Author: Jack Fitzgerald

# CyberDefenders Write-up


## Blue team CTF Challenges

Lab: Lockdown

Date: 29/12/2025

https://cyberdefenders.org/blueteam-ctf-challenges/lockdown/

# Table of Contents

# Summary

Reconstruct a multi-stage intrusion by analyzing network traffic, memory, and malware artifacts using Wireshark, Volatility, and VirusTotal, mapping findings to MITRE ATT&CK.

Category: Network Forensics

Tactics: Execution | Persistence | Privilege Escalation | Defense Evasion | Discovery | Lateral Movement | Command and Control

Tools: Wireshark | MemProcFS | Volatility 3 | FLOSS/Strings | Threat Intel tools

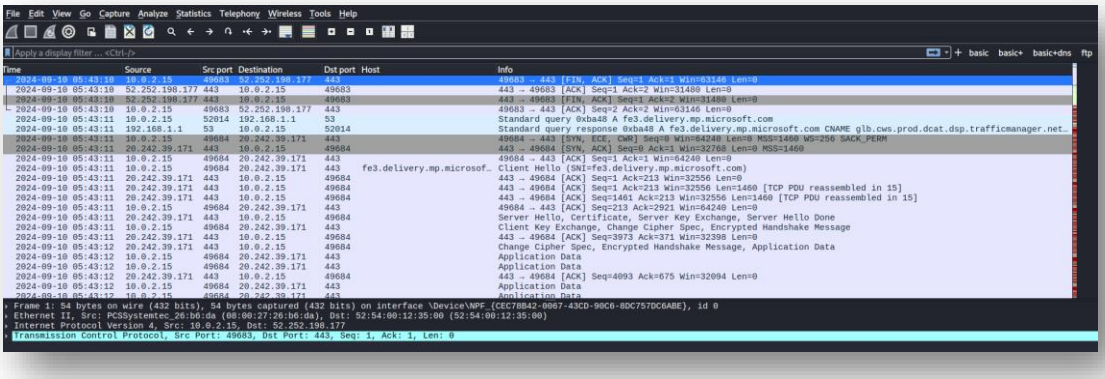
## Scenario

TechNova Systems' SOC has detected suspicious outbound traffic from a public-facing IIS server in its cloud platform—activity suggestive of a web-shell drop and covert connections to an unknown host.

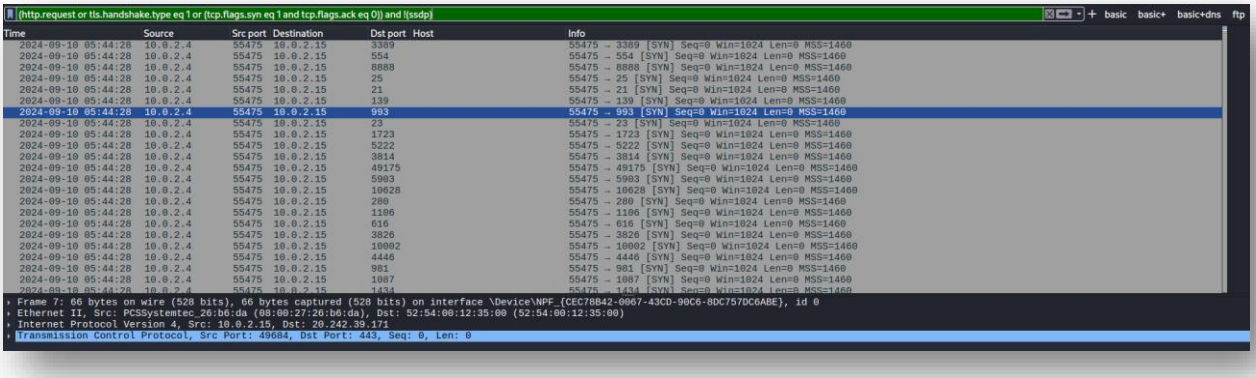
As the forensic examiner, you have three critical artefacts in hand: a PCAP capturing the initial traffic, a full memory image of the server, and a malware sample recovered from disk. Reconstruct the intrusion and all of the attacker's activities so TechNova can contain the breach and strengthen its defenses.

## PCAP Analysis

Our first file to investigate is ‘capture.pcap’, using Wireshark.



I applied a preset filter I have on my Wireshark install to find the rapid-fire probes the attacker is flooding the IIS host with. This identifies the attacker as ‘10.0.2.4’, and the IIS host as ‘10.0.2.15’.



**Question 1:** After flooding the IIS host with rapid-fire probes, the attacker reveals their origin. Which IP address generated this reconnaissance traffic?

10.0.2.4

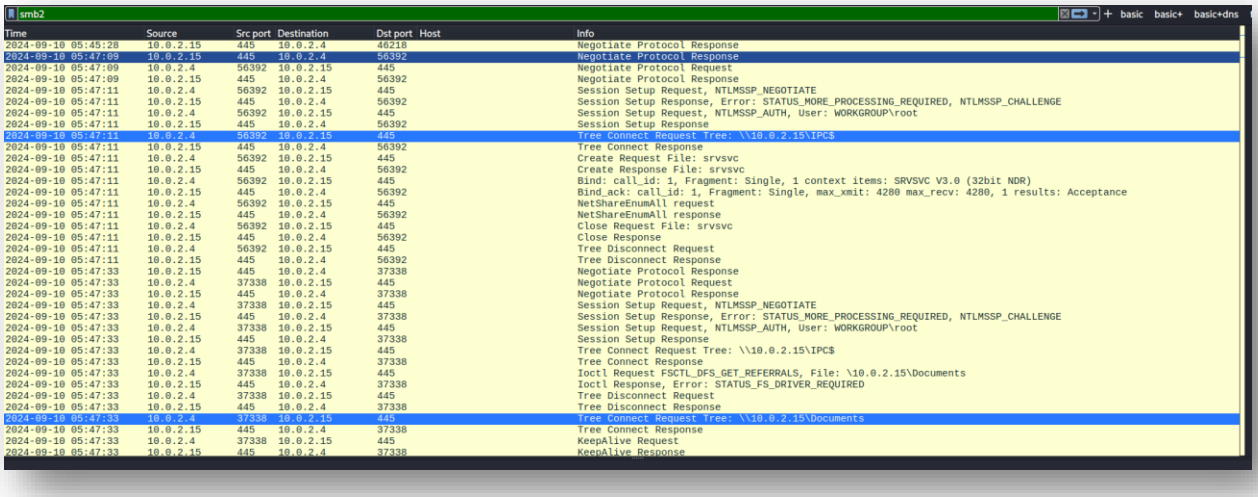
Since the attacker is sending repeated probes to a single open service (targeted enumeration), this behaviour identifies with the MITRE ATT&CK tactic Discovery, specifically T1046 Network Service Discovery.

According to MITRE ATT&CK, adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port, vulnerability, and/or wordlist scans using tools that are brought onto a system.

**Question 2:** Zeroing in on a single open service to gain a foothold, the attacker carries out targeted enumeration. Which MITRE ATT&CK technique ID covers this activity?

T1046

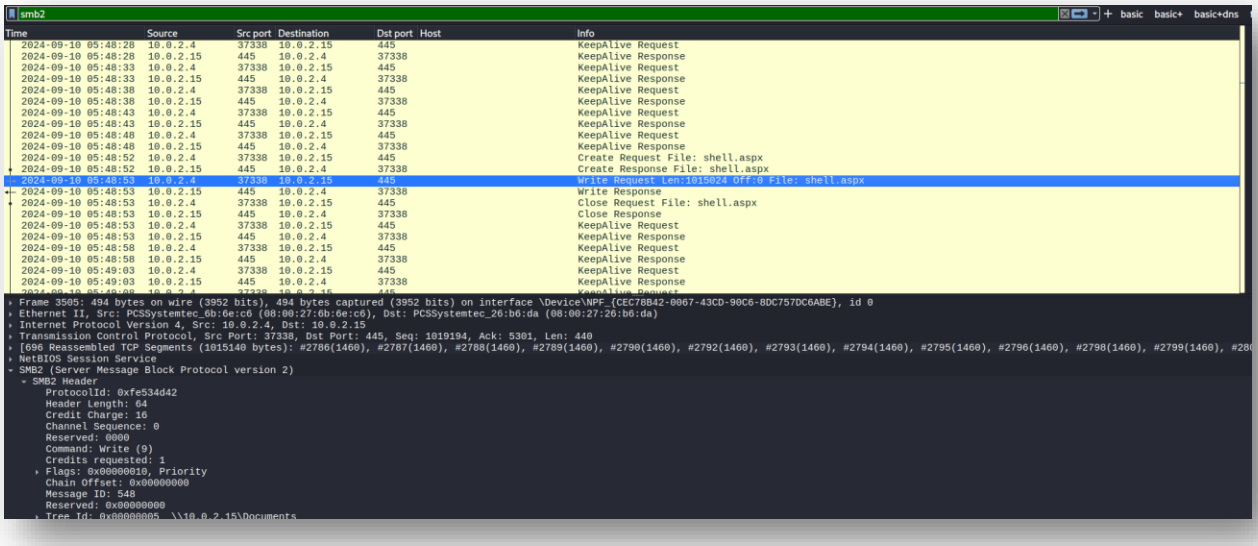
To identify the two consecutive Tree Connect requests, I queried smb2 in the filter bar, exposing 'Documents' and 'IPC$' as the first shares the intruder probed.




**Question 3:** While reviewing the SMB traffic, you observe two consecutive Tree Connect requests that expose the first shares the intruder probes on the IIS host. Which two full UNC paths are accessed?

\\10.0.2.15\Documents, \\10.0.2.15\IPC$

It is important to continue enumerating the smb2 search for any files/payloads the attacker might plant. We identify the shell.aspx file which was planted inside the 'Documents' share.




**Question 4:** Inside the share, the attacker plants a web-accessible payload that will grant remote code execution. What is the filename of the malicious file they uploaded, and what byte length is specified in the corresponding SMB2 Write Request?

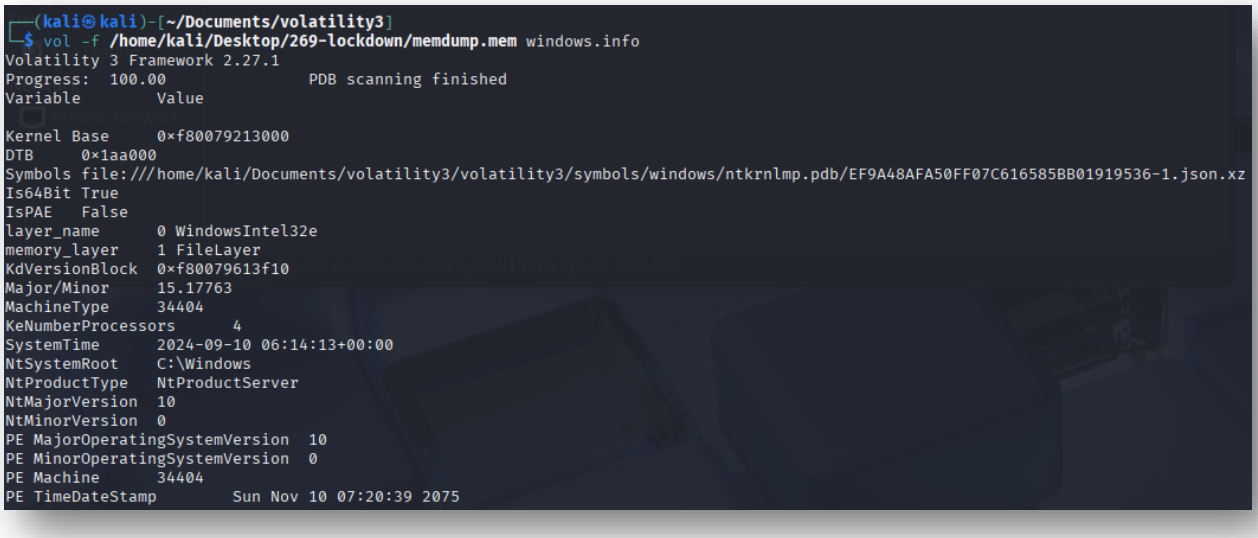
shell.aspx, 1015024

**Question 5:** The newly planted shell calls back to the attacker over an uncommon but firewall-friendly port. Which listening port did the attacker use for the reverse shell?

4443

## Memory Dump Analysis

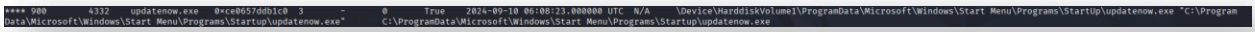
Now that we are finished with the pcap file, we can move onto 'memdump.mem'. Our first command we can use to investigate this memory dump is by using the tool volatility 3 with the parameter 'windows.info' to show OS & kernel details of the memory sample being analyzed.




**Question 6:** Your memory snapshot captures the system's kernel in situ, providing vital context for the breach. What is the kernel base address in the dump?

0xf80079213000

To identify a suspicious process, we start by enumerating processes and their parent-child relationships using volatility 3 with the parameter 'windows.pstree'.




We found a suspicious process. While the image is very hard to see, the following data was retrieved:

- PID: 900
- PPID: 4332
- ImageFileName: updatenow.exe
- Offset(V): 0xce0657ddb1c0
- Threads: 3

- Handles: -
- SessionId: 0
- Wow64: True
- CreateTime: 2024-09-10 06:08:23.000000 UTC
- ExitTime: N/A
- Audit: \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\updatenow.exe
- Cmd: "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\updatenow.exe"
- Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\updatenow.exe

The corresponding MITRE ATT&CK tactic would be Persistence, specifically T1547 Boot or Logon Autostart Execution.

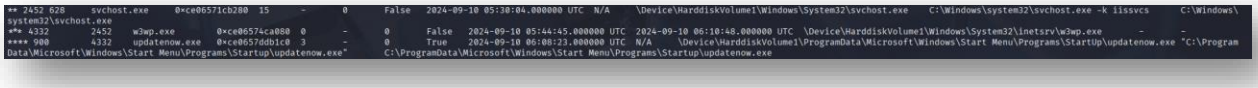
Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.

**Question 7:** A trusted service launches an unfamiliar executable residing outside the usual IIS stack, signalling a persistence implant. What is the final full on-disk path of that executable, and which MITRE ATT&CK persistence technique ID corresponds to this behaviour?

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\updatenow.exe, T1547

The w3wp.exe (World Wide Web Publishing Worker Process) is the core executable for Microsoft's Internet Information Services (IIS) web server, responsible for running web applications, handling HTTP requests, executing code (like ASP.NET), and isolating application pools for security and stability, essentially being the engine that serves your websites and web services on a Windows server.

The process is the parent process of the suspicious executable ‘updatenow.exe’.

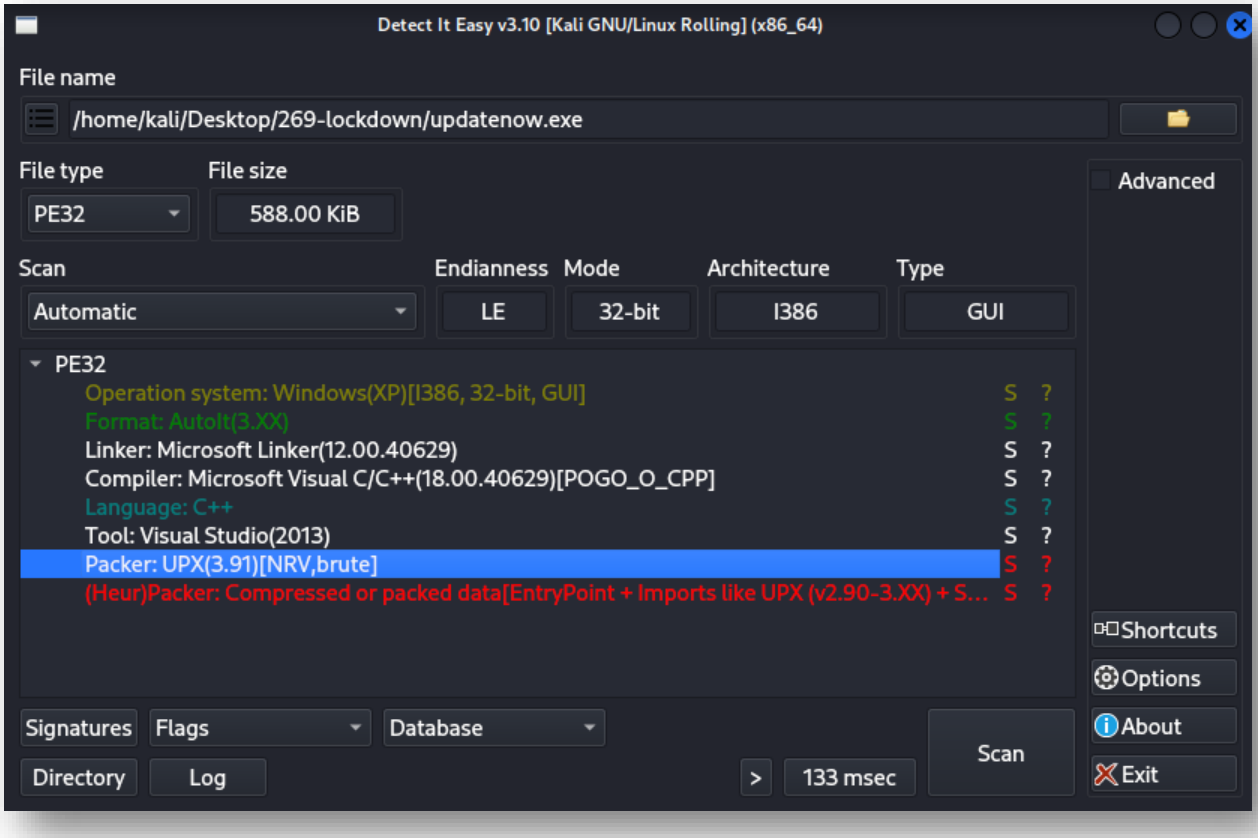



**Question 8:** The reverse shell's outbound traffic is handled by a built-in Windows process that also spawns the implanted executable. What is the name of this process, and what PID does it run under?

w3wp.exe, 4332

## Malware Sample Analysis

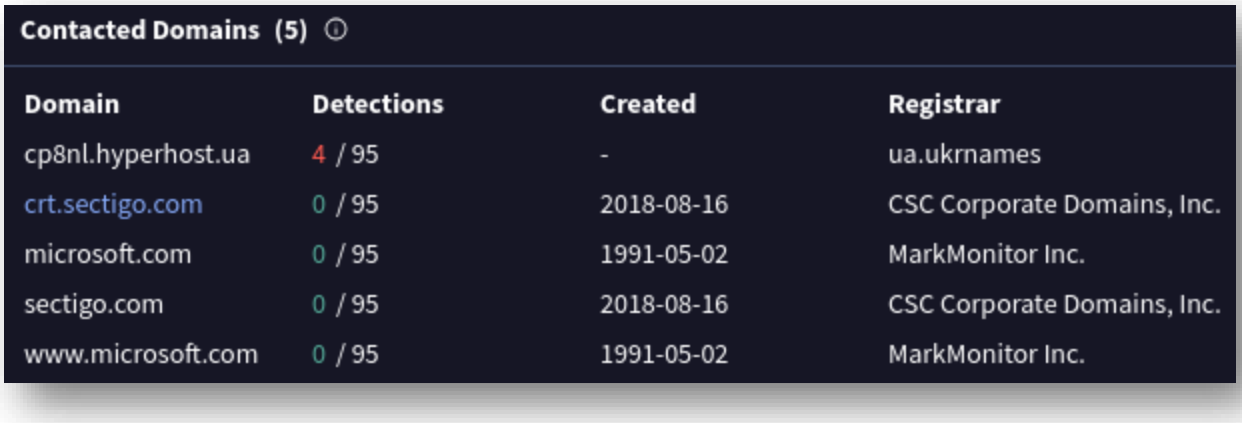
Using Detect It Easy (DIE), plug the ‘updatenow.exe’ file into the tool, and it identifies the packer used UPX to obfuscate the binary.




**Question 9:** Static inspection reveals the binary has been packed to hinder analysis. Which packer was used to obfuscate it?

UPX

Uploading the file to virustotal shows us the contacted domain, allowing us to determine the C2 host at ‘cp8nl.hyperhost.ua’.



**Contacted Domains (5)**

| Domain | Detections | Created | Registrar |
|---|---|---|---|
| cp8nl.hyperhost.ua | 4 / 95 | - | ua.ukrnames |
| crt.sectigo.com | 0 / 95 | 2018-08-16 | CSC Corporate Domains, Inc. |
| microsoft.com | 0 / 95 | 1991-05-02 | MarkMonitor Inc. |
| sectigo.com | 0 / 95 | 2018-08-16 | CSC Corporate Domains, Inc. |
| www.microsoft.com | 0 / 95 | 1991-05-02 | MarkMonitor Inc. |

**Question 10:** Threat-intel analysis shows the malware beaconing to its command-and-control host. Which fully qualified domain name (FQDN) does it contact?

cp8nl.hyperhost.ua

**Question 11:** Open-source intel associates that hash with a well-known commodity RAT. To which malware family does the sample belong?

AGENTTESLA