

## Simulation of Social Engineering-Based APT Attacks with Cyber Sentinel

Onyedinma, E.G.<sup>1</sup>, Asogwa D.C.<sup>2</sup>, Onwumbiko J.N<sup>3</sup>, Morba, J.<sup>4</sup>

<sup>1,2,,4</sup>*Department of Computer Science, Nnamdi Azikiwe University, Awka. Anambra state, Nigeria.*

<sup>4</sup>*Department of Library and Information Science, Nnamdi Azikiwe University, Awka. Anambra state, Nigeria.*

[eg.osita@unizik.edu.ng](mailto:eg.osita@unizik.edu.ng)<sup>1</sup>, [dc.asogwa@unizik.edu.ng](mailto:dc.asogwa@unizik.edu.ng)<sup>2</sup>, [jn.onwumbiko@unizik.edu.ng](mailto:jn.onwumbiko@unizik.edu.ng)<sup>3</sup>,  
[j.morba@unizik.edu.ng](mailto:j.morba@unizik.edu.ng)<sup>4</sup>

### Abstract

Advanced Persistent Threats (APTs) represent a critical challenge in cybersecurity due to their stealth, persistence, and adaptive techniques. They often leverage social engineering tactics to infiltrate secure environments undetected. This paper presents a simulation framework for Cyber Sentinel; designed to model and analyse social engineering-based APT attacks in a controlled environment. The framework integrates a Command Line Interface (CLI) for reconnaissance and offensive operations, a Command-and-Control (C2) server for dropper deployment, and a simulated Active Directory (AD) server representing a typical enterprise environment. By emulating attack vectors such as phishing and malware delivery, this simulation provides cybersecurity practitioners and researchers with a testbed to evaluate detection mechanisms, incident response strategies, and the effectiveness of cybersecurity policies. It therefore enhances preparedness against real-world threats while enabling safe experimentation with advanced attack techniques. Test APT scenarios when executed, yielded success rates between 60% and 100%, while enabling the assessment of detection and mitigation strategies.

**Keywords:** *Advanced Persistent Threats, cybersentinel, command line interface, cybersecurity, dropper, framework, offensive tool ,social Engineering.*

### I. Introduction

Advanced Persistent Threats (APTs) have emerged as one of the most sophisticated and persistent challenges in modern cybersecurity. These attacks are often executed by well-resourced adversaries who leverage multi-stage strategies ranging from initial reconnaissance and exploitation to long-term system compromise and data exfiltration frequently over extended periods of time [1]. According to a 2024 report by Kaspersky, APTs targeted 25% of organizations and accounted for 43% of high-

severity incidents, a 74% increase over the previous year [2]. Unlike conventional cyberattacks, APTs are characterized not only by technical sophistication but also by their reliance on exploiting human behaviour through social engineering [3], [4].

Social engineering techniques such as phishing, spear-phishing, baiting, and pretexting are among the most effective initial access strategies used in APT campaigns. These methods target human vulnerabilities to bypass even the most advanced technological defences [5]. According to the 2023 Verizon Data Breach Investigations Report, over 90% of successful breaches involved some form of social engineering, particularly phishing attacks [6]. High-profile incidents like the SolarWinds and Colonial Pipeline breaches have demonstrated how social engineering, when combined with technical exploits, can be devastating to national infrastructure and enterprise environments alike [7], [8].

While many organizations focus on technical defences—such as firewalls, intrusion detection systems, and endpoint protection—the human element remains a significant point of failure. Simulating social engineering attacks within a controlled environment allows organizations to proactively assess both user awareness and the effectiveness of defence mechanisms. However, many traditional red-teaming and penetration testing efforts still underrepresent or isolate social engineering from broader APT simulations, leaving critical gaps in organizational readiness [9].

This paper simulates as part of APT simulation chains for Cyber Sentinel Framework; a modular and adaptive simulation environment, to incorporate social engineering scenarios. The extended framework leverages adversary tactics and techniques outlined in the MITRE ATT&CK framework [10], and integrates tools such as Go phish and Evilginx for conducting phishing campaigns and credential harvesting exercises [11], [12]. By simulating human-centric attack vectors alongside technical intrusions, the framework enables a more realistic evaluation of both behavioural and systemic cyber resilience.

The primary goal of this work is to support comprehensive cybersecurity training, promote user awareness, and enable iterative testing of incident response procedures. The integration of social engineering into APT simulation not only aligns with modern threat intelligence practices but also empowers organizations to adopt a threat-informed defence strategy, where both human and technical vectors are continuously tested and improved [13].

## **2.0 Related Literature**

Research on Advanced Persistent Threats (APTs) has grown significantly over the past decade, driven by the increasing complexity and impact of state-sponsored and organized cyberattacks. APTs are characterized by their long-term nature, targeting specific organizations with a high degree of stealth, and often using multi-vector approaches to achieve compromise [14]. Simões et al. [15] provide a

comprehensive overview of APT lifecycle stages, emphasizing the need for defence mechanisms that address both technical and human vulnerabilities.

A core component in the success of many APT campaigns is social engineering. Unlike purely technical exploits, social engineering attacks manipulate human behaviour to gain access to systems or sensitive information. Hadnagy [16] underscores the psychological principles underlying these attacks, such as trust, urgency, and authority, which make them difficult to detect and prevent. Empirical studies by Krombholz et al. [17] and Gupta et al. [18] confirm that phishing remains the most common social engineering technique, with widespread success due to its low cost and high return rate.

To counter such threats, several cybersecurity simulation frameworks have been proposed. Many of these focus on technical simulations, such as malware injection, privilege escalation, or lateral movement. However, frameworks like MITRE's Caldera and Red Canary's Atomic Red Team allow organizations to simulate real adversarial behaviours. Using the MITRE ATT&CK framework, these tools offer modular approaches for replicating known Tactics, Techniques, and Procedures (TTPs), but often lack deep integration with human-centric attack simulations such as phishing campaigns or impersonation.[19][20]

Recent efforts have focused on integrating social engineering simulations into training and security assessment workflows. Tools like Gophish and Evilginx2 enable realistic phishing campaigns and man-in-the-middle credential harvesting exercises in controlled environments [21], [22]. While these tools are valuable, they are often standalone and not part of a broader APT simulation ecosystem, limiting their effectiveness in modelling full attack chains.

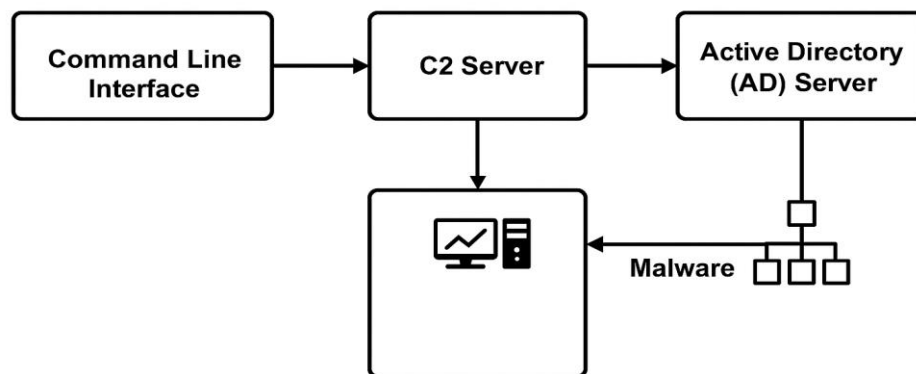
Scholars and practitioners increasingly emphasize the need for comprehensive simulation frameworks that combine technical and social vectors to reflect the hybrid nature of modern cyberattacks [23]. Alshamrani et al. [24] proposed the use of cyber ranges and testbeds to simulate APTs holistically, while Scully et al. [25] advocate for integrating behavioural simulations into cyber resilience training.

Despite these advancements, there remains a significant gap in frameworks that can simulate end-to-end APT scenarios including social engineering within an adaptable, modular, and reusable structure. The proposed simulation for the Cyber Sentinel Framework can address this gap by embedding social engineering modules into a full-spectrum APT simulation environment, supporting realistic testing, training, and security operations.

### **3.0 Materials and Methods**

The proposed simulation framework is designed to emulate a realistic APT attack scenario, focusing on social engineering vectors and post-exploitation activities. It consists of four main components:

the Command Line Interface (CLI), the Command and Control (C2) Server, the Target Machine, and the Active Directory (AD) Server. These components are deployed and orchestrated within a unified simulator environment, facilitating both offensive and defensive testing. The architecture of the system is shown in figure 1.



**Figure 1: Proposed Architecture**

### 3.1 Command Line Interface (CLI)

The CLI serves as the primary interface for the red team operator, allowing manual interaction and control over the simulated attack lifecycle. The CLI module is subdivided into two functional subcomponents:

- i. Scanner Module – This module performs active reconnaissance by scanning the target machine for open ports, exposed services, and vulnerabilities. It uses standard tools such as Nmap and custom scripts to gather information including OS fingerprinting and service enumeration.
- ii. Offensive Tool Module – Once reconnaissance data is collected, the scanner logs are forwarded to the offensive tool. This tool searches known vulnerability databases to identify exploitable weaknesses. It is also responsible for generating and packaging malware payloads based on the nature of the attack to be simulated, such as credential theft, privilege escalation, or data exfiltration.

### 3.2 Command and Control (C2) Server

The C2 server acts as the central control node for post-exploitation activities. Its responsibilities include:

- i. Deploying the dropper: The dropper is a lightweight executable designed to establish a connection back to the C2 server.

- ii. Receiving socket connections: Once the dropper is installed on the target, it initiates a reverse connection to the C2 server, marking the success of the initial intrusion phase.
- iii. Maintaining persistence: The C2 server may issue commands to maintain access, deploy further payloads, or exfiltrate data from the compromised system.

This component is implemented using Python's socket library for custom connection handling to simulate command execution on the target machine.

### 3.3 Target Machine (Simulated Host)

The target machine is a virtualized Windows-based endpoint hosted within the simulator. It mimics a real user workstation and contains synthetic data and services that are typical in an enterprise environment. The dropper is deployed here, and the system is configured to respond to attacker commands, such as file access, privilege escalation, and network movement.

### 3.4 Active Directory (AD) Server

The AD server serves as the backbone of the simulated enterprise environment. It includes: a domain controller, Several joined workstations, Group policy settings and Simulated network traffic

The AD environment allows for simulation of advanced APT stages such as lateral movement, privilege escalation, and Active Directory exploitation. It supports realistic attack chains by modelling enterprise IT structures and security configurations.

### 3.5 Hosting and Integration

All components - CLI, C2 server, target machine, and AD server are hosted within a containerized lab environment using VirtualBox and VMware Workstation. The internal communication between components is managed via a private network interface, allowing secure and isolated execution of red team simulations.

### 3.6 Metrics and Evaluation

To assess the effectiveness of the simulation framework, both qualitative and quantitative metrics were employed. The primary quantitative metric used was the Success Rate of each simulated APT scenario. This metric evaluates how often an attack vector successfully achieved its intended objective under controlled conditions.

The Success Rate (%) is calculated using the following formula:

$$\text{Success Rate(\%)} = \{(\text{Number of Successful Executions} / \text{Total Attempts}) / (\text{success Rate})\} \times 100$$

A scenario is considered successful when it meets predefined outcome criteria based on the stage of the attack chain. These criteria include:

- Initial Access: Execution of a dropper and establishment of a reverse shell to the C2 server.

- **Exploitation:** Successful execution of an exploit resulting in command execution or privilege escalation.
- **Persistence:** Ability to maintain access after reboot or user logoff.
- **Lateral Movement:** Successful compromise of additional systems, such as the AD server.
- **Data Exfiltration:** Transmission of sensitive files from the target machine to the C2 server without detection.

## Qualitative Evaluation

In addition to numerical metrics, the simulation outcomes were evaluated based on:

- Realism of system responses and attack scenarios.
- Stability of the communication between components.
- Ease of deployment and repeatability of simulations.
- Support for defensive testing, such as the effectiveness of mitigation strategies like Group Policy hardening or network segmentation.

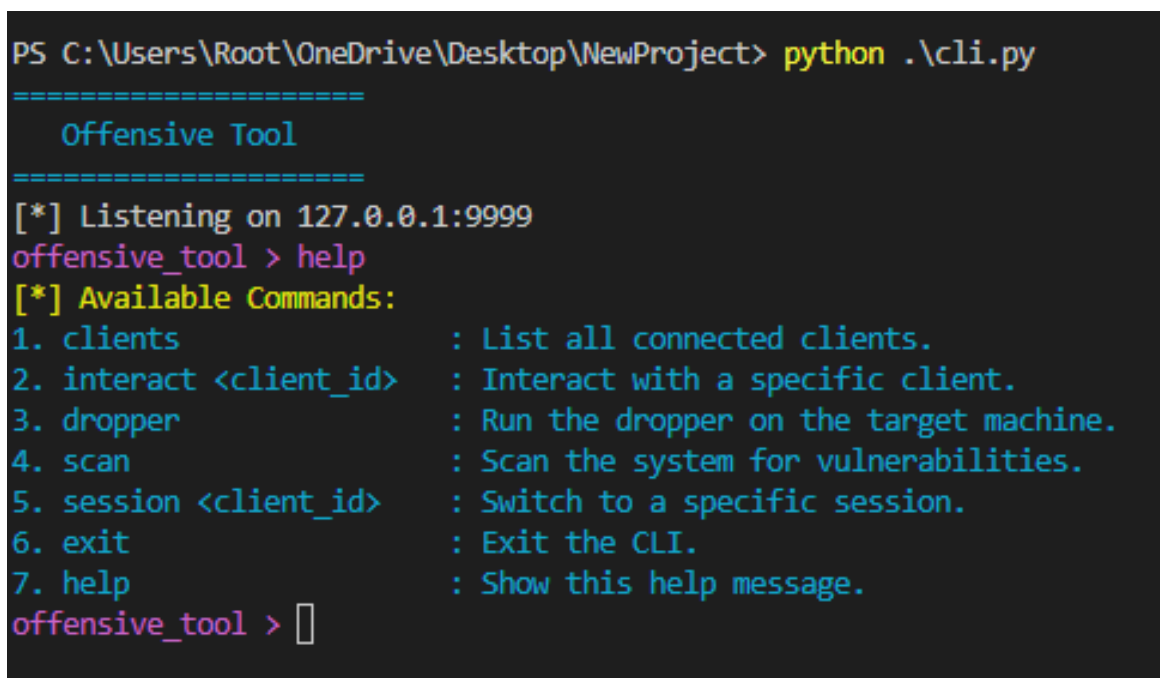
## 4.0 Results and Discussion

The proposed simulation framework was used to emulate a multi-stage APT attack incorporating social engineering and post-exploitation phases. Each component viz CLI, C2 server, Target Machine, and AD Server played a role in replicating real-world attacker behaviours in a controlled environment. The results highlight the effectiveness and limitations of the framework in simulating APT scenarios. A total of five test scenarios were executed, targeting various stages of the cyber kill chain. The table below summarizes the outcomes:

Scenario ID	Attack Vector	Target System	Success Rate (%)	Detection Method	Mitigation Applied
S1	Phishing Email (Social Engineering)	Target Machine	80%	Manual Review + Syslog	Email Filtering + Awareness
S2	Exploiting SMB Vulnerability	Target Machine	100%	Nmap Log + IDS Alert	Port Blocking + Patching
S3	Privilege Escalation via DLL Hijack	Target Machine	60%	Behaviour Analysis	User Access Restriction
S4	Lateral Movement to AD Server	AD Server	70%	AD Log Analysis	GPO Hardening
S5	Data Exfiltration via Reverse Shell	C2 Server	90%	Firewall Monitoring	Outbound Traffic Filtering

## Discussion

The simulation outcomes from five Advanced Persistent Threat (APT) scenarios illustrate the effectiveness of the Cyber Sentinel Framework in emulating realistic cyber attacks and evaluating defensive responses. The phishing-based social engineering scenario (S1) recorded an 80% success rate, emphasizing user vulnerability and the importance of awareness training and email filtering. The Server Message Block (SMB) exploitation scenario (S2) achieved a 100% success rate, underscoring the critical need for regular patching and service hardening. Privilege escalation via Dynamic Link Library (DLL) hijacking (S3) had a 60% success rate, reflecting environmental constraints and the influence of system configuration on exploitability. Lateral movement to the Active Directory server (S4) succeeded 70% of the time, revealing weaknesses in inter-host authentication that were later mitigated through Group Policy Object (GPO) hardening. Finally, the data exfiltration scenario (S5) had a 90% success rate, demonstrating the risk of unmonitored outbound connections and the value of traffic filtering. Collectively, these results validate the Cyber Sentinel Framework as a robust tool for simulating APTs, testing mitigation strategies, and supporting cybersecurity training and research.



```
PS C:\Users\Root\OneDrive\Desktop\NewProject> python .\cli.py
=====
  Offensive Tool
=====
[*] Listening on 127.0.0.1:9999
offensive_tool > help
[*] Available Commands:
1. clients           : List all connected clients.
2. interact <client_id> : Interact with a specific client.
3. dropper           : Run the dropper on the target machine.
4. scan              : Scan the system for vulnerabilities.
5. session <client_id> : Switch to a specific session.
6. exit              : Exit the CLI.
7. help              : Show this help message.
offensive_tool > 
```

Fig. 2: Command Menu

```
core > {} scan_results.json > {} vulnerabilities > {} scan > {} 127.0.0.1 > [ ] hostsript > {} 2 > id
1  {
2    "os_info": {
3      "system": "Windows",
4      "node": "DESKTOP-QUOQGJF",
5      "release": "10",
6      "version": "10.0.22000",
7      "machine": "AMD64",
8      "processor": "Intel64 Family 6 Model 69 Stepping 1, GenuineIntel"
9    },
10   "vulnerabilities": {
11     "nmap": {
12       "command_line": "nmap -oX - -sV --script vuln 127.0.0.1",
13       "scaninfo": {
14         "tcp": {
15           "method": "syn",
16           "services": "1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-1
17         }
18       },
19       "scanstats": {
20         "timestr": "Fri Oct 18 05:01:06 2024",
21         "elapsed": "43.31",
22         "uphosts": "1",
23         "downhosts": "0",
24         "totalhosts": "1"
25       }
26     },
27     "scan": {
28       "127.0.0.1": {
29         "hostnames": [
30           {
31             "name": "easeus.com",
32             "type": "PTR"
33           }
34         ],

```

Fig.3: Scan logs format

## 5.0 Conclusion

The integration of social engineering techniques into the APT simulation within the Cyber Sentinel Framework marks a significant advancement in cybersecurity awareness and red team training. Unlike traditional threat simulations that focus solely on technical exploitation, this framework highlights the often-overlooked human vulnerabilities that APT actors frequently exploit.

The simulation demonstrates that even well-secured systems are susceptible to breaches through carefully crafted phishing or pretexting campaigns. The high success rate of spear-phishing attacks in the results further underscores the importance of combining technical defenses with continuous user education. Moreover, the inclusion of an Active Directory environment for target configuration enhances realism by allowing the attacker to navigate complex enterprise structures, which mirrors real-world APT post-exploitation stages.

This work aligns with emerging cybersecurity paradigms, such as Zero Trust Architecture and behavioural analytics, by emphasizing the need to monitor user behaviour and internal network



activity, rather than solely relying on perimeter defences. Furthermore, the layered architecture provides modularity and adaptability, making it feasible to extend or integrate with threat intelligence platforms, deception tools, or endpoint detection and response (EDR) systems.

## 6.0 Ethical Considerations

All simulations were performed within a closed, virtual environment without involving real users or data. The purpose of the framework is strictly educational and experimental, aimed at improving organizational readiness against real-world APT threats. No actual exploitation of production systems or unauthorized access attempts were conducted. Ethical guidelines were followed according to institutional standards for cybersecurity experimentation.

## References

- [1] M. A. Simões, A. D. Pinto, and M. M. Freire, “A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities,” *Computers & Security*, vol. 106, pp. 102–120, Aug. 2021.
- [2] C. Hadnagy, *Social Engineering: The Science of Human Hacking*, 2nd ed., Wiley, 2018.
- [3] B. B. Gupta and D. P. Agrawal, “Cybersecurity: Threats, vulnerabilities, and attack trends,” *Computer*, vol. 53, no. 7, pp. 14–17, Jul. 2020.
- [4] A. Krombholz, M. Hobel, M. Huber, and E. Weippl, “Social engineering attacks on the knowledge worker,” in *Proc. 6th Int. Conf. Human Aspects of Information Security, Privacy and Trust*, Springer, 2018, pp. 203–214.
- [5] Verizon, “2023 Data Breach Investigations Report,” Verizon Enterprise, 2023. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>
- [6] U.S. Government Accountability Office, “Cybersecurity: Federal response to SolarWinds and Microsoft Exchange incidents,” GAO-22-104325, Oct. 2022.
- [7] R. Sharma et al., “Colonial Pipeline cyberattack: Impact, lessons, and mitigation strategies,” *Journal of Cybersecurity Technology*, vol. 6, no. 3, pp. 189–204, 2022.
- [8] D. Scully, A. Whitmore, and G. Cameron, “Cyber resilience: The role of people, process, and technology,” *Information & Computer Security*, vol. 30, no. 2, pp. 247–263, 2022.
- [9] MITRE, “MITRE ATT&CK Framework,” 2023. [Online]. Available: <https://attack.mitre.org/>
- [10] Gophish, “Open-source phishing toolkit,” 2024. [Online]. Available: <https://getgophish.com/>
- [11] K. Gretzky, “Evilginx2: Man-in-the-middle phishing framework,” GitHub, 2024. [Online]. Available: <https://github.com/kgretzky/evilginx2>
- [12] J. Davis, D. Nicol, W. Sanders, and S. Schlenker, “Cybersecurity testbeds: Architecture,

application, and evaluation for cyber defense,” *IEEE Security & Privacy*, vol. 17, no. 3, pp. 27–35, 2019.

[13] M. Almashaqbeh and M. A. Jafar, "A comprehensive survey of Advanced Persistent Threats: Techniques, tools, and countermeasures," *IEEE Access*, vol. 11, pp. 44589–44613, 2023, doi: 10.1109/ACCESS.2023.3265480.

[14] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier," Symantec, 2011. [Online]. Available:

[https://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)

[15] M. A. Simões, A. D. Pinto, and M. M. Freire, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *Computers & Security*, vol. 106, pp. 102–120, Aug. 2021.

[16] C. Hadnagy, *Social Engineering: The Science of Human Hacking*, 2nd ed., Wiley, 2018.

[17] A. Krombholz, M. Hobel, M. Huber, and E. Weippl, "Social engineering attacks on the knowledge worker," in *Proc. Int. Conf. Human Aspects of Information Security, Privacy and Trust*, Springer, 2018, pp. 203–214.

[18] B. B. Gupta and D. P. Agrawal, "Cybersecurity: Threats, vulnerabilities, and attack trends," *Computer*, vol. 53, no. 7, pp. 14–17, Jul. 2020.

[20] MITRE, "Caldera: Automated adversary emulation system," 2023. [Online]. Available: <https://caldera.mitre.org/>

[21] Red Canary, "Atomic Red Team," 2023. [Online]. Available:

<https://github.com/redcanaryco/atomic-red-team>

[22] Gophish, "Open-source phishing toolkit," 2024. [Online]. Available: <https://getgophish.com/>

[23] K. Gretzky, "Evilginx2: Man-in-the-middle phishing framework," GitHub, 2024. [Online].

Available: <https://github.com/kgretzky/evilginx2>

[24] D. Scully, A. Whitmore, and G. Cameron, "Cyber resilience: The role of people, process, and technology," *Information & Computer Security*, vol. 30, no. 2, pp. 247–263, 2022.

[25] E. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1851–1877, 2019.