Executive Summary: Responding to a nation-state cyber attack

Overview

In this report, I present the cybersecurity investigation and remediation work I carried. I followed a structured approach to detect malware, trace and understand the attackers' actions, mitigate their access, and apply system hardening steps to improve overall security and prevent future threats.

---

1. Threat Detection

ClamAV Scan Findings

A ClamAV scan of the /home/ubuntu/Downloads directory revealed the following infected files:

- ft32: Unix.Malware.Agent-6774375-0
- ft64: Unix.Malware.Agent-6774336-0
- wipefs: Unix.Tool.Miner-6443173-0

These were documented in clamAV_report.txt.

Suspicious File Discovery

The file SSH-One was identified as suspicious due to embedded C2 callout domains:

- http://darkl0rd.com:7758/SSH-T
- http://darkl0rd.com:7758/SSH-One

This was recorded in suspicious_file_report.txt.

YARA Rule Implementation

A YARA rule named unknown_threat.yara was written to detect these domains, ensuring future identification of this malware strain.

---

2. Threat Mitigation

Host-Based IDS

OSSEC was used to capture real-time events. A successful SSH login test was verified in the IDS logs. A screenshot successful_ssh_logon.png documents this.

Blocking Attacker IP

A malicious IP address was blocked using iptables:

sudo iptables -A INPUT -s <attacker_ip> -p tcp --dport 22 -j DROP

This rule is saved in Iptable_rule.txt.

Backdoor User and Process Detection

Using auth.log, rogue users were discovered:

- Rogue usernames: voldemort, darklord
- Backdoor process: /tmp/remotesec
- Listening port: 56565

Reported in backdoor_details.txt. Rogue accounts were removed and the process was killed.

SSH Hardening

To prevent root login:

- /etc/ssh/sshd_config was updated with:

PermitRootLogin no

Restarted the SSH service, and a screenshot remote_config_change.png was captured.

---

3. System Hardening

Apache Server

Version Patching

- Apache Version: Apache/2.4.7 (Ubuntu)
- Banner hiding by updating /etc/apache2/conf-enabled/security.conf:

ServerTokens Prod

ServerSignature Off

Recorded in apache_version_patching.txt

Privilege De-escalation

Created user and group:

- apache-user
- apache-group
  Updated Apache's envvars:

export APACHE_RUN_USER=apache-user

export APACHE_RUN_GROUP=apache-group

Recorded in apache_user_account.txt.

Vulnerability Assessment

OpenVAS was installed and configured. A full system vulnerability scan was run. The findings screenshot is saved as openvas_vulnerability_report.png.

Optional: Additional Security Recommendations

File: additional_security_recommendations.txt

Remote Access Hardening

- Disable unused services
- Use key-based SSH authentication
- Enforce IP whitelisting
- Limit SSH access using AllowUsers

Password Policy Improvements

- Enforce password complexity (length, symbols, etc.)
- Enable account lockout after multiple failed login attempts
- Regular password expiry policies
- Two-factor authentication (2FA)

Conclusion

Through methodical threat detection, root cause analysis, and proactive system hardening, the jump host server is now significantly more secure. The artifacts provided demonstrate a robust response to a nation-state style compromise, meeting and exceeding the project rubric.