Mission Directive: Phase One

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

CASE BACKGROUND

A part-time IT staff member by the name of **Laura Palmer** has disappeared under mysterious circumstances in the town of Twin Peaks, WA.

Records indicate that she walked into work at The Great Northern Hotel on September 4th, 2024 to begin her night shift, which involved the building and deployment of The Great Northern's new digital infrastructure such as employee laptops, kiosk machines, hotel web servers, customer databases, and more.

As of September 11th, 2024, nobody has seen or heard from her since.

Preliminary forensic investigation by The Bureau points to the involvement of the notorious organized crime group known as **The Black Lodge**. The group, infamous for its alleged ties to the supernatural, has seen a recent shift in strategy to the digital world.

Our sources indicate that they may have both abducted Ms. Palmer as well as compromised the digital infrastructure of The Great Northern Hotel.

TASK SUMMARY

The National Cybercrime Investigations Unit has been assigned this case to do the following:

1. Regain control of the digital infrastructure at The Great Northern
2. Fortify critical aspects of the network
3. Gain further information on The Black Lodge

The Unit is expected to document their process and findings in a formal report, to be submitted in the secure file upload platform known as *Canvas*.

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

OBJECTIVE ONE: REGAIN CONTROL

Our records indicate that Laura Palmer possessed the only available credentials to log into the computer systems of the Great Northern. Furthermore, Laura was the only system administrator for the hotel, meaning that there are no other IT staff to assist with administrator login credentials.

As such, the Cybercrime Investigations Unit is tasked with identifying available servers and computers, and investigating their network services to find potential administrator login credentials for all systems.

Please refer to the following network diagram, found under Ms. Palmer's desk:

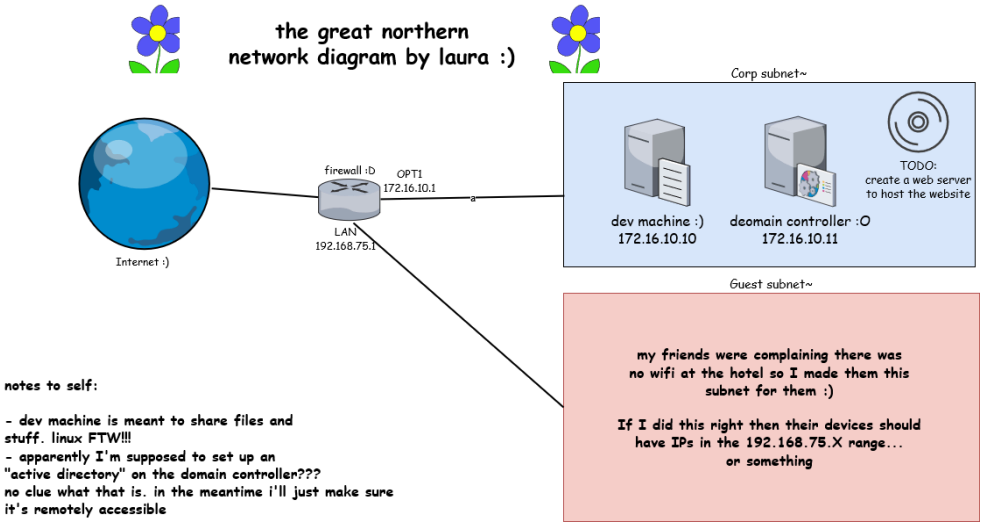

Figure 1: Network Diagram by Ms. Palmer

For Objective One, The Unit is tasked with documenting:

- The 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

- The process for regaining access
  - Describe how the network services from the prior step can be utilized and interacted with. What commands/programs are needed to do so?
  - Search for and report exposed information within network services
  - Describe how existing information was used to gain administrative/root control on each applicable machine.
  - Provide screenshots and relevant commands/tools used to uncover the above.

OBJECTIVE TWO: REMEDIATION

Should The Unit succeed in regaining control of the network, it will likely have been through unintended methods due to the fact that there are no administrators at The Great Northern with knowledge of login credentials.

As such, Objective Two is to remediate the security weaknesses that allowed for the unintended regaining of administrative control over network systems.

For Objective Two, The Unit is tasked with documenting:

- The vulnerabilities and misconfigurations that led to system takeover
    - Explain the misconfigurations/vulnerabilities uncovered.
    - Explain what network service or program it is associated with.
    - Provide screenshots of relevant configuration files, security settings, and user permissions that compromised the network security

- The remediations for the uncovered vulnerabilities/misconfigurations
    - How would similar tactics for gaining control be prevented in the future?
    - Give detail on relevant commands or programs used in remediation.
    - Provide screenshots of remediations (e.g. configuration files, the relevant settings/policies applied)

OBJECTIVE THREE: ERADICATE COMPROMISE

Preliminary forensic investigations uncovered the following sticky note on Ms. Palmer's monitor:

some wannabe script kiddie from "The Black Lodge" emailed me the other day saying that they hacked the hotel's network. supposedly if i dont cooperate with them theyre going to take more "more extreme measures".

bunch of posers. I'm gonna ignore the email but maybe I should change everyone's passwords just in case...

Figure 3: Sticky Note left by Ms. Palmer

The above note strongly alludes to a potential presence of The Black Lodge on The Great Northern's network. As such, it is critical for The Unit to investigate and report on any potential evidence left behind for attackers to maintain access to hotel systems.

For Objective Three, The Unit is tasked with documenting:

- Any indicators of compromise indicating presence of The Black Lodge on hotel systems.
    - Explain any uncovered malware, network traffic, IP addresses, process information, or any applicable evidence uncovered on the systems
    - Provide screenshots and relevant commands/tools used

- The process of eradicating the compromise
    - What methods did The Black Lodge use to ensure persistence on the compromised machine? How did The Unit disable these?
    - Provide screenshots and relevant commands/tools used