Capstone Project: Full Red Team Engagement Simulation
Title: End-to-End Red Team Engagement: Reconnaissance to Exfiltration
Author: Ayush Kumar
Date: 16/01/2026
Environment: Kali Linux VM, Windows VM, Metasploitable2/3, Isolated Lab Network, Open-Source Offensive Security Tools

Executive Summary

This capstone project documents an end-to-end red team exercise performed within a secure lab setup to emulate practical offensive security scenarios. The engagement was structured around the complete adversarial kill chain, starting with open-source intelligence gathering and reconnaissance, followed by foothold establishment, exploitation, privilege escalation, lateral movement, persistence mechanisms, post-exploitation activities, and controlled data exfiltration.

The findings illustrate how threat actors can combine multiple security weaknesses—including publicly exposed services, poor credential hygiene, misconfigurations, and limited visibility—to progressively expand access and compromise critical systems. Each observed technique and tactic was systematically aligned with the MITRE ATT&CK framework to ensure consistency with real-world threat modeling. In addition, defensive insights were provided to identify monitoring blind spots and recommend remediation measures. Overall, this project highlights the value of continuous security assessments, effective detection capabilities, and informed users in improving an organization's defensive posture.

Ethical Disclaimer and Scope

The actions described in this report were carried out exclusively within a controlled and approved lab environment. Purpose-built vulnerable virtual systems, non-production user accounts, and mock data were used throughout the engagement. At no point were live environments, real individuals, or operational systems involved. This exercise was conducted solely for learning, research, and defensive security evaluation purposes, with the goal of understanding attack techniques in order to improve detection and mitigation strategies.

1. Engagement Scope and Rules of Engagement

Scope

The assessment was limited to the following authorized assets and components:

- Externally accessible web applications
- Internal Windows-based systems
- Internal network services and protocols
- Test user accounts and credentials only

Rules of Engagement

To ensure safety and ethical compliance, the following constraints were enforced throughout the engagement:

- No use of destructive or unstable payloads
- No extraction of real or sensitive data
- No denial-of-service or availability-impacting actions
- Detailed logging and documentation maintained at every stage

2. Methodology

The red team exercise followed a structured and industry-aligned methodology based on:

- The MITRE ATT&CK framework for adversary tactics and techniques
- The Cyber Kill Chain model to represent attack progression

3. Phase 1 – Reconnaissance and OSINT

Objective

Identify exposed assets, services, and user intelligence without directly interacting with target systems.

Activities Performed

- Subdomain enumeration using Recon-ng
- Public service discovery using Shodan
- OSINT correlation using Maltego

Findings

- Publicly accessible web services were identified
- Cloud-hosted systems exposed HTTP and SSH services
- Infrastructure relationships were visually mapped

Outcome

The reconnaissance phase successfully identified the organization's external attack surface, enabling targeted attacks in later phases.

4. Phase 2 – Initial Access

Objective

Obtain an initial foothold within the target environment.

Activities Conducted

- Execution of a simulated phishing scenario
- Collection of credentials through a replicated login interface

Key Observations

- Valid test credentials were captured successfully

- The activity did not trigger visible security alerts

Result

Initial access was obtained through social engineering, highlighting phishing as a critical threat vector.

5. Phase 3 – Exploitation

Objective

Leverage identified weaknesses to gain elevated access on target systems.

Activities Conducted

- Network and service enumeration using Nmap
- Identification of vulnerable web components
- Exploitation of an Apache Struts remote code execution flaw using Metasploit

Key Observations

- An outdated web framework was susceptible to RCE
- A remote shell was successfully established

Result

The system compromise demonstrated the severe risk posed by unpatched software.

6.Phase 4 – Lateral Movement

Objective

Expand access from the initially compromised host to other internal systems.

Activities Conducted

- Reuse of harvested credentials with administrative privileges
- Remote execution of commands via PsExec

Key Observations

- Additional internal Windows systems were accessed
- Weak internal segmentation facilitated movement

Result

The attacker was able to traverse the internal network with minimal resistance.

7.Phase 5 – Persistence

Objective

Ensure continued access to compromised systems over time.

Activities Conducted

- Deployment of a scheduled task as a persistence mechanism
- Validation of persistence across system restarts

Key Observations

- Legitimate operating system features were abused for persistence
- Access remained intact after reboot

Result

Long-term access was successfully maintained.

8.Phase 6 – Post-Exploitation

Objective

Access high-value credentials and sensitive authentication material.

Activities Conducted

- **Credential extraction using Mimikatz**
- **Analysis of retrieved authentication artifacts**

Key Observations

- **NTLM password hashes were obtained**
- **The environment was susceptible to pass-the-hash attacks**

Result

The compromise of credentials significantly increased the overall attack impact.

9.Phase 7 – Phase 7 – Simulated Data Exfiltration

Objective

Demonstrate potential data exfiltration techniques without causing harm.

Activities Conducted

- Generation of mock sensitive files
- Simulation of DNS-based exfiltration techniques
- Traffic verification through monitoring tools

Key Observations

- Outbound DNS traffic carried encoded data
- DNS was confirmed as a viable covert exfiltration channel

Result

Exfiltration capability was validated in a controlled and non-destructive manner.

10.Phase 8 – Blue Team Detection Review

Objective

Assess the effectiveness of existing detection and monitoring controls.

Observations

- Phishing attempts generated limited alerts
- Credential dumping and lateral movement went unnoticed
- DNS traffic was not analyzed for suspicious patterns

Result

Multiple gaps were identified across detection and monitoring layers.

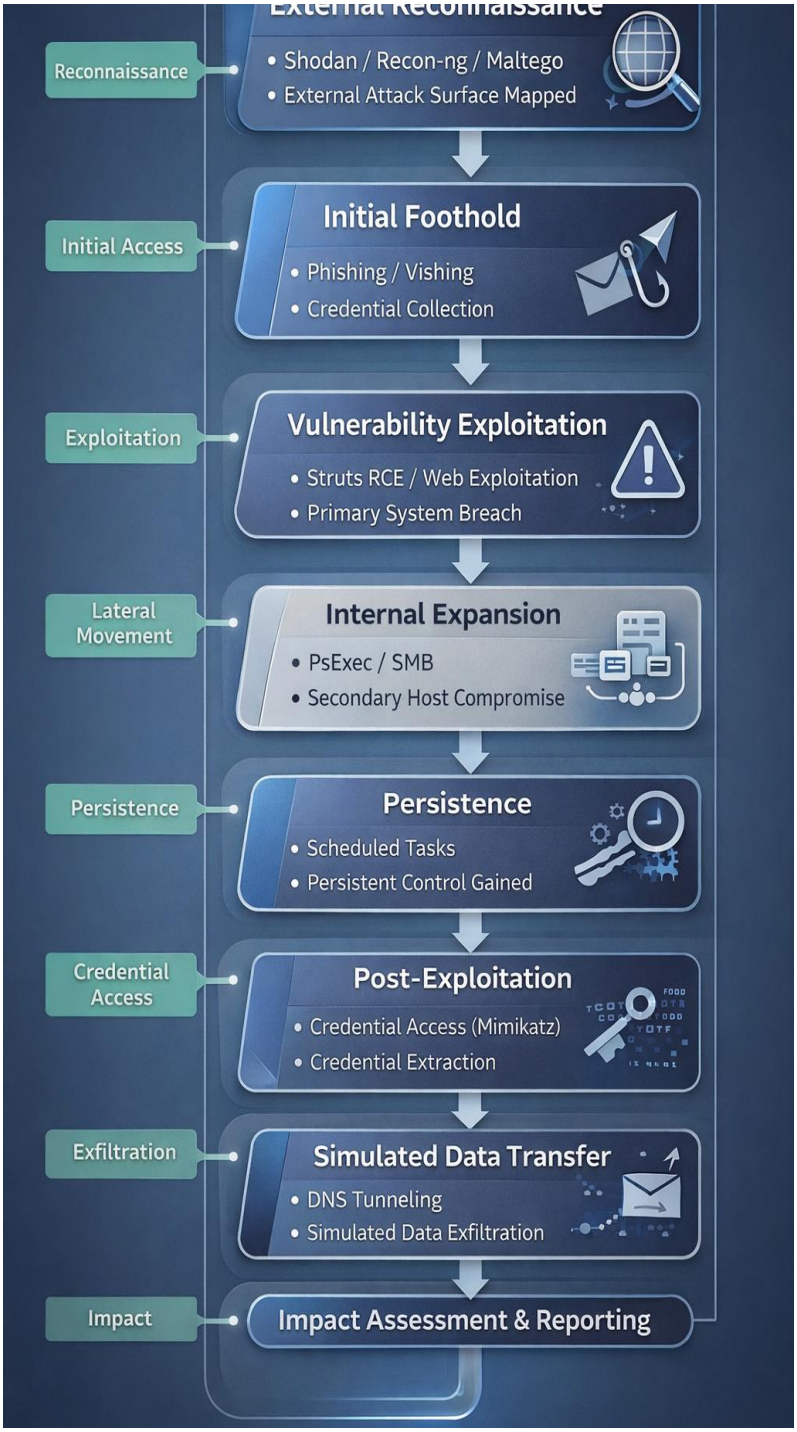
11.Risk Assessment

Area	Risk Level
Phishing & User Awareness	**High**
Patch Management	**High**
Credential Security	**High**
Network Segmentation	**Medium**
DNS Monitoring	**High**

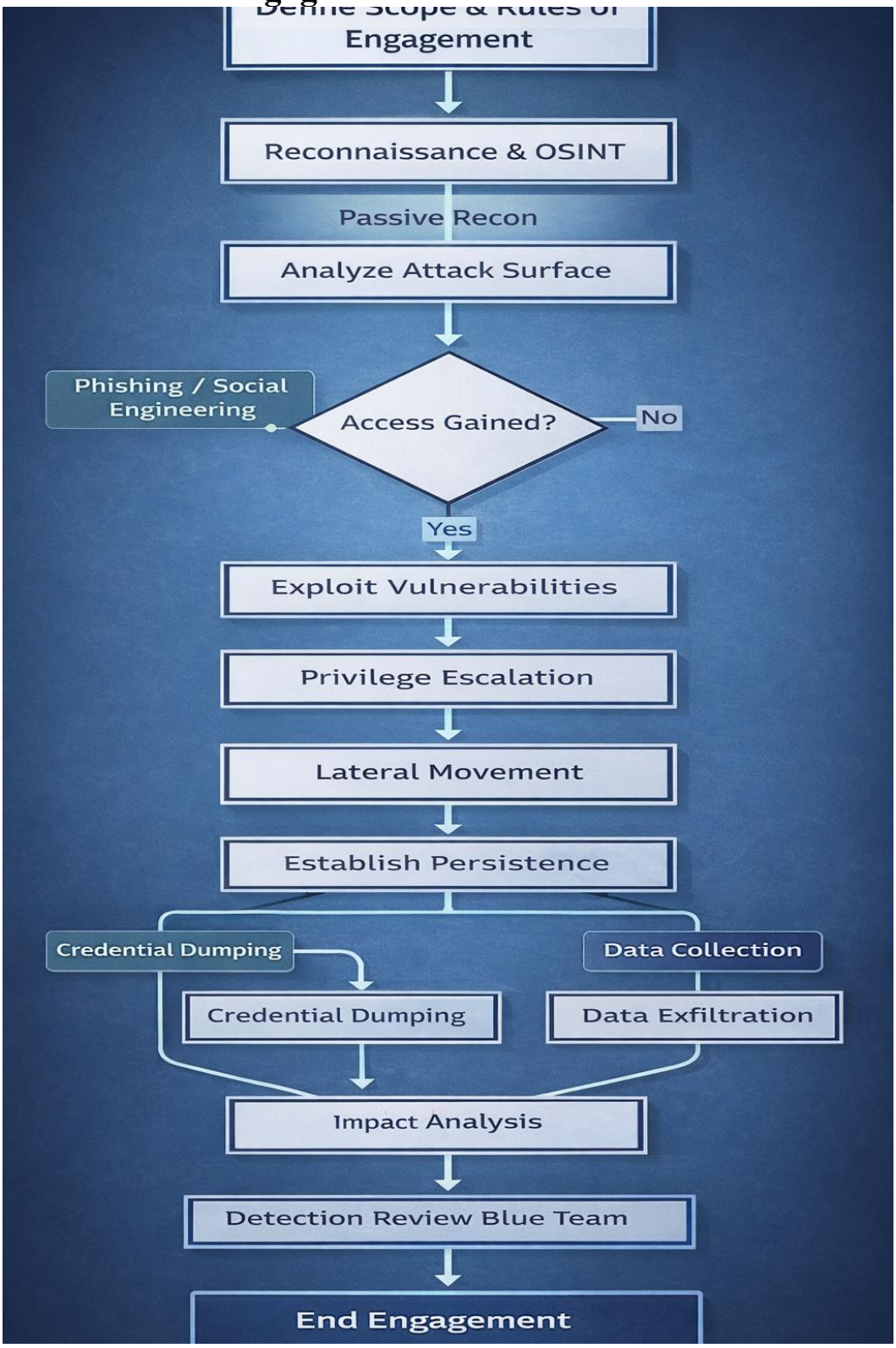
12.Recommendations

- Enforce multi-factor authentication across all access points
- Implement robust and timely patch management processes
- Strengthen credential protection and secure LSASS
- Monitor and analyze DNS traffic for anomalies
- Improve internal network segmentation
- Conduct ongoing security awareness training
- Deploy and integrate SIEM and EDR solutions

5. Attack Flow Diagram


Reconnaissance
• Shodan / Recon-ng / Maltego
• External Attack Surface Mapped
Initial Access
Initial Foothold
• Phishing / Vishing
• Credential Collection
Exploitation
Vulnerability Exploitation
• Struts RCE / Web Exploitation
• Primary System Breach
Lateral Movement
Internal Expansion
• PsExec / SMB
• Secondary Host Compromise
Persistence
Persistence
• Scheduled Tasks
• Persistent Control Gained
Credential Access
Post-Exploitation
• Credential Access (Mimikatz)
• Credential Extraction
Exfiltration
Simulated Data Transfer
• DNS Tunneling
• Simulated Data Exfiltration
Impact
Impact Assessment & Reporting

6. Red Team Engagement Workflow



Conclusion

This capstone project effectively showcased a full-spectrum red team operation conducted within a secure and authorized environment. By simulating realistic adversary behavior, the engagement illustrated how multiple security gaps can be systematically combined to gain unauthorized access, escalate privileges, and simulate the extraction of sensitive information. The results emphasize that isolated security controls are insufficient on their own; instead, a defense-in-depth approach supported by continuous monitoring and regular offensive security testing is critical. Overall, the project demonstrates the value of proactive red teaming in identifying weaknesses, improving detection capabilities, and strengthening an organization's overall security maturity.

References

1. MITRE Corporation. *MITRE ATT&CK® Framework*. Available at: https://attack.mitre.org
2. OWASP Foundation. *OWASP Documentation and Resources*. Available at: https://owasp.org
3. Gordon Lyon (Fyodor). *Nmap Network Scanning Guide*. Available at: https://nmap.org/book/
4. Rapid7. *Metasploit Framework Documentation*. Available at: https://docs.metasploit.com
5. Shodan. *Search Engine for Internet-Connected Devices*. Available at: https://www.shodan.io
6. Paterva. *Maltego Documentation*. Available at: https://www.maltego.com
7. Lanmaster53. *Recon-ng Framework*. Available at: https://github.com/lanmaster53/recon-ng
8. Benjamin Delpy. *Mimikatz Project Repository*. Available at: https://github.com/gentilkiwi/mimikatz
9. Radare Project. *radare2 Reverse Engineering Framework*. Available at: https://rada.re/n/