FINAL PROJECT TEMPLATE

THREAT SUMMARY

Summary of Situation: In hospitals A, B, and C, the employees receive a pop-up message while trying to login to the centralized log management systems indicating that all the personal files are encrypted by attackers with ransomware, and they will only decrypt the data if the hospitals pay the ransom in bitcoins.

This incident happened after an employee in the technology department clicked and opened an email attachment.

Note that this incident hasn't happened yet with Hospital X.

- **Asset:** Personal documents, filescontrol systems used to monitor patient stats and doctors' report feature was inaccessible Also the log analysis tool was no longer accessible.
- **Impact:** All the CIA triad will be impact.
- **Threat Actor: There was two threat actors.**

External threat → Attackers (FIN4) with a finial or political reasons.

Internal threat → Employee because they unintentionally open the attachment and caused the incident.

- **Threat Actor Motivation:**

The motivation could be by terminated employee who have access to the data, or they steal data after leaving or by the employee that are unhappy about the organization and want to make damage or revenge to the organization by exploit the data.

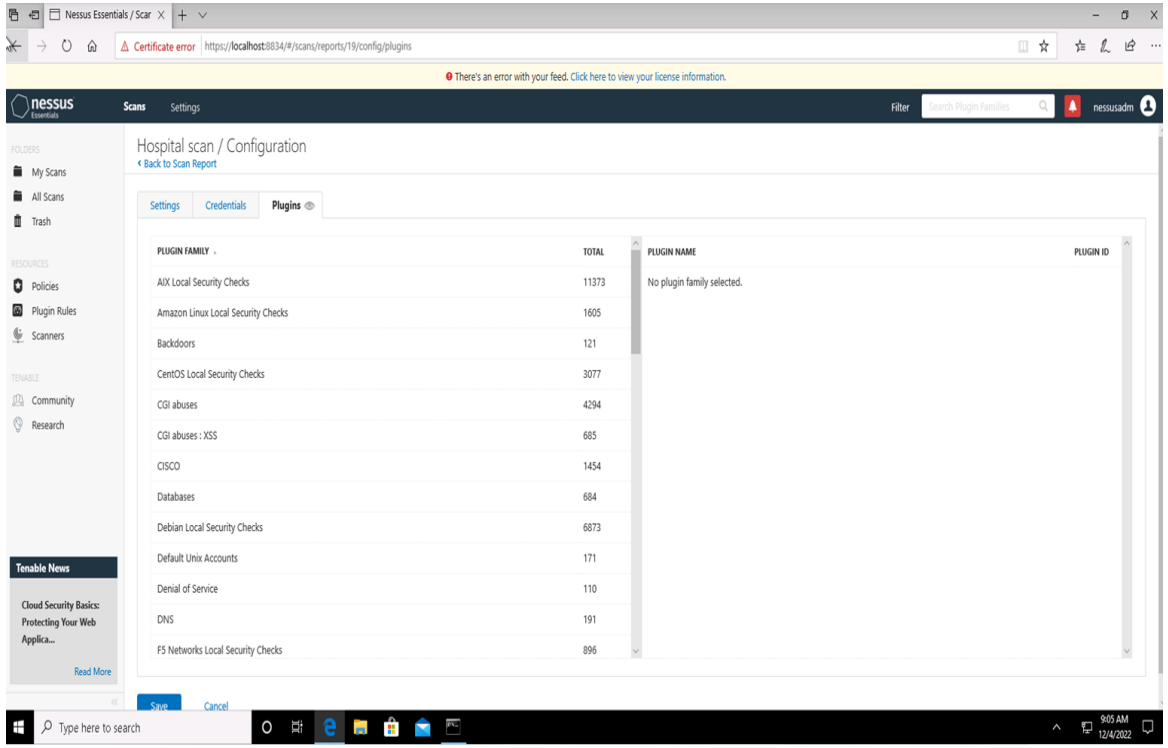
- **Common Threat Actor Techniques:**

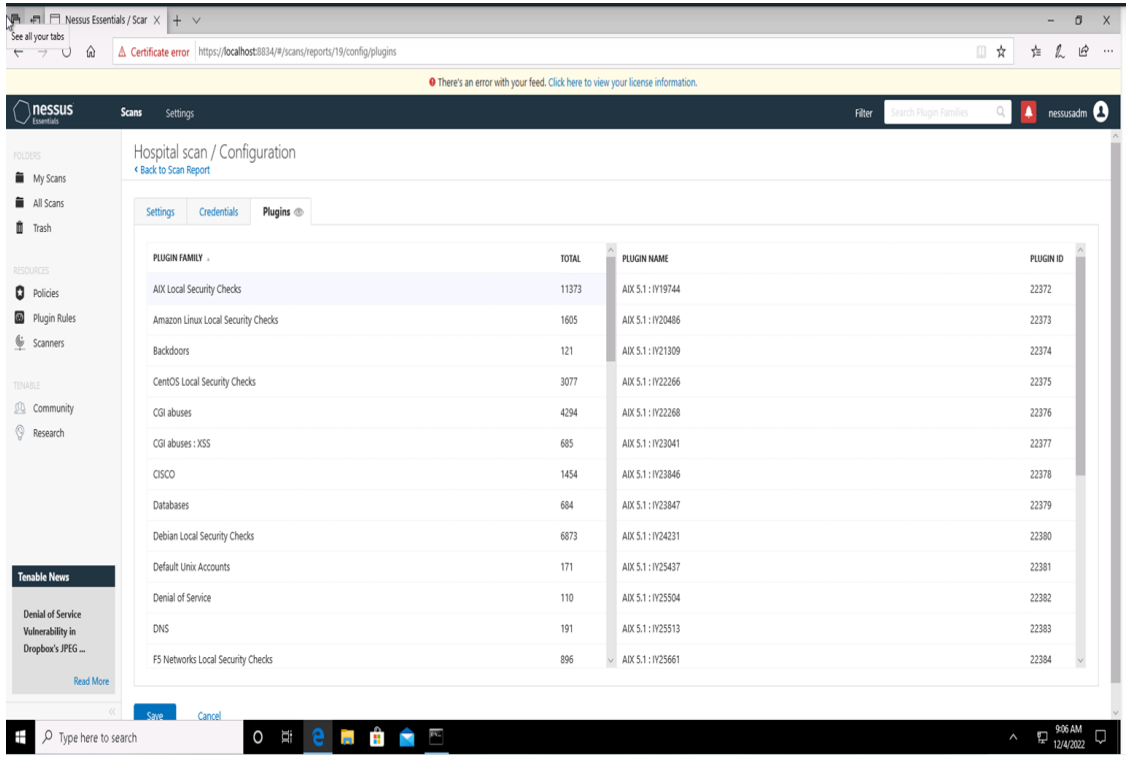
Attackers here are intentionally using phishing technique through email attachment to access the sensitive data.

Employees could be Unintentionally be a victim to this type of phishing since they don't have a background about the security procedure and this type of attack like social engineering.

VULNERABILITY SCANNING TARGETS

- **Summary of scan targets:**
  - Number of devices scanned: One device was scanned
  - Device type: Windows virtual machine
  - Primary purpose of device: General purpose machine (The device is used as centralized device for logs, files and backups)
  - (insert 2 screenshots from scan configuration window – one of the settings tab and one of the plugins tab)

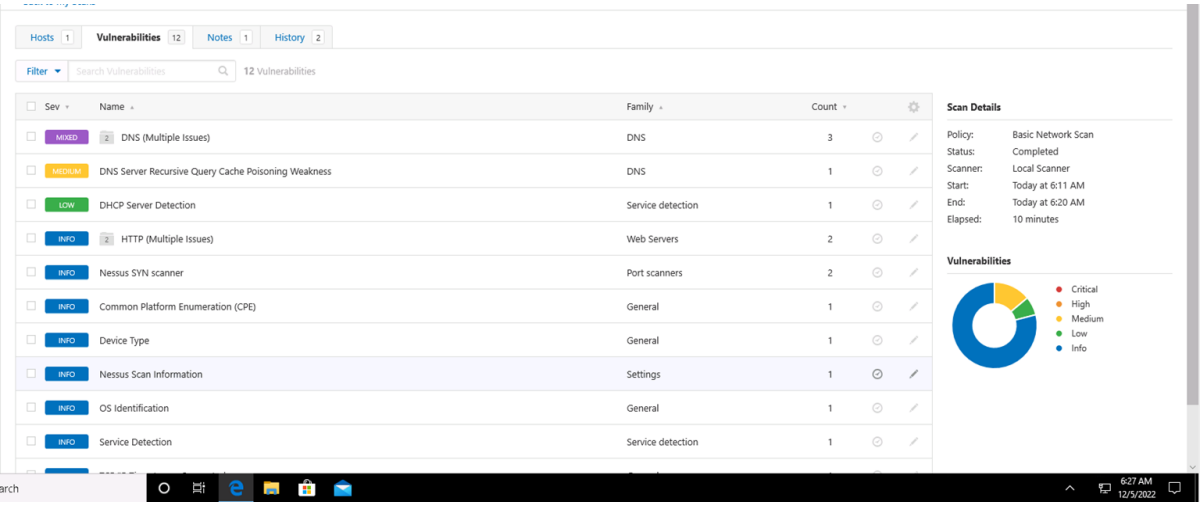


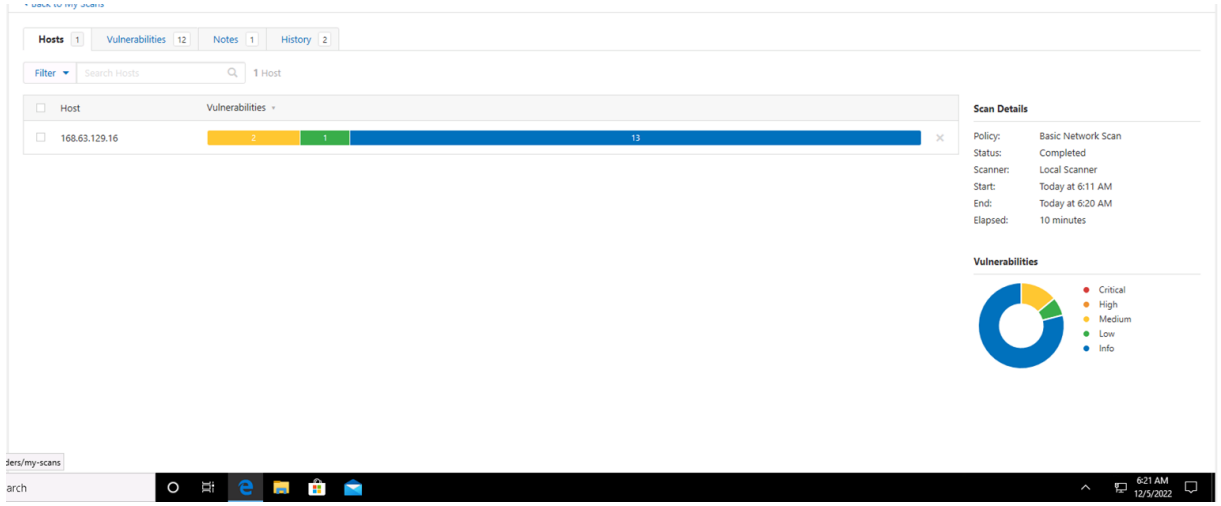


VULNERABILITY SCAN RESULTS

- **Summary of findings:**
  - Total number of actionable findings: 12
    - Critical: 0
    - High: 0
    - Medium: 2
    - Low: 1

(insert screenshot from scan results dashboard)





REMEDIATION RECOMMENDATION

- Fix within 30 days

Finding	Severity Rating	Recommended Fix
DNS Server Recursive Query Poisoning Weakness	Medium	Restrict recursive queries to the hosts that should use this nameserver. If you are using another name server, consult its documentations.
DNS Server Spoofed Request amplification DDoS	Medium	Restrict access to your DNS server from public network or reconfigure it to reject such queries

- Fix within 60 days

Finding	Severity Rating	Recommended Fix
DHCP Server Detection	Low	Apply filtering to keep this information off the network and remove any options that are not in use

PASSWORD PENETRATION TEST OUTCOME

- **Methodology:** I used Hashcat to try to cracking the hashed password given in the hashes.txt file using the hashcat tool.
- **hashcat -a 0 -m 0 text.txt rockyou.txt**
- -a → Dictionary attack
- -m → MD5
- **Number of passwords tested:** 41
- **Number of passwords cracked:** 5
- **Evidence of weak passwords:**

```
5f4dcc3b5aa765d61d8327deb882cf99:password
fc5e038d38a57032085441e7fe7010b0:helloworld
098f6bcd4621d373cade4e832627b4f6:test
Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password- and salt-length (typically down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

8743b52063cd84097a65d1633f5c74f5:hashcat
0e9b09b77fc5391bf20f68095f867ed0:ihatepasswords
```

- **Recommended steps to improve passwords security:**

<u>The below are some criteria user should follow to avoid brute force attack:</u>

1- Password long should be at least 8 characters.

2-Avoid to use password to contain your name or your birthday because it's easy to guess.

3-Password must contain digital, alphanumeric and special characters.

4- Password should be changed every 90 days.

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

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

    Attackers (FIN4 Bit Cryptor) encrypt documents and they ask for a ransom in bitcoin in order to decrypt the documents, all the operations will be on hold because the staff and doctors and nurse they can't open the files because of the centralized log management systems was encrypted.

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

  - Step 1: We need to make a cybersecurity team to handle these problem.
  - Step 2: Decide what is the impact of this ransomware and we shouldn't obey directly because we don't trust them if they will decrypt the files or not.
  - Step 3: Restore the files from the backups.
  - Step 4:Search for the attackers of this incident.
  - Step 5:Isolate the attackers.
  - Step 6:Search for another way to avoid to pay the ransom.
  - Step 7:Train all the staff members about the procedure and security steps.
  - Step 8: Don't forgot to make the backups for all the servers and files.

INCIDENT RESPONSE RECOMMENDED ACTION

- Summarize recommendation to contain, eradicate, and recover:
  - Describe the overall recommended containment, eradication, and recovery plan

    First, we need to detect the source of the attach secondly, we need to inform all the staff to delete the received email and avoid to open it.

    We should have a back up of the files to achieve the business continuity.

    After that the recovery plan which is delete the software and all the remaining traces.
- Documented actions and notes from the IR checklist

- Step 7: Make a malware response and DOS response.
- Step 8: Make sure if the incident was intentional or unintentional.
- Step 9:Make a regular backups and updates and system are patched.
- Step 10:Make a regular logs to all files.
- Step 11:Make sure you have a proper plan and mechanism until the incident is solved.