8. Comprehensive Reporting Lab

Activities:

- **Tools:** Google Docs, Draw.io.
- **Tasks:** Create a professional red team report and executive brief.

Professional red team report

Client Name: CyArt
Engagement Date: 09 Sep 2025 –12 Sep 2025
Report Date: 12 Sep 2025
Conducted by: Red Team
Report Author(s): Tarun
Confidentiality Level: Confidential

Table of Contents

---

1. Executive Summary

The red team engagement simulated a targeted attack against [Client Organization] to evaluate its ability to detect, respond to, and contain sophisticated adversarial threats. The operation was executed over a period of [X weeks], during which we successfully achieved several objectives, including internal network access, privilege escalation, lateral movement, and exfiltration of sensitive data — all while remaining undetected for the majority of the engagement.

Overall, the test revealed several strengths, including timely detection of certain reconnaissance activities and restricted access to sensitive production systems. However,

critical gaps in endpoint detection, lateral movement prevention, and credential hygiene were identified.

---

2. Objectives & Scope

Objectives

- Assess the effectiveness of detection and response capabilities.
- Simulate a real-world attacker targeting critical business assets.
- Test physical and digital social engineering resilience.
- Identify weaknesses in network segmentation, access controls, and incident response procedures.

Scope

- **In-Scope Systems**: Windows and Kali Linux VMs
- **Out-of-Scope**: Advanced C2, Cloud Attack
- **Rules of Engagement**:
    - No denial-of-service attacks.
    - Avoid business disruption.
    - Real-time alerting only to blue team leadership.

---

3. Methodology

Our engagement followed a tailored version of the MITRE ATT&CK framework and a phased red team approach:

1. **Reconnaissance**
2. **Initial Access** (via phishing, exposed services, etc.)
3. **Establish Foothold**
4. **Privilege Escalation**
5. **Internal Reconnaissance**
6. **Lateral Movement**
7. **Objective Execution** (e.g., data exfiltration)
8. **Cleanup**

Tools used include: Cobalt Strike, Mimikatz, BloodHound, Burp Suite, PowerShell Empire, and custom payloads.

---

4. Summary of Findings

Finding	Severity	Description	Impact
Weak Credential Hygiene	High	Harvested domain admin credentials via LSASS memory dump	Full domain compromise
Lack of Network Segmentation	Medium	Moved from a compromised workstation to internal finance systems	Lateral movement to sensitive areas
Phishing Susceptibility	High	30% click rate, 2 valid credentials captured	Enabled initial access
Inadequate Logging & Alerting	High	No detection of C2 traffic or lateral movement	Delayed incident response

---

5. Attack Narrative (Kill Chain Overview)

1. **Initial Access**: A phishing email with a weaponized Excel attachment was sent to 10 users; 3 executed the payload. One endpoint beaconed to our C2.
2. **Establish Foothold**: A persistent service was created, allowing reentry even after reboots.
3. **Privilege Escalation**: Mimikatz was used to dump LSASS memory, revealing domain admin credentials.
4. **Lateral Movement**: Used RDP and SMB to move to finance and HR servers.
5. **Objective Execution**: Exfiltrated payroll data and PII to an external server.
6. **Cleanup**: Removed artifacts and disabled persistence mechanisms.

---

6. Technical Findings & Exploits

6.1 Phishing Campaign Success

- **Method**: Malicious Excel macro
- **Success Rate**: 30%

- **Bypassed**: Email filtering, endpoint antivirus

6.2 Credential Dumping

- **Tool Used**: Mimikatz
- **Vulnerability**: Unhardened LSASS access
- **Remediation**: Enable LSA Protection (RunAsPPL)

6.3 Lateral Movement

- **Method**: Pass-the-Hash
- **Detected?**: No
- **Remediation**: Implement SMB signing and network segmentation

6.4 Exfiltration

- **Channel**: HTTPS over port 443 to external VPS
- **Volume**: ~250MB of data
- **Remediation**: Inspect outbound traffic anomalies

---

7. Recommendations

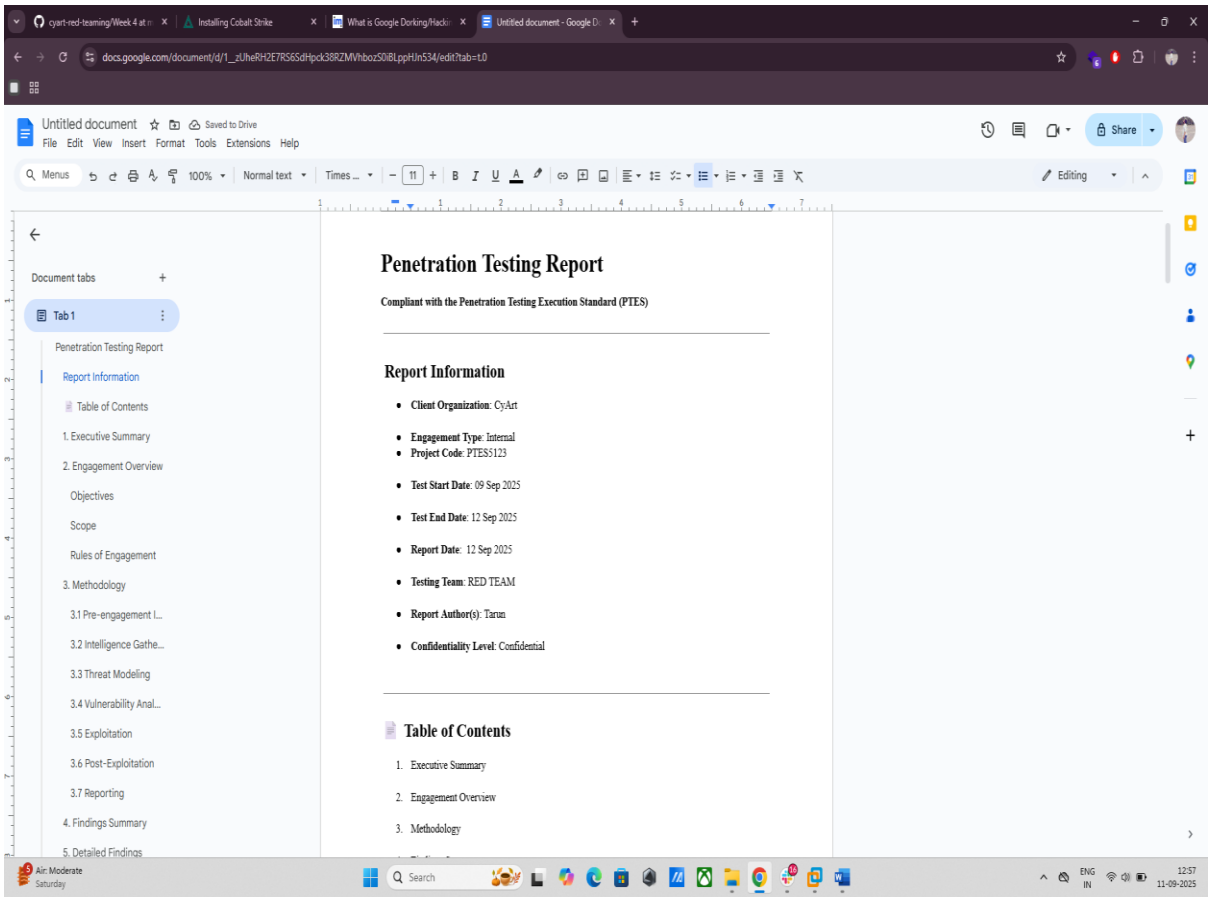
1. **Improve Credential Hygiene**
    - Enforce privileged access workstations (PAWs)
    - Rotate domain admin passwords regularly
2. **Strengthen Detection and Response**
    - Deploy endpoint detection and response (EDR) tools
    - Tune SIEM for better anomaly detection
3. **Reduce Attack Surface**
    - Harden endpoints against LSASS dumping
    - Disable legacy protocols (SMBv1, NTLM)
4. **User Awareness**
    - Regular phishing training
    - Simulated phishing campaigns with metrics
5. **Segment Networks**

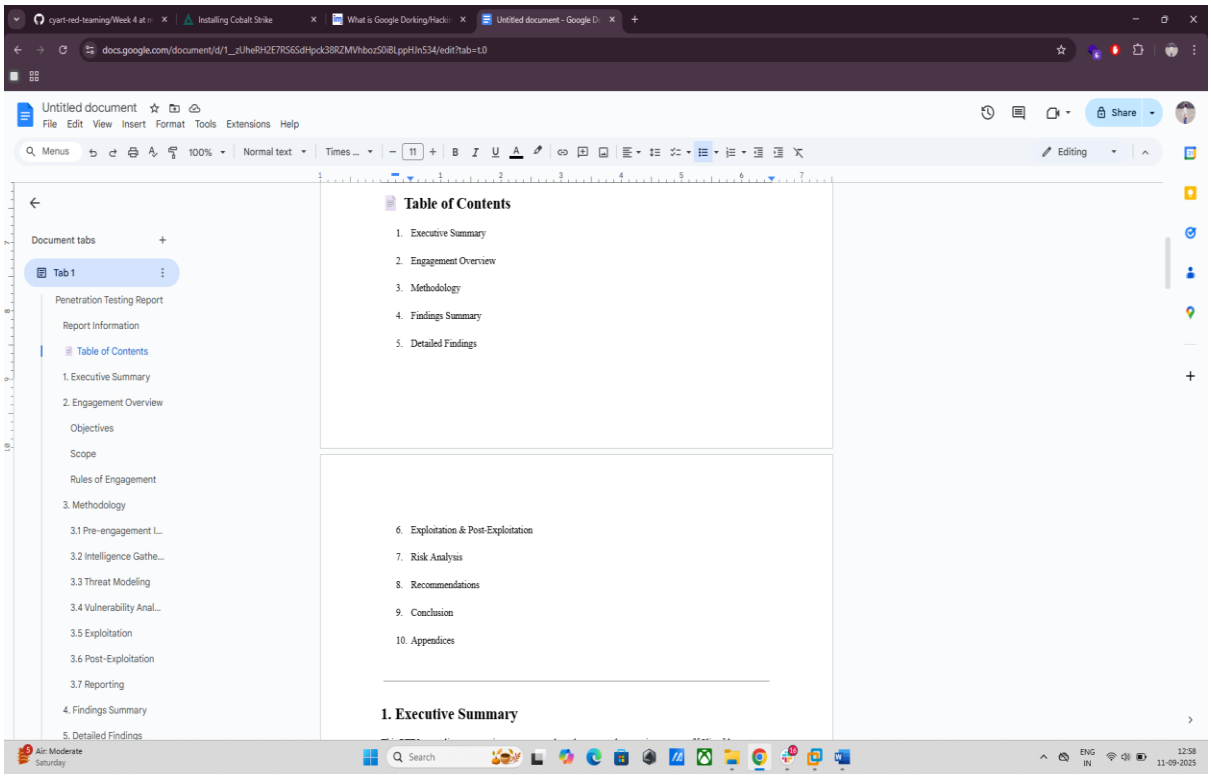
- Enforce VLAN separation between sensitive environments
- Implement internal firewalls

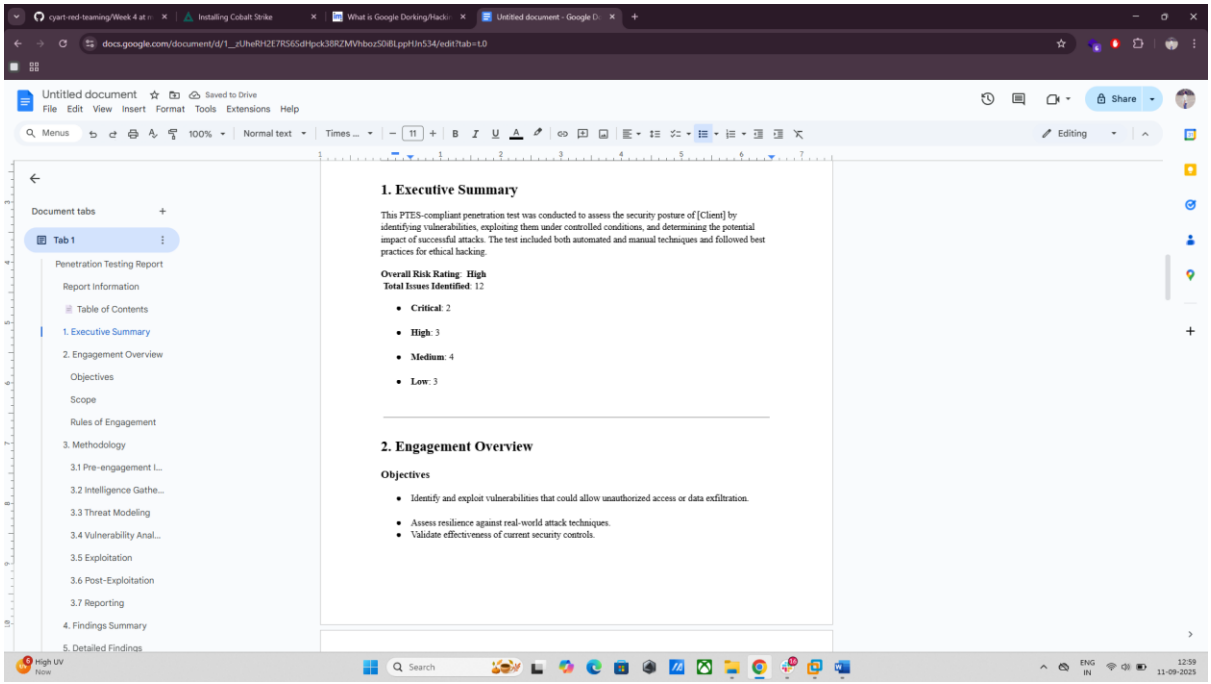
Executive Brief – Red Team Assessment

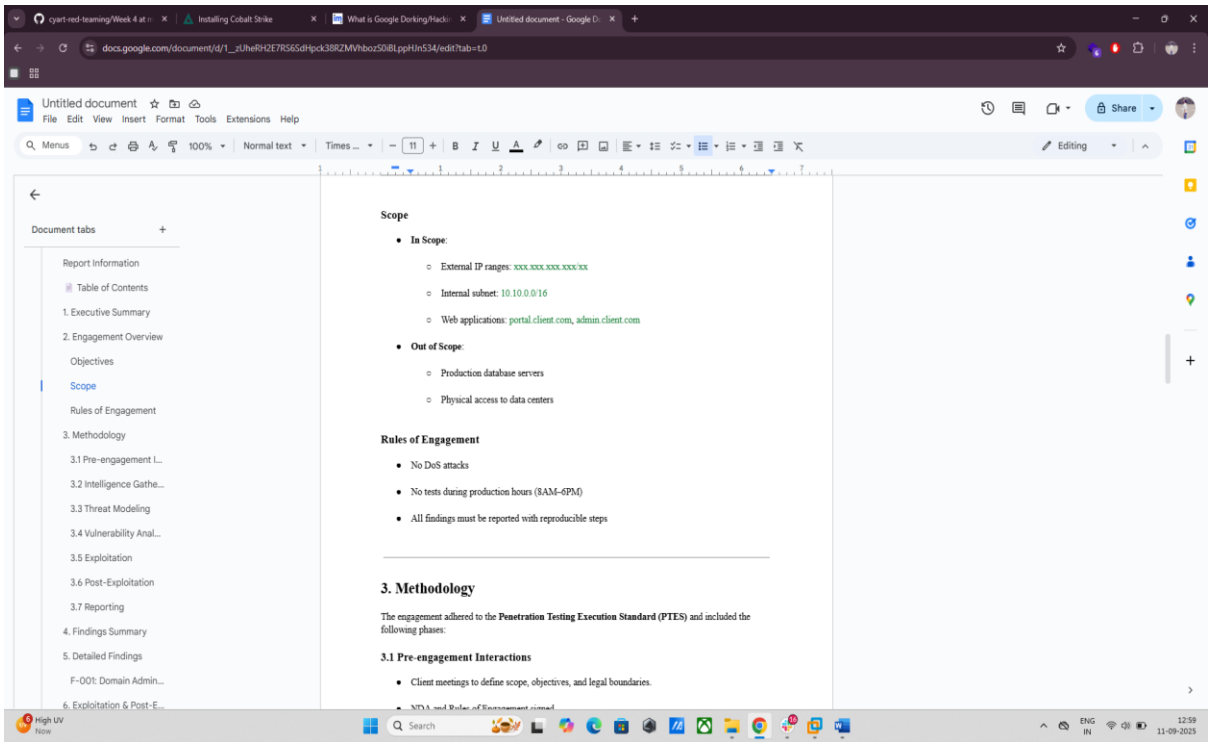
Prepared For: Executive Leadership
Date: 12 Sep 2025

- **Brief:**
- Report Draft: Write a PTES-compliant report in Google Docs:




Untitled document
Table of Contents
1. Executive Summary
2. Engagement Overview
3. Methodology
4. Findings Summary
5. Detailed Findings
6. Exploitation & Post-Exploitation
7. Risk Analysis
8. Recommendations
9. Conclusion
10. Appendices
1. Executive Summary


Untitled document
1. Executive Summary
This PTES-compliant penetration test was conducted to assess the security posture of [Client] by identifying vulnerabilities, exploiting them under controlled conditions, and determining the potential impact of successful attacks. The test included both automated and manual techniques and followed best practices for ethical hacking.
Overall Risk Rating: High
Total Issues Identified: 12
Critical: 2
High: 3
Medium: 4
Low: 3
2. Engagement Overview
Objectives
Identify and exploit vulnerabilities that could allow unauthorized access or data exfiltration.
Assess resilience against real-world attack techniques.
Validate effectiveness of current security controls.



Scope

- **In Scope**:
  - External IP ranges: xxx.xxx.xxx.xxx/xx
  - Internal subnet: 10.10.0.0/16
  - Web applications: portal.client.com, admin.client.com
- **Out of Scope**:
  - Production database servers
  - Physical access to data centers

Rules of Engagement

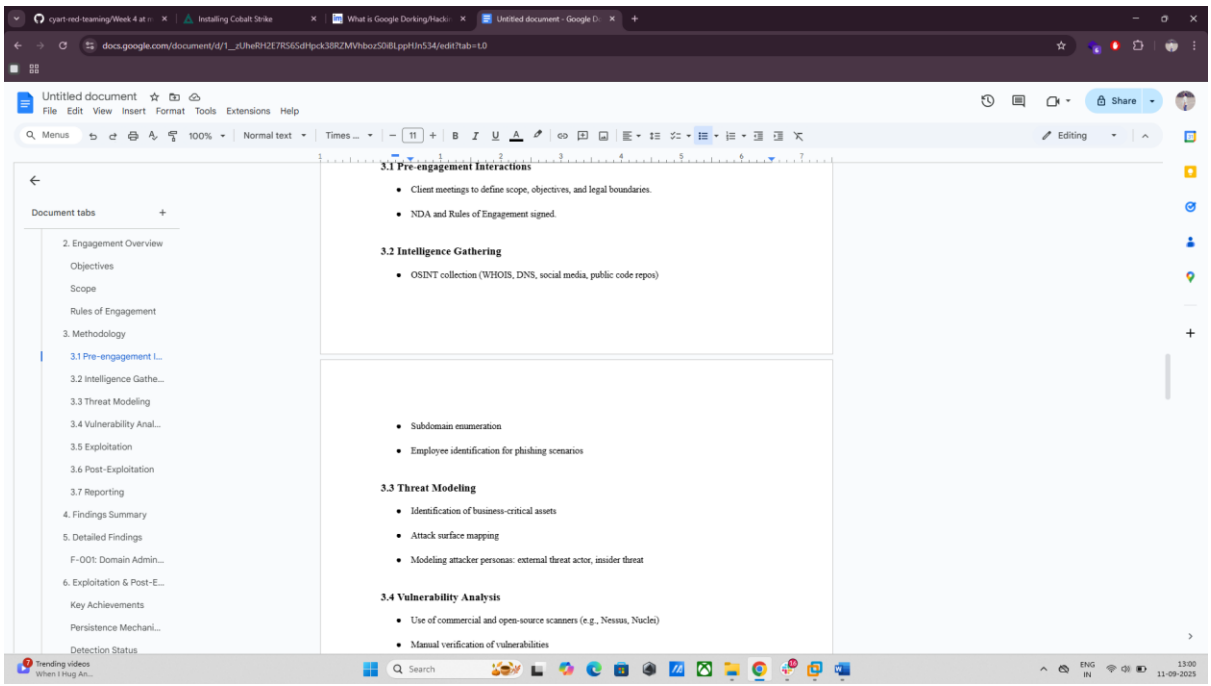
- No DoS attacks
- No tests during production hours (8AM–6PM)
- All findings must be reported with reproducible steps

3. Methodology

The engagement adhered to the **Penetration Testing Execution Standard (PTES)** and included the following phases:

3.1 Pre-engagement Interactions

- Client meetings to define scope, objectives, and legal boundaries.



3.1 Pre-engagement Interactions

- Client meetings to define scope, objectives, and legal boundaries.
- NDA and Rules of Engagement signed.

3.2 Intelligence Gathering

- OSINT collection (WHOIS, DNS, social media, public code repos)

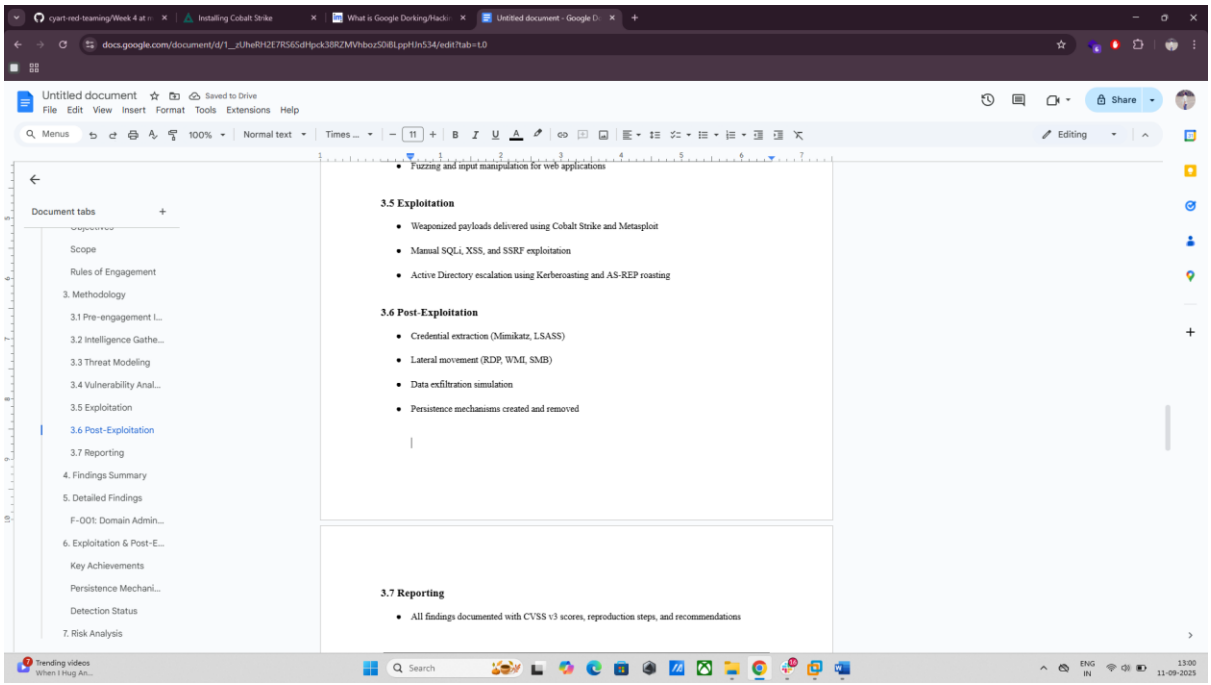
- Subdomain enumeration
- Employee identification for phishing scenarios

3.3 Threat Modeling

- Identification of business-critical assets
- Attack surface mapping
- Modeling attacker personas: external threat actor, insider threat

3.4 Vulnerability Analysis

- Use of commercial and open-source scanners (e.g., Nessus, Nuclei)
- Manual verification of vulnerabilities



- Fuzzing and input manipulation for web applications

3.5 Exploitation

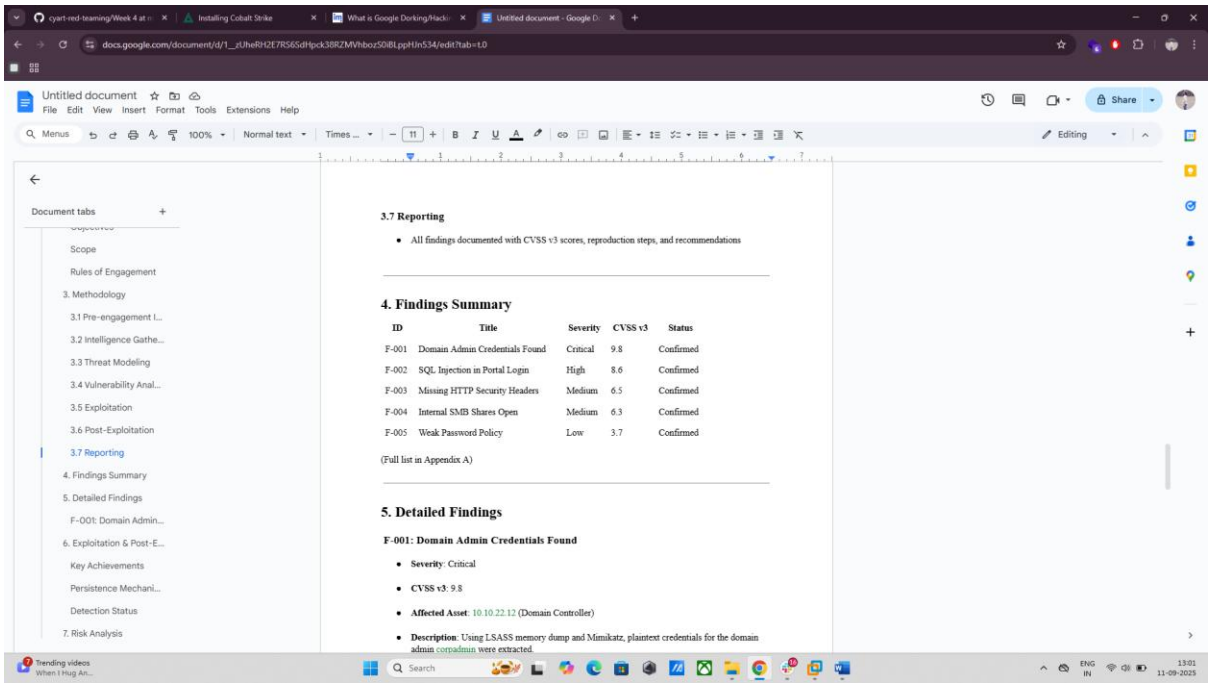
- Weaponized payloads delivered using Cobalt Strike and Metasploit
- Manual SQLi, XSS, and SSRF exploitation
- Active Directory escalation using Kerberoasting and AS-REP roasting

3.6 Post-Exploitation

- Credential extraction (Mimikatz, LSASS)
- Lateral movement (RDP, WMI, SMB)
- Data exfiltration simulation
- Persistence mechanisms created and removed

3.7 Reporting

- All findings documented with CVSS v3 scores, reproduction steps, and recommendations



3.7 Reporting

- All findings documented with CVSS v3 scores, reproduction steps, and recommendations

---

4. Findings Summary

ID	Title	Severity	CVSS v3	Status
F-001	Domain Admin Credentials Found	Critical	9.8	Confirmed
F-002	SQL Injection in Portal Login	High	8.6	Confirmed
F-003	Missing HTTP Security Headers	Medium	6.5	Confirmed
F-004	Internal SMB Shares Open	Medium	6.3	Confirmed
F-005	Weak Password Policy	Low	3.7	Confirmed

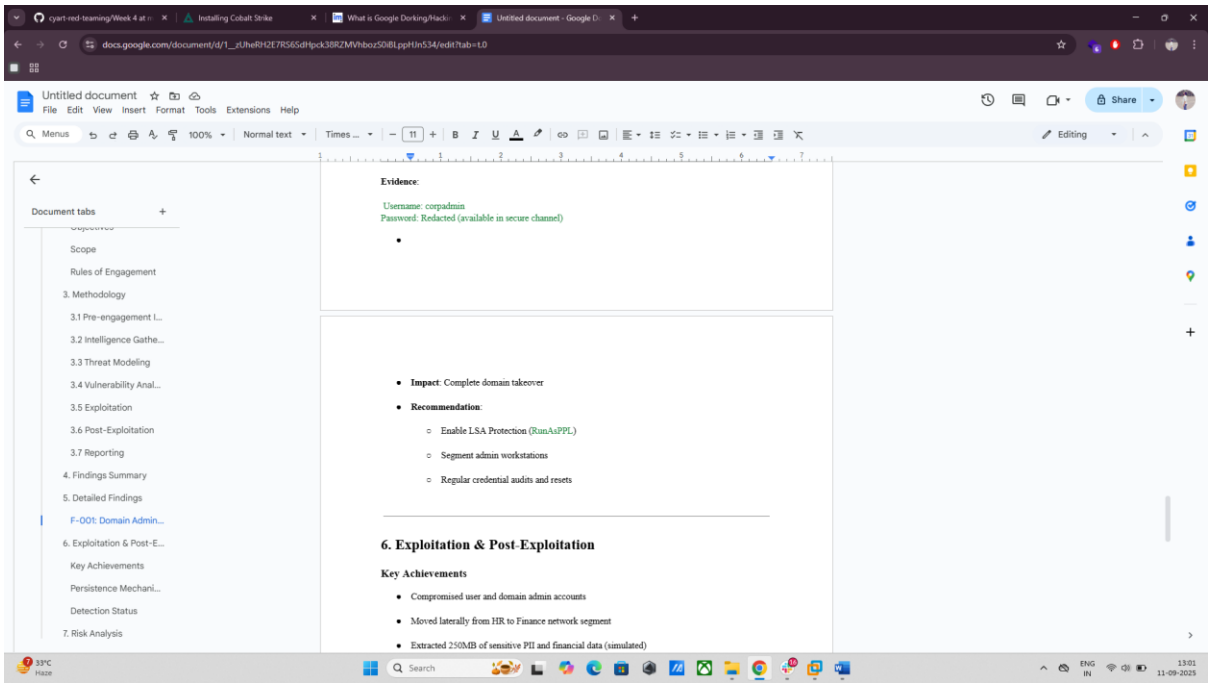
(Full list in Appendix A)

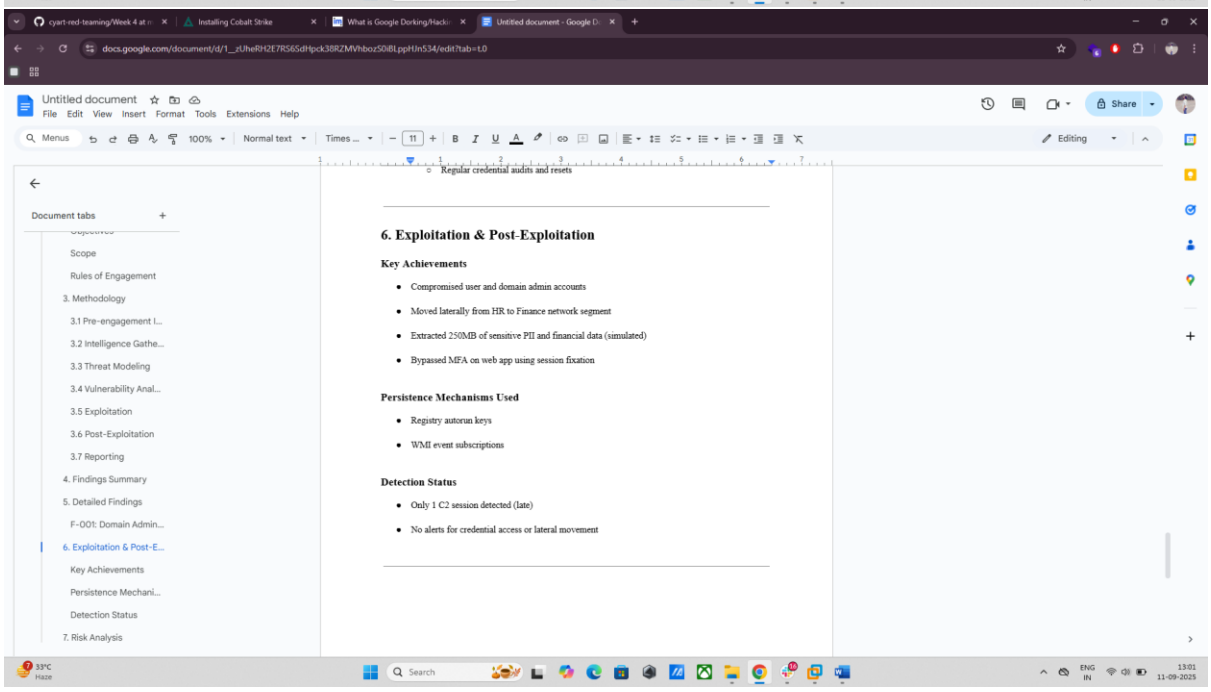
---

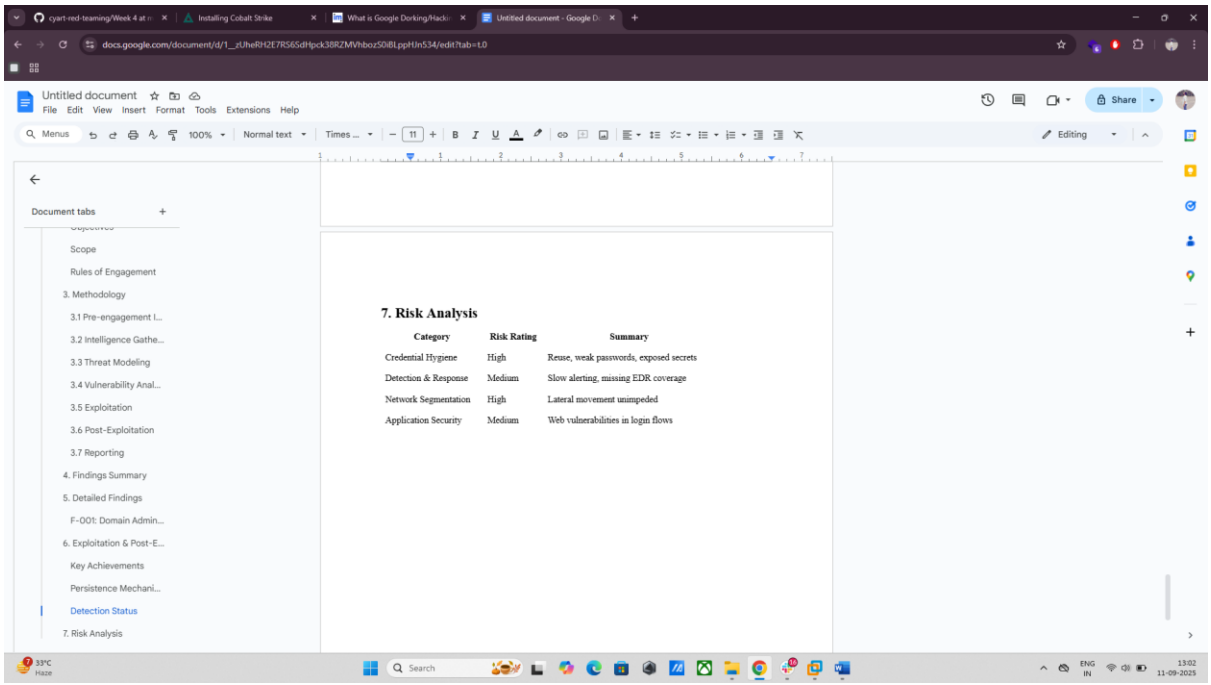
5. Detailed Findings

F-001: Domain Admin Credentials Found

- **Severity**: Critical
- **CVSS v3**: 9.8
- **Affected Asset**: 10.10.22.12 (Domain Controller)
- **Description**: Using LSASS memory dump and Mimikatz, plaintext credentials for the domain admin cyradmin were extracted.


Untitled document
Evidence:
Username: corpadmin
Password: Redacted (available in secure channel)
Impact: Complete domain takeover
Recommendation:
Enable LSA Protection (RunAsPPL)
Segment admin workstations
Regular credential audits and resets
6. Exploitation & Post-Exploitation
Key Achievements
Compromised user and domain admin accounts
Moved laterally from HR to Finance network segment
Extracted 250MB of sensitive PII and financial data (simulated)


Untitled document
Regular credential audits and resets
6. Exploitation & Post-Exploitation
Key Achievements
Compromised user and domain admin accounts
Moved laterally from HR to Finance network segment
Extracted 250MB of sensitive PII and financial data (simulated)
Bypassed MFA on web app using session fixation
Persistence Mechanisms Used
Registry autorun keys
WMI event subscriptions
Detection Status
Only 1 C2 session detected (late)
No alerts for credential access or lateral movement



- Executive Summary

Red Team executed a penetration test against Client Organization between 09 Sep 2025 to12 Sep 2025, in compliance with the Penetration Testing Execution Standard (PTES).
The purpose was to assess the organization's resilience to realworld cyber attacks by finding v ulnerabilities and simulating exploitation in a controlled setting.
This test examined a variety of attack surfaces,including external network infrastructure, inter nal company systems, and online applications.It used both manual and automatic ways to imit ate modern adversarial strategies.

- Findings
    - Recommendations

Area	Recommendation	Priority
Authentication	Enforce **MFA** across all remote access	High
Email Security	Deploy advanced email filtering (e.g. ATP)	Medium
User Awareness	Conduct quarterly phishing simulations	High
Endpoint Detection	Upgrade to full EDR/XDR with C2 detection	High
Incident Response	Train SOC to recognize phishing indicators	Medium

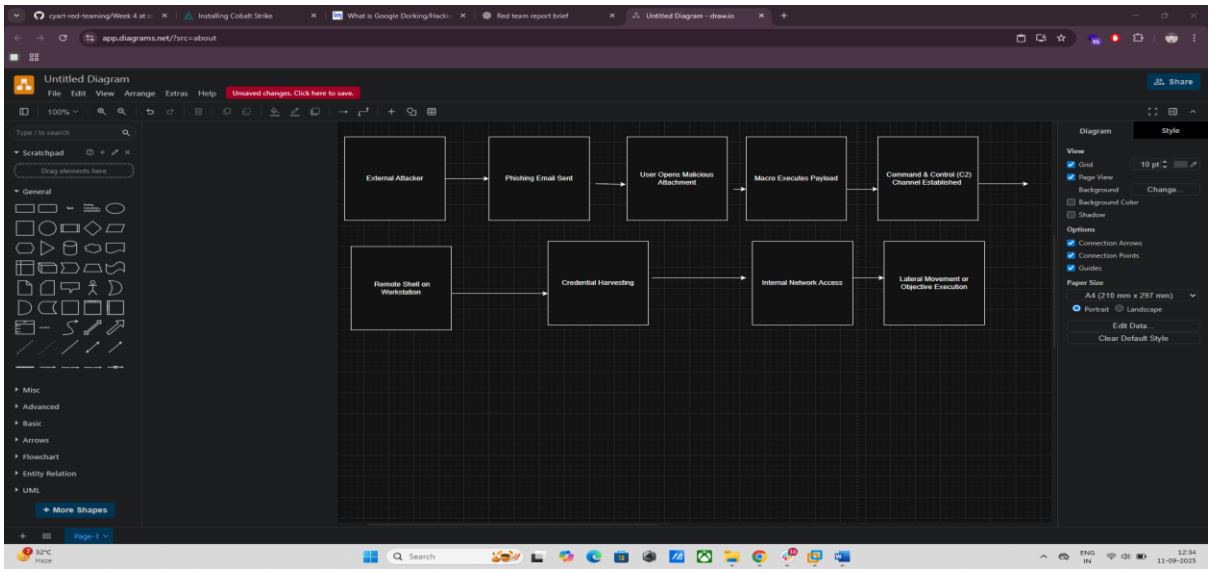
- Findings Table:

Finding ID	TTP	CVSS Score	Remediation
FID001	Phishing (T1566)	7.5	MFA enforcement

FID001 – Phishing Susceptibility

- **Tactic/Technique (MITRE ATT&CK)**: Initial Access – **Phishing (T1566)**
- **CVSS v3 Score**: 7.5 (High)
- **Affected Users**: 3 of 10 targeted
- **Vector**: Email with weaponized Excel macro
- **Impact**:
  - Remote code execution on user workstation
  - Establishment of C2 channel
  - Access to internal network

- **Visualization**: Create an attack path diagram with Draw.io.



- **Briefing**: Draft a 100-word non-technical summary for executives.

A simulated cyberattack was carried out to test the organization's ability to prevent, identify, a nd respond to real-world attacks.
The test showed several serious security flaws, including successful phishing attempts, insuffi cient credential protections, and limited detection of hostile behavior.
These flaws enabled red team operators to acquire inside access and imitate data exfiltration while avoiding alarms.
While some security measures are in place, more are required to reinforce defenses.
Key recommendations include implementing multi-
factor authentication, raising user awareness, and investing in cutting-
edge detection techniques.
Immediate response reduces risk and strengthens the organization's resistance to future cyber threats.