

Assignment Title:

Team Plan

By

Blue Team

Joshwa Edsall, Michael Moore,

Kristen Netter, Courtney Roberts, Steven Trudell

OPSC-590

Fall 2 2024

By submitting this assignment I acknowledge that I have read and agree to abide by the Champlain College Academic Honesty Policy. I declare that all work within this assignment is my own or appropriately attributed. I accept that failure to follow the academic honesty policy may result in a failure grade, or expulsion from Champlain College.

Date Due: November 10, 2024

Date Submitted: November 10, 2024

**Introduction**

This document outlines the initial actions that the Blue Team wishes to implement during the first cyber warfare simulation. The Blue Team has minimal information about the simulated environment. What we know is that we have a pfSense firewall, a Kali Linux, and a Windows system. The Blue Team is aware that both its environment and the Red Team's environment are identical. Both teams do not know what versions or configurations are in place. Knowing this, the Blue Team is aware that documentation is critical throughout all phases of the simulation. The Red Team and the Blue Team have the exact same environment, and documentation may provide the Blue Team with a strategic, defensive, and offensive advantage. Below is an outline of the Blue Team’s members’ skill sets.

*Team Leadership*

Mike Moore - Blue Team leader. Plan Responsibilities Incident Response and Pen Testing

* Over 6 years of technical writing, specifically analytical writing
* Over 6 years of intelligence and cybersecurity analysis with Federal Law Enforcement and other civilian agencies.
* Has previously led five academic groups to a high level of achievement.
* Over 15 years of stakeholder relationship-building and communication experience.
* Over 4 years of cyber supply chain experience, including standard operating procedures writing and identifying suspicious information.
* Certificates obtained: CompTIA Security +

Joshwa Edsall - Blue Team Back-up Lead. Plan Responsibilities Pen Testing and System Admin

* 7 Years of Physical Security, specifically regulation compliance
* 2 Years of Joint Task Force - Security Threat Groups intelligence analysis with State/Federal Law Enforcement
* Certificates obtained: CompTIA Security +

*Team Members*

Kristen Netter - Network Defender and Incident Responder

* 2+ years of experience as a Cybersecurity Analyst with proficiency in using various SIEM tools like Splunk, responding to incidents, and working with IDS/IPS systems.

Courtney Roberts - System Admin and Network Defender

* 15+ years of experience with investigative and analysis of cyber intrusions.
* She brings a different perspective on how to defend against malicious actors and how to target and attack networks.
* Certificates Obtained: GISF, GSEC, GCIH, and GCIA.

Steven Trudell - Network Defense (Firewalls) and Pen Testing.

* 13+ years of Armed Security to include (NOC) Network Operation Center.
* Generated Cyber awareness training for Security Officers.
* Previous cyber experience as SOC Analyst and Information Security Analyst.
* Currently hold Bachelor's in Computer Forensic
* Recently employed as PCI-DSS Compliance Specialist
* Certificate: CompTIA Security+, Various Vendor Specific certificates

**Step 1 System Admin**

1. Snapshot images of the PfSense Firewall, Kali Linux, and Windows terminals will be taken. This will assist if there are issues after a modification or patch update and the systems are no longer functioning correctly. The team can go back to the original image to identify where the modification caused a malfunction. The images will also assist with rebuilding the terminals if there is an intrusion or malicious activity.
2. Access to the Kali Linux and Windows terminals needs to be controlled. This will require changes to the default settings and default passwords. Changing default settings and default passwords will ensure unauthorized individuals are not granted access. Setting up access to the least privileges will also prevent pivoting if a malicious actor is able to gain access via compromised credentials.
3. System Monitoring (sysmon) will be configured on the terminals. Sysmon is a Windows system service that is also compatible with Linux. After reboots, Sysmon remains to monitor and log system activity and provides detailed information about process creation, network connections, and file changes. It will provide evidence of any changes to the systems, both by team members and potentially malicious actors.
4. Patch management involves updating and patching software to fix bugs and improve usability. Patch management also addresses known security vulnerabilities and reduces exposure to publicly known vulnerabilities.
   1. Deployment of Heimdal Patch & Asset Management. This platform supports multiple platforms and has a centralized console. It offers swift patch deployment.
5. All system modifications will be documented. This will allow quick identification of potential errors or misconfigurations. This will specifically assist with sysmon, with the notes of when Blue Team members changed modifications. If the Red Team makes a modification, the Blue Team will be able to identify that change based on the notes.

**Step 2 - System hardening and firewall Rule Configuration**

1. Keep both Windows and Linux systems up-to-date with the latest versions.
2. Uninstall unnecessary software is not needed on both Windows and Linux.
3. Configure pfSense to block incoming traffic and issue alerts for specific incidents, such as failed firewall rules or suspicious login attempts. This strategy ensures a strong first line of defense against any potential unauthorized access by the Red Team.
4. Rename our built-in admin account for both environments. The built-in admin account names are well known and could potentially be targeted by the Red Team trying to infiltrate our environment.
5. Regularly update our servers with the latest updates and security patches.
6. Identify open network-accessible ports and shut down any processes associated with them.
7. Set account login and lockout policies to limit the number of failed login attempts, reducing the risk of a brute force attack.
8. Regularly conduct network and vulnerability scans and tests to find and fix any issues.

**Step 3 - Threat Detection**

Upon completion of hardening and configuring the firewall(s), the Blue team plans to establish threat detection tools that may include honey pot(s), behavioral analysis, and activity logging (e.g., SIEMs). A honey pot is a decoy asset such as a server, system, or data file deployed next to the defending environment (Fortinet). These decoys are designed to be attractive targets for the Red Team that can allow the Blue Team to monitor security responses and potentially redirect the Red Team. The honey pot has a few potential locations, including in front of the firewall, directly behind the firewall, in the Linux environment, or in the Windows environment. Exact placement and configuration may vary depending on the environmental layout.

There are multiple methods to detect anomalous behavior to alert incident response (IR) or start the IR process. The Blue Team will attempt to establish a behavioral analysis methodology to identify the Red Team’s efforts to attempt to breach the Blue Team’s environment. Behavioral analysis is a program(s) that spot suspicious behavior through constant analysis of user and malicious actor behavior (Xcitium). The method analyzes network traffic, database, and user activities to establish a baseline and to send alerts if there are significant changes to the baseline (Stanham, 2023). There is a risk of false positives, which are alerts of potentially illegitimate activity that is legitimate since the Blue Team will be testing and working with malicious tools from the Blue Team’s offensive unit. Behavioral analysis can potentially be incorporated into a security information and event management (SIEM) tool.

SIEMs are a set of technologies that assist with threat detection and incident response (Gartner). A SIEM is a centralized utility that provides insights from multiple sources within an organization’s network infrastructure (Kidd). Sources can be servers, systems, devices, or applications that incorporate rule sets for continuous monitoring. An example of logging is a ‘failed login attempt’ where a potential user fails to log in to the appropriate account. This particular scenario may not be a reason to start the IR process. To eliminate this potential noise, the IR team member can create a rule set such as ‘after three failed attempts, lock the account.’ This rule will trigger an alert to send to the IR team leader to examine the log. This should assist with mitigating noise. The IR team will attempt to use Splunk, a system that can incorporate behavioral analysis along with incorporating the system administrator and firewall logs to assist with incident responders. Additionally, the IR team will work closely with the pentest team to identify new potential threats and try to incorporate insights into the Splunk ruleset.

As with all the other phases, it is critical that notes of what is being detected, changes, rulesets, and processes are in place in case of an event. This will also assist with evaluations for improving the defensive strategy and IR process.

**Step 4 - Reconnaissance, initial access, persistence, evasion, data exfiltration**

In conjunction with Step 1 (System Admin), an offensive actor for Blue Team will attempt to access the Red Teams platform. Since the platforms are identical at the start of the War Games, Blue Team will attempt to gain their foothold prior to Red Team making modifications to their platform. Blue Team will take advantage of the default passwords being the same across the platforms. Additionally, the Blue Team will manipulate the identified vulnerabilities identified during their assessment to attack the Red Team’s platform.

Blue Team will also attempt to gain either an unwitting or a witting insider from the Red Team. An email will be drafted for social engineering on the Red Team. The email will contain the language of a Blue Team member being reassigned to the Red Team, and with the re-assignment, the new team member needs access to the Red Team’s environment. If that is not successful, another email will be sent from a different Blue Team member containing a malicious link or file, stating it is important information regarding either the PfSense Firewall or the Kali Linux Virtual Machine. If either one of these spearphishing attempts is successful, the Blue Team could gain unvetted access to the Red Team’s environment. There is also the possibility of recruiting a witting insider from the Red Team to provide passwords or to purposefully leave an access point open for the Blue Team.

In preparation for the upcoming offensive operations, Blue Team will implement a targeted exploitation strategy to gain and maintain access to critical systems within the network while avoiding detection. This approach will be executed in conjunction with Step 1 (System Admin) and incorporate both technical and social engineering elements aimed at undermining the Red Team’s defenses before they make significant modifications to their platform.

The first phase will involve initial reconnaissance and discovery, using tools like Nmap and Shodan to identify open services and potential vulnerabilities and gather information about the target network’s infrastructure. Given that the platforms for both teams are identical at the start of the War Games, the Blue Team will capitalize on any default configurations and shared passwords that the Red Team may not yet change. This early-stage effort will focus on identifying misconfigured ports, outdated services, or unpatched software that could be exploited for initial access.

Once the network has been mapped, Blue Team will focus on exploiting web application vulnerabilities, including identifying weaknesses like SQL Injection (SQLi), Cross-Site Scripting (XSS), and Remote File Inclusion (RFI). Tools like Burp Suite and OWASP ZAP will be used to scan critical web services such as login forms, which often serve as entry points for an attacker. This process will allow Blue Team to manipulate identified vulnerabilities from their assessment to gain a foothold within Red Team's platform.

Additionally, the team will initiate credential harvesting and brute force attacks against weak authentication mechanisms using tools like Hydra and Medusa. This phase will focus on common services such as SSH and FTP, taking advantage of any unchanged default credentials to compromise user accounts, escalate privileges, and pivot deeper into the network.

Following initial access, the team will implement privilege escalation and lateral movement techniques. Using tools like Metasploit, LinEnum, and PowerShell Empire, Blue Team will exploit weak file permissions, kernel vulnerabilities, or misconfigurations to elevate privileges to root or administrator levels. Once administrative access is secured, Blue Team will move laterally across the network, compromising additional systems and critical services.

A key part of the offensive strategy will also involve targeting unpatched vulnerabilities (CVE exploits) in the network. Leveraging well-known CVEs through Metasploit or custom scripts, the team will aim to compromise any outdated systems or applications within Red Team's environment, particularly those vulnerable to high-severity attacks. The primary focus will be on older systems that may not have been updated or patched by the Red Team, maximizing the chances of successful exploitation.

Simultaneously, Blue Team will employ social engineering tactics in an attempt to gain unwitting or witting insider access to Red Team’s environment. An email will be drafted to impersonate a team member re-assigned to the Red Team, requesting access to their environment under the pretext of needing operational information. If unsuccessful, another spear phishing email will be sent from a different Blue Team member containing a malicious link or file, purporting to be urgent information regarding the PfSense Firewall or Kali Linux Virtual Machine. The goal is to trick a Red Team member into granting access or executing the payload, which would provide Blue Team with unvetted access to the target environment.

As a contingency, the Blue Team will also explore the possibility of recruiting an insider threat from the Red Team. This strategy could involve bribing or coercing a Red Team member to intentionally leave an access point open or provide critical information such as passwords. If successful, this would allow Blue Team to bypass standard defenses entirely.

In the post-exploitation phase, the focus will be on maintaining persistence and conducting data exfiltration. After gaining access, the team will establish backdoors using tools like Netcat or encrypted SSH tunnels, ensuring continued access to compromised systems. The primary goal here will be to exfiltrate valuable data, such as credentials or sensitive files, without alerting defenders.

This multifaceted offensive strategy, blending technical exploitation with social engineering, ensures that the Blue Team will be able to penetrate the Red Team’s defenses and maintain operational control throughout the exercise. By targeting both infrastructure and personnel vulnerabilities, the Blue Team will increase the likelihood of success in disrupting the Red Team’s operations while maintaining a stealthy and strategic approach.

**Step 5 - Incident Response**

The Blue Team plans to take the following steps if an incident occurs. The phases highlight best practices and may not incorporate all necessary actions. Note that these phases may run concurrently and are a general guideline.

1. *Identification*

As mentioned in Step Three, the first step is to identify that an incident is occurring. There is constant monitoring of the established tools and analyzing suspected anomalies (Exabeam). An important skill is analytical cybersecurity skills that enable The Blue Team to differentiate a false positive from an ongoing/real event. The first responsibility is to pinpoint the signs of an incident, which can be indicators of compromise (IoC) or indicators of attack (IoA) that something is occurring (Cranford, 2023). If the Blue Team discovers multiple incidents, it must prioritize which must be completed first. The Blue Teams IR lead notifies the rest of the team that something is going on and that all team members may need to respond. As mentioned previously, documenting is essential throughout the simulation. Documentation is one of the most critical components throughout IR so that the team understands when, where, and how the event occurred and to improve in follow-ups.

1. *Containment*

Once the Blue Team identifies that an event or breach has occurred, it is important to contain the incident. If an attack is not contained, then the incident can become worse and crash the network infrastructure. Steps to include in containment may include blocking traffic (i.e., working with firewall team leads), deactivating compromised accounts, and other actions to save resources and keep other network infrastructure up and running (Exabeam). It is crucial to maintain a balance between practical IT security efforts and regular organizational needs. Note that containment efforts will change depending on the type of attack. For example, a ransomware attack will require a different response than an unauthorized login.

1. *Eradication*

When the IR team has contained the incident, they will take measures to remove whatever malicious items may be in the environment. The IR team, firewall, and system admins will take necessary actions, including but not limited to uninstalling malicious software, deleting malicious files, deleting unauthorized accounts, implementing required patching, and other essential actions (Exabeam). Similar to containment, different eradication actions may need to be taken for various incidents.

1. *Recovery*

Recovery is where the environment is running as designed without signs of infection or an ongoing cyber incident. Actions may include working with the pentest team to ensure that the initially discovered loopholes are closed and tested. This ensures that there is a stable environment. System Admin takes a snapshot of the current stable environment to use as a fallback in the event we need to restore our systems. IR team will support other efforts as needed.

**Step 6 - After action, Lessons learned, Weekly summary.**

After an incident response, several crucial steps follow to ensure that the team learns from the event and strengthens our security posture. Here’s a general outline:

*After-Action Review (AAR):*

Conduct a review to analyze what happened, what was done well, and what could be improved.

*Lessons Learned Meeting:*

Host a session where the team discusses what they learned from the incident. This could involve feedback on detection, containment, eradication, and recovery efforts. Each team member provides insights to ensure a well-rounded view of the incident.

*Documentation and Incident Summary Report:*

A report can be established for a tangible set of evidence that includes the timeline, causes, affected systems, detection and response measures, and the impact of the incident. The report should clearly document findings, corrective actions, and any areas needing improvement.

*Root Cause Analysis (RCA):*

Identifying the root cause of the incident to prevent recurrence involves analyzing logs, reviewing configurations, and examining attack vectors to understand how the threat actor infiltrated the system.

*Weekly Summary:*

Summarize incident findings and actions. This is especially useful with continuous monitoring, where multiple incidents or security events may occur weekly.

*Reflection:*

Evaluate whether existing tools, alerts, and processes were effective in detecting and containing the incident. This may reveal gaps in monitoring, alerting thresholds, or response workflows.

*Security Posture Improvements:*

Implement corrective actions. This could include a new plan of action, additional focused training for the team, or introducing new detection mechanisms/tools needed to mitigate similar incidents in the future.

*Procedure Updates:*

Update incident response plans to reflect the insights gained from the incident. If new threats are identified, ensure that response procedures include steps to address them.

**Summary**

The details above are a preliminary version of the Blue Team’s initial cyber warfare simulation. To reiterate, the Blue Team has no knowledge of the environment or how it works. This plan was derived from brainstorming and research of potentialities. It should be regarded as a baseline of what we would like to do through practical or academic experience. The Blue Team understands that once the wargame commences, this plan may be thrown out the window, and it reserves the right to do so.

**References**

Abu-Dabaseh, F., & Alshammari, E. (2018). Automated Penetration Testing: An Overview. Computer Science & Information Technology. Retrieved from https://doi.org/10.5121/csit.2018.80610

Atumu, M. (2024). Tactical server hardening checklist for Windows and Linux security. Retrieved from https://www.liquidweb.com/blog/server-hardening-checklist/#:~:text=Operating%20System%20(OS)%20hardening%20is,Additional%20important%20steps%20include:

Canada Centre for Cyber Security. (2021). Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089). Retrieved from https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10089

Crandford, J.J. (2023). Incident Response Plan: Frameworks and Steps. Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/incident-response/incident-response-steps/

Exabeam. (n.d.). SANS Incident Response: 6-Step Process & Critical Best Practices. retrieved from https://www.exabeam.com/explainers/incident-response/sans-incident-response-6-step-process-critical-best-practices/

Fortinet. (n.d.). What Are Honeypots (Computing)? retrieved from https://www.fortinet.com/resources/cyberglossary/what-is-honeypot

Gartner. (n.d.). Security Information And Event Management (SIEM). retrieved from https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

Holik, F., Horalek, J., Marik, O., Neradova, S., & Zitta, S. (2014). Effective penetration testing with Metasploit framework and methodologies. 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics(CINTI). Retrieved from https://doi.org/10.1109/cinti.2014.7028682

Kidd, C. (n.d.). SIEM: Security Information & Event Management Explained. retrieved from https://www.splunk.com/en\_us/blog/learn/siem-security-information-event-management.html

LaBarge, R. (2012). Cloud Penetration Testing. International Journal on Cloud Computing: Services and Architecture. Retrieved from https://doi.org/10.5121/ijccsa.2012.2604

Netwrix. (n.d.). Linux Server Hardening and Security Best Practices. Retrieved from https://www.netwrix.com/linux\_hardening\_security\_best\_practices.html

Russinovich, M. & Garnier, T. (2024). Sysmon v.15.15.Retrieved from https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

SolarWinds. (2024). What is Packet Capture (PCAP)? Retrieved from https://www.solarwinds.com/resources/it-glossary/pcap

Stanham, L. (2023). Behavioral Analytics. retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/behavioral-analytics/?srsltid=AfmBOoqYJ6aDcgvQqmej4xTI-VljPEr3yr7DqCOfpw9WZYmW-2N9HPpU

Tatam, R. (2023). Automatic system hardening: Checklist + examples to ensure system security. Retrieved from https://www.puppet.com/blog/system-hardening

Udochukwu ThankGod Ikechukwu Igwenagu, Abidemi Ayodotun Salami, Abayomi Shamsudeen Arigbabu, Cassandra Esambe Mesode, Tunbosun Oyewale Oladoyinbo, & Oluwaseun Oladeji Olaniyi. (2024). Securing the Digital Frontier: Strategies for Cloud Computing Security, Database Protection, and Comprehensive Penetration Testing. Journal of Engineering Research and Reports, 26(6), 60–75. https://doi.org/10.9734/jerr/2024/v26i61162

Xcitium. (n.d.). What are Types of Detection? retrieved from https://www.xcitium.com/what-are-types-of-detection/

**Appendix A –** Offensive Planned Procedure and Responses

1. **Reconnaissance:**
   1. *Objective:*Gather as much information as possible about the target network before launching any attacks.
   2. *Steps:* 
      1. Passive Reconnaissance:
         1. Use tools like **whois, nslookup,** and **theHarvester** to gather domain, DNS, and email information without alerting the defenders.
         2. Conduct OSINT (Open-Source Intelligence) by checking publicly available information related to the target organization.
      2. Active Reconnaissance:
         1. Use network scanners such as **NMap** to map the network and identify live hosts, open ports, and services running on each machine.
         2. Utilize tools like **Netcat** to manually test services for potential weaknesses.
      3. Planned Response*:*
         1. Gather this information and map out potential entry points.
         2. Identify possible social engineering or phishing entry points based on the information gathered.
2. **Scanning and Enumeration:**
   1. *Objective:*Identify specific vulnerabilities within the discovered services or systems that can be exploited.
   2. *Steps:*
      1. Port Scanning:Use Nmap’s service/version detection (nmap –sV) to gather detailed information on open ports and associated services.
      2. Vulnerability Scanning:Use tools like Nikto and OpenVAS to scan web applications and systems for known vulnerabilities.
      3. Enumeration*:*Tools like enum4linux for SMB enumeration or RPCClient to pull detailed information from target systems.
      4. Planned Response:
         1. If vulnerabilities are found (e.g., outdated services, weak configurations), document them and move to the exploitation phase.
         2. If none are found, escalate with more aggressive scanning techniques.
3. **Exploitation:**
   1. *Objective:*Exploit vulnerabilities to gain access or control over the target systems.
   2. *Steps:*
      1. Web Application Attacks:
         1. SQL Injection:Use SQLMap to identify and exploit SQL injection vulnerabilities in web applications.
         2. Cross-Site Scripting (XSS):Use Burp Suite to identify XSS and injection points that can be leveraged to execute malicious scripts.
      2. Buffer Overflow Attacks:
         1. For any services with outdated versions, attempt buffer overflow attacks using Metasploit’s modules (for example, exploit/windows/smb/ms08\_067\_netapi ).
      3. Password Cracking:
         1. Use Hydra for brute-forcing login pages (e.g., SSH, FTP, web forms)
         2. JohntheRipper or Hashcat to crack password hashes, if any, are captured through network sniffing or compromised credentials.
      4. Planned Response:
         1. If an exploit succeeds, escalate privileges using **Privilege Escalation Exploits** like Linux PrivChecker or Windows Privilege Escalation scripts (e.g., exploit/windows/local/ms16\_032\_secondary\_logon\_handle\_privsec ).
         2. If exploitation fails, pivot by trying lateral movement using credentials or accessing other systems in the network.
4. **Post-Exploitation:**
   1. *Objective:*Maintain access and move laterally through the network, gathering sensitive data and expanding control.
   2. *Steps:*
      1. Establish Persistence:
         1. Use backdoor techniques like creating scheduled tasks or cron jobs to maintain access to compromised systems.
         2. Tools like Netcat or Meterpreter can be used to create persistent shell access.
      2. Privilege Escalation:
         1. Escalate privileges from user to root/admin using known exploits (e.g., Sudo Exploits or Kernel Exploits).
      3. Data Extraction:
         1. Search for sensitive files containing credentials, such as configuration files, password lists, or database dumps.
         2. Use tools like Mimikatz (on Windows) to extract plaintext passwords from memory or LaZagne to extract passwords from browsers and other applications.
      4. Planned Response:
         1. Ensure that any critical data is exfiltrated securely (e.g., using FTP over encrypted channels or Netcat in reverse shell mode).
         2. Document all discovered credentials or sensitive data for further exploitation or post-engagement reporting.
5. **Lateral Movement:**
   1. *Objective:*Move through the network to gain access to additional systems or sensitive data.
   2. *Steps:*
      1. Credential Reuse:
         1. Utilized captured credentials (e.g., through phishing and password cracking) to access other machines on the network.
      2. Pass-the-Hash:
         1. If hashes were captured, use Pass-the-Hash techniques with Metasploit to move across machines in the Windows environment.
      3. SSH Pivoting:
         1. Use SSH tunnels to pivot into other networks or systems based on the compromised machine.
      4. Planned Response:
         1. Always ensure traffic remains encrypted while moving laterally.
         2. Document newly accessed systems and continue to scan for vulnerabilities within these machines.
6. **Cleanup and Reporting:**
   1. *Objective:*Cover tracks and prepare a detailed offensive report on the findings and exploited vulnerabilities.
   2. *Steps:*
      1. Log Clearing:
         1. Remove traces of activity from logs, especially on Linux systems (e.g., using logrotate or manually clearing bash history and logs)
      2. Exit Strategy:
         1. Remove backdoors, malware, or any tools left on the compromised systems before disengaging.
      3. Report:
         1. Document all vulnerabilities, successful exploitation techniques, data gathered, and the impact of these actions.
      4. Planned Response:
         1. The report should include actionable remediation steps for the Blue Team. Provide proof of concepts (PoCs) for each vulnerability exploited, along with detailed logs of the attacks conducted.
7. **Offensive Tools Used:**
   1. Nmap: For network discovery and active scanning.
   2. SQLMap: For automated SQL injection discovery and exploitation.
   3. Burp Suite: For web application testing and XSS/CSRF vulnerability identification.
   4. Hydra: For password brute-force attacks.
   5. Metasploit Framework: For exploiting known vulnerabilities and privilege escalation.
   6. Netcat: For establishing reverse shells and persistence.
   7. Mimikatz/LaZagne: For extracting credentials post-exploitation.
   8. Pass-the-Hash techniques: For lateral movement across Windows machines