Mission Directive: Phase 2

"The Owls are Not What They Seem"

Case: The Disappearance of Laura Palmer
Division of National Cybercrime Investigations - FBI
Classification: TOP SECRET
September 2024

PHASE 1 RECAP

Our reports from the Bureau indicate that Phase 1 was carried out with considerable success.

With its seasoned network threat hunters, The Cybercrime Investigation Unit was able to regain administrative access to The Great Northern Hotel's network systems, patch critical security weaknesses in its Linux and Windows machines, as well as identify initial indicators of compromise related to the abduction of Laura Palmer.

TASK SUMMARY: PHASE 2

As we enter Phase 2 of the investigation into the case of Laura Palmer, the team realizes that The Great Northern Hotel may be under active attack by The Black Lodge.

It is crucial to not tip our hand. If The Unit tries to kick out Black Lodge attackers too early, they might slow down or try to further hide their techniques. Instead, the team seeks to expand the hotel's network and install threat detection/logging measures to lure further activity from The Black Lodge.

To accomplish this, The Bureau has enlisted the help of Margaret Lanterman, also known as *The Log Lady.* Being familiar with system monitoring and logging, she has offered to donate her special **Logging Workstation** to the hotel's network, along with other machines. This will become the main server that we will use to monitor all of the hotel's digital infrastructure.

You are tasked with the following objectives:

1. Perform network reconnaissance to discover machine information
2. Gain administrative access to the new systems
3. Install and configure an adequate system monitoring and logging solution
4. Test threat detection against Black Lodge attacker techniques

Your FBI workstation (*Kali Purple)* for this task can be accessed with the following login:
Username: `agentcooper`
Password: `SuperSecretPassword`

Document your process and findings in a formal report, to be submitted in Canvas.

The next section of this document addresses the four points above in detail.

OBJECTIVE ONE: NETWORK RECONNAISSANCE

When asked about what IP addresses our new machines, Ben Horne said the following:

> *"What the hell is an IP address? I just plugged them in and pressed the power button."*

As such, the first objective revolves around finding the IPs of the new infrastructure.

Your skills with nmap will prove to be useful for this.

For Objective One, The Unit is tasked with documenting:

- The *new* infrastructure they uncovered
    - Include machine IPs and the network services they are hosting
    - Include brief explanations for the network services being hosted, and why an organization might need them
    - Provide screenshots and relevant commands/tools used to uncover the above

OBJECTIVE TWO: ACCESSING THE NEW SYSTEMS

Having uncovered the Logging workstation, an issue arose. The Log Lady mentions:

"Oh dear… I forgot the login information for the logging machine. Not to worry. ***I have it stored in the Administrator desktop*** *on one of the new Windows machines I gave you guys.*

Wait… I also don't have the login information for that Windows machine. Well, it's a pretty ancient machine, there's probably some critical vulnerability on it that you can exploit to get Administrator access."

For Objective Two, The Unit is tasked with documenting:

- The attack path for gaining access to this "ancient" Windows machine
  - Explain what the vulnerability is on the machine. What program/service is affected? How is it abused? Extensive technical details are not needed
  - Show the program you used to exploit the vulnerability, including any important commands and settings you configured.
  - Find the uncovered credentials that The Log Lady left behind
  - Provide relevant screenshots

- The newfound access to the Workstation log
  - Demonstrate that the uncovered credentials are valid <u>administrative</u> credentials for the logging workstation machine
  - Provide relevant screenshots

OBJECTIVE THREE: MONITORING AND LOGGING

The time has come to install our logging tools. When consulting with The Log Lady, she mentioned the following:

"Yeah. Wazuh is nice. It's kind of like a combination of a SIEM and an EDR.

It's also great cause it's free. Probably a good monitoring solution for The Great Northern considering how much of a cheapskate Ben Horne is. It would be great for your operation."

Director Gordon Cole has advised the team to be familiar with the concepts of the **manager** and **agents** in the context of SIEMs (Security Information and Event Management systems) / EDRs (Endpoint Detection and Response systems).

The **manager** refers to the machine that receives and processes security-relevant data from across the network.

The **agents** refer to the machines that, when connected to the manager, send security-relevant data to it. (i.e. the logs of programs/services, network connection changes, filesystem changes, etc.).

The Log Lady left one more message for the team:

"You know me… I love my logging. But even before that, I love my network security. Fedora is great because it has a host-based firewall enabled by default.

You may need to edit the firewall to allow agent traffic to flow into the manager… The firewall program is called "firewalld", if memory serves. You should check what services/ports it's allowing through by default.

This page should help you identify what port numbers to allow traffic through with firewalld: https://documentation.wazuh.com/current/user-manual/agent/agent-enrollment/troubleshooting.html"

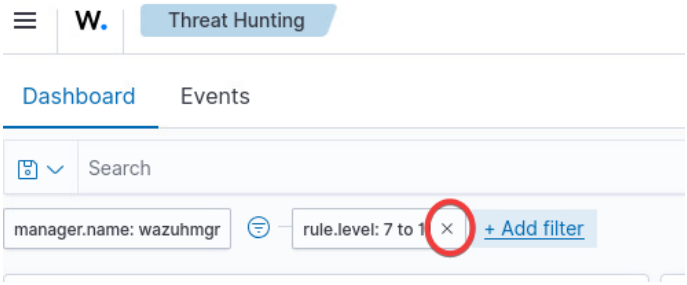
Ultimately, Margaret recommends the following actions be taken:

1. Install the Wazuh Manager on the logging workstation machine.
    - Use the Quickstart installation guide
    - **Note:** Skip any minimum hardware requirement errors with the `-i` flag
    - **Note:** Before running the quickstart install command, ensure that the full disk space is being used by running the following two commands:
      ```
      sudo lvextend -l +100%FREE /dev/mapper/fedora-root
      sudo xfs_growfs /
      ```
    - You can check that it was installed fully by logging into its web interface on a web browser. Check the installation command output on the terminal, too.

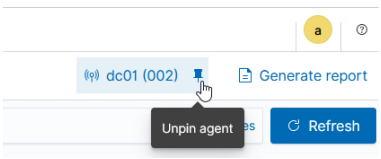
2. Install the Wazuh *Agents* on the following machines:
    a. The *Ubuntu ("dev")* machine.
        - Before installing, ensure the full disk space is being used by running:
          ```
          lvextend -r -l +100%FREE /dev/ubuntu-vg/ubuntu-lv
          ```
        - Give this an agent name of "dev01"
    b. The *Windows Server 2025 ("domain controller")* machine
        - Give this an agent name of "dc01"
    - To install an agent, go to Wazuh Manager web UI > Top left menu **>** Server Management > Endpoints Summary > Deploy New Agent
        - For the Linux agent, The Bureau is entrusting the team to find out which OS architecture is in use (e.g. aarch64, amd64, amd32…), along with which package manager type is in use (e.g. DEB or RPM).
        - The "Server address" refers to the address of the Wazuh workstation (manager) machine.

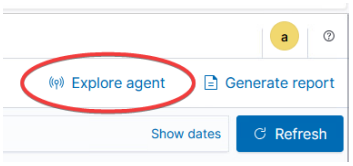
For Objective Three, The Unit is tasked with documenting:

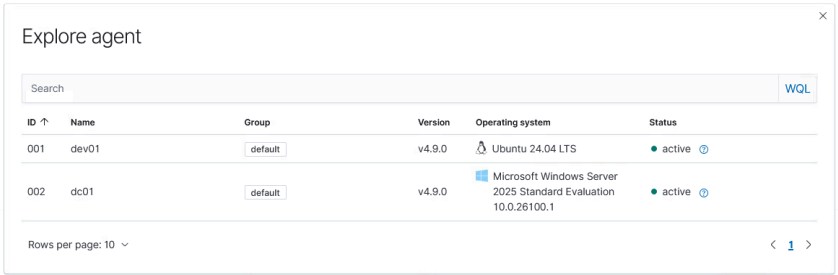
- The installation of Wazuh on the logging workstation machine
  - Show the completed installation message
  - Provide a screenshot of the the working web UI
  - Check to see if any logs have been generated. Take a screenshot of some of them to prove that information is being logged. (Top left menu > Threat Intelligence > Threat Hunting). Make sure that all logs are being shown (there may be a "rule.level: 7 to 11" filter being applied -- remove it if so).

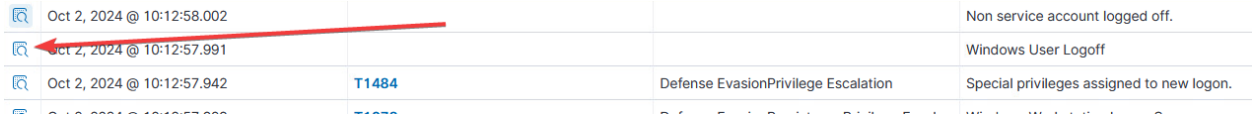


- The installation of the Wazuh agents on the Ubuntu and Windows Server 2025 machines
  - On the Wazuh Manager web UI, go to Server Management > Endpoints Summary, and take a screenshot of all the connected machines (agents).
  - With screenshots, show some of the logs that have been recorded on each of the different connected machines (Top left menu > Threat Intelligence > Threat Hunting > Unpin Agent/Explore Agent).
  - SSH/RDP into the machine and then exit the session. Can you see the logs that show that you logged in?









OBJECTIVE FOUR: THREAT DETECTION TESTING

Based on data gathered from the internet as well as other investigations, sources from The Bureau indicate that The Black Lodge may be using a C2 (Command-and-Control) framework called *Sliver*.

To understand their tactics, it is imperative that the team understands this tool. This involves:

1. Using and mastering the tool, offensively
2. Detecting and preventing the tool, defensively

Using the documentation from this Wazuh article, https://wazuh.com/blog/detecting-sliver-c2-framework-with-wazuh/, FBI Director Agent Cole is ordering the team to run a test against their infrastructure to both gather information about Sliver and learn to detect and counteract it, now that they have a foundation for logging and monitoring.

- At a minimum, carry out the "***Using detection rules***" and "***Sliver C2 attack emulation***" sections from the blog post.
- The instructions under "*Using YARA to detect the Sliver C2 implant*" and "*Using command monitoring to detect network communication*" can be carried out for additional security (**extra credit**).

The process for this objective involves four steps:

a) Installing and configuring Sysmon (from the Sysinternals suite)
b) Extra credit: Setting up Yara to scan malicious bytes in all files in C:\Users\Administrator\Downloads
- Advice: You will want to change the syscheck "`<frequency>`" in `C:\Program Files (x86)\ossec agent\ossec.conf` from `42000` (12 hours) to something smaller, like `60` (seconds).

c) Extra credit: Configuring command monitoring to check for Sliver-related network activity
- Advice: You can change the "`<frequency>300</frequency>`" value from `300` to something smaller, e.g. 6`0`.

d) Carrying a sliver attack against the test machine from an attacker machine.

For this purpose, the **Windows Server 2025** (“domain controller”) will be the test machine. Your FBI workstations will be the attacker machine.

For the fourth objective, The Unit is tasked with documenting:

- The changes made on the Wazuh manager and the dc01 agent to be able to detect Sliver
    - What did you have to install/configure before being able to detect Sliver? (Refer to the Wazuh blog post above). Why?
    - Describe what Wazuh “rules” are and why you would use them.
    - Describe what Wazuh “active detection” is and why you would use it.
    - Describe what Wazuh “command monitoring” is and why you would use it.
    - Provide screenshots and relevant commands/tools used to uncover the above

- The execution of the Sliver against the test machine.
    - Show the process of spawning a reverse shell
    - Show the process of injecting a process
    - Provide screenshots and relevant commands/tools used to uncover the above

- The detection of this Sliver beacon
    - In the Wazuh web manager, go to the Top left menu > Threat Intelligence > Threat Hunting > filter for logs from dc01. Show the different logs associated with this Sliver detection
    - Provide screenshots and relevant commands/tools used to uncover the above.