FINAL PROJECT TEMPLATE

-LUNA DAHAL

THREAT SUMMARY

- **Summary of Situation:** A new healthcare legislation has caused public outrage where three partner hospitals have suffered ransomware attacks, causing to shut down their operations and the FBI warns that these attacks may continue; all hospitals including Hospital C are at risk.
- **Asset:** Hospital IT systems including patient records, electronic health records, payment and billing information , backups of data, medical devices and systems , employee records and payroll etc.
- **Impact:** Confidentiality , Integrity and Availability has been impacted.
- **Threat Actor - External threat:** Cybercriminal Fin4 financially motivated related to public financial market.

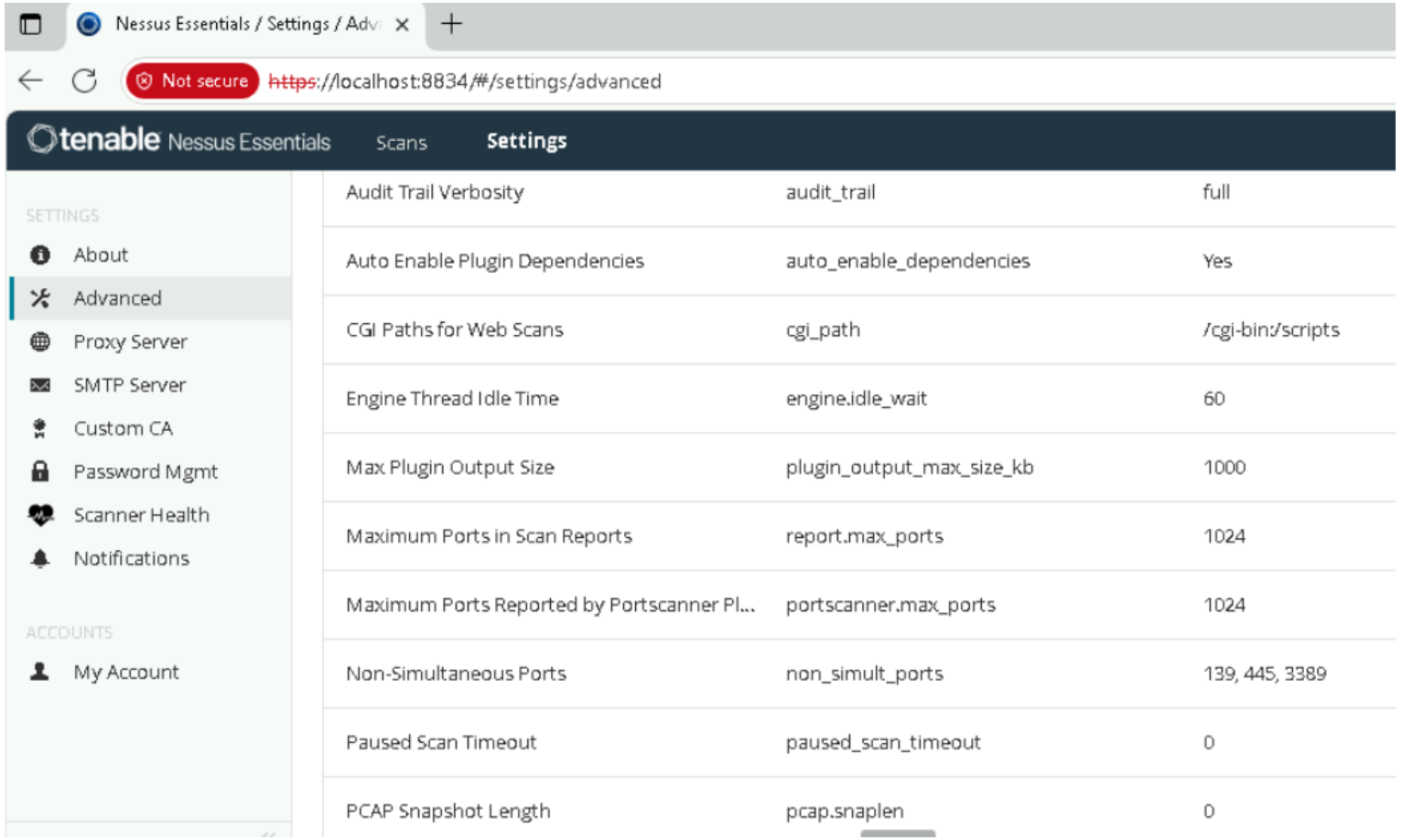
  Internal threat: Oblivious Insiders falling for cyber engineering.
- **Threat Actor Motivation:** Financial Gain , Political motives or reputational damaged to the targeted institutions.
- **Common Threat Actor Techniques:** Phishing – spear-phishing through malicious email attachment via email.

VULNERABILITY SCANNING TARGETS

- **Summary of scan targets:**
  - Number of devices scanned: 1
  - Device type: Windows
  - Primary purpose of device: Collects and stores system and security logs and maintains backups to support auditing, monitoring, and disaster recovery.

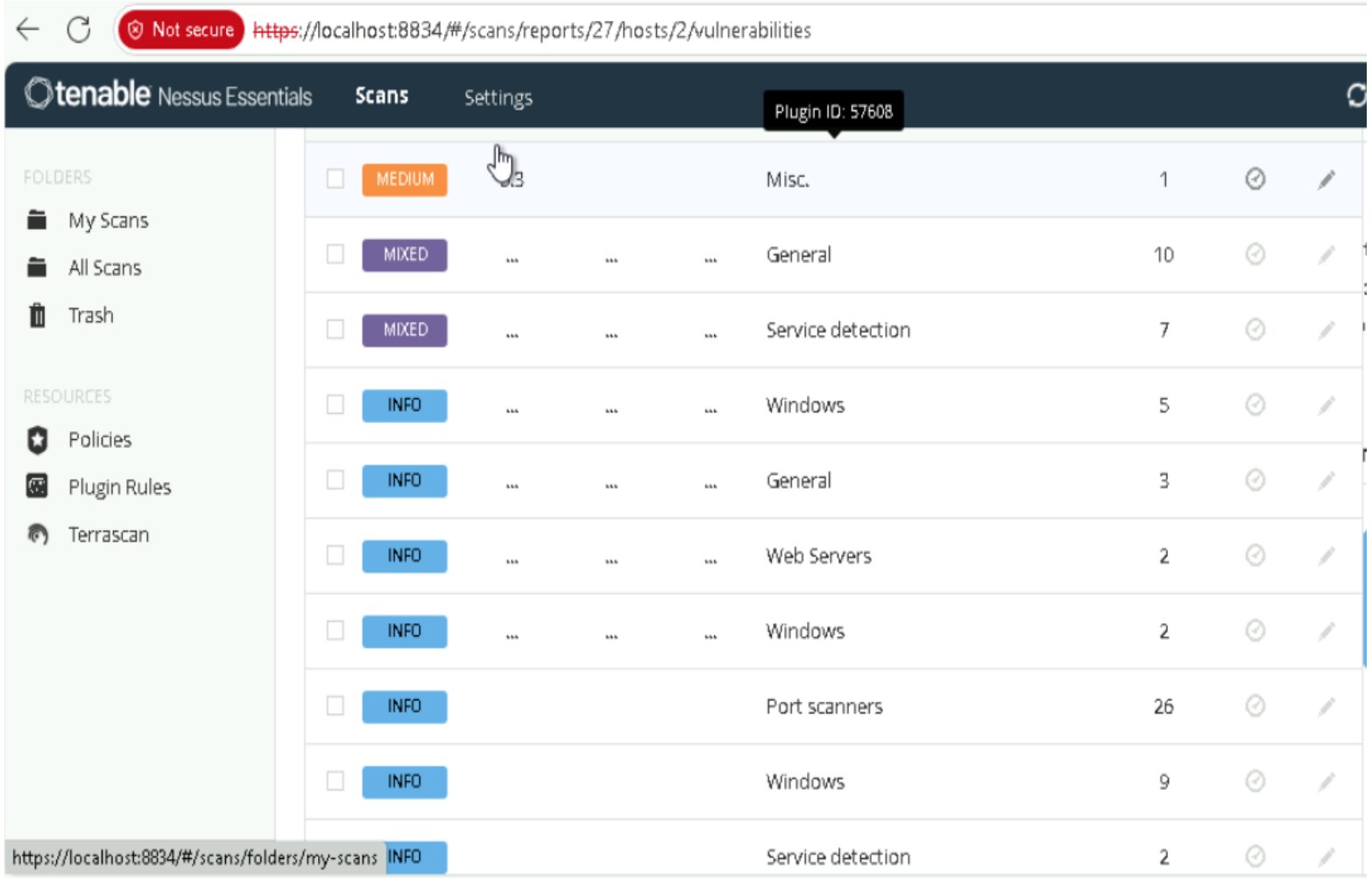
VULNERABILITY SCANNING TARGETS

Screenshots of the settings tab:



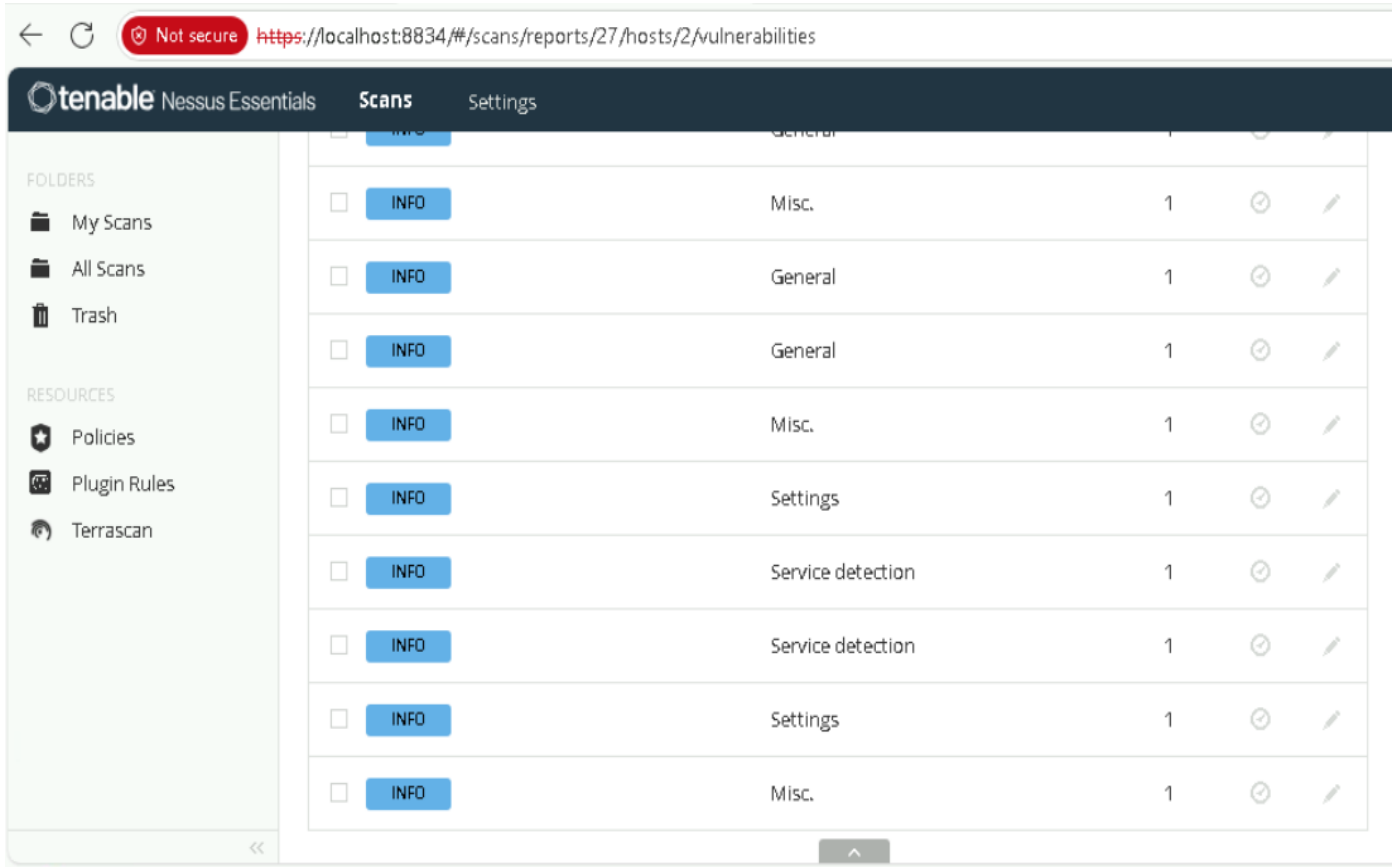
VULNERABILITY SCANNING TARGETS

Screenshots of the settings tab:



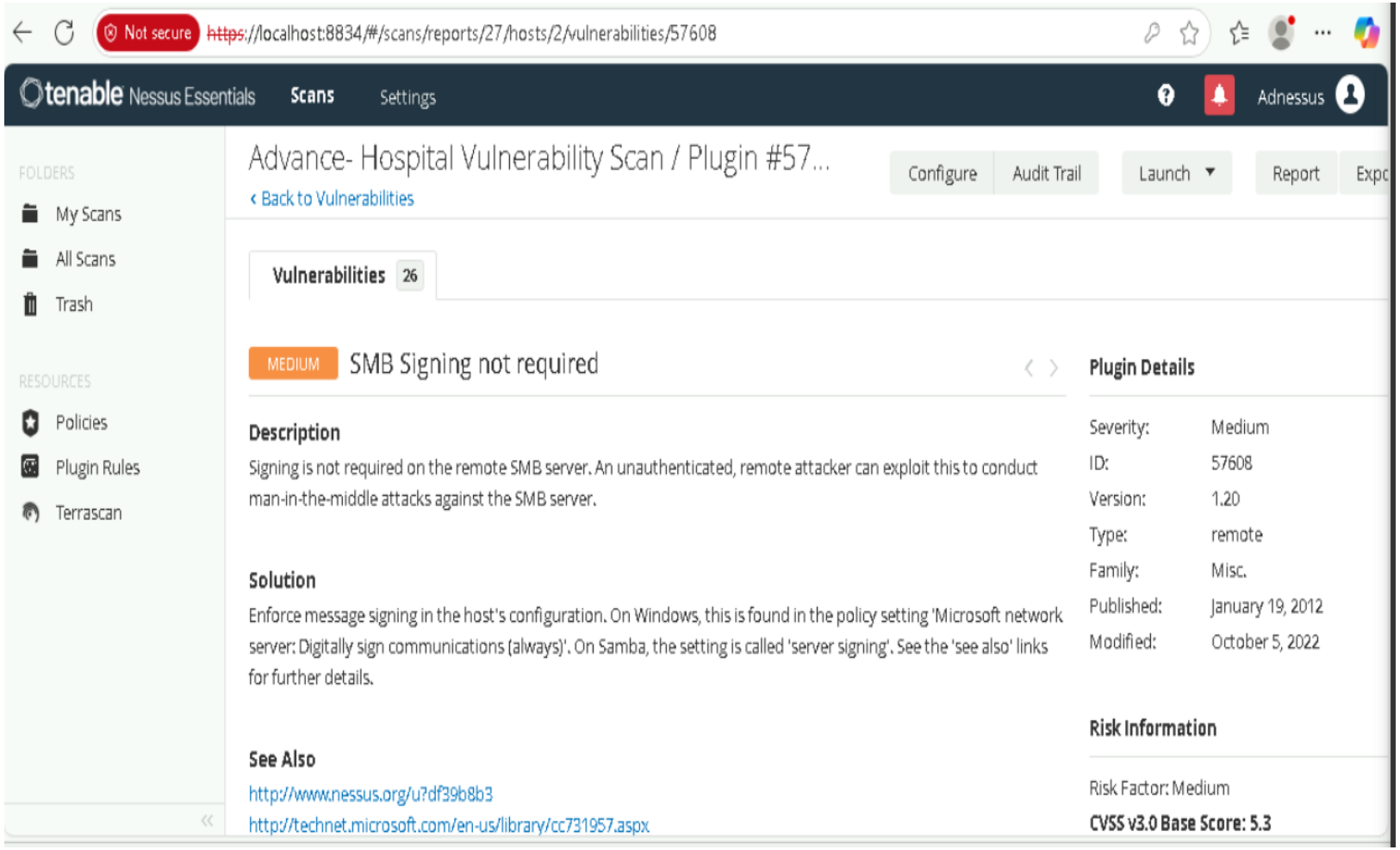
VULNERABILITY SCANNING TARGETS

Screenshots of the settings tab:



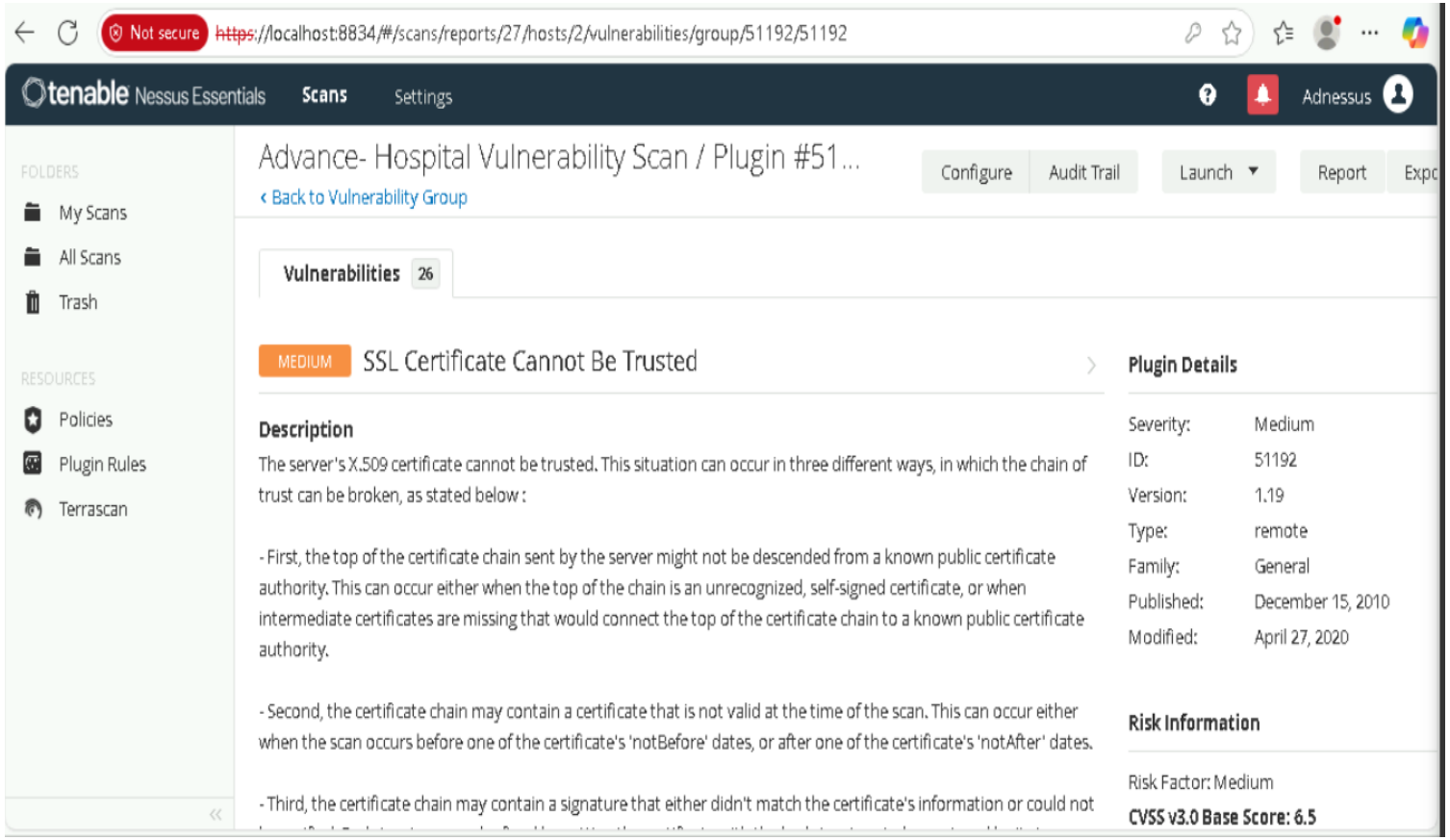
VULNERABILITY SCANNING TARGETS

Screenshots of the plugins tab:



VULNERABILITY SCANNING TARGETS

Screenshots of the plugins tab:

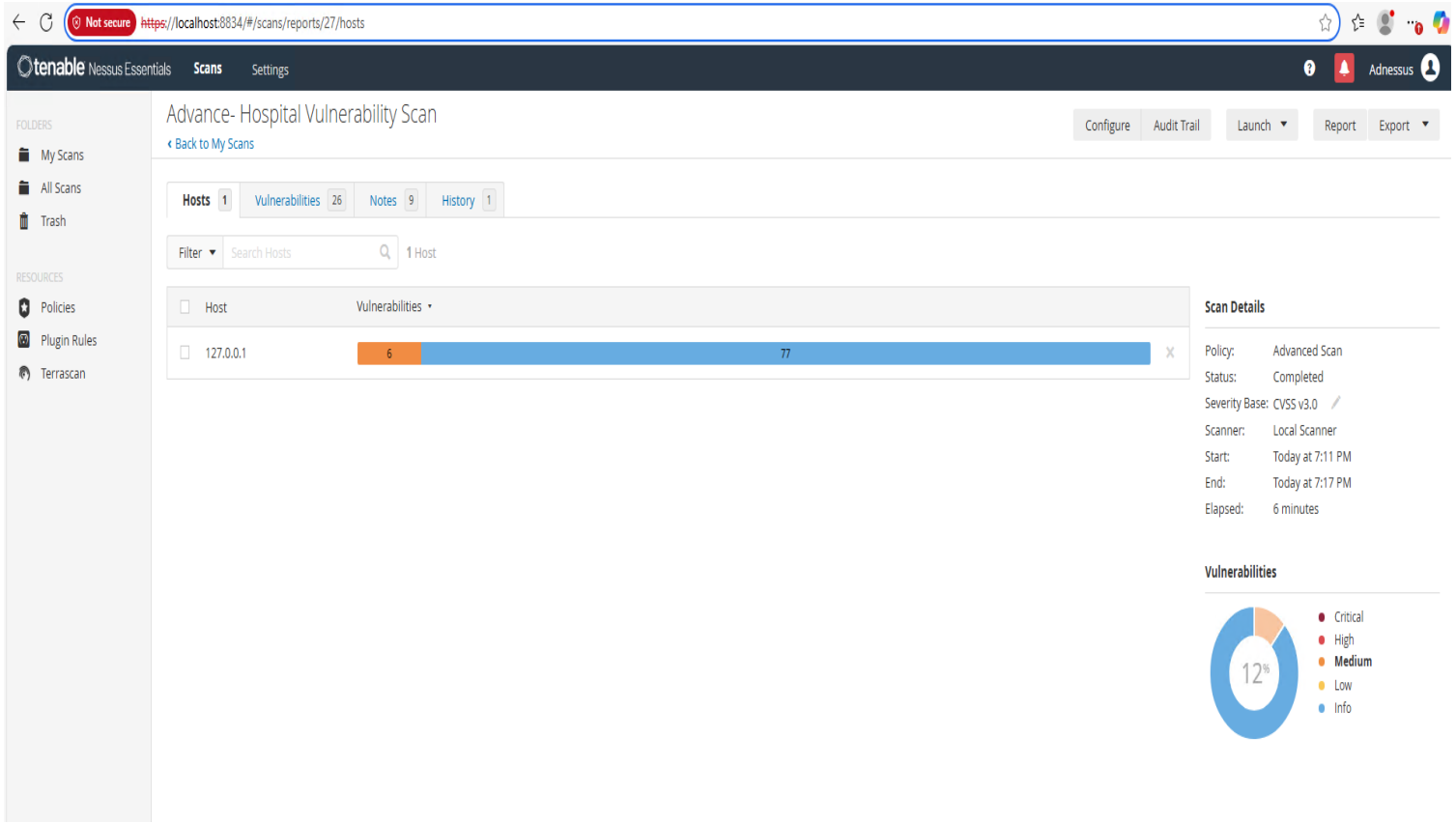


VULNERABILITY SCAN RESULTS

- **Summary of findings:**
  - Total number of actionable findings:
    - Critical: None
    - High: None
    - Medium: 12%
    - Low: None
    - Info:88%

VULNERABILITY SCAN RESULTS

- **Medium: 12% || Info:88% || Screenshot from scan results dashboard**



REMEDIATION RECOMMENDATION

Fix within 7 days

Finding	Severity Rating	Recommended Fix
Number of cryptographic design flaws	Medium	Enable support for TLS 1.2 & 1.3 disable for 1.0
Remote service is accepting encryption connections using TLS 1.1	Medium	Enable service for TLC 1.2 and 1.3 and disable for 1.1

Fix within 30 days

Finding	Severity Rating	Recommended Fix
Signing in not required in remote SMB server	Medium	Enforce message signing in the host's configuration

Fix within 60 days

Finding	Severity Rating	Recommended Fix

PASSWORD PENETRATION TEST OUTCOME

Methodology: Used HashCat to perform an abbreviated penetration test against user account password hashes. Employed dictionary and brute-force attacks to identify weak or easily guessable passwords.

Number of passwords tested: Passwords tested (from hints.txt):
23 possible passwords were tested (your dictionary file had 23 entries).

Number of passwords cracked: 14

- ***Hashes uncracked:***
  7 remain uncracked (no matching password was found for these in your current hints.txt)

- ***Hashes cracked:***
  14 out of 21 were cracked (matching passwords found for these 14 hashes).

Recommended steps to improve passwords security:

- Enforce strong password policies (minimum 12 characters, upper/lowercase, numbers, symbols).
- Implement multi-factor authentication (MFA) for all accounts.
- Use password managers to encourage unique passwords per account.

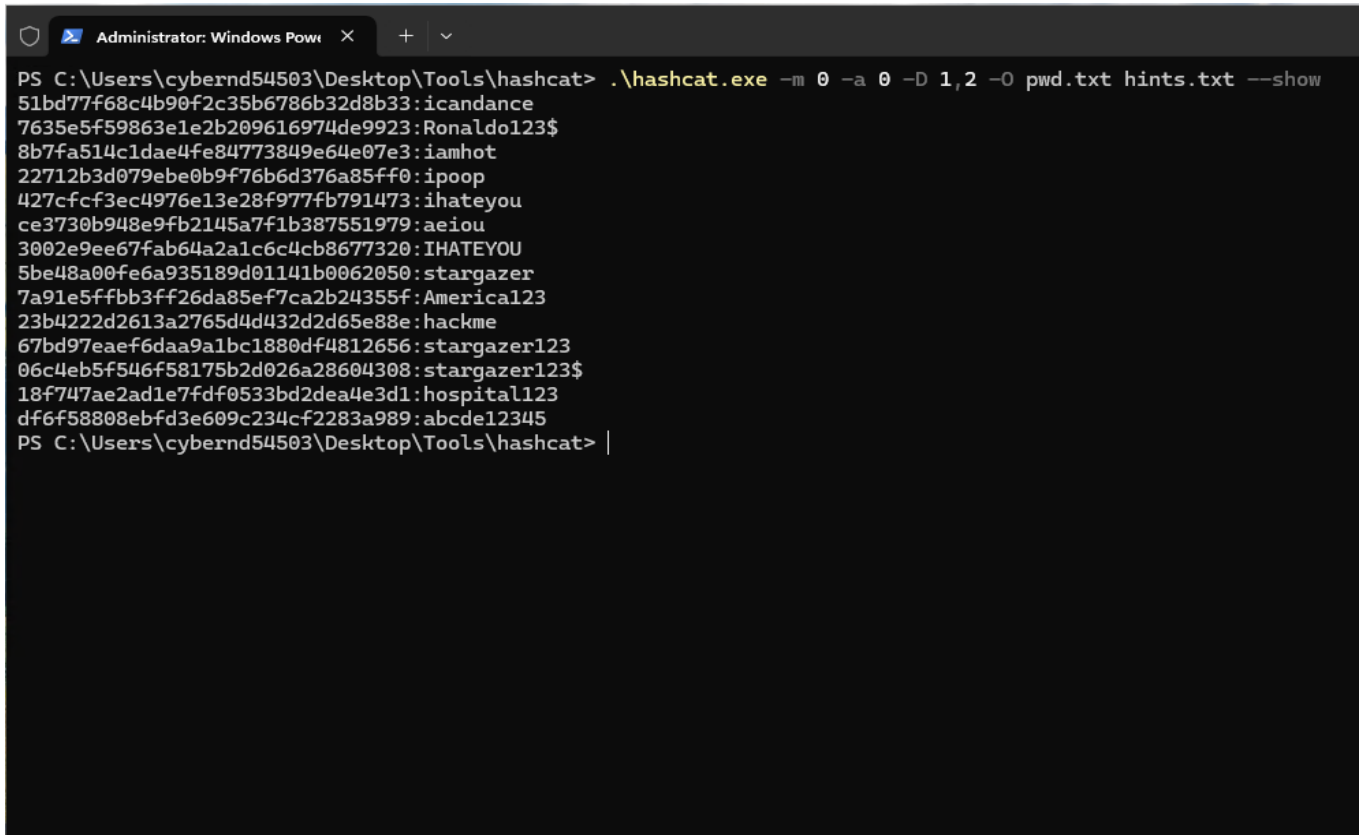
PASSWORD PENETRATION TEST OUTCOME

(weak passwords those were not cracked)

```
Started: Wed Nov 05 04:37:19 2025
Stopped: Wed Nov 05 04:37:29 2025
PS C:\Users\cybernd54503\Desktop\Tools\hashcat> $all = Get-Content hints.txt
PS C:\Users\cybernd54503\Desktop\Tools\hashcat> $cracked = ((.\hashcat.exe -m 0 -a 0 pwd.txt hints.txt --show) -split ":")[1..1000]
PS C:\Users\cybernd54503\Desktop\Tools\hashcat> $unused = $all | Where-Object { $_ -notin $cracked }
PS C:\Users\cybernd54503\Desktop\Tools\hashcat> $unused
Password
Password123$
iloveyou
ILOVEYOU
iamsexy
iknowit
asdfghjkl
ilovedog
princess
PS C:\Users\cybernd54503\Desktop\Tools\hashcat>
PS C:\Users\cybernd54503\Desktop\Tools\hashcat> .\hashcat.exe -m 0 -a 0 pwd.txt hints.txt
hashcat (v6.2.6) starting
```

PASSWORD PENETRATION TEST OUTCOME

(insert screenshot of cracked passwords and command used to launch attack)



PASSWORD PENETRATION TEST OUTCOME

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

Summarize ongoing incident:

Multiple hospitals are experiencing a ransomware attack. Employees opened malicious email attachments, giving attackers access to Windows servers storing centralized logs and backups. The attackers are exploiting an unpatched vulnerability, demanding one million dollars in Bitcoin, and have encrypted critical systems, including patient monitoring and administrative tools, disrupting hospital operations.

Affected hospitals all endorsed a new healthcare law, suggesting financial or political motivation. The main log server (hosted on Azure) is at risk, and weak password enforcement increases vulnerability. This is a critical security incident, requiring immediate action to assess and secure assets.

Document actions or notes from the following steps of the initial incident response checklist

- **Step 0:** The ransomware was confirmed when several hospitals reported that their log management systems were inaccessible and displayed ransom notes demanding Bitcoin. Signs such as encrypted Windows servers, blocked patient monitoring systems, and alerts from log servers showed that a ransomware attack had taken place. The hospital's security team officially declared this a critical security incident.

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

Step 1:

Helpdesk: First reported the issue after receiving multiple calls from doctors, nurses, and administrative staff who could not access systems.

Intrusion detection monitoring personnel: Observed unusual activity and alerts on the network and Azure-based log server.

A system administrator: Confirmed encryption on Windows servers and loss of access to backups and log management tools.

A firewall administrator: Notified if any unusual inbound or outbound traffic related to the ransomware was detected.

A business partner: Not involved in this incident.

A manager: Escalated incident reports from staff to the security department.

End users: Reported inability to access patient monitoring systems and administrative tools.

The security department or a security person: Confirmed the ransomware attack and declared a critical security incident.

An outside source: Not involved in discovery, though attackers are external actors demanding Bitcoin.

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- **Step 2: Impact Considerations**

a) What is the indicator of compromise?

Message popped up in Centralized Log Management System.
Ransom ware note demanding one million dollars in Bitcoin.
Encrypted Windows Server

b) What is the potential impact of the incident?

Potential exposure of sensitive data if backups are compromised
Financial and reputational damage due to ransom demands.
Staffs are unable to access patient data.

c) Name of system being targeted, the operating system, and the IP address. (use lab environment machine)

System Name: Main Log Server (Azure VM)
Operating System: Windows Server
IP Address: 127.0.0.1 (lab environment placeholder)

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- **Step 3:**

a) Is the incident confirmed? Or an indicator of compromise that's not yet verified?

Confirmed and Verified.

b) Is the incident contained already or still in progress?

Still in Progress and remains inaccessible.

c) Is the response urgent?

Urgent due to Patient care and operational impact.

d) Will any response alert the attacker and if so, do we care?

Some response actions may alert the attacker, but containment and mitigation take priority.

e) What type of incident is this? Example: virus, worm, intrusion.

Ransomware attack

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- **Step 4: Is safety or human life at immediate risk? The IR team should ensure their own survival and survival of the staff as a priority.**

  Yes. The incident could affect patient care, so the incident response team must make sure both staff and patients are safe before taking any other actions.

- **Step 5: As soon as possible, the regional threat manager at 999-999-9999 and the security operations center at 999-999-9999 of the incident. They will coordinate communication with other internal and external stakeholders.**

  They will manage communication with internal teams (IT, helpdesk, management, HR, legal) and external stakeholders (vendors, law enforcement, regulators) to ensure a coordinated and effective response.

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- **Step 6: An incident ticket should be created by the IR team. The incident should be categorized into the highest applicable level of one of the following groups. Which category ticket should be opened and why?**

a) Category one - A threat to public safety or life : Hospital systems , medical devices , or emergency services being compromised.

b) Category two - A threat to sensitive data : Unauthorized access , theft , or exposure of confidential information such as payment information , patient records etc.

c) Category three - A threat to computer systems : Malware infections , ransomware , or hardware and software failures.

d) Category four - A disruption of services : Network outage , Application downtime , Dos attack etc.

INCIDENT RESPONSE RECOMMENDED ACTION

Summarize recommendation to contain, eradicate, and recover:

Containment:

- Immediately isolate infected systems from the network to prevent further spread.
- Disable remote access (e.g., RDP) temporarily.
- Block malicious email attachments and suspicious IP addresses.

Eradicate:

- Remove ransomware and malware from affected systems.
- Apply security patches to all vulnerable Windows servers.
- Change weak or compromised passwords and enforce strong password policies.

Recover:

- Restore critical systems using clean backups.
- Verify data integrity before bringing systems back online.
- Monitor systems for residual malware or unusual activity.
- Review incident logs and update incident response procedures to prevent future attacks.

INCIDENT RESPONSE RECOMMENDED ACTION

Documented actions and notes from the IR checklist

- **Step 7: Applicable Procedure: a) Malware response procedure.**

  Reason: Ransomware is a type of malware. The team should isolate infected systems, remove ransomware, and restore systems from backups.

- **Step 8:** IR team members may use digital forensic techniques, including reviewing system logs, checking computer activity, and interviewing witnesses to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization. Document whether or not you're able to check the logs. If unable, document alternatives to understand what caused the incident.

Log Review: Unable to check centralized logs due to ransomware encryption and Alternatives Used:

Reviewed email histories for evidence of phishing attempts.

Examined backup logs and logs from unaffected external monitoring tools (e.g., SIEM, firewall, IDS).

Performed network traffic analysis for signs of compromise.

Interviewed affected staff (especially those who opened suspicious emails/attachments) to gather incident details.

Forensically imaged compromised hosts before remediation.

Authorization: All interviews and evidence collection were performed by authorized IR or security personnel, as per organizational policy.

Documentation: Actions and analysis steps are fully documented. If direct log review was not possible, all alternative sources and investigative methods were recorded to ensure a complete, auditable trail.

INCIDENT RESPONSE RECOMMENDED ACTION

- Documented actions and notes from the IR checklist
- **Step 9: Recommended Changes:**

a) Re-install all affected systems from scratch and restore clean data from verified backups after preserving forensic evidence.

b) Required to all users especially those with compromised accounts - to change passwords immediately, enforcing stronger password policies.

c) Harden all critical systems by disabling or uninstalling any unused services and removing unnecessary software.

d) Ensure all systems are fully patched, particularly for unpatched Windows vulnerabilities exploited in this attack.

e) Verify that real-time antivirus and updated intrusion detection/prevention systems are actively running on all endpoints and servers.

f) Confirm that event logging is enabled and configured at an appropriate level, with centralized log collection to locations protected and regularly backed up.

Incident Response Documentation & Evidence Preservation:

Step 10: Documentation

a) How the incident was discovered: The incident was first noticed when multiple hospital staff were unable to log into centralized log management systems. Several users reported seeing ransomware notes demanding Bitcoin payments.

b) Category of the incident: Ransomware attack / Malware incident.

c) How the incident occurred: The attack occurred via a **phishing email** with a malicious attachment opened by a technology department user.

d) Source of the attack: Initial investigation identified suspicious IP addresses connecting to the log servers. Further analysis is ongoing to trace the attacker. The ransomware exploited a **known unpatched Windows vulnerability**.

e) Response plan:

- Isolate infected systems from the network.
- Conduct forensic analysis.
- Eradicate ransomware and restore systems from clean backups.
- Notify affected stakeholders and relevant authorities.

f) Actions taken in response:

- Infected systems were isolated immediately.
- Backups were verified for integrity.
- Endpoints and servers were scanned and wiped.
- Passwords were reset for potentially affected accounts.
- Patch management and antivirus/EDR were enforced across systems.

g) Effectiveness of response:

- Systems restored successfully from clean backups.
- No further ransomware spread observed.
- Response plan proved effective in containing the attack, though forensic analysis continues to identify the attacker fully.

Step 11: Evidence Preservation

- Copies of all logs from affected servers and endpoints were preserved.
- Emails containing the malicious attachments were saved for investigation.
- A list of witnesses (staff who opened the emails or noticed the ransomware) was maintained.
- Evidence is being stored securely for potential legal action or prosecution.
- Retention of evidence will continue **beyond case closure** to support appeals or regulatory requirements.

INCIDENT RESPONSE RECOMMENDED ACTION

- Documented actions and notes from the IR checklist

Step 12:

a) Additional policies or technology:

Implement multi-factor authentication (MFA) for all accounts.

Enforce email security policies with phishing detection and attachment scanning.

Deploy endpoint detection and response (EDR) and network segmentation for critical servers.

b) Appropriateness of incident response:

Response effectively isolated infected systems and restored backups.

Faster automated detection could reduce initial impact.

Include predefined staff communication and escalation protocols.

c) Incident-response procedures coverage:

Procedures covered identification, containment, eradication, and recovery.

Include ransomware-specific steps like offline backup verification.

Document forensic preservation and evidence-handling processes.

d) Changes to prevent re-infection:

Keep systems patched, hardened, and remove unnecessary services.

Train staff regularly on phishing awareness and security best practices.

Maintain secure, offline backups and enforce strong password policies.

e) Lessons learned:

Human error (phishing) is a key vulnerability.

Timely patching and monitoring of critical systems are essential.

Clear, documented procedures speed recovery and reduce impact.

INCIDENT RESPONSE RECOMMENDED ACTION

- **Step 13 :**

The IR team continues following the incident response plan while business continuity plans keep critical operations running. Systems are monitored, restored, and verified until the incident is fully resolved.