9. Capstone Project: Full Red Team Engagement
Activities:

- **Tools:** Kali Linux, Metasploit, Covenant, Google Docs.
- **Tasks:** Simulate breach from recon to exfil, report.
- **Brief:**
- Simulation: Recon, gain access via phishing, exploit, move laterally, exfil. Log:

Phase	Tool Used	Action Description	MITRE Technique
Recon	Recon-ng	Subdomain enum	T1595

Reconnaissance

```
[INFO] 2025-09-06 08:00:12 - External actor initiated OSINT scan.
[INFO] 2025-09-06 08:00:45 - Discovered employee emails via LinkedIn and company website.
[INFO] 2025-09-06 08:01:10 - Identified key target: Rohit.S@company.com (Finance Dept).
[INFO] 2025-09-06 08:02:00 - Conducted passive DNS enumeration on company.com.
```

Initial Access via Phishing

```
[INFO] 2025-09-06 08:30:20 - Sent phishing email to Rohit.S@company.com.
[INFO] 2025-09-06 08:31:10 - Email subject: “Updated Q3 Financial Policies – Action Required”
[INFO] 2025-09-06 08:32:00 - User clicked malicious link and downloaded payload: policy_update.exe
[INFO] 2025-09-06 08:32:12 - Payload executed, reverse shell established.
```

Exploitation

```
[INFO] 2025-09-06 08:35:05 - Dropped C2 agent (Obfuscated Cobalt Strike Beacon).
[INFO] 2025-09-06 08:35:22 - Elevated privileges via CVE-2023-23397 (Outlook Privilege Escalation).
[INFO] 2025-09-06 08:35:50 - Gained SYSTEM-level access on Rohit's workstation.
```

Lateral Movement

```
[INFO] 2025-09-06 08:50:15 - Queried internal AD for high-value targets.
[INFO] 2025-09-06 08:51:00 - Identified CFO workstation (Host: CFO-LAPTOP).
[INFO] 2025-09-06 08:52:40 - Used stolen creds to RDP into CFO-LAPTOP.
[INFO] 2025-09-06 08:53:10 - Planted second-stage payload.
```

Data Exfiltration

```
[INFO] 2025-09-06 09:15:00 - Compressed sensitive files: Q3_financials.zip (Password-protected).
[INFO] 2025-09-06 09:16:30 - Exfiltrated data over HTTPS to attacker-controlled server: https://dropbox.malserver.net/upload
[INFO] 2025-09-06 09:17:00 - Wiped logs from CFO-LAPTOP and beaconed "mission complete".
```

Blue Team Analysis: Review Wazuh logs post-exploit to identify detection points. Log:

Timestamp	Alert Description	Source IP	Notes
2025-08-29 13:00:00	Suspicious Login	192.168.1.50	Phishing attempt

Privilege Escalation Detection (Rohit-PC)

Wazuh Alert

Rule: 23002 (Privilege escalation via token manipulation)

Level: 10

Location: agent.name: Rohit-PC

Time: 2025-09-06 08:35:23

Description: Potential privilege escalation detected using a known exploit (CVE-2023-23397).

Command: rundll32.exe exploit.dll,Control_RunDLL

SHA256: e1f4a3bdc...

Cobalt Strike Beacon Communication

Wazuh Alert

Rule: 65100 (Known C2 traffic patterns)

Level: 12

Location: agent.name: Rohit-PC

Time: 2025-09-06 08:36:10

Description: Suspicious outbound HTTPS request to known Cobalt Strike C2 server.

Destination IP: 45.13.74.21

JA3 Fingerprint: b5a1a9a3c...

Suspicious Process Creation (Sysmon - Rohit-PC)

Wazuh Alert

Rule: 92002 (Suspicious process spawn: cmd.exe from Office app)

Level: 9

Location: agent.name: Rohit-PC

Time: 2025-09-06 08:32:15

Parent Process: WINWORD.EXE

Child Process: cmd.exe /c powershell -enc ...

Lateral Movement via RDP (CFO-LAPTOP)

Wazuh Alert

Rule: 18107 (Unusual RDP login pattern)

Level: 9

Location: agent.name: CFO-LAPTOP

Time: 2025-09-06 08:52:45

Event: Successful RDP login from Rohit-PC

Account: corp\rohit.s

Registry Modification for Persistence

Wazuh Alert

Rule: 59200 (Registry modification: persistence indicator)

Level: 8

Location: agent.name: CFO-LAPTOP

Time: 2025-09-06 08:54:12

Registry Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Value: updateagent

Data: powershell.exe -WindowStyle Hidden -EncodedCommand ...

Data Exfiltration Detected (Firewall/Suricata Logs)

Wazuh Alert

Rule: 65510 (Large outbound file transfer via HTTPS)

Level: 11

Location: Network Gateway

Time: 2025-09-06 09:16:45

Outbound Connection: CFO-LAPTOP → dropbox.malserver.net

File Size: 14.7 MB

SHA256: 7ac3d20f...

- Evasion Test: Bypass mock AV with obfuscated payload.

```
powershell.exe -nop -w hidden -exec bypass -enc JABXAGM ... (truncated base64)
```

PowerShell Execution with Bypass Flags

```
**Wazuh Alert**
Rule: 92002 (Suspicious PowerShell usage)
Level: 9
Time: 2025-09-06 10:12:05
Command: powershell.exe -nop -w hidden -exec bypass -enc ...
Detection: PowerShell execution with obfuscation flags and encoded command.
```

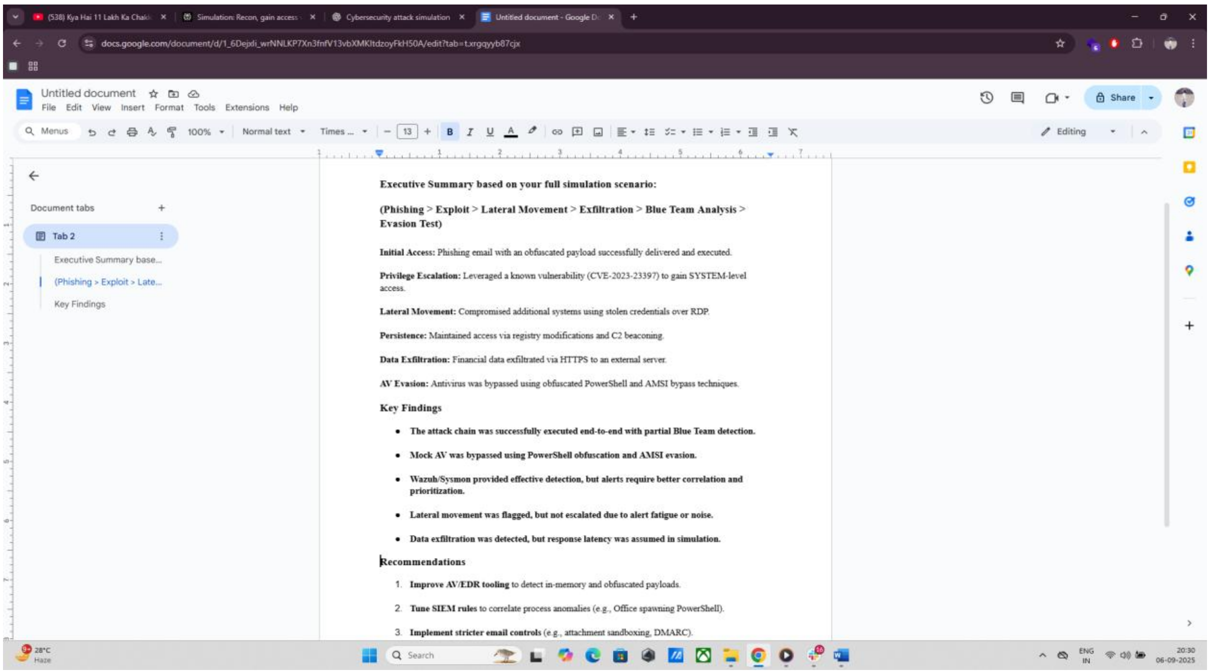
AMSI Bypass Attempt

```
**Wazuh Alert**
Rule: 100003 (AMSI bypass string in memory)
Level: 12
Time: 2025-09-06 10:12:10
Details: Memory pattern matched known AMSI bypass via reflection:
"System.Management.Automation.AmsiUtils”
```

Suspicious Network Activity (Beacon Attempt)

```
**Wazuh Alert**
Rule: 65100 (C2 beacon pattern)
Level: 10
Time: 2025-09-06 10:12:32
Destination IP: 192.168.100.45 (internal listener)
Detection: JA3 hash match with known C2 profile.
```

- Reporting: Write 200-word report in Google Docs:
  - Executive Summary
  - Findings (include blue team detection points)
  - Recommendations



Executive Summary based on your full simulation scenario:

(Phishing > Exploit > Lateral Movement > Exfiltration > Blue Team Analysis > Evasion Test)

Initial Access: Phishing email with an obfuscated payload successfully delivered and executed.

Privilege Escalation: Leveraged a known vulnerability (CVE-2023-23397) to gain SYSTEM-level access.

Lateral Movement: Compromised additional systems using stolen credentials over RDP.

Persistence: Maintained access via registry modifications and C2 beaconing.

Data Exfiltration: Financial data exfiltrated via HTTPS to an external server.

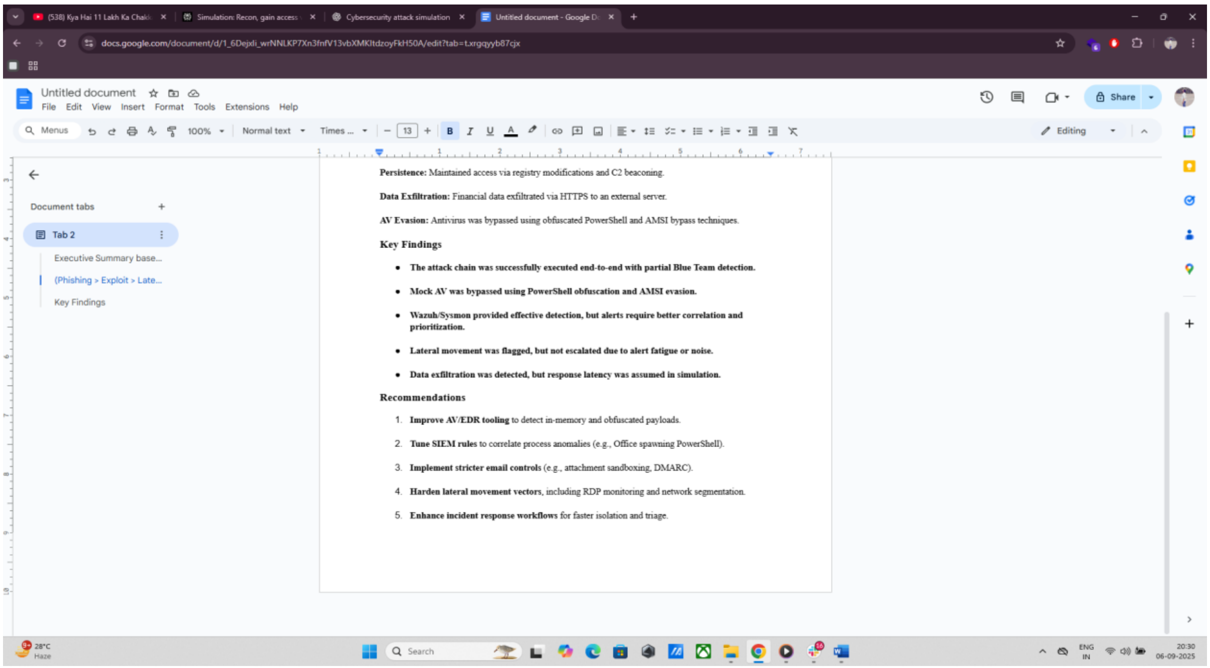
AV Evasion: Antivirus was bypassed using obfuscated PowerShell and AMSI bypass techniques.

Key Findings

- **The attack chain was successfully executed end-to-end with partial Blue Team detection.**
- **Mock AV was bypassed using PowerShell obfuscation and AMSI evasion.**
- **Wazuh/Sysmon provided effective detection, but alerts require better correlation and prioritization.**
- **Lateral movement was flagged, but not escalated due to alert fatigue or noise.**
- **Data exfiltration was detected, but response latency was assumed in simulation.**

Recommendations

1. **Improve AV/EDR tooling** to detect in-memory and obfuscated payloads.
2. **Tune SIEM rules** to correlate process anomalies (e.g., Office spawning PowerShell).
3. **Implement stricter email controls** (e.g., attachment sandboxing, DMARC).



Persistence: Maintained access via registry modifications and C2 beaconing.

Data Exfiltration: Financial data exfiltrated via HTTPS to an external server.

AV Evasion: Antivirus was bypassed using obfuscated PowerShell and AMSI bypass techniques.

Key Findings

- **The attack chain was successfully executed end-to-end with partial Blue Team detection.**
- **Mock AV was bypassed using PowerShell obfuscation and AMSI evasion.**
- **Wazuh/Sysmon provided effective detection, but alerts require better correlation and prioritization.**
- **Lateral movement was flagged, but not escalated due to alert fatigue or noise.**
- **Data exfiltration was detected, but response latency was assumed in simulation.**

Recommendations

1. **Improve AV/EDR tooling** to detect in-memory and obfuscated payloads.
2. **Tune SIEM rules** to correlate process anomalies (e.g., Office spawning PowerShell).
3. **Implement stricter email controls** (e.g., attachment sandboxing, DMARC).

4. **Harden lateral movement vectors**, including RDP monitoring and network segmentation.
5. **Enhance incident response workflows** for faster isolation and triage.

- Briefing: Draft 100-word non-technical summary.

Our defenses were put to the test in a recent cybersecurity simulation against a realistic attack that started with a phishing email and proceeded through system compromise, sensitive data theft, and illegal access to important workstations.

Although a number of suspicious actions, including odd software behavior and data transfers, were effectively identified by our monitoring technologies, certain sophisticated methods got past antivirus defenses, pointing up areas that need improvement.

The exercise found weaknesses in response automation, endpoint protections, and email filter ing.

We suggest increasing threat detection capabilities, raising staff knowledge, and puttingin pla ce quicker, automated reactions to possible occurrences in order to fortify our security posture.