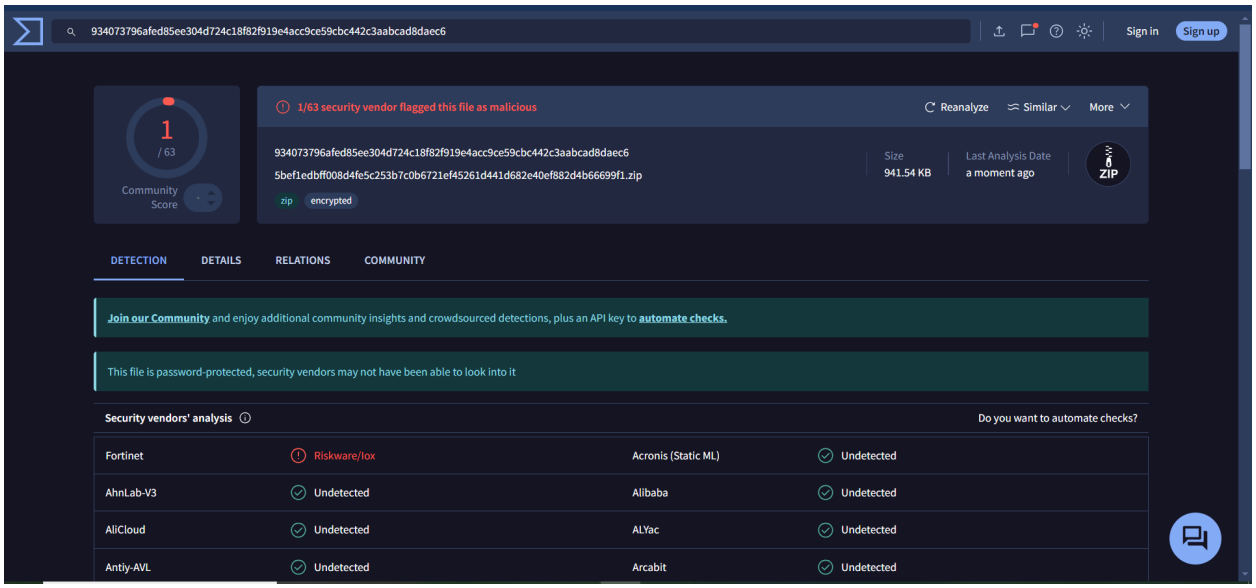
Cyber Threat Analysis Report



1. File Overview

- **File Hash:** `934073796afed85ee304d724c18f82f919e4acc9ce59cbc442c3aabcad8daec6`
- **File Type:** ZIP (Password-Protected)
- **File Size:** 941.54 KB
- **Encryption:** Yes (VirusTotal indicates that security vendors may not have been able to analyze contents)

2. Detection Results

- **1/63 Security Vendors Detected the File as Malicious**
- **Vendor:** Fortinet
- **Detection:** Riskware/lox
- **Other Vendors:** Marked as "Undetected"

3. Behavioral Indicators

- The file is password-protected, making it harder for automated scanners to inspect the contents.
- "Riskware/lox" by Fortinet suggests it could contain potentially unwanted programs (PUPs) or software that may have security concerns.
- Since only 1 out of 63 vendors flagged the file, this could be a false positive, but manual analysis is needed.

4. Potential Impact

- If the file contains malware, it could execute harmful actions such as:

    - **Data Theft:** If it includes spyware or keyloggers.
    - **System Compromise:** If it contains trojans or backdoors.
    - **Persistence Mechanisms:** If it modifies registry keys or system startup behavior.

5. Recommended Actions

- **Further Analysis:** Use a sandbox (e.g., Any.Run, Hybrid Analysis) to execute the file safely.
- **Manual Inspection:** Extract contents in a controlled environment.
- **Monitor Behavior:** Look for unusual system activity post-execution.
- **Check False Positives:** Since only one vendor flagged it, submit to Fortinet for further review.

APT29 - SolarWinds Attack

APT29 (also known as Cozy Bear) is linked to Russia's **SVR intelligence agency** and has conducted cyber espionage against government agencies, think tanks, and private companies. The **SolarWinds attack** was one of the most sophisticated cyber-espionage campaigns in history.

MITRE ATT&CK Mapping of the SolarWinds Attack:

Phase	Tactic (MITRE ATT&CK)	Technique Used
Initial Access	T1195.002 - Supply Chain Compromise	APT29 injected malicious code into **SolarWinds Orion** updates.
Execution	T1059 - Command and Scripting Interpreter	Used **PowerShell** scripts to execute payloads.
Persistence	T1546.008 - Registry Run Keys	Created persistence via registry modifications.
Privilege Escalation	T1078 - Valid Accounts	Stole legitimate credentials for privilege escalation.
Defense Evasion	T1027 - Obfuscated Files or Information	Used encoded PowerShell scripts to avoid detection.
	T1070.004 - File Deletion	Deleted logs and traces to cover tracks.
Credential Access	T1555 - Credentials from Password Stores	Harvested credentials from LSASS memory dumps.
Discovery	T1018 - Remote System Discovery	Identified additional networked systems to laterally move.

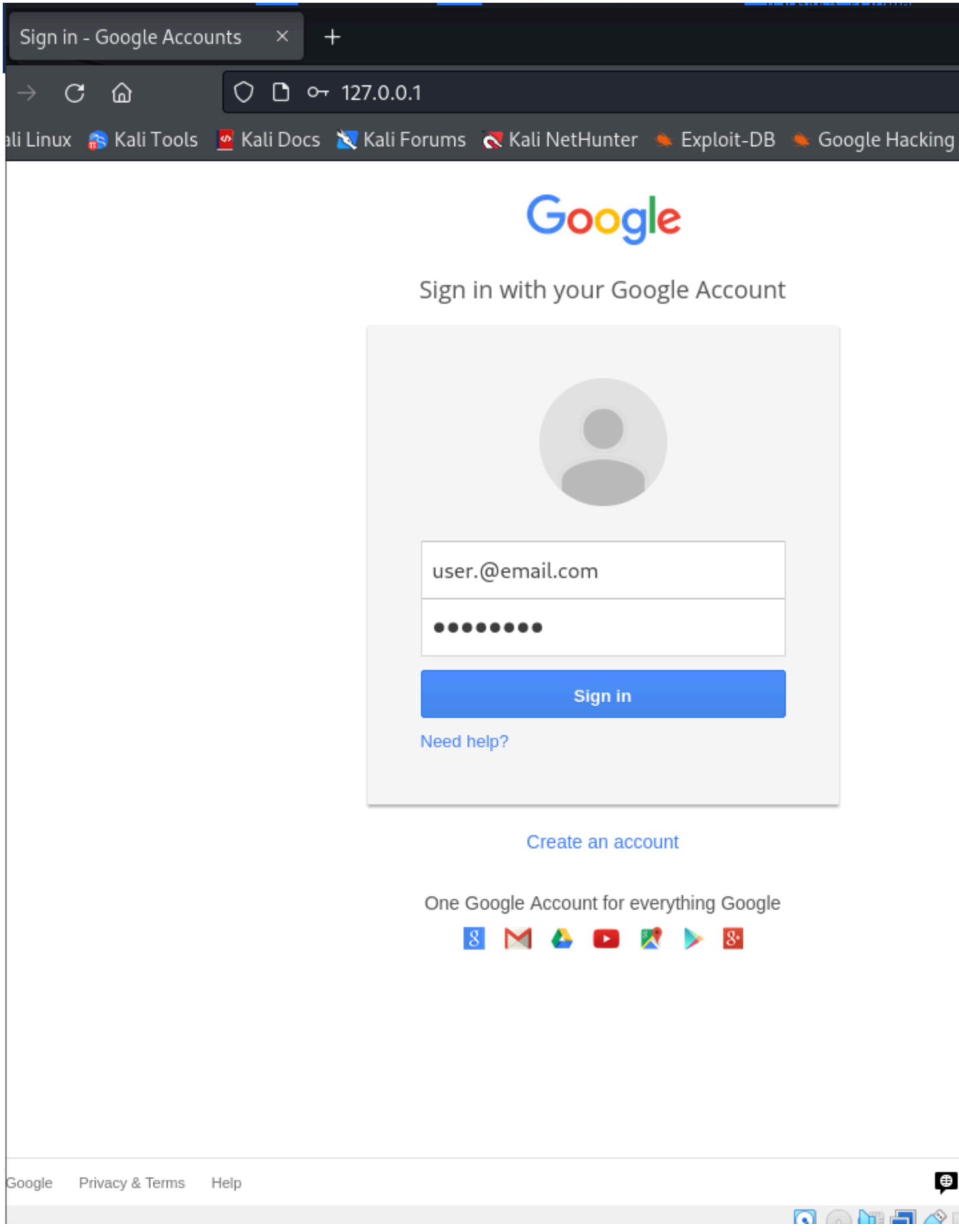
Lateral Movement	T1021 - Remote Services	Used **Remote Desktop Protocol (RDP)** and **WinRM** for movement.
Collection	T1114 - Email Collection	Exfiltrated **Microsoft 365 and Exchange** emails from victims.
Exfiltration	T1041 - Exfiltration Over C2 Channel	Sent stolen data via **encrypted HTTPS connections**.
Impact	T1562.001 - Disable Security Tools	Disabled **endpoint detection and response (EDR)** solutions.

Key Takeaways:

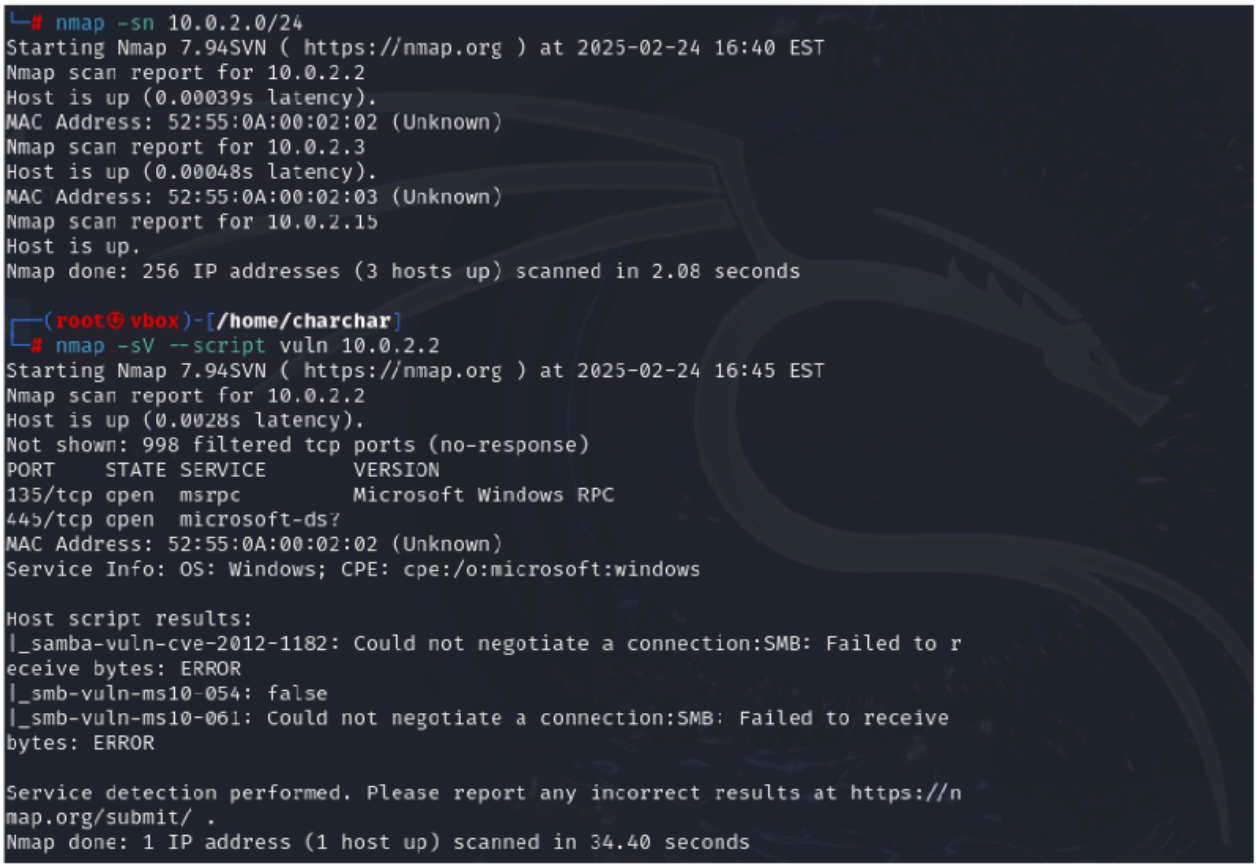
1. **Supply Chain Attack**: Instead of targeting victims directly, APT29 compromised **SolarWinds**, a trusted IT provider, and infected **thousands of organizations** via software updates.
2. **Highly Stealthy Approach**: Used legitimate accounts and obfuscated scripts to avoid detection for months.
3. **Targeted High-Profile Entities**: Victims included **U.S. government agencies**, Microsoft, and cybersecurity firms.


Shell No. 1
File Actions Edit View Help
The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order t
The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-bas
applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits th
ploit payload.

```
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: 127.0.0.

        **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: 2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Re
on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [24/Feb/2025 17:51:05] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [24/Feb/2025 17:51:06] "GET /favicon.ico HTTP/1.1" 404 -
```


Sign in - Google Accounts
127.0.0.1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking
Google
Sign in with your Google Account
user.@email.com
Sign in
Need help?
Create an account
One Google Account for everything Google
Google
Privacy & Terms
Help

Apply Vulnerability Assessment Techniques



III. Network Vulnerability Scanner Report (Nmap --script vuln) (10.0.2.2)

- **Scan Details:**
  - Nmap was used with the `--script vuln` option to perform a vulnerability scan on host 10.0.2.2.
  - The scan aimed to identify potential vulnerabilities in the services running on the host.
- **Scan Results:**
  - Host 10.0.2.2 is identified as a Microsoft Windows system.
  - Open ports:
    - 135/tcp (msrpc - Microsoft Windows RPC)
    - 445/tcp (microsoft-ds)
  - Vulnerability scan results:
    - `smb-vuln-ms10-054`: false (indicating the host is likely not vulnerable to MS10-054).
    - `smb-vuln-ms10-061` and `samba-vuln-cve-2012-1182` returned errors related to SMB connection negotiation.
    - Not shown: 998 filtered tcp ports (no-response)
- **Analysis:**
  - The open SMB ports (135 and 445) present potential security risks.
  - The SMB errors during the vulnerability scan require further investigation to determine the root cause. This could be firewalls blocking the connection, or misconfiguration.
  - Microsoft RPC is running on the host.
  - The filtered ports show that a firewall is likely in place.

IV. Network Penetration Testing Tool Output (Nmap -sn) (10.0.2.0/24)

- **Scan Details:**
  - Nmap was used with the `-sn` option to perform a ping scan on the 10.0.2.0/24 subnet.
  - The scan aimed to identify active hosts on the network.
- **Scan Results:**
  - The scan identified three active hosts: 10.0.2.2, 10.0.2.3, and 10.0.2.15.
  - MAC addresses were identified for 10.0.2.2 (52:55:04:00:02:02) and 10.0.2.3 (52:55:04:00:02:03), both labeled as "Unknown".
  - Nmap done: 256 IP addresses (3 hosts up) scanned in 2.08 seconds
- **Analysis:**
  - The ping scan successfully identified active hosts on the network.
  - The unknown MAC addresses could indicate virtual machines or specialized network devices.

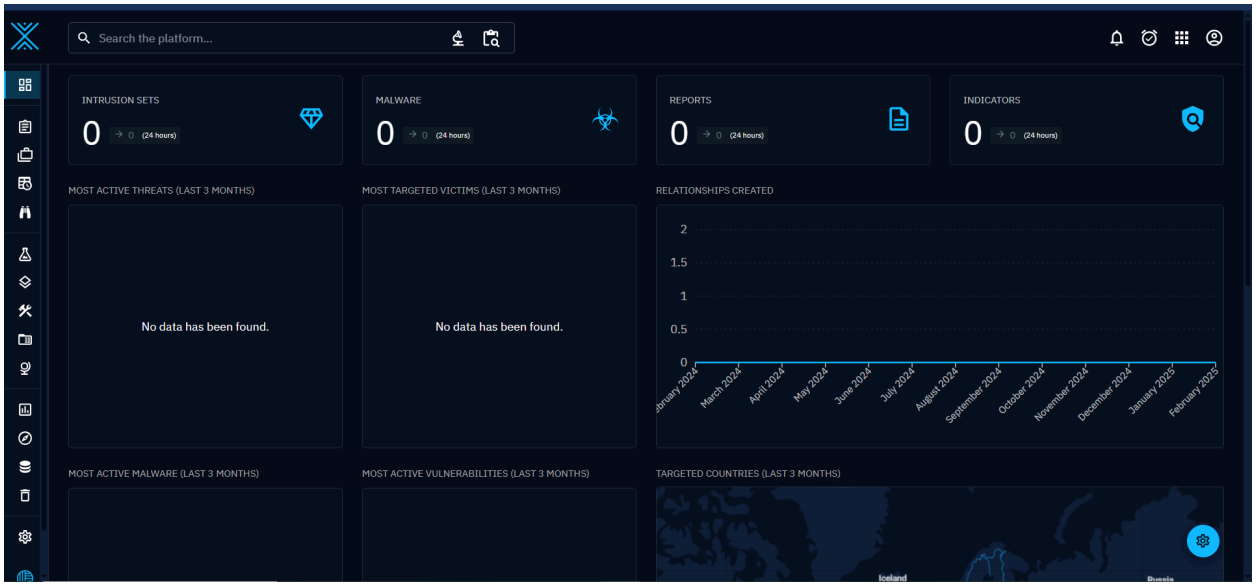
V. Recommendations

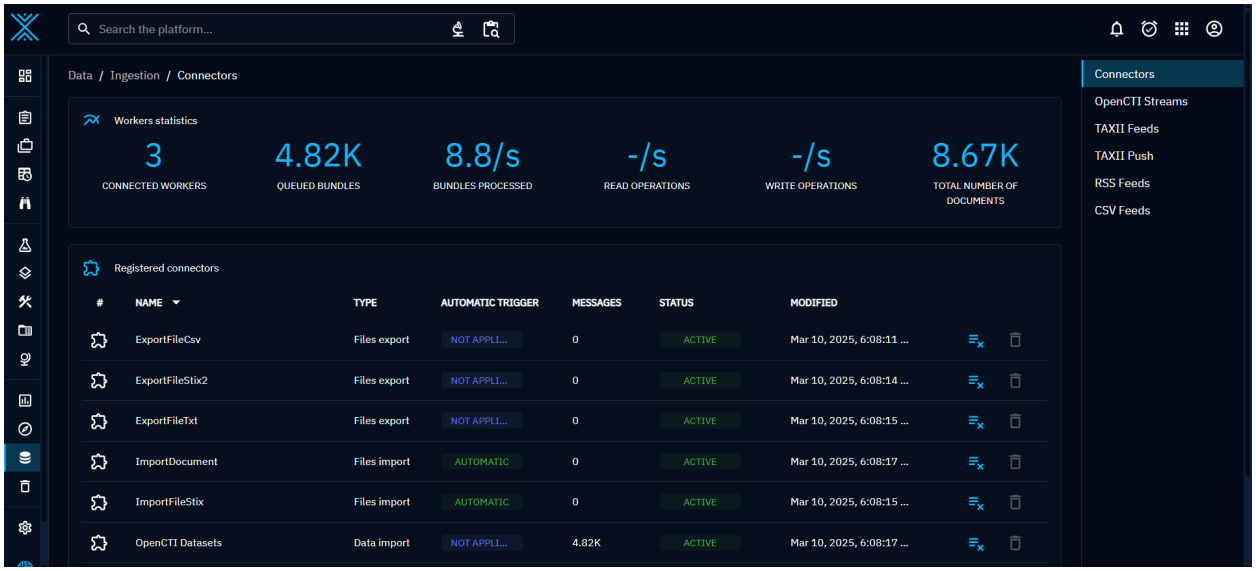
- **10.0.2.2 Hardening:**
  - Review and harden the SMB configuration on 10.0.2.2.
  - Investigate the SMB errors from the vulnerability scan to ensure no misconfigurations or vulnerabilities are present.
  - Ensure that the windows host is fully patched.
  - If not needed, disable the Microsoft RPC service.
  - Review the firewall rules.
- **10.138.16.39 Monitoring:**
  - Monitor the host's network activity for any unusual behavior.
  - Ensure the host's software is up to date to mitigate potential vulnerabilities.
- **Network Security:**
  - Implement network intrusion detection/prevention systems (IDS/IPS) to monitor for malicious activity.
  - Regularly review and update firewall rules.
  - Monitor for unusual broadcast traffic.
  - Investigate the unknown MAC addresses.

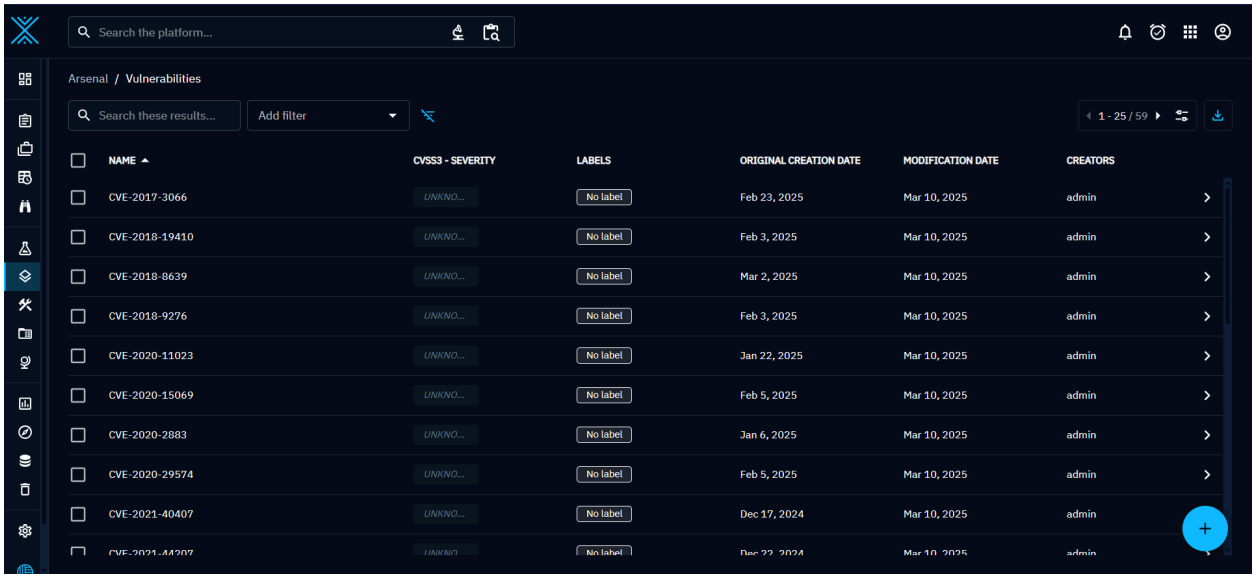
VI. Conclusion

This report demonstrates the effectiveness of Wireshark and Nmap in network security assessments. The findings highlight potential security concerns and provide actionable recommendations for improving the security posture of the analyzed networks. Regular security assessments and continuous monitoring are essential for maintaining a secure network environment.

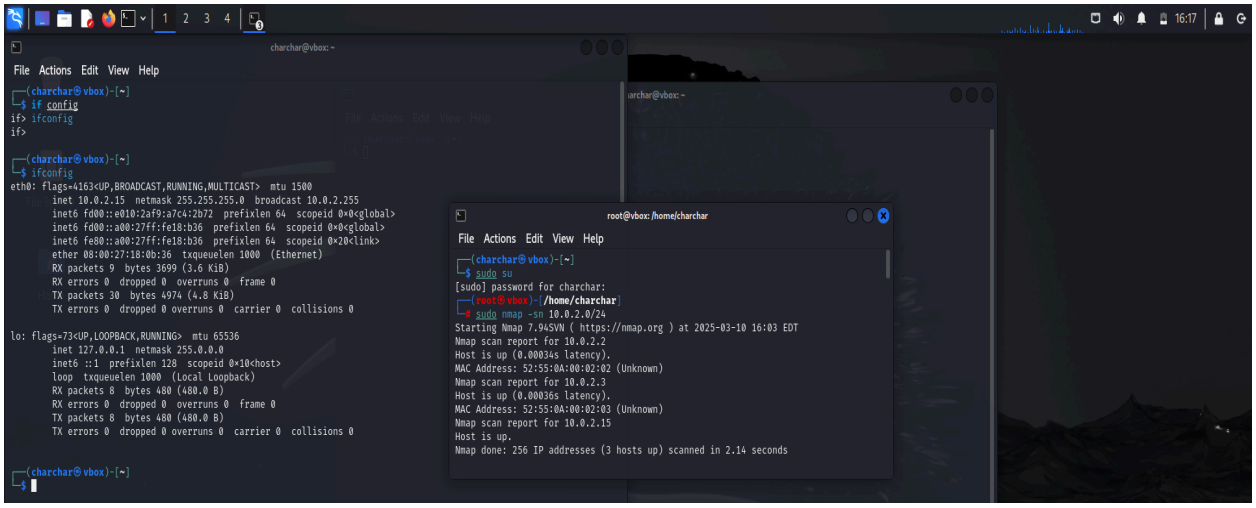
Implement Threat Intelligence Principles

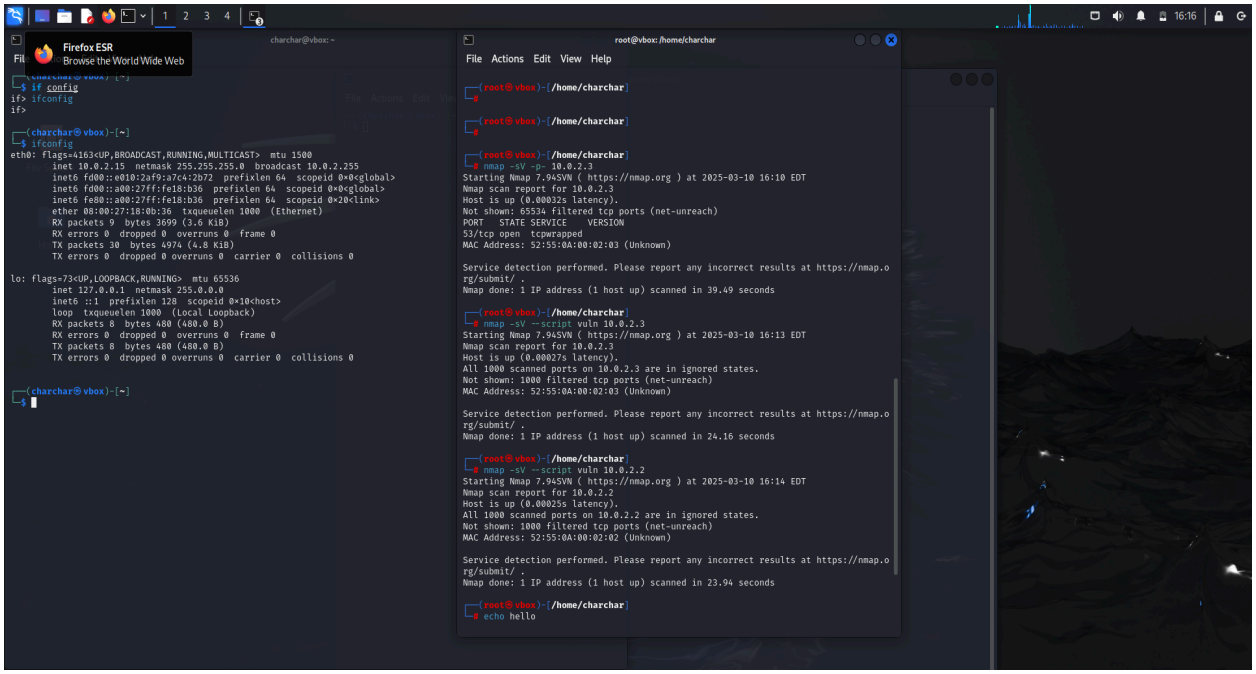

Search the platform...
INTRUSION SETS
0
MALWARE
0
REPORTS
0
INDICATORS
0
MOST ACTIVE THREATS (LAST 3 MONTHS)
No data has been found.
MOST TARGETED VICTIMS (LAST 3 MONTHS)
No data has been found.
RELATIONSHIPS CREATED
MOST ACTIVE MALWARE (LAST 3 MONTHS)
MOST ACTIVE VULNERABILITIES (LAST 3 MONTHS)
TARGETED COUNTRIES (LAST 3 MONTHS)


Search the platform...
Data / Ingestion / Connectors
Workers statistics
3
CONNECTED WORKERS
4.82K
QUEUED BUNDLES
8.8/s
BUNDLES PROCESSED
-/s
READ OPERATIONS
-/s
WRITE OPERATIONS
8.67K
TOTAL NUMBER OF DOCUMENTS
Registered connectors
Connectors
OpenCTI Streams
TAXII Feeds
TAXII Push
RSS Feeds
CSV Feeds



Develop and Apply Risk Management Strategies / Implement Security Monitoring and Incident Response





- **10.0.2.3:** All 1000 scanned ports are filtered (net-unreach). This means Nmap couldn't establish a TCP connection. This could indicate:
    - A firewall blocking traffic.
    - The host being down.
    - Network issues preventing reachability.
- **10.0.2.2:** Similar to 10.0.2.3, all 1000 ports are filtered.
- **53/tcp Open (Unwrapped):** Port 53 (DNS) is open on an unspecified host (likely 10.0.2.3 based on the first scan). The service is "unwrapped," meaning Nmap couldn't determine the specific DNS software version.

Critical Risks:

1. **Open DNS Service (Port 53):**

    - **Explanation:** An open DNS service without version information poses a significant risk. Attackers can exploit known vulnerabilities in older or misconfigured DNS servers for DNS spoofing, cache poisoning, or denial-of-service attacks. The "unwrapped" status suggests potential misconfiguration or an outdated version.
    - **Treatment Recommendation:** Immediately identify the host with the open DNS service and determine the specific DNS software and version. If outdated, update to the latest stable version. Implement access control lists (ACLs) to restrict DNS queries to authorized sources only.
    - **Basic Mitigation Steps:**

1. Identify the host IP address.
2. Run a more detailed Nmap scan with version detection (`nmap -sV -p 53 <IP>`).
3. Check the DNS server configuration for open recursion and restrict it.
4. Apply the latest security patches.

2. **Unreachable Hosts (10.0.2.3 and 10.0.2.2):**

    - **Explanation:** The "net-unreach" status for all ports on these hosts is concerning. It could mean they are down, firewalled, or there are network routing issues. If they are critical systems, this constitutes a significant availability risk. If they are unknown devices, it poses a security risk as they could be unauthorized devices.
    - **Treatment Recommendation:** Investigate the cause of unreachability. If intentional (e.g., firewalled servers), document the configuration. If unintentional, troubleshoot network connectivity or system status.
    - **Basic Mitigation Steps:**
        1. Ping the hosts to check basic connectivity.
        2. Trace the route to the hosts (`traceroute <IP>`).
        3. Check firewall rules on the hosts and network devices.
        4. Verify the hosts are powered on and network interfaces are active.

B. Risk Monitoring Procedure

Risk Monitoring Procedure: Open DNS Service (Port 53)

- **Risk:** Vulnerable or misconfigured DNS service on port 53.
- **Monitoring Frequency:** Weekly.
- **Monitoring Method:**
    1. **Automated Nmap Scan:** Schedule a weekly Nmap scan with version detection (`nmap -sV -p 53 <IP>`) against the identified host.
    2. **DNS Server Logs:** Regularly review DNS server logs for suspicious activity, such as unusually high query rates, queries for unknown domains, or error messages.
    3. **Vulnerability Scanner:** Use a vulnerability scanner (e.g., Nessus Essentials, OpenVAS) to scan the DNS server for known vulnerabilities.
- **Metrics:**
    1. DNS software version.
    2. Number of failed DNS queries.
    3. Number of detected vulnerabilities.
    4. CPU and memory utilization of the DNS server.
- **Reporting:**
    1. Generate a weekly report summarizing the scan results, log analysis, and vulnerability scan findings.
    2. Escalate any critical vulnerabilities or suspicious activity to the security team immediately.

- **Review:**
    1. Review the monitoring procedure quarterly to ensure its effectiveness and make necessary adjustments.

II. Implement Security Monitoring and Incident Response

A. Security Monitoring Setup

Tool: We'll use `tcpdump` (or `Wireshark` if a GUI is preferred) for basic security monitoring.

Use Case: Detecting Unauthorized DNS Queries

- **Detection Rule:** Monitor DNS traffic (port 53) for queries to domains not on an approved list.
- **Implementation:**
    1. **Capture DNS Traffic:** `tcpdump -i <interface> port 53 -w dns_capture.pcap`
    2. **Analyze Traffic:** Open `dns_capture.pcap` in Wireshark or use `tshark` to filter and analyze the queries.
    3. **Create Approved Domain List:** Maintain a list of approved domains in a text file.
    4. **Script for Alerting:** Write a script that parses the `dns_capture.pcap` file, extracts the queried domains, and compares them against the approved list. If a non-approved domain is found, send an alert (e.g., email, Slack message).
- **Alert Prioritization:**
    1. **Severity:** High if the domain is known to be malicious. Medium if it's an unknown domain. Low if it's a new but potentially legitimate domain.
    2. **Context:** Consider the source IP address, time of day, and user associated with the query.
- **Response Procedures:**
    1. **Verify:** Check the query against threat intelligence sources to confirm if the domain is malicious.
    2. **Block:** Block the domain at the firewall or DNS level.
    3. **Investigate:** Investigate the source IP address and user account to determine the cause of the unauthorized query.
    4. **Notify:** Notify the affected user and relevant stakeholders.

B. Incident Response Scenario

Incident: A user reports that their system is slow and they are seeing pop-up ads for unknown products.

- **Classification:** Malware infection (potentially adware).
- **Response Steps:**

1. **Isolate:** Disconnect the affected system from the network to prevent the spread of malware.
2. **Scan:** Perform a full system scan with an updated antivirus and anti-malware tool.
3. **Analyze:** Review system logs, network traffic, and running processes for suspicious activity.
4. **Remove:** Remove any detected malware and clean up any residual files or registry entries.
5. **Restore:** If necessary, restore the system from a clean backup.
6. **Patch:** Ensure the system is fully patched with the latest security updates.
7. **Educate:** Educate the user about safe browsing practices and how to avoid malware infections