# FINAL PROJECT TEMPLATE

# THREAT SUMMARY

- **Summary of Situation:** (Summarize the current threat situation)
  we targeted by ransomware attack . we know that the group behind is FIN 4.
Several doctors, nurses, and administrative staff have called in noting that they are being asked to pay one million dollars in Bitcoin to access their systems. The control systems used to monitor patient stats are no longer available through the standard user interface. Some doctors report being unable to render treatments because they cannot view detailed information about patient status.

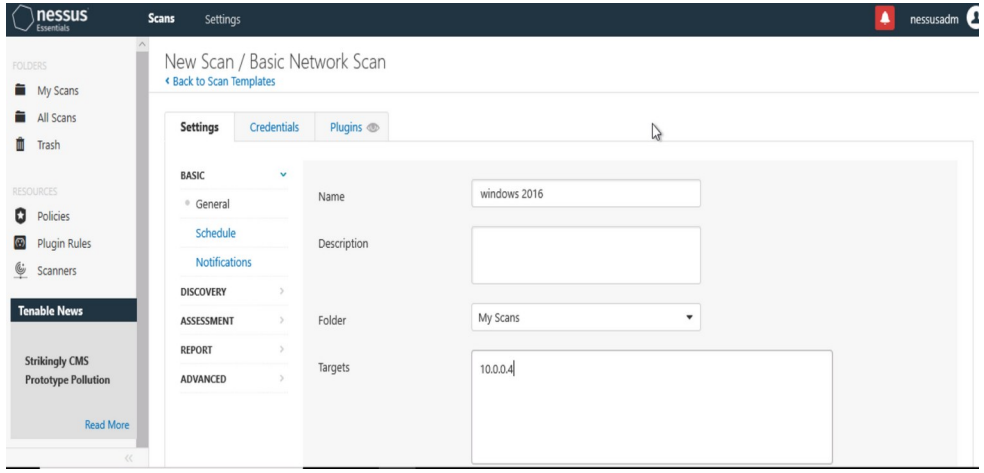
- **Asset:** (What assets are being targeted?)  the asset is being here target is log management system  patient record , hospital servers, personal documents , bank records.
- **Impact:** (What part of the CIA triad is being impacted?) highly impacting on availability , integrity and confidentiality.
- **Threat Actor:** (Identify potential threat actors)external threat actor is FIN 4 and internal threat actor which are also involved in this threat by clicking on the phishing link intentionally or unintentionally.
- **Threat Actor Motivation:** (Share potential motivations behind the attacks)  FIN 4 is a financially – motivated threat group that has targeted confidential information related to the healthcare and pharmaceutical companies . and hacktivists who are motivated for social or political ends.
- **Common Threat Actor Techniques:** (Share attack methods commonly used by the threat actor.)  FIN 4 has used spearphishing emails containing malicious links to give username and password. Username and password use to ransom attack to install something malicious in our organization. And then access to the network and then infict the rest of the network use ransom malware.
- *Hint: Carefully check the ransom note for additional clues.*

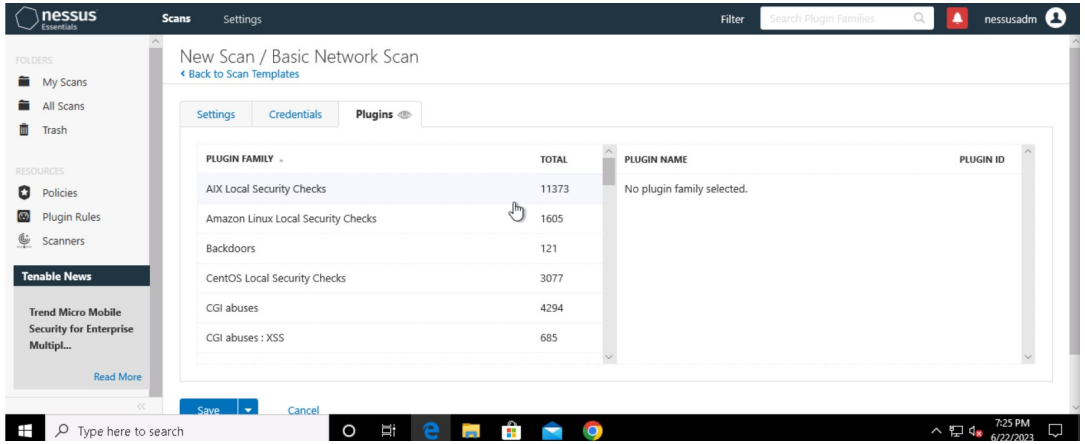
# VULNERABILITY SCANNING TARGETS

## Summary of scan targets:

- Number of devices scanned: 1
- Device type: (operating system and version) windows server 2016
- Primary purpose of device: (describe what the devices are used for and what kind of data might be on them)
  - its basically used to find any vulnerabilities exits in system and unpatched vulnerabilities.

(insert 2 screenshots from scan configuration window – one of the settings tab and one of the plugins tab. Be sure to click on and display a plugin group relevant to your machines operating system)

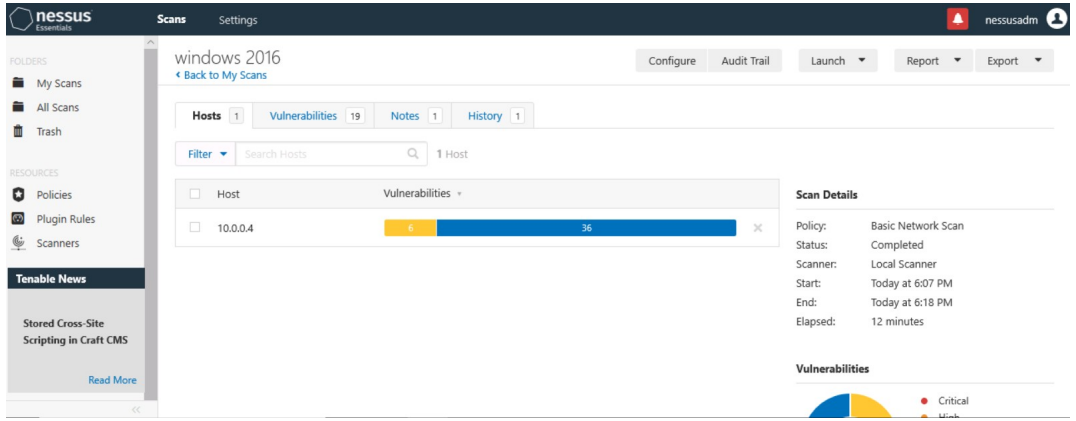


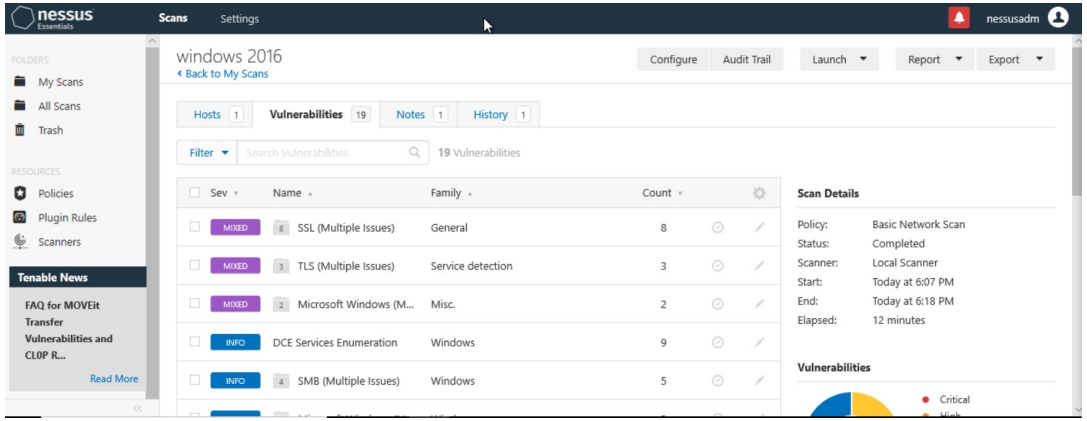



# VULNERABILITY SCAN RESULTS

- **Summary of findings:**
  - Total number of actionable findings:  42
    - Critical: 0
    - High: 0
    - Medium:  6
    - Low: 0
    - Info: 36

(insert screenshot from scan results dashboard)



# REMEDIATION RECOMMENDATION

Prioritization Notes:
(Summarize your thought process for how you organized these here)

■Fix within 7 days critical

| Finding | Severity Rating | Recommended Fix |
|---|---|---|
| SSL certificate cannot be trusted | 6.5 | Purchase or generate a proper ssl certificate |
| Ssl medium strength cipher suites supported | 7.5 | Reconfigure the affected application if possible to avoid use of medium strength ciphers |
| Ssl self signed certificate | 6.4 | Purchase or generate a proper ssl certificate |

■Fix within 30 days high

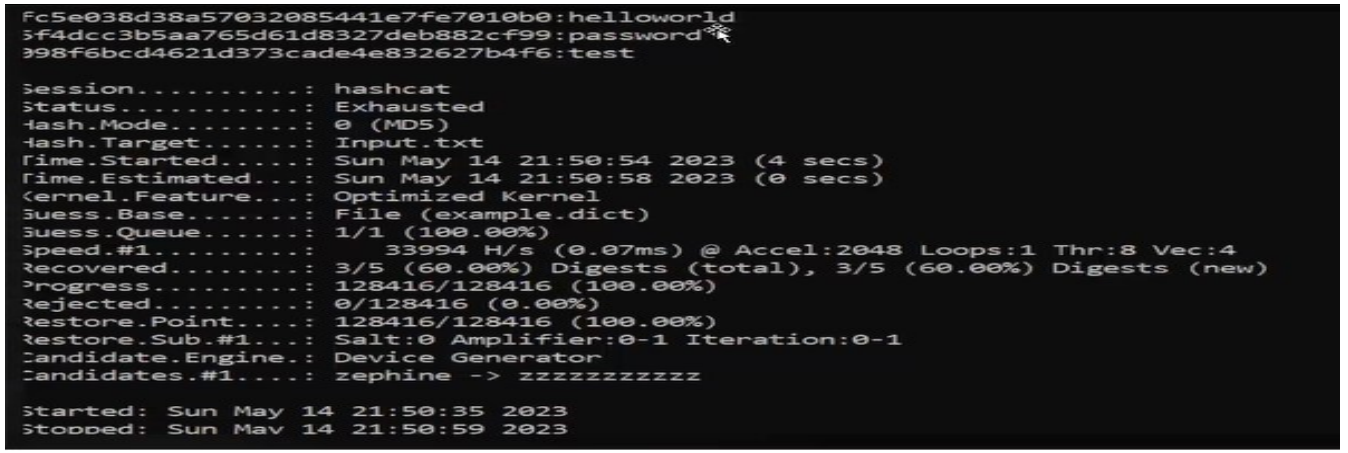
| Finding | Severity Rating | Recommended Fix |
|---|---|---|
| TLS version 1.0 protocol detection | 6.5 | Enable support for tsl 1.2 and 1.3 and disable support for tsl 1.0 |
| SMB signing not required | 5.3 | Enforce message signing in the host's configuration |
| Dce services enumeration | - | none |

■Fix within 60 days

| Finding | Severity Rating | Recommended Fix |
|---|---|---|
| Micrisoft windows smb service detection | none | none |
| Micrisoft windows smb versions supported | none | none |
| Windows NetBIOS remote host information disclosure | none | none |

# PASSWORD PENETRATION TEST OUTCOME

- **Methodology:** (Summarize steps taken to test password security) we try to crack the hash using hashcat tool
- **Number of passwords tested:** (insert number)  5
- **Number of passwords cracked:** (insert number)  3
- **Evidence of weak passwords:**




- **Recommended steps to improve passwords security:** (Summarize best practice recommendations to avoid brute force attacks in the future) don’t use md 5 for hash because it is easy to  crack .  Use very complex password .

# INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- Summarize ongoing incident:
  - What do you know so far?

    we targeted by ransomware attack . we know that the group behind is FIN 4. the asset is being here target is log management system
- Document actions or notes from the following steps of the initial incident response checklist

- Step 1:  helpdesk
- Step 2: a lot of doctors and nurses are complaining to need money to assess. The potential impact of the incident you can go all the way of lost human life because we cannot take any action because we don’t know

  the log management system is been targeted . Operating system windows 2016 and IP address is 10.0.0.4.
- Step 3: Incident is the confirmed by security leaders and FIN 4 ask the amount of bitcoin for decrypt the data.

  Incident still in the progress Several doctors, nurses, and administrative staff have called in noting that they are being asked to pay one million dollars in Bitcoin to access their systems.

  response is the urgent because doctors report being unable to render treatments because they cannot view detailed information about patient status.

  attacker inside the our system so we carefull about any action because it alert to the hacker.

  it is the ransomware attack.
- Step 4: safety or human life at immediate risk because doctors report being unable to render treatment because they cannot view detailed information about patient status. The IR team should ensure their own survival and survival of the staff as a priority.
- Step 6: Category two - A threat to sensitive data should be opened because attacker attack the hospital log management system it contain a patient critical data.

(Add another slide if needed)

# INCIDENT RESPONSE RECOMMENDED ACTION

Documented actions and notes from the IR checklist

- Step 7: *(Tip: Select procedures you'd recommend for this type of incident) I recommend to* Malware response procedure *for this type of incident because it is the ransomware attack.*
- Step 8: hospitals have a unpatched windows system .attacker are also taking advantage of an unpatched Windows vulnerability to execute the attack. And some user use the weak password.
- Step 9: update all the system form latest version.

  user change the password and use at least 12 charactar in password.

  hospitals follow the least privilege benchmark.

  Be sure real time virus protection and intrusion detection is running
- Step 12: NIST and CIS framework could have prevent the intrusion.

(b) incident response was appropriate. It will improve use additional frameworks like CIS

(c) incident response procedure were detailed and it cover the entire situation. It can improve by increase end user awareness and learn from past incident.

(d) update all the system form latest version.

user change the password and use at least 12 charactar in password

Be sure real time virus protection and intrusion detection is running.

Be sure the system is logging the correct events and to the proper level.

(e) We learn that use the updated software and use the strong password ,deploy the right tools ,upgrade our monitoring system.

(Add another slide if needed)