



8. Red Team Report Creation

Activities:

- **Tools:** Google Docs, Draw.io.
- **Tasks:** Document a simulated engagement.
- **Brief:**
- **Report Draft:** Write report (recon to exfil) in Google Docs:
 - Executive Summary
 - Findings
 - Recommendations
 - Attack Flowchart: Diagram with Draw.io (Recon → Initial Access → Exploitation → Lateral Movement).

The screenshot shows a Google Docs interface with a document titled "week3_task08". The document content is as follows:

Executive summary

From preliminary reconnaissance to data exfiltration, the lifespan of a recent cyber intrusion incident is described in this study. To breach the target organization's internal systems and steal confidential information, the threat actor used a mix of lateral movement, phishing, privilege escalation, and open-source intelligence (OSINT) tactics.

This report's goals are to give a thorough explanation of the attack procedures, point out important security flaws, and suggest corrective measures to stop future attacks of this kind.

Findings

1. Surveying

The attacker used OSINT tools (e.g., Shodan, LinkedIn) to perform passive reconnaissance. Email addresses and the organization's technology stack (outdated VPN service, Apache web servers) were found.

Using programs like Nmap, I discovered exposed services on ports 443 and 3389.

2. First Access

obtained entry by means of a fruitful phishing attempt aimed against mid-level staff members. A malicious attachment masquerading as a PDF of the company's HR policy was included in the email.

The embedded macro downloaded and ran a remote access trojan (RAT) when it was opened.

3. Abuse

A command-and-control (C2) channel was created by the RAT.

The attacker used a known vulnerability (CVE-2021-34527 - PrintNightmare) to escalate privileges.

SYSTEM-level access was obtained on several endpoints.

4. Lateral Motion

RDP and SMB were used to travel laterally using compromised admin credentials.



The screenshot shows a Google Docs interface with a document titled "week3_task08". The document content is as follows:

privileges.
SYSTEM-level access was obtained on several endpoints.

4. Lateral Motion

RDP and SMB were used to travel laterally using compromised admin credentials.
Mimikatz was used to dump the LSASS memory.
accessed databases and file servers.

5. Exfiltration of Data

Sensitive information (internal papers, customer PII) was compressed and encrypted.
used DNS tunneling to exfiltrate data in order to avoid discovery.
Unusual DNS traffic and outgoing connections to dubious IP addresses were examples of indicators of compromise (IoCs).

Recommendations

Quick Actions

Reset all company passwords and remove compromised credentials.

Attack Flowchart

You can create this diagram using [Draw.io (<https://app.diagrams.net>)]:

Flow Diagram

The bottom of the screenshot shows a Windows taskbar with the date "05-09-2025" and time "07:21".



The screenshot shows a Google Docs interface with a document titled "week3_task08". The document content includes the following text:

Attack Flowchart

You can create this diagram using [Draw.io (<https://app.diagrams.net/>)]:

Flow Diagram

Below the text is an embedded image of a flowchart diagram. The diagram is a horizontal sequence of five rectangular boxes connected by arrows, representing a process flow. The boxes are labeled: "Network", "Web", "Server", "Database", and "User". The flow starts from "Network" and proceeds through each box in sequence to "User". The diagram is displayed within a window that appears to be a screenshot of the Draw.io application interface.