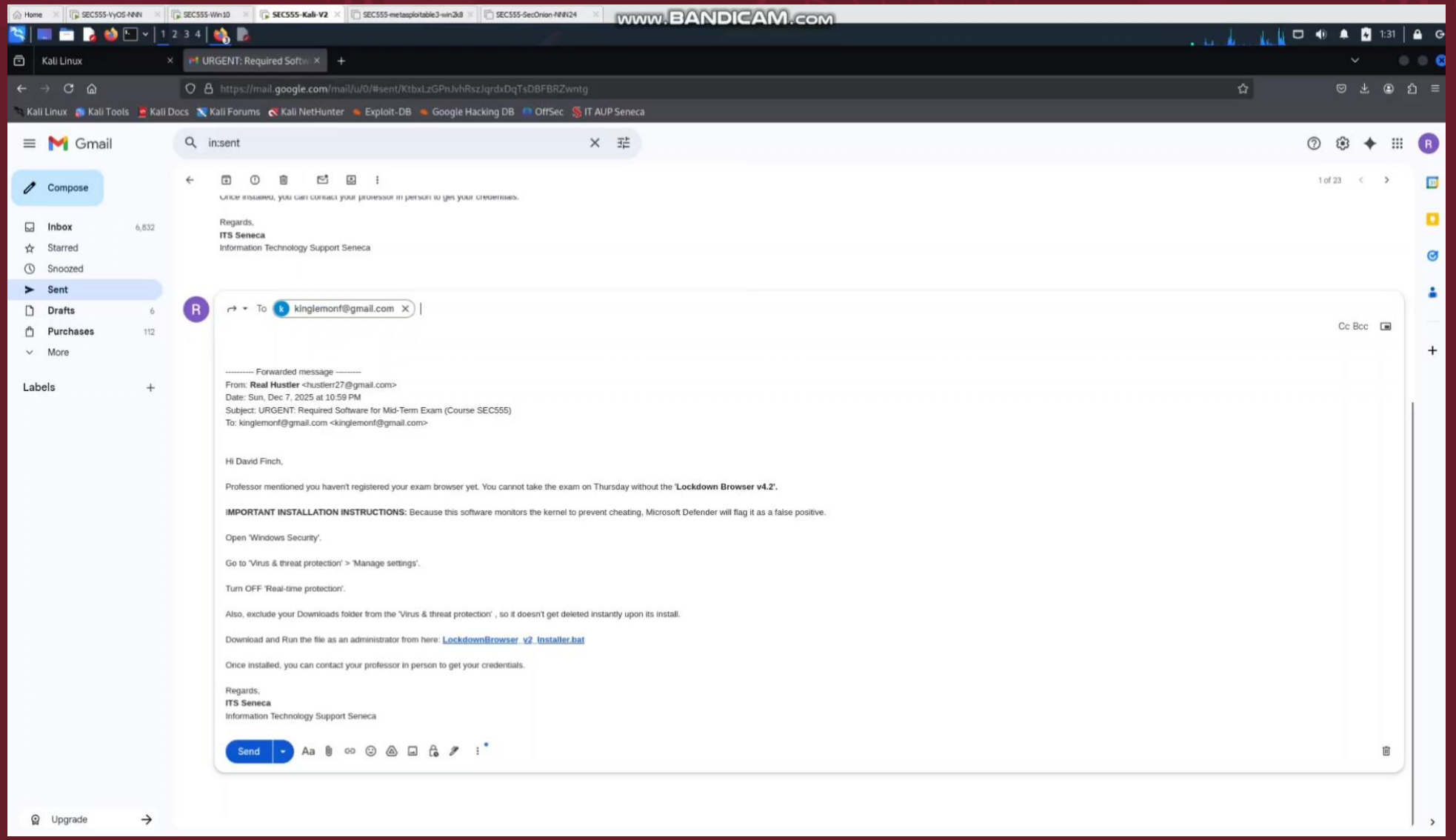
- The console confirmed the registry key was successfully written to HKCU\Software\Microsoft\Windows\CurrentVersion\Run.
- Insert Screenshot: persistance successfully gained ss 12.png







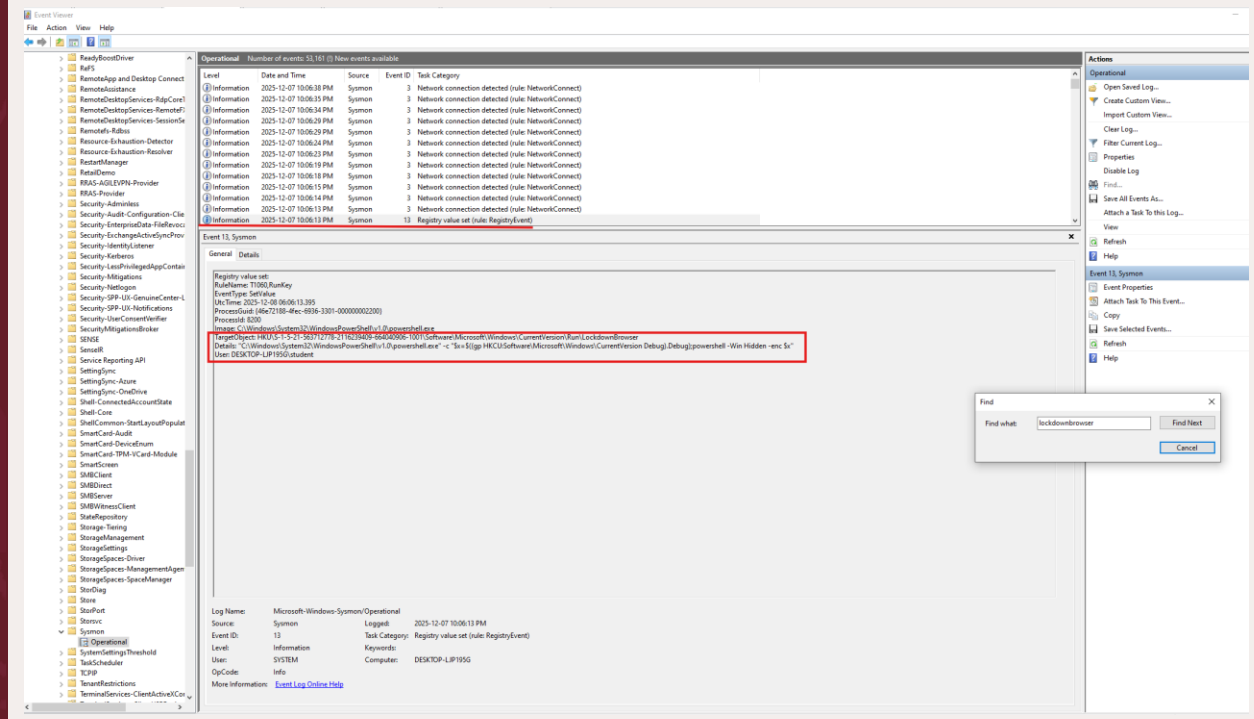
Complete Attack Video with Persistence Group 18

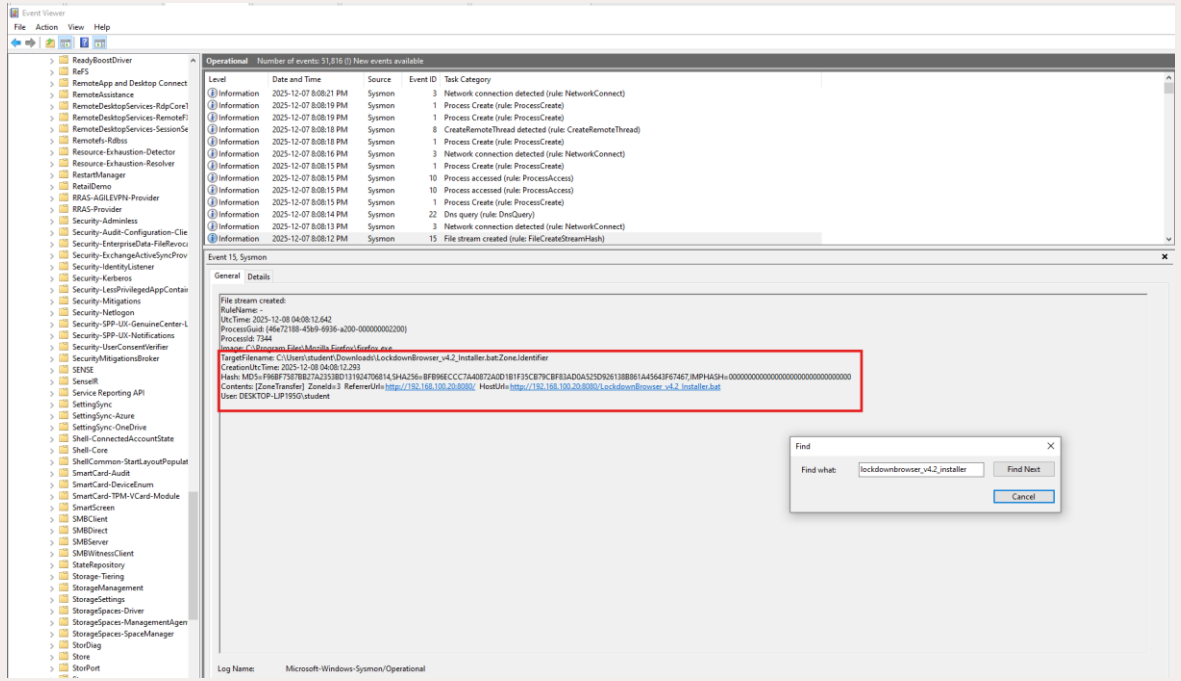


Indicators of Compromise (IOCs)

- **IOCs for Threat Hunting & Containment**
- **1. Network Indicators (Block & Alert)**
- Malicious C2 IP: 192.168.100.20
- Context: Any internal workstation communicating with this IP is compromised.
- Malicious Domain: kali.group18.lan
- Source: Found in the Empire agent configuration
- **2. Port: TCP/80 (HTTP traffic).**
- Payload URL: http://192.168.100.20:8080/LockdownBrowser%20v4.2%20Installer.bat

- **2. Host-Based Indicators (Scan & Remediate)**
- Malicious Filename: LockdownBrowser v4.2 Installer.bat
- Location: C:\Users\student\Downloads\
- Persistence Mechanism (Registry):
- Key Path: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Key Name: Updater
- Value Data: Contains LockdownBrowser / Hidden PowerShell script.
- Infected Hostname: DESKTOP-LJP195G (The patient zero).





Defender:Incident Summary (Rubric 2.d.i)

- **Incident Report:** The "Lockdown Browser" Compromise
- **Date of Incident:** December 8, 2025
- **Affected Asset:** Workstation DESKTOP-LJP195G (192.168.100.50)
- **Summary:**

- The SOC detected unauthorized network communication to an external IP (192.168.100.20).
- Investigation revealed the user fell victim to a phishing campaign disguised as an exam software update.
- The attacker achieved Remote Code Execution (RCE) and successfully established Persistence via the Windows Registry.

Infection Analysis - Initial Access (Rubric 2.d.ii.1)

- **The Start of the Chain:**
- I identified the delivery vector as a malicious email instructing the user to download a batch file.
- **Artifact Discovery:** Malicious email identified in user inbox instructing Anti Virus bypass.

URGENT: Required Software for Mid-Term Exam (Course SEC555) Inbox ×

ITS Seneca <ITSSenaca@mysenaca.ca>
to me

Hi David Finch,

Professor mentioned you haven't registered your exam browser yet. You cannot take the exam on Thursday without the **'Lockdown Browser v4.2'.**

IMPORTANT INSTALLATION INSTRUCTIONS: Because this software monitors the kernel to prevent cheating, Microsoft Defender will flag it as a false positive.

Open 'Windows Security'.

Go to 'Virus & threat protection' > 'Manage settings'.

Turn OFF 'Real-time protection'.

Also, exclude your Downloads folder from the 'Virus & threat protection' , so it doesn't get deleted instantly upon its install.

Download and Run the file as an administrator from here: LockdownBrowser_v2_Installer.bat

Once installed, you can contact your professor in person to get your credentials.

Regards,
ITS Seneca
Information Technology Support Seneca

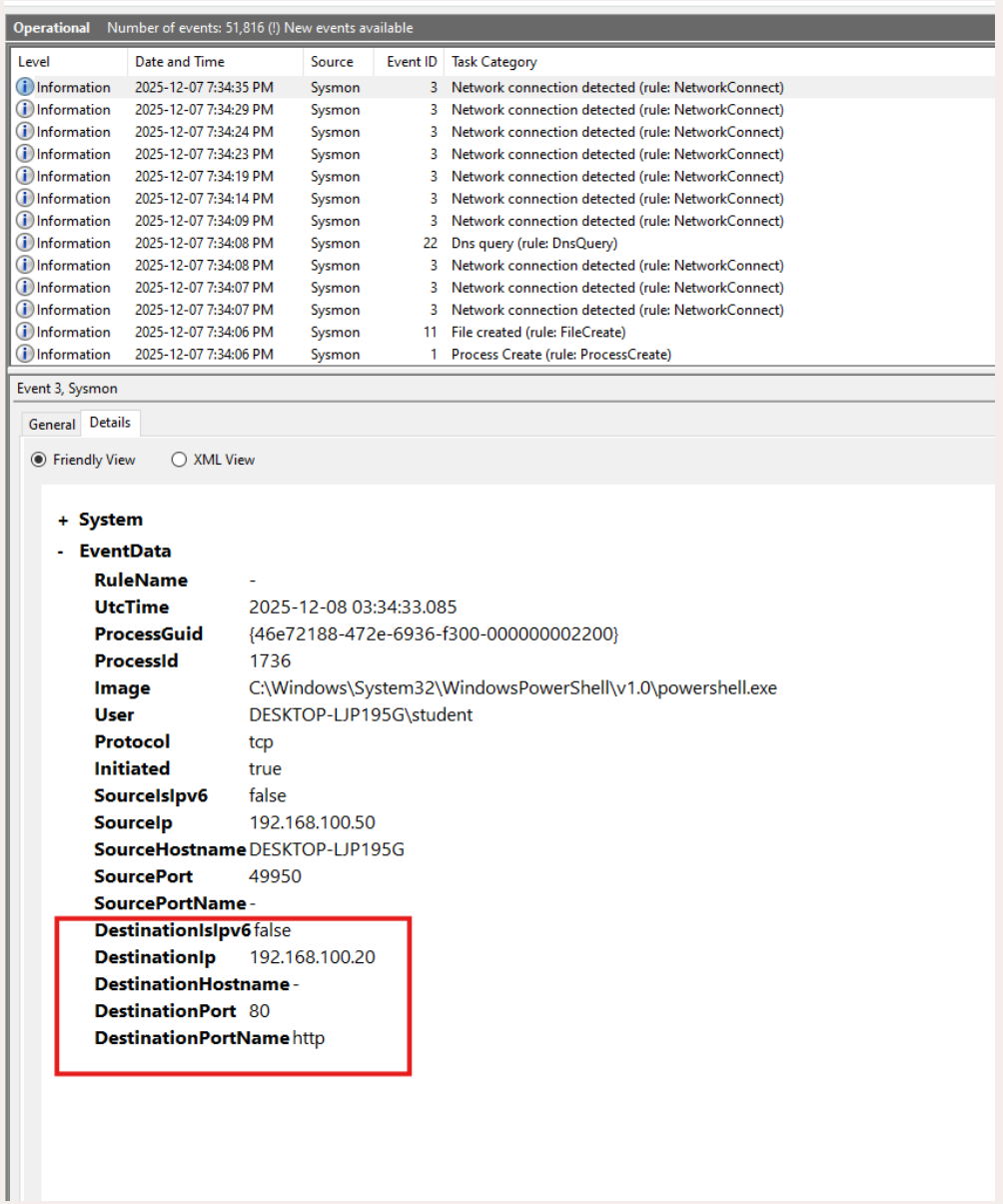
Reply Forward

Network Detection (C2 Communication)

- **The Beacon:**
- Sysmon Event ID 3 (Network Connection) captured the malicious process calling back to the attacker.

- **Analysis of Evidence:**
- Process: powershell.exe (Spawns from the batch file).
- Destination: 192.168.100.20 (Attacker Node).
- Port: 80 (HTTP).

- **Proof:**
- Attacker's ip detected in a network connection
- Attacker's ip detected in a network connection SS3 DETAILS TAB
- Sysmon Event 3: Detailed view confirming outbound connection to known threat IP



Operational Number of events: 51,816 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	2025-12-07 7:34:35 PM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	2025-12-07 7:34:29 PM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	2025-12-07 7:34:24 PM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	2025-12-07 7:34:23 PM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	2025-12-07 7:34:19 PM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	2025-12-07 7:34:14 PM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	2025-12-07 7:34:09 PM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	2025-12-07 7:34:08 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	2025-12-07 7:34:08 PM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	2025-12-07 7:34:07 PM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	2025-12-07 7:34:07 PM	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	2025-12-07 7:34:06 PM	Sysmon	11	File created (rule: FileCreate)
Information	2025-12-07 7:34:06 PM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 3, Sysmon

General Details

Friendly View XML View

+ System

- EventData

RuleName	-
UtcTime	2025-12-08 03:34:33.085
ProcessGuid	{46e72188-472e-6936-f300-000000002200}
ProcessId	1736
Image	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
User	DESKTOP-LJP195G\student
Protocol	tcp
Initiated	true
SourceIsIpv6	false
SourceIp	192.168.100.50
SourceHostname	DESKTOP-LJP195G
SourcePort	49950
SourcePortName	-
DestinationIsIpv6	false
DestinationIp	192.168.100.20
DestinationHostname	-
DestinationPort	80
DestinationPortName	http

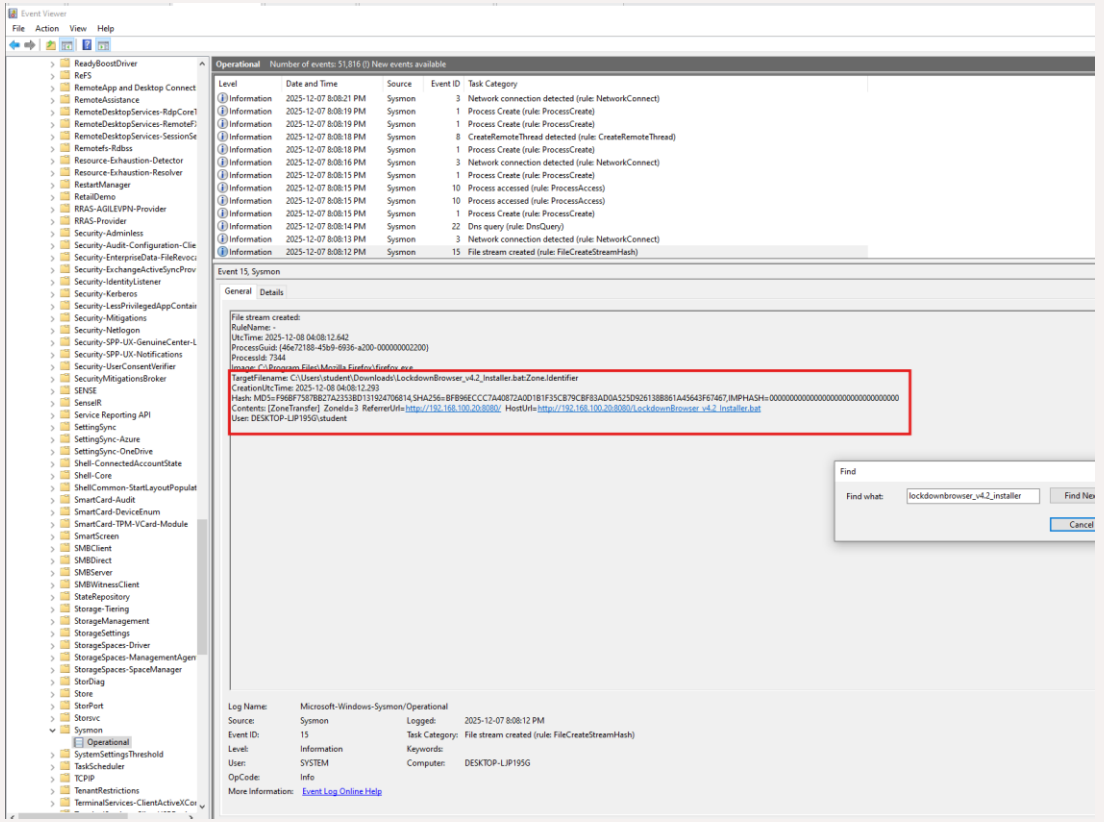
Root Cause Analysis - Payload Discovery

- **Source of Infection Identified:** The Open Directory containing the payload.
- **Investigation Step:**
- Following the detection of suspicious network traffic to 192.168.100.20 on port 8080, we investigated the destination URL.

- **Critical Finding:**
- The attacker hosted an unprotected web directory containing the malicious payload.
- File Identified: LockdownBrowser_v4.2_Installer.bat

- **Conclusion:**
- This confirms the "Delivery" phase of the attack chain. The user was directed to this specific URL through the phising email to download the infected batch file.

- **Visual Evidence:**
- Forensic Discovery: **Attacker's hosting directory revealing the malicious batch file used for initial compromise.**
- I saw the user's computer communicating with the IP ending in .20 on port 8080, we navigated to that address to see what was being hosted.
- **I discovered an open directory containing a single file: LockdownBrowser v4.2 Installer.bat.** This definitively links the network traffic to the malware. It proves that this specific URL was the distribution point for the infection, confirming that the attacker hosted the file here for the user to download.



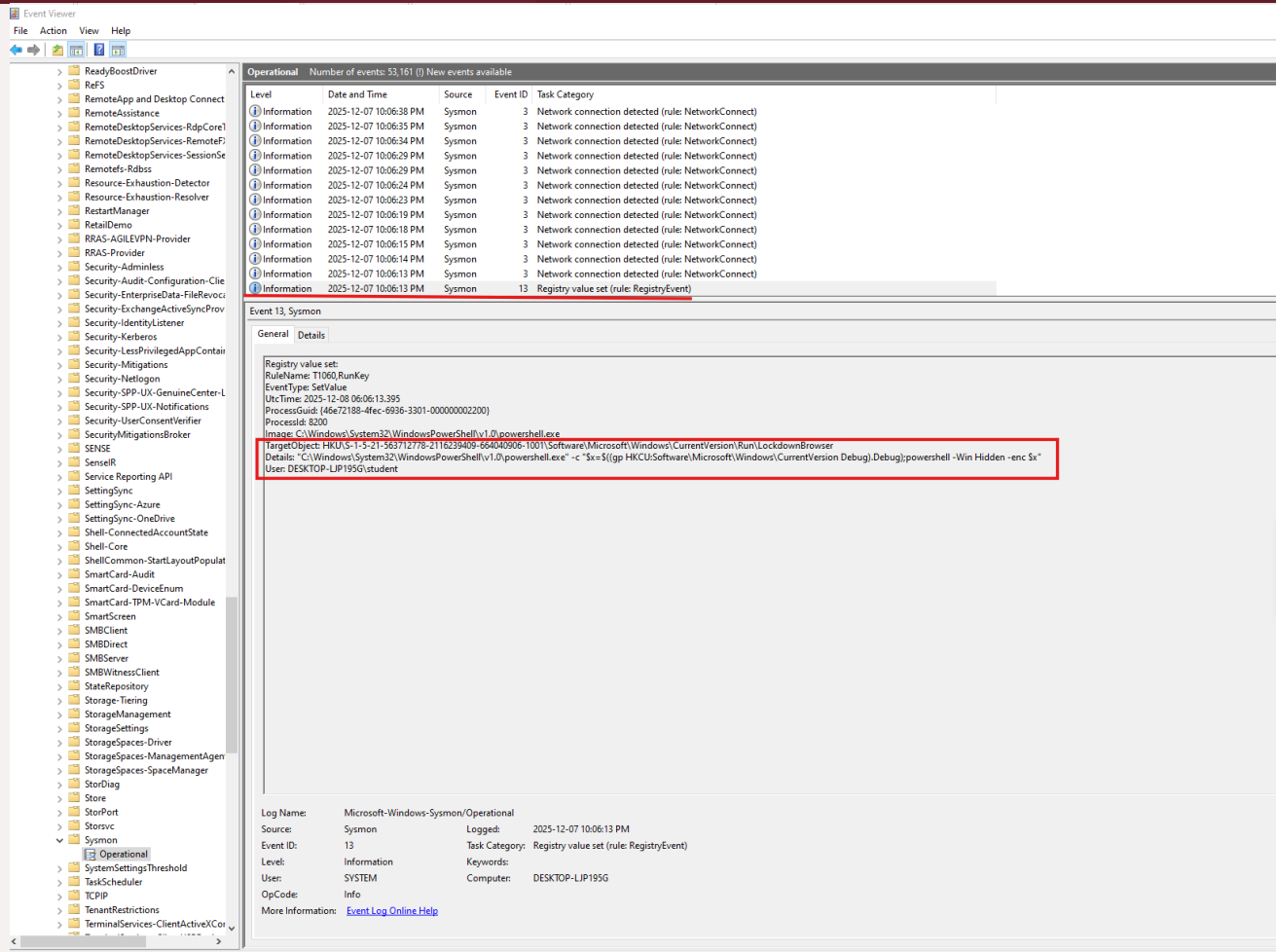
Persistence Detection (Rubric 2.d.ii.4)

- **Was the attacker able to get persistence**?
- YES. Logs confirm the attacker modified the system configuration to survive reboots.

- **The Smoking Gun:**
- **Sysmon Event ID 13 (Registry Value Set) captured the modification of the "Run" keys**

- Evidence:
- Target Object:
  HKCU\Software\Microsoft\Windows\CurrentVersion\Run\LockdownBrowser
- Details: This key ensures the malware launches automatically when the student logs in.

- **Proof:**
- REGISTRY KEY EDITED TO MAINTAIN PERSISTANCE
- Sysmon Event 13: Alert generated by unauthorized modification of Registry Run keys.

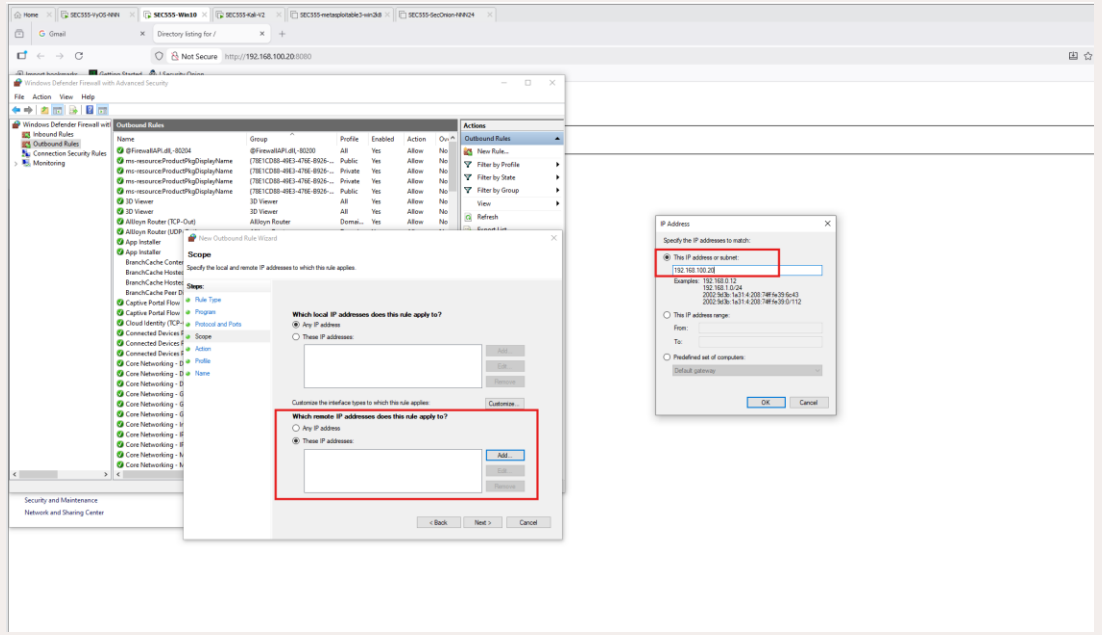


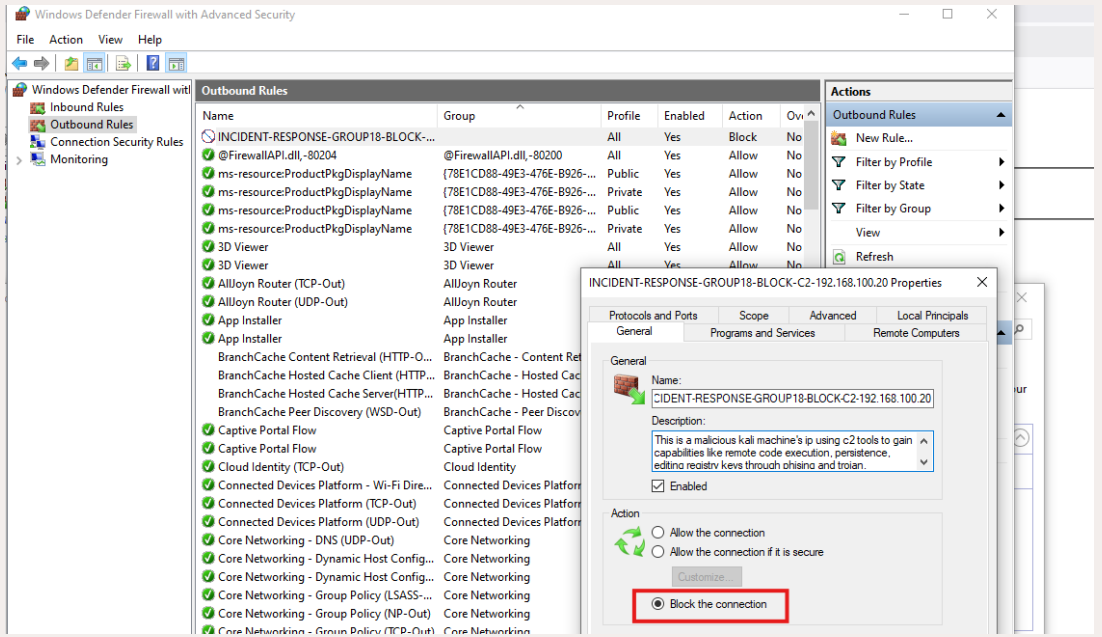
Phase 1 - Containment (Stopping the Attack)

- **Goal:** Sever the connection between the infected host and the attacker to prevent further data theft.

- **Action Taken:**
- Identified the C2 IP (192.168.100.20) from Sysmon logs.
- Created a Windows Firewall Outbound Rule to explicitly block all traffic to this IP.

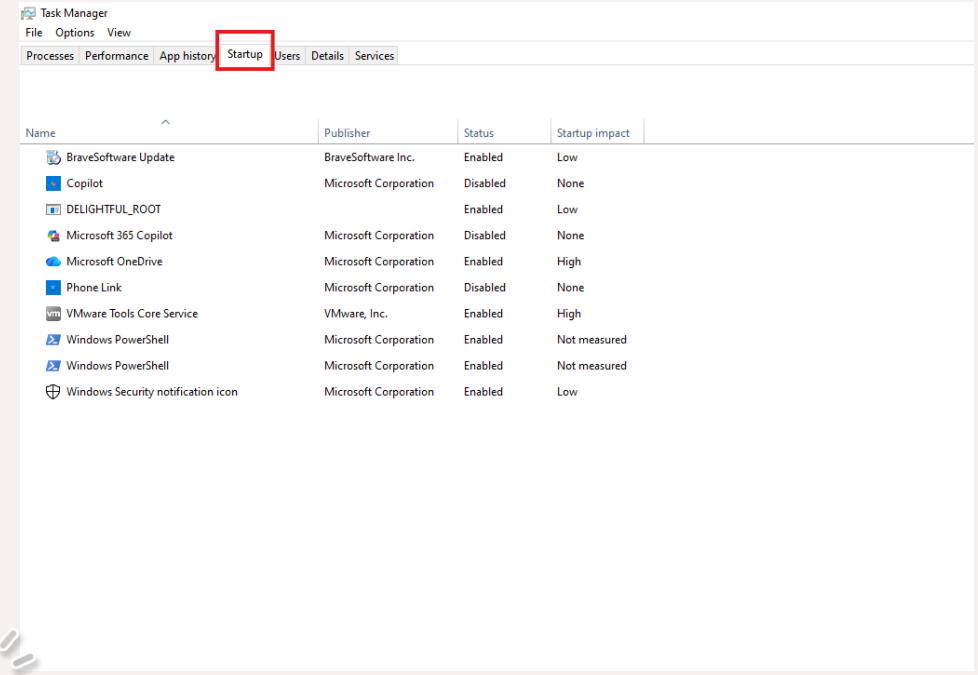
- **Visual Evidence:**
- Creating an outbound rule as a part of containment to be safe in future.png
- Final outbound rule created blocking the contact with malicious ip.png
- Network Containment: Configuring a blocking rule to isolate the attacker's IP address.

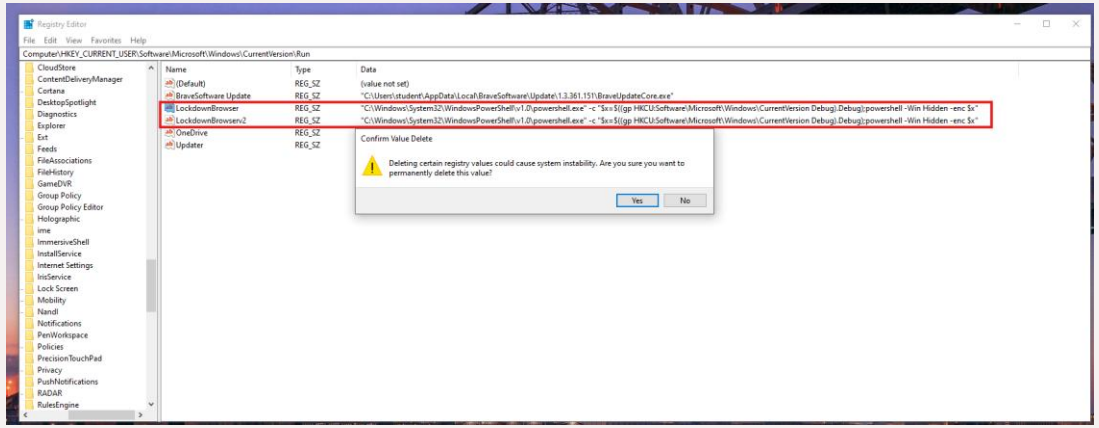




Phase 2 - Eradication (Removing Persistence)

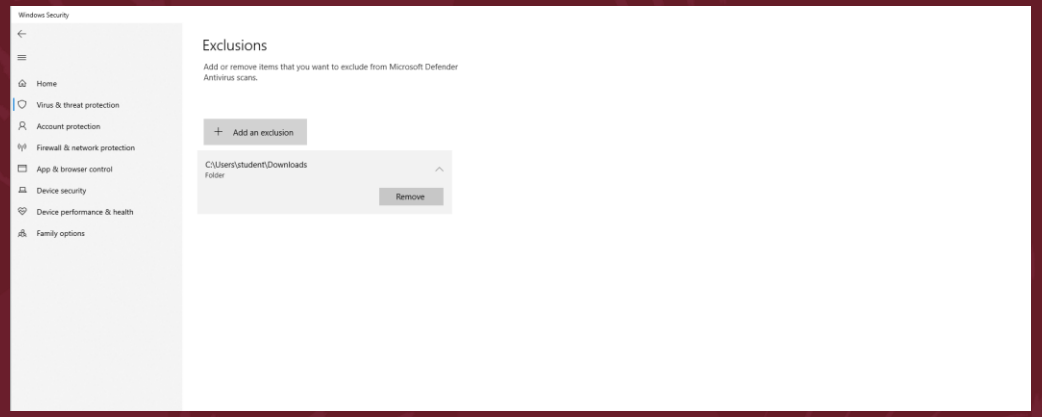
- **Goal:** Remove the malicious mechanisms that allow the attacker to return.
- **Action Taken:**
  - **Registry:** Navigated to HKCU\Software\Microsoft\Windows\CurrentVersion\Run and deleted the malicious Updater key.
  - **Startup:** Verified the Startup folder and Registry were clean of any unauthorized entries.
- **Visual Evidence:**
  - Cleaning up by deleting the registry key changes
  - **Checking** and removing for any changing in the startup directory.
- Eradication: Removal of the persistence registry key to prevent re-infection upon reboot.

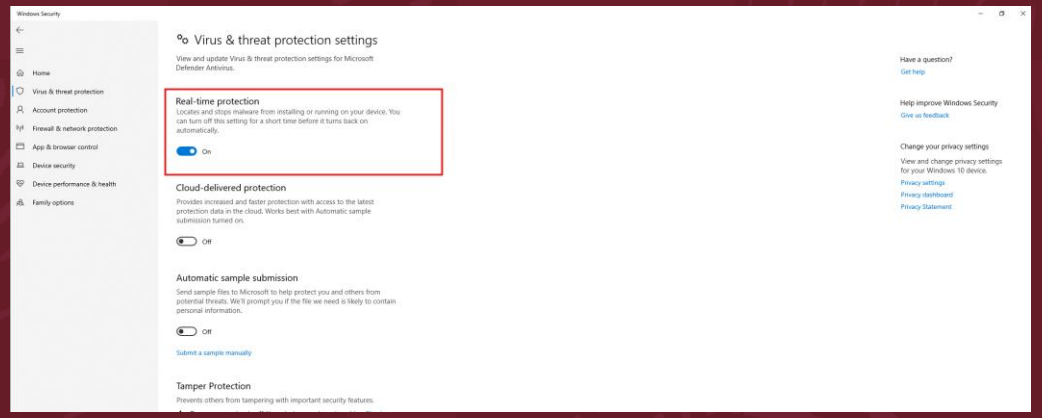


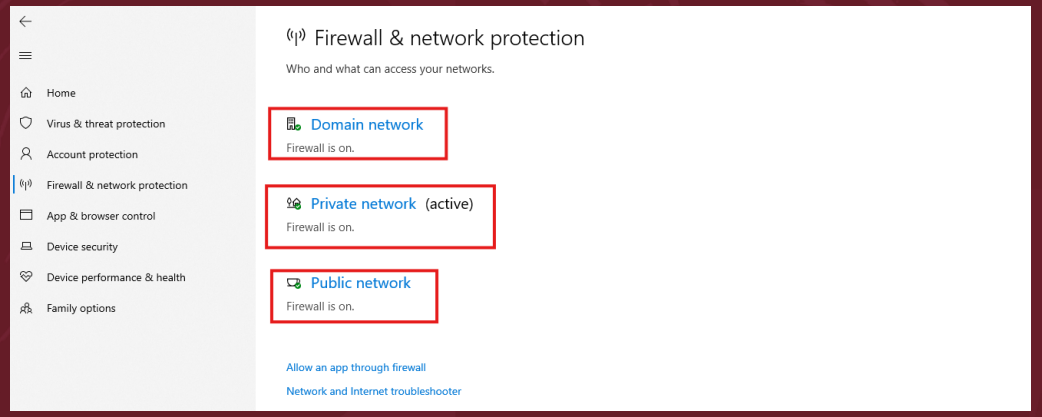


Phase 3 - Recovery (Restoring Security Posture)

- **Goal:** Revert the dangerous changes made by the user and bring the system back to full security.
- **Step 1: Hardening:**
  - Removed the "Exclusion" for the Downloads folder, allowing Antivirus to scan that directory again.
- **Step 2: Reactivation:**
  - Re-enabled **Real-Time Threat Protection** and Cloud-delivered protection.
- **Step 3: Network Security:**
  - Ensured all Windows Defender Firewall profiles (Domain, Private, Public) were active.

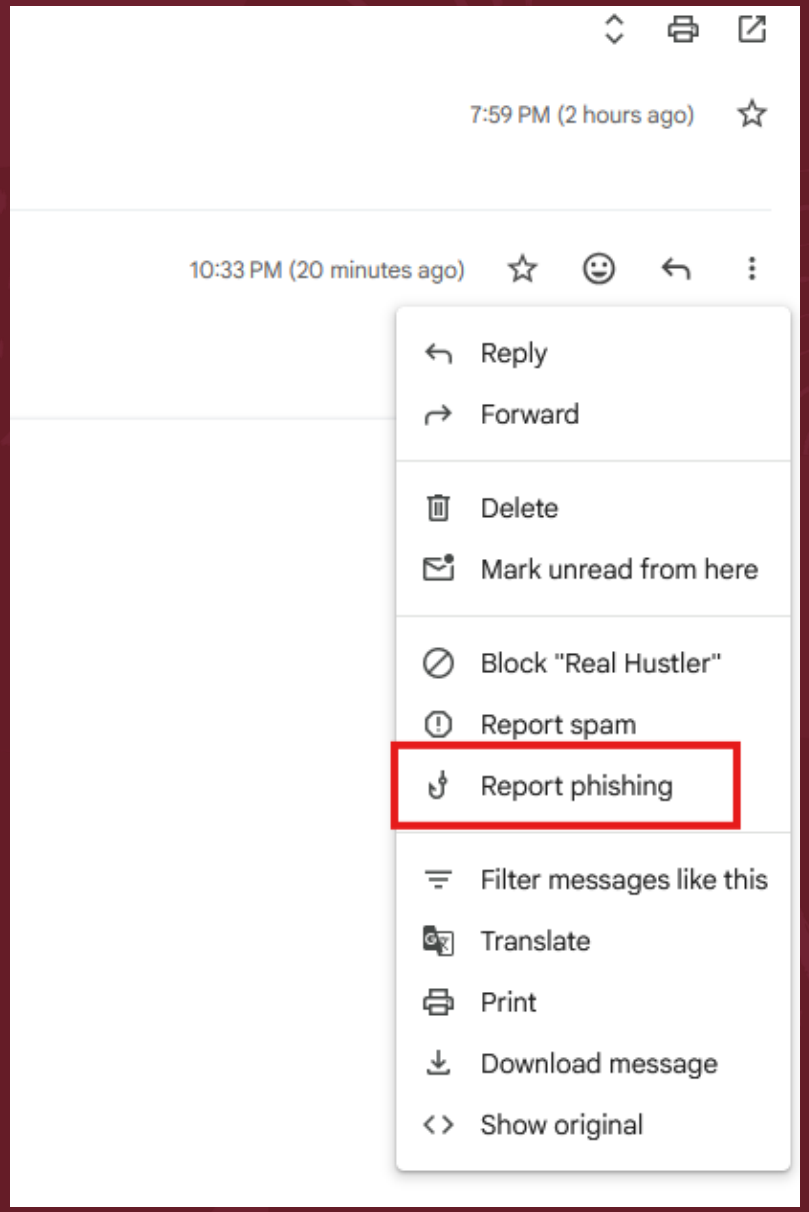






Phase 4 - Reporting (Lessons Learned)

- **Goal:** Close the incident loop and improve future defenses.
- **Action Taken:**
  - The phishing email was flagged and reported to the internal security team for analysis.
  - This helps update spam filters to block similar attacks in the future.
- **Visual Evidence:**
- Reporting the phishing artifact to improve organizational email filters.



References

- **BC Security.** (n.d.). *Empire*. GitHub. https://github.com/BC-SECURITY/Empire
- **BC Security.** (n.d.). *Starkiller*. GitHub. https://github.com/BC-SECURITY/Starkiller
- **Carnegie Mellon University.** (n.d.). *Social Engineering*. Information Security Office. https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html
- **MITRE.** (2024, October 10). *Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder*. MITRE ATT&CK. https://attack.mitre.org/techniques/T1547/001/
- **Microsoft.** (2023, February 15). *Sysmon v15.15*. Microsoft Learn. https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
- **Rapid7.** (n.d.). *Metasploitable*. https://www.rapid7.com/products/metasploit/
- **Tenable.** (n.d.). *Nessus Essentials*. https://www.tenable.com/products/nessus/nessus-essentials
- **The C2 Matrix.** (n.d.). *The C2 Matrix Project*. https://howto.thec2matrix.com/