Capstone Project: Full Red Team Engagement Simulation
Title: End-to-End Red Team Engagement: Reconnaissance to Exfiltration
Author: Utkarsh Kumar
Date: 07/01/2026
Environment: Kali Linux VM, Windows VM, Metasploitable2/3, Isolated Lab Network, Open-Source Offensive Security Tools

Executive Summary

This capstone project presents a complete red team engagement conducted in a controlled laboratory environment to simulate real-world offensive security operations. The engagement followed the full attack lifecycle, beginning with reconnaissance and OSINT, progressing through initial access, exploitation, lateral movement, persistence, post-exploitation, and simulated data exfiltration.

The assessment demonstrates how attackers chain multiple weaknesses—such as exposed services, weak credentials, insecure configurations, and insufficient monitoring—to achieve deep network compromise. All activities were mapped to the MITRE ATT&CK framework to align with industry-standard adversary techniques. Defensive observations were also included to highlight detection gaps and mitigation strategies. This capstone emphasizes the importance of proactive security testing, monitoring, and user awareness in strengthening organizational resilience.

Ethical Disclaimer and Scope

All activities documented in this report were performed strictly in an isolated and authorized laboratory environment using intentionally vulnerable virtual machines, test accounts, and simulated data. No real organizations, users, or production systems were targeted. The objective of this engagement is educational and defensive in nature.

1. Engagement Scope and Rules of Engagement

Scope

- Public-facing web application
- Internal Windows hosts
- Internal network services
- User credentials (test accounts only)

Rules of Engagement

- No destructive payloads

- No real data exfiltration
- No denial-of-service attacks
- Logging and documentation at each phase

2. Methodology

The engagement followed a structured red team methodology aligned with:

- MITRE ATT&CK Framework
- Cyber Kill Chain Model

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

Gain the first foothold into the target environment.

Activities Performed

- Simulated phishing campaign
- Credential harvesting using a cloned login page

Findings

- Valid test credentials were successfully captured
- No security warnings were triggered during the attack

Outcome

Initial access was achieved via social engineering, confirming phishing as an effective attack vector.

5. Phase 3 – Exploitation

Objective

Exploit identified vulnerabilities to gain system-level access.

Activities Performed

- Network and service scanning using Nmap
- Web vulnerability identification
- Exploitation of Apache Struts RCE using Metasploit

Findings

- Outdated web framework vulnerable to remote code execution
- Successful remote shell obtained on the target system

Outcome

System compromise confirmed, demonstrating the impact of unpatched vulnerabilities.

6. Phase 4 – Lateral Movement

Objective

Move from the initially compromised system to other internal hosts.

Activities Performed

- Credential reuse and administrative authentication
- Remote command execution using PsExec

Findings

- Additional internal Windows host compromised
- Network segmentation weaknesses identified

Outcome

The attacker was able to expand access within the internal network.

7. Phase 5 – Persistence

Objective

Maintain long-term access to compromised systems.

Activities Performed

- Creation of a scheduled task for persistence
- Verification of task execution

Findings

- Persistence established using legitimate OS functionality
- Persistence survived system reboot

Outcome

Long-term access was successfully maintained.

8. Phase 6 – Post-Exploitation

Objective

Extract high-value assets after compromise.

Activities Performed

- Credential dumping using Mimikatz
- Identification of authentication material

Findings

- NTLM credential hashes successfully extracted
- Potential for pass-the-hash attacks identified

Outcome

Credential compromise significantly increased attack impact.

9. Phase 7 – Exfiltration (Simulated)

Objective

Demonstrate how attackers can exfiltrate data.

Activities Performed

- Creation of mock sensitive data
- Simulation of DNS-based exfiltration
- Verification via network monitoring

Findings

- Outbound DNS traffic successfully observed
- DNS identified as a covert exfiltration channel

Outcome

Data exfiltration capability was validated in a non-destructive manner.

10. Phase 8 – Blue Team Detection Review

Objective

Evaluate defensive detection capabilities.

Observations

- Phishing activity generated minimal alerts
- Lateral movement and credential dumping were not detected
- DNS traffic was not inspected for anomalies

Outcome

Detection and monitoring gaps were identified across multiple stages of the attack.

11. Risk Assessment

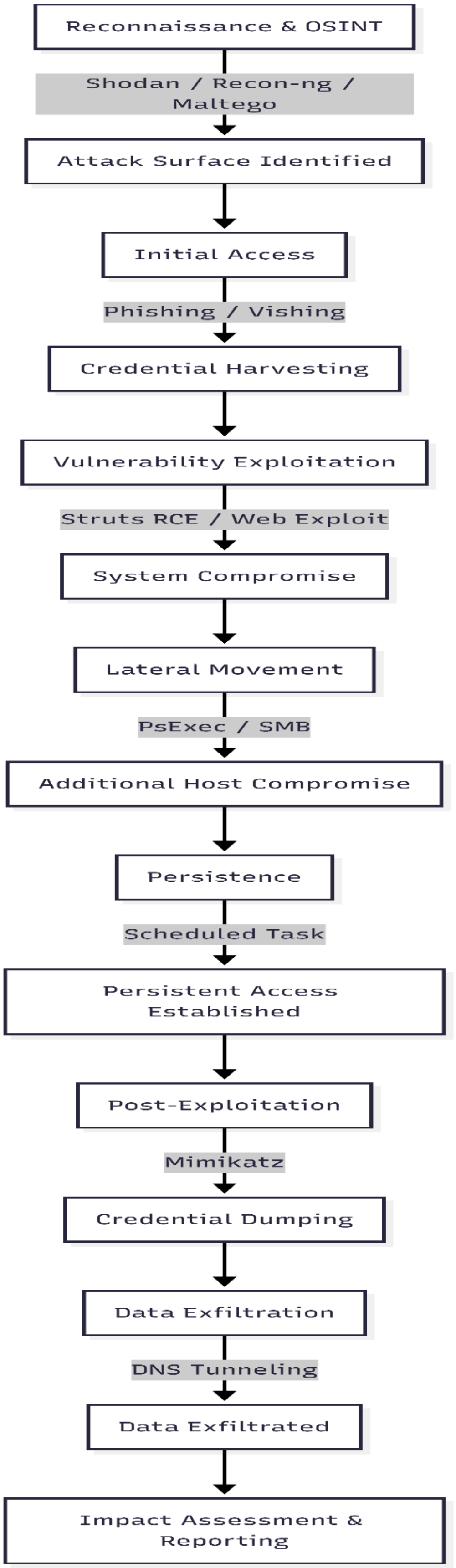
Area	**Risk Level**
Phishing & User Awareness	High
Patch Management	High
Credential Protection	High
Network Segmentation	Medium

Area	Risk Level
DNS Monitoring	High

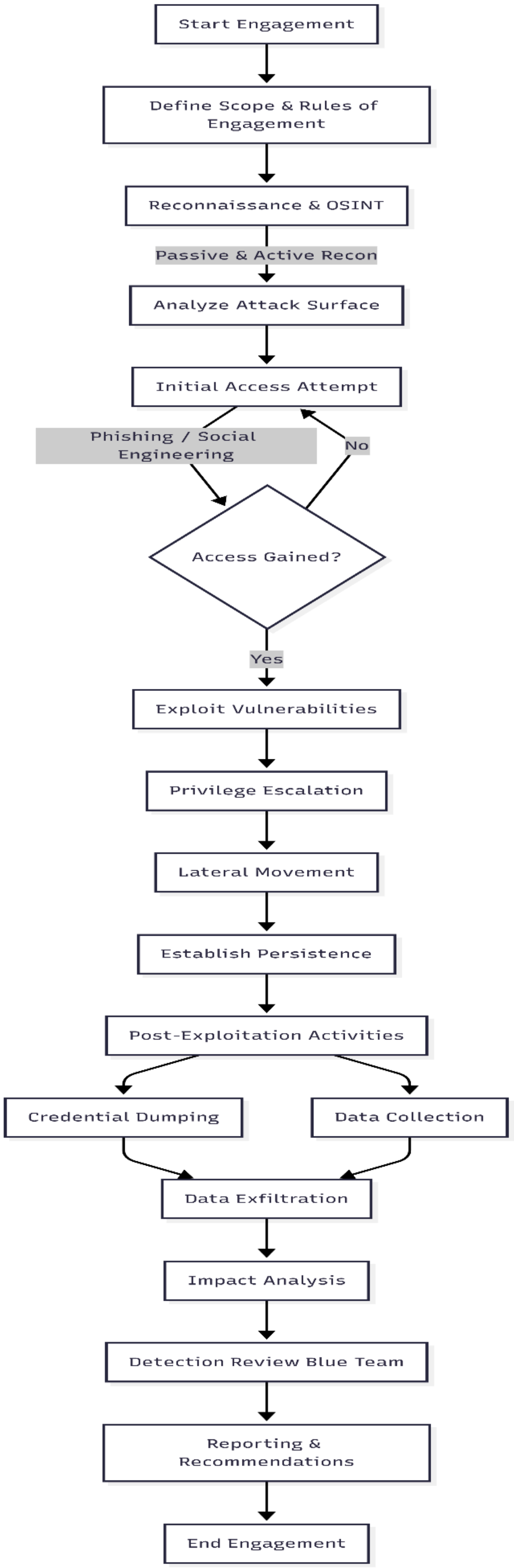
12. Recommendations

- Implement multi-factor authentication
- Enforce strict patch management
- Harden credential storage and LSASS protection
- Monitor DNS traffic for anomalies
- Improve network segmentation
- Conduct regular security awareness training
- Deploy SIEM and EDR solutions

13. Attack Flow Diagram


Reconnaissance & OSINT
Shodan / Recon-ng / Maltego
Attack Surface Identified
Initial Access
Phishing / Vishing
Credential Harvesting
Vulnerability Exploitation
Struts RCE / Web Exploit
System Compromise
Lateral Movement
PsExec / SMB
Additional Host Compromise
Persistence
Scheduled Task
Persistent Access Established
Post-Exploitation
Mimikatz
Credential Dumping
Data Exfiltration
DNS Tunneling
Data Exfiltrated
Impact Assessment & Reporting

14. Red Team Engagement Workflow



Conclusion

This capstone project successfully demonstrated an end-to-end red team engagement using ethical and controlled methods. The engagement highlighted how attackers chain multiple weaknesses to compromise systems and extract sensitive data. The findings reinforce the importance of layered security controls, continuous monitoring, and proactive red team assessments to improve organizational security posture.

References

1. MITRE ATT&CK Framework – https://attack.mitre.org
2. OWASP Documentation – https://owasp.org
3. Nmap Documentation – https://nmap.org/book/
4. Metasploit Framework Documentation – https://docs.metasploit.com
5. Shodan – https://www.shodan.io
6. Maltego Documentation – https://www.maltego.com
7. Recon-ng Documentation – https://github.com/lanmaster53/recon-ng
8. Mimikatz Project – https://github.com/gentilkiwi/mimikatz
9. radare2 Documentation – https://rada.re/n/