Lab 1 - Advanced Offensive Cyber Operations – Operation Shadow Strike

Version 1.0

Table of Content

1. Executive Summary

This lab assignment involved simulating a sophisticated multi-stage Advanced Persistent Threat (APT) campaign, codenamed "Operation Shadow Strike - Advanced Edition," against a fictional IT services provider, GlobalTech Solutions—a mid-sized IT services provider—to uncover vulnerabilities within their infrastructure. The simulation encompassed five key phases: Disruption via DDoS Attack, Initial Access via Spear Phishing, Establishing Persistence, Lateral Movement, and Data Exfiltration. The objective was to identify vulnerabilities in GlobalTech's network and systems by replicating real-world cyber attack techniques. This hands-on approach not only demonstrates the offensive techniques employed in real-world cyber threats but also reinforces the importance of robust and layered security measures, including proactive defense strategies, user awareness training, and continuous monitoring.. The exercise provided tangible insights into system performance degradation, the psychological impact of persistent attacks, and the critical need for layered security measures.

1.1. Lab Objectives

The primary objectives of this lab assignment were to:

- To emulate an APT campaign, identify vulnerabilities and propose strategic recommendations that enhance organizational defenses in a real-world operational context.
- To understand and implement advanced offensive techniques—DDoS, spear phishing, persistence, lateral movement, and data exfiltration—and appreciate their corresponding defensive countermeasures.
- To cultivate an understanding of digital forensics through evidence collection and analysis, reinforcing the importance of incident response in mitigating cyber threats.

2. Methodology

The simulation was designed to mirror a multi-stage Advanced Persistent Threat (APT) campaign targeting GlobalTech’s web and network infrastructure. The approach was structured around five key phases: a DDoS attack simulation, a spear phishing campaign, establishing persistence, lateral movement, and data exfiltration. The primary objective was to expose vulnerabilities at each stage and evaluate the effectiveness of current security controls. This methodology is based on a stepwise progression through each phase, with continuous monitoring and logging enabled to capture screenshots, system logs, and output data.

2.1. Tools & Resources

Each tool and resource was selected to mirror realistic attack scenarios and provide a comprehensive platform for both offensive operations and subsequent forensic analysis.

Hardware & Virtualization (Software & Operating Systems):

- Virtual machines to simulate attacker and victim environments
- Apache Web Server: Installed on the attacker'sVM to host a simple website
- Kali Linux for offensive operations

Attack & Simulation Tools:

- *Hping3* for simulating SYN flood DDoS attacks
- *SET (Social Engineering Toolkit)* for spear phishing and credential harvesting
- *Metasploit Framework* (msfconsole and msfvenom) for payload generation and persistence
- *nmap* for network enumeration
- *Hydra* for brute-force credential attacks
- *Meterpreter* for session management and privilege escalation
- *psexec* and *wmiexec* for lateral movement
- Text Editor: For creating and modifying configuration files and scripts.

Monitoring & Analysis Tools:

- *Wireshark* for network traffic analysis
- *htop, top,* and *netstat* for real-time system performance monitoring

Encryption & Data Handling:

- Python's *cryptography.fernet* library for AES encryption in data exfiltration

2.2. Attack Phases (Analysis & Findings)

Phase 1: DDoS Attack Simulation

The first phase was to simulate a Distributed Denial of Service (DDoS) attack aimed at overwhelming GlobalTech's web server to disrupt its online services.

1. A virtual machine running on Kali Linux was configured with Apache Web Server. The server hosted a simple website accessible via its IP address.
2. Using hping3, Ilaunched a SYN flood attack against the web server. The tools were configured to send a high volume of SYN packets to port 80, mimicking the behavior of a volumetric DDoS attack.
3. System performance was continuously monitored using tools such as htop and netstat. Network traffic was captured via Wireshark to analyze packet flows and identify traffic anomalies.

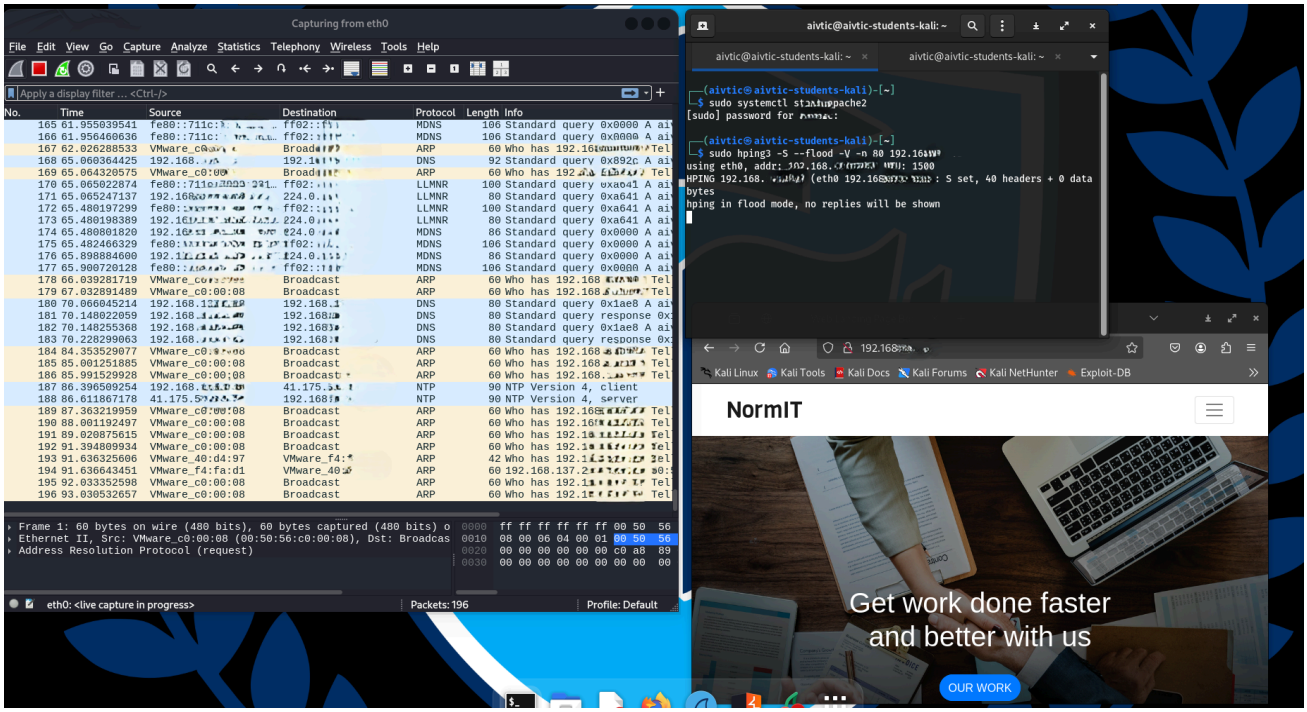

Figure 1: *Wireshark interface showing captured network traffic (left); Captured image of htop (top left); and Attackers Website hosted on Apache Server (bottom left)*

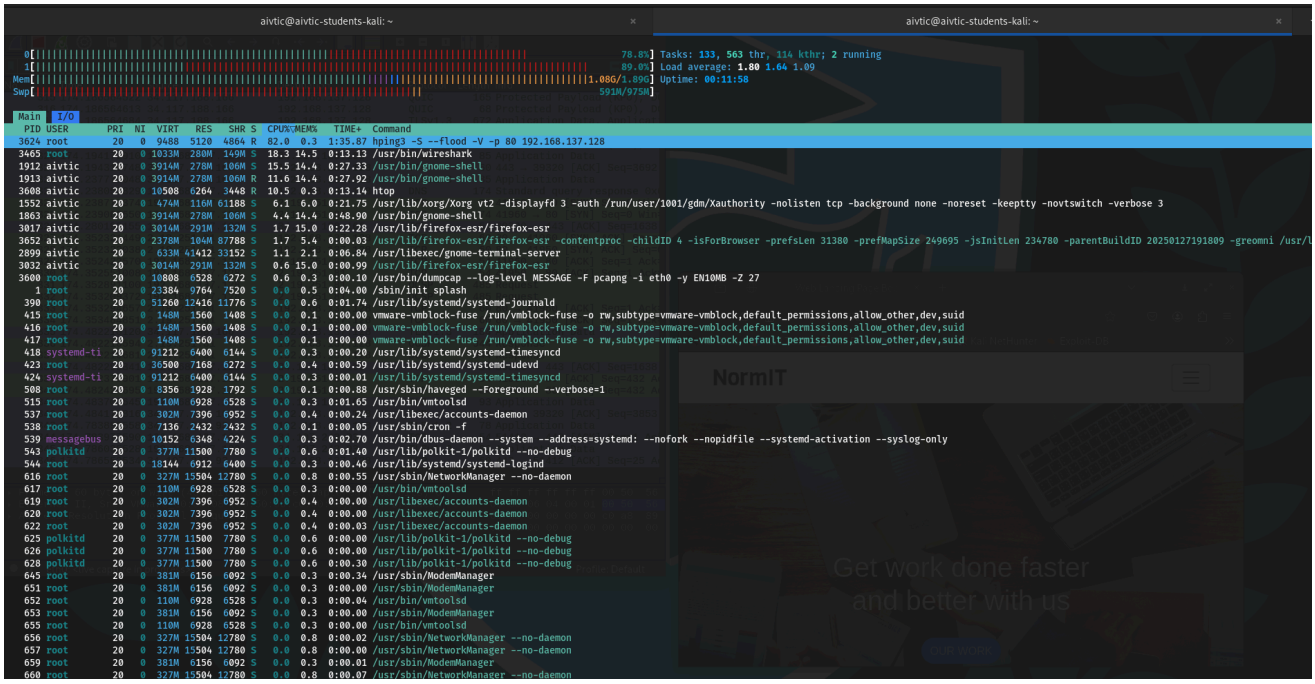

Figure 2: *Captured image of system monitors*

During the attack, CPU usage spiked, and network traffic logs displayed a dramatic increase in SYN packets. The system logs corroborated the drop in legitimate traffic and server responsiveness.The simulated DDoS attack demonstrated that GlobalTech's web server could be overwhelmed by excessive traffic, leading to service unavailability. This

phase highlighted the need for robust DDoS mitigation strategies such as rate limiting, firewalls, and load balancers.

Phase 2: Spear Phishing Campaign

The goal of the second phase was to execute a spear phishing campaign targeting privileged accounts within GlobalTech. This phase aimed to harvest credentials through a carefully crafted phishing email.

1. Personalized phishing emails were designed and sent to simulated user accounts using the Social-Engineer Toolkit (SET). The emails were made to appear as if they originated from the internal IT department, urging recipients to update their passwords immediately.
2. Once the victim clicked on the provided link, they were directed to a cloned login page. Any credentials entered were captured and logged by the SET interface.

Figure 3: *Cloning the Victims Website using SEToolkit*

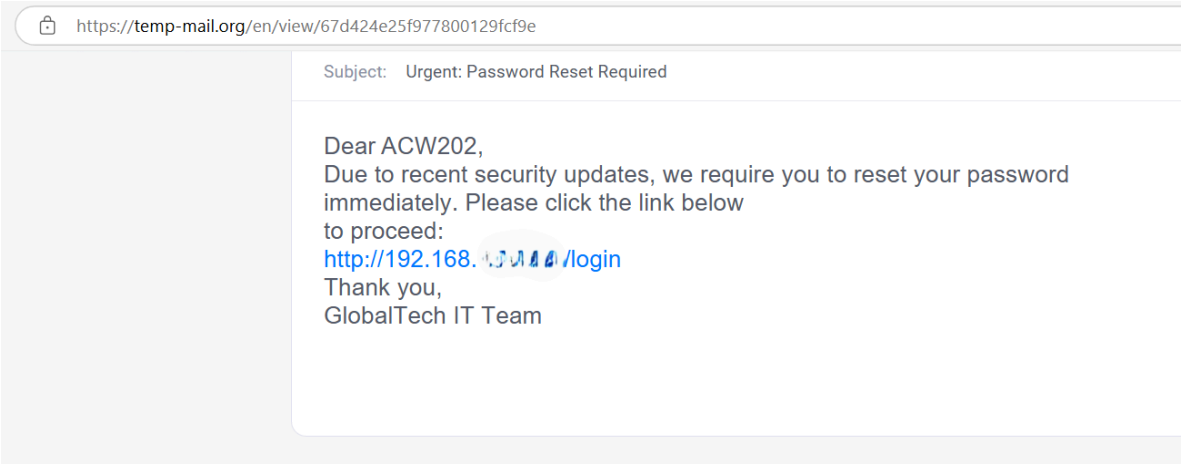

Figure 4: *Copy of the phishing emails sent*

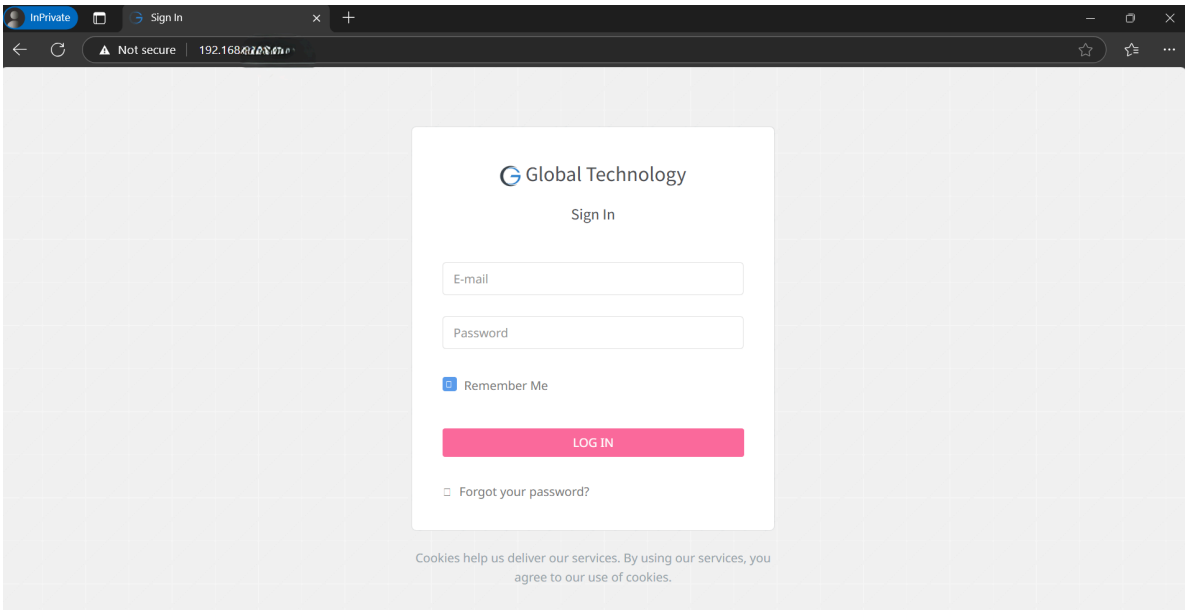

Figure 5: *Attacker's website clicked by the victim*

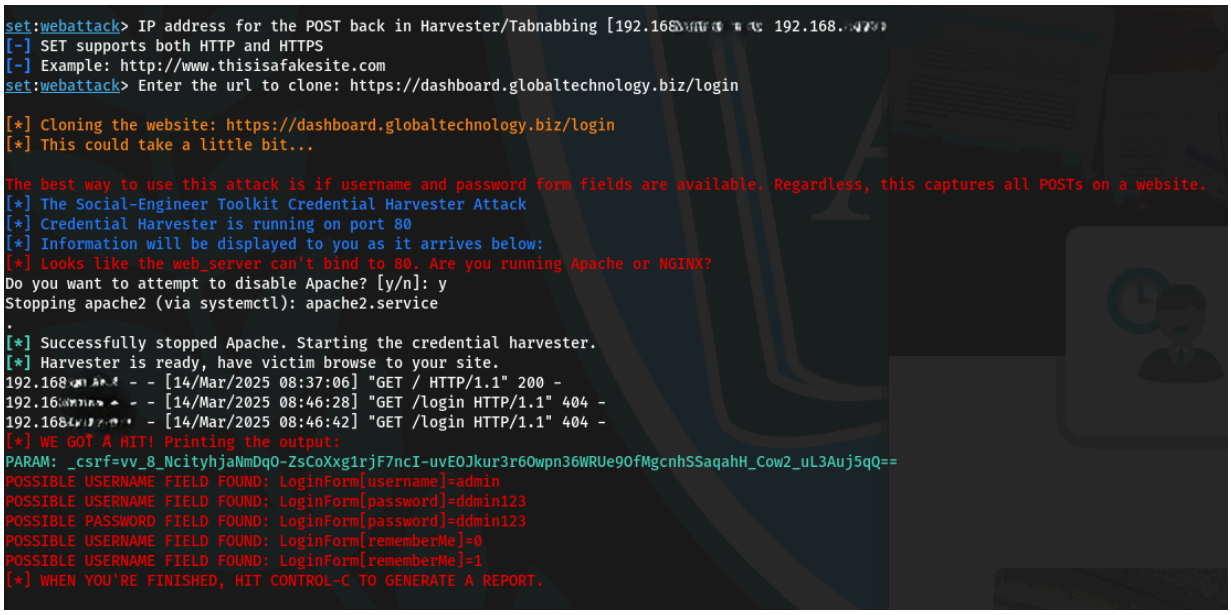

Figure 6: *Victims harvested credentials on the Attackers SET interface*

Our spear phishing attack was executed by sending highly targeted, personalized emails to key personnel. The Social-Engineer Toolkit (SET) was instrumental in cloning legitimate login pages and capturing credentials. The evidence included copies of the phishing emails and logs of harvested credentials, confirming that users could be deceived into divulging sensitive information. The successful harvesting of credentials indicated that GlobalTech's user awareness and email security practices need reinforcement, thus underlining the critical need for robust employee training, multi-factor authentication (MFA), and advanced email filtering mechanisms.

Phase 3: Establishing Persistence

The third phase focused on deploying a backdoor to maintain long-term access to the compromised systems. This persistence is critical for attackers to execute extended campaigns without repeated re-entry. In this phase, I deployed a backdoor using Metasploit and msfvenom to create a reverse shell payload that ensured continued access even after system reboots. The persistence was verified by monitoring system logs and using tools like Process Explorer to detect unauthorized processes. The backdoor installation was successful, demonstrating that once an attacker gains initial access, they can implant methods to survive subsequent system defenses.

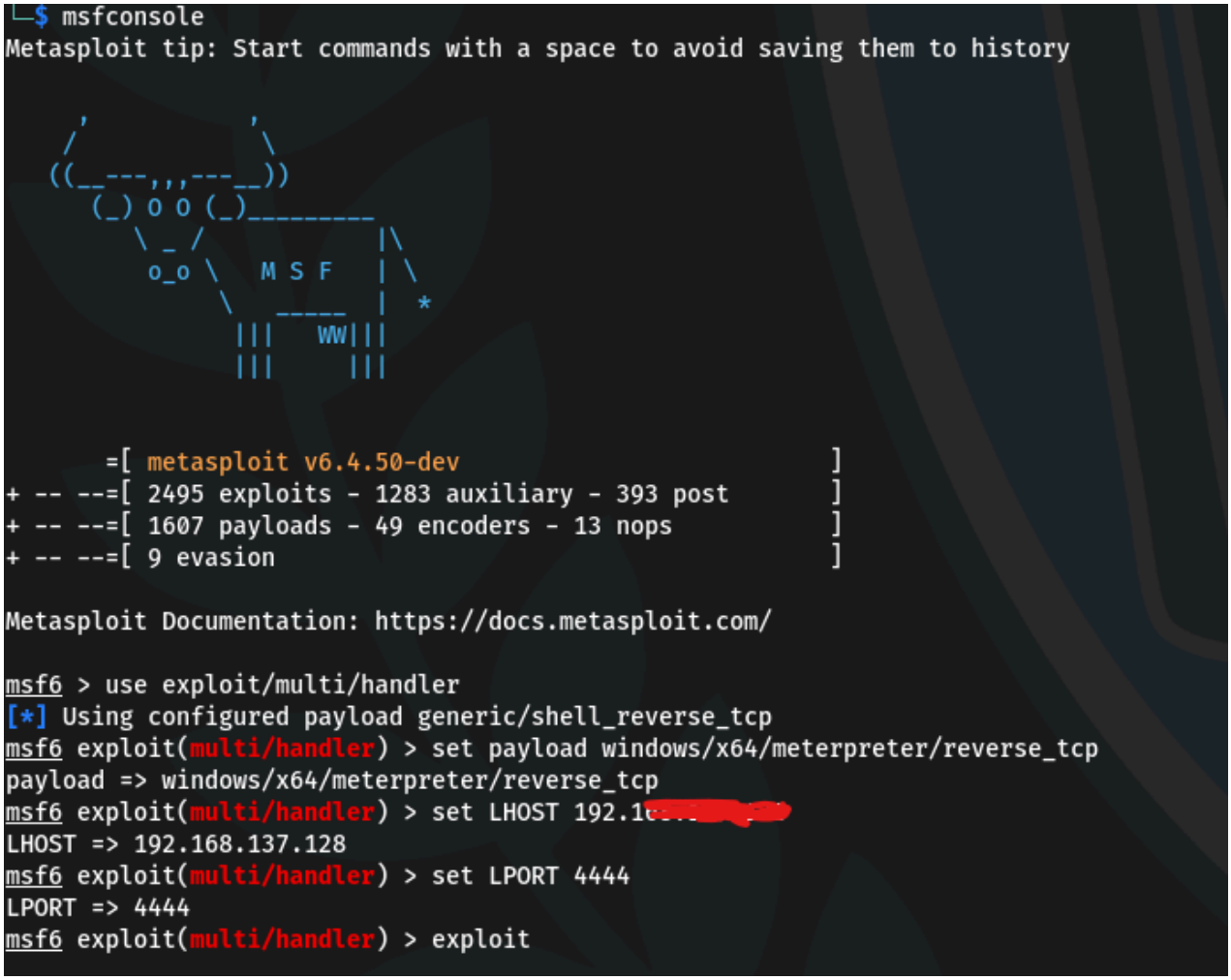

Figure 7: *Attacker setting up Metasploit reverse shell*

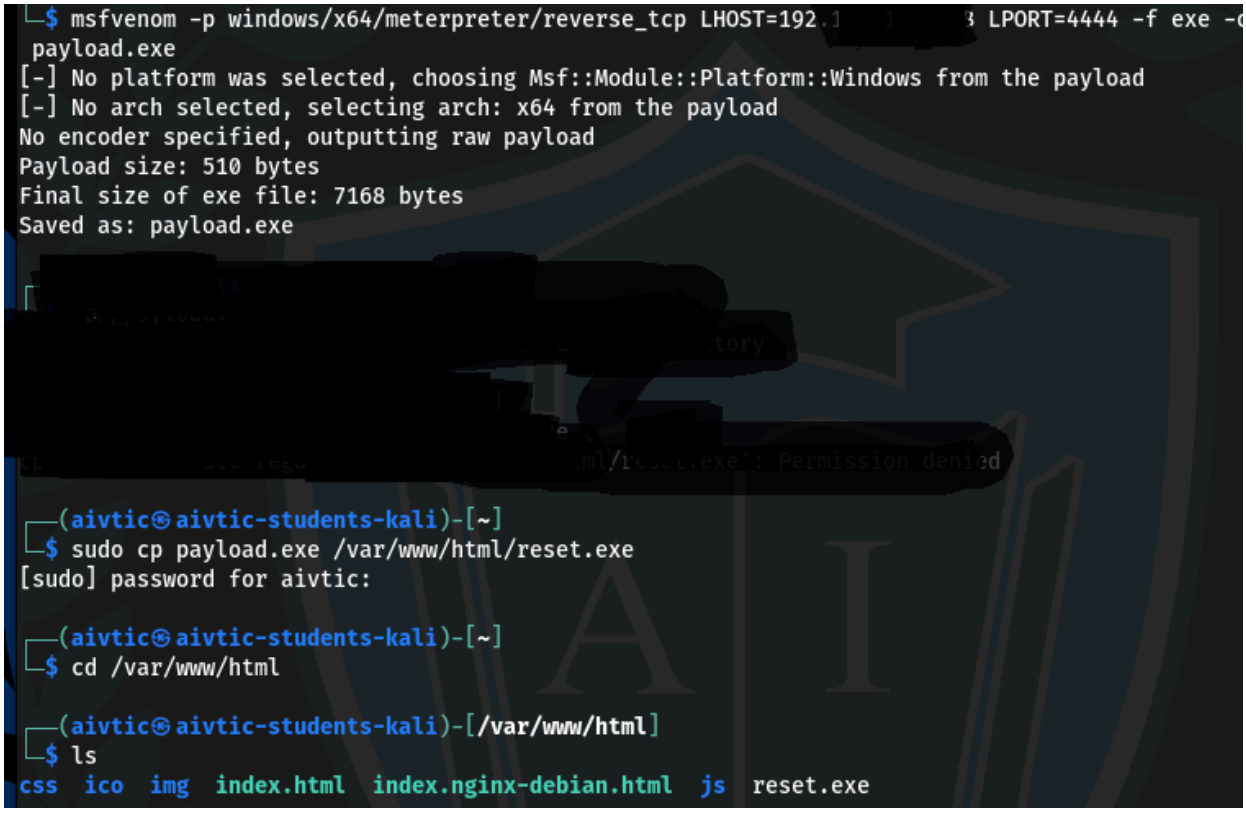

Figure 8: *Attacker creating the windows payload using msfvenom*

The ease with which persistence mechanisms were established underscores the importance of continuous system monitoring, regular integrity checks, and endpoint detection and response (EDR) solutions to detect and remove such unauthorized access points..

Phase 4: Lateral Movement

The fourth phase aimed to simulate lateral movement within the network, enabling the attacker to escalate privileges and access critical systems beyond the initial point of compromise.

1. Using nmap, I scanned the network to map out connected systems and identify vulnerable entry points.
2. With harvested credentials from Phase 2, I employed tools like Hydra and Meterpreter's getsystem command to exploit weak passwords and elevate privileges on additional systems.
3. Once inside a secondary system, tools such as psexec and wmiexec facilitated movement to adjacent systems. The objective was to reach high-value targets like servers hosting sensitive data.

Lateral movement is especially dangerous because it allows attackers to penetrate deeper into the network, often going undetected due to the use of legitimate credentials and common administrative tools. This phase revealed that without proper network

segmentation and strict access controls, an attacker who compromises one system can access the entire network, making lateral movement one of the most dangerous aspects of an APT attack.

Phase 5: Data Exfiltration

The final phase involved exfiltrating sensitive data from GlobalTech's internal servers using encrypted channels to avoid detection.

1. I employed Meterpreter's search function to locate files of interest, such as confidential documents and proprietary data.
2. Before exfiltration, data was compressed and encrypted using AES encryption via Python's cryptography library. This step ensured that even if intercepted, the data would remain unreadable.
3. Encrypted data was then transferred to an external location using secure protocols such as SCP (Secure Copy Protocol). The transfer was monitored to ensure that it did not trigger network alarms.

This phase highlighted the stealth with which data exfiltration can occur. The use of encryption and secure channels allows attackers to bypass conventional monitoring systems. The ability to exfiltrate data in an encrypted and covert manner emphasizes the necessity for robust Data Loss Prevention (DLP) systems and anomaly detection to identify and block unauthorized data transfers.

2.3. Challenges & Solutions

During the spear phishing phase, the Social-Engineer Toolkit (SET) failed to run due to a "command not found" error. This was a significant obstacle as it delayed the simulation and risked compromising the exercise timeline. I had to manually clone the SET repository from GitHub, adjusted dependencies (replacing pycrypto with pycryptodome), and configured Metasploit's path in the set.config file. Once resolved, SET operated correctly, and the simulation continued.

3. Conclusion

The simulated attack campaign against GlobalTech provided a detailed view of the vulnerabilities present in multi-layered cyber environments. Each phase—from the initial DDoS attack to the eventual data exfiltration—revealed specific weaknesses in network infrastructure, user behavior, and security controls. The campaign not only demonstrated how an attacker can exploit these vulnerabilities in a sequential manner but also highlighted the significant psychological impact on the target organization, including loss of trust and operational disruption.

From a strategic standpoint, the exercise not only highlighted technical deficiencies but also exposed the psychological impact on the organization. Employees' trust in internal communications was eroded after witnessing a successful spear phishing campaign,

while the ability of an attacker to maintain persistence instilled a sense of ongoing vulnerability. The compounded effect of these phases creates an environment of uncertainty and fear, which can lead to diminished confidence in the organization's overall security posture. The exercise underscored the importance of ethical hacking as a proactive measure. By responsibly simulating these attack phases, organizations can gain valuable insights into their security posture and implement targeted improvements before a real attacker exploits these weaknesses.

3.1. Recommendations

Based on the comprehensive analysis and the findings of the simulation, it is imperative for GlobalTech to adopt a multi-layered cybersecurity strategy that addresses vulnerabilities at every phase of a potential attack.

First, **strengthening network defenses** must be prioritized. GlobalTech should invest in advanced DDoS mitigation technologies that go beyond basic rate limiting, incorporating intelligent traffic analysis and real-time filtering systems. By deploying robust web application firewalls and integrating Content Delivery Networks (CDNs), the organization can distribute and balance incoming traffic more efficiently, reducing the likelihood of overwhelming any single server during an attack. These measures not only protect against volumetric attacks but also enhance the overall reliability of web services, thereby preserving customer trust and operational continuity.

In addition to bolstering network infrastructure, **enhancing endpoint security and user authentication** is crucial. GlobalTech must mandate the use of multi-factor authentication (MFA) for all critical systems and privileged accounts. This approach provides an essential additional layer of security, ensuring that even if an attacker manages to acquire a user's credentials through spear phishing, they will be thwarted by the requirement for secondary verification. Coupled with this, a comprehensive, ongoing security awareness program should be implemented. Regular training sessions, phishing simulations, and updates on emerging threats will help cultivate a security-conscious culture among employees, thereby reducing the risk of successful social engineering attacks.

Furthermore, GlobalTech should **integrate advanced endpoint detection and response (EDR) solutions** into its security framework. These systems are designed to monitor endpoint activities in real time, detect anomalies such as unauthorized process creation or unexpected file modifications, and provide rapid incident response. By continuously monitoring system integrity and conducting regular security audits, GlobalTech can quickly identify and remediate any persistence mechanisms or backdoors that might have been installed by an attacker.

The dangers of lateral movement within a network underscore the need for strict internal segmentation and access control. GlobalTech should **segment its network** into isolated zones, each with tailored security policies, to ensure that even if one segment is compromised, the attack cannot easily spread to critical systems. Implementing strict access controls, based on the principle of least privilege, will further minimize the risk by ensuring that users and devices only have the minimum access necessary to perform their functions.

Finally, to address the risk of data exfiltration, GlobalTech must adopt a **robust data loss prevention (DLP) strategy**. This strategy should include the deployment of advanced DLP tools capable of monitoring and analyzing data flows across the network. These tools can help detect and prevent unauthorized data transfers by flagging unusual patterns or large volumes of data leaving the network. In parallel, sensitive data should be encrypted both at rest and in transit. Encryption serves as a critical safeguard, ensuring that even if data is intercepted during an exfiltration attempt, it remains indecipherable and secure.

In summary, by adopting a **holistic approach** that combines advanced network defense technologies, rigorous endpoint security measures, continuous user education, and robust data protection mechanisms, GlobalTech can significantly enhance its cybersecurity posture. This integrated strategy will not only mitigate the risks associated with sophisticated multi-phase cyber attacks but also foster an organizational culture that is proactive in its defense against evolving cyber threats.

4. References

CrowdStrike. (n.d.). *Understanding lateral movement*. Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/lateral-movement/
IBM Security. (n.d.). *Spear phishing and its impact on data breaches*. Retrieved from https://www.ibm.com/think/topics/spear-phishing
LastPass. (n.d.). *The psychological impact of cyber attacks*. Retrieved from https://blog.lastpass.com/posts/the-psychological-impact-of-cyber-attacks
Metasploit Unleashed. (n.d.). *Persistence techniques in penetration testing*. Retrieved from https://www.metasploit.com/
National Security Agency. (n.d.). *Cybersecurity mitigation strategies*. Retrieved from https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/
Splunk. (n.d.). *Detecting data exfiltration*. Retrieved from https://www.splunk.com/en_us/blog/learn/data-exfiltration.html
Teramind. (n.d.). *Data exfiltration examples and prevention tactics*. Retrieved from https://www.teramind.co/blog/data-exfiltration-examples/