FINAL PROJECT TEMPLATE

THREAT SUMMARY

- **Summary of Situation:** Three hospitals A, B and C have noticed that when trying to log into their centralized log management system, a message popped out. The attacker encrypted all the personal files and the control systems used to monitor patient stats are no longer available through standard user interface. The attacker wants one million dollars in bitcoins to decrypt the personal files. The hospitals have disclosed that each incident started with a user in the technology department opening an email attachment resource. This activity has not yet been seen in hospital X.

- **Asset:** control systems, patient stats, doctor reports and log analysis tools

- **Impact:** Confidentiality, Integrity and Availability

- **Threat Actor: T**he attacker is the external threat. Criminals who want to steal sensitive data, money and personal information seeks financial gain. That's why here the attacker who is a cyber criminal has asked the staff (doctors and administrators) for a ransomware which is 1 million dollars in bitcoins. His potential is financial. the internal threat is the employee who opened the attachment in the email. Maybe the employee was security unaware and victim to social engineering, or maybe he do it intentionally either financially motivated or for revenge because he was terminated for example.

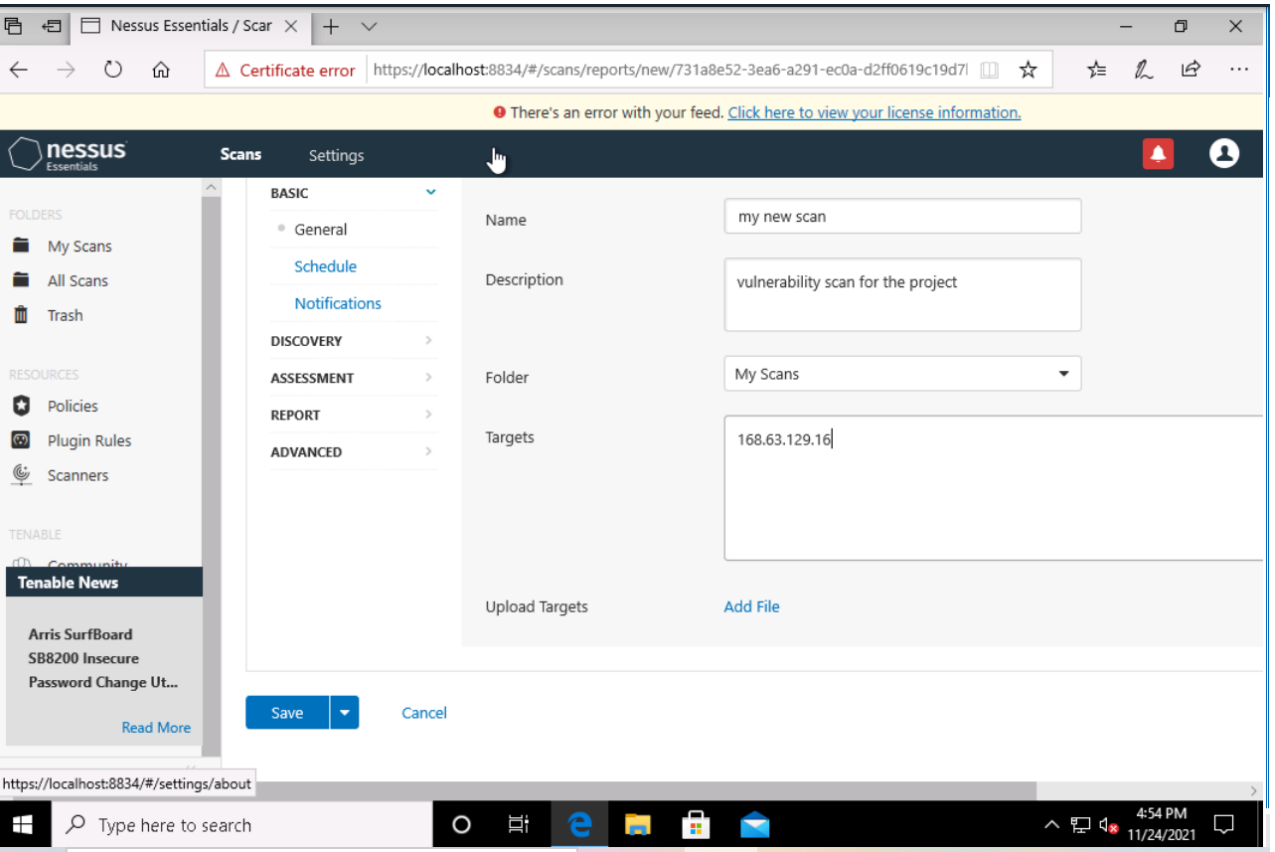
- **Threat Actor Motivation:** terminated people who seeks revenge by stealing data when they were leaving or for some how still have access even after termination and any employee that still working but is angry from the organization due to any reason. **Common Threat Actor Techniques:** there are two common threat actor techniques (intentionally and unintentionally).

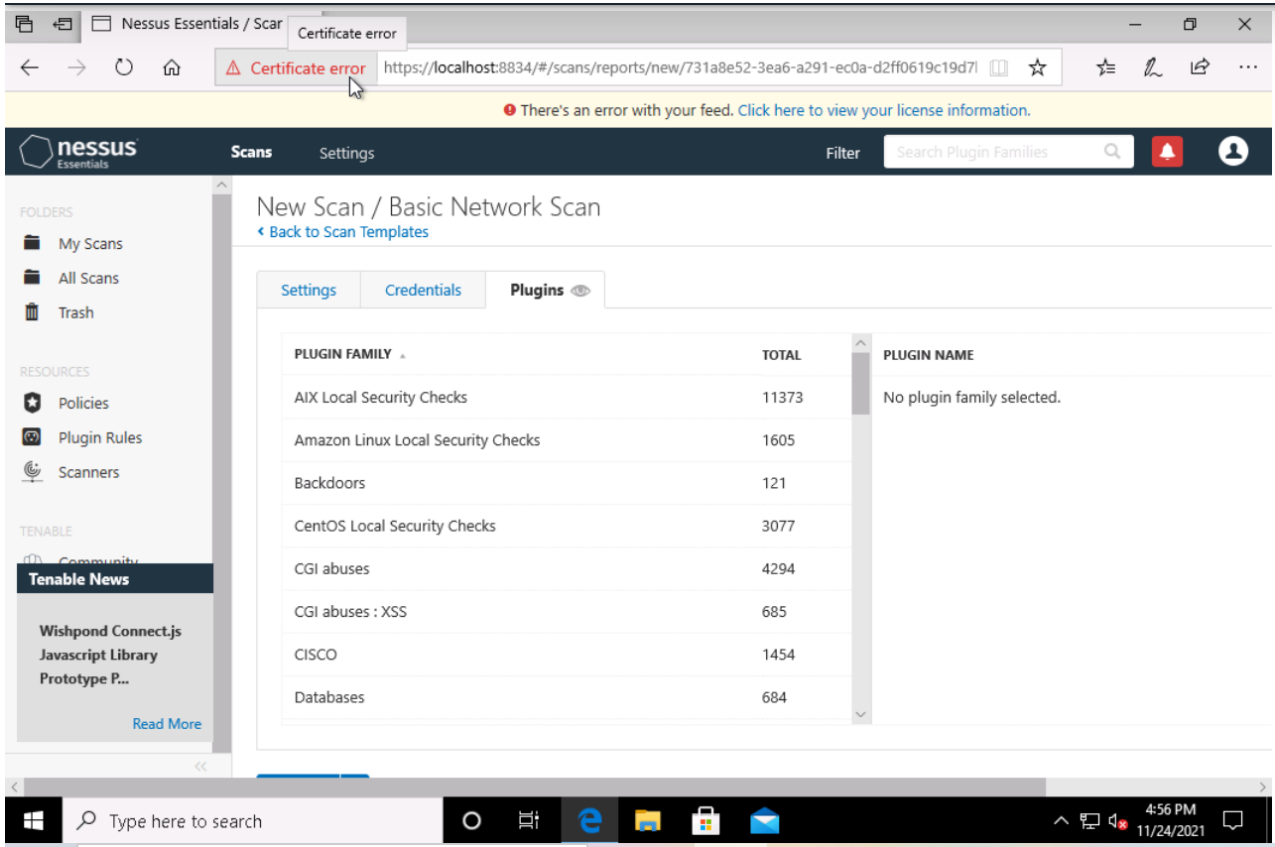
1) intentionally: attacker seeks to have access to sensitive data by using phishing or spear phishing. it is done through email attachments.

2) unintentionally: the victim employee who easily fall by social engineering and not aware to much by security

VULNERABILITY SCANNING TARGETS

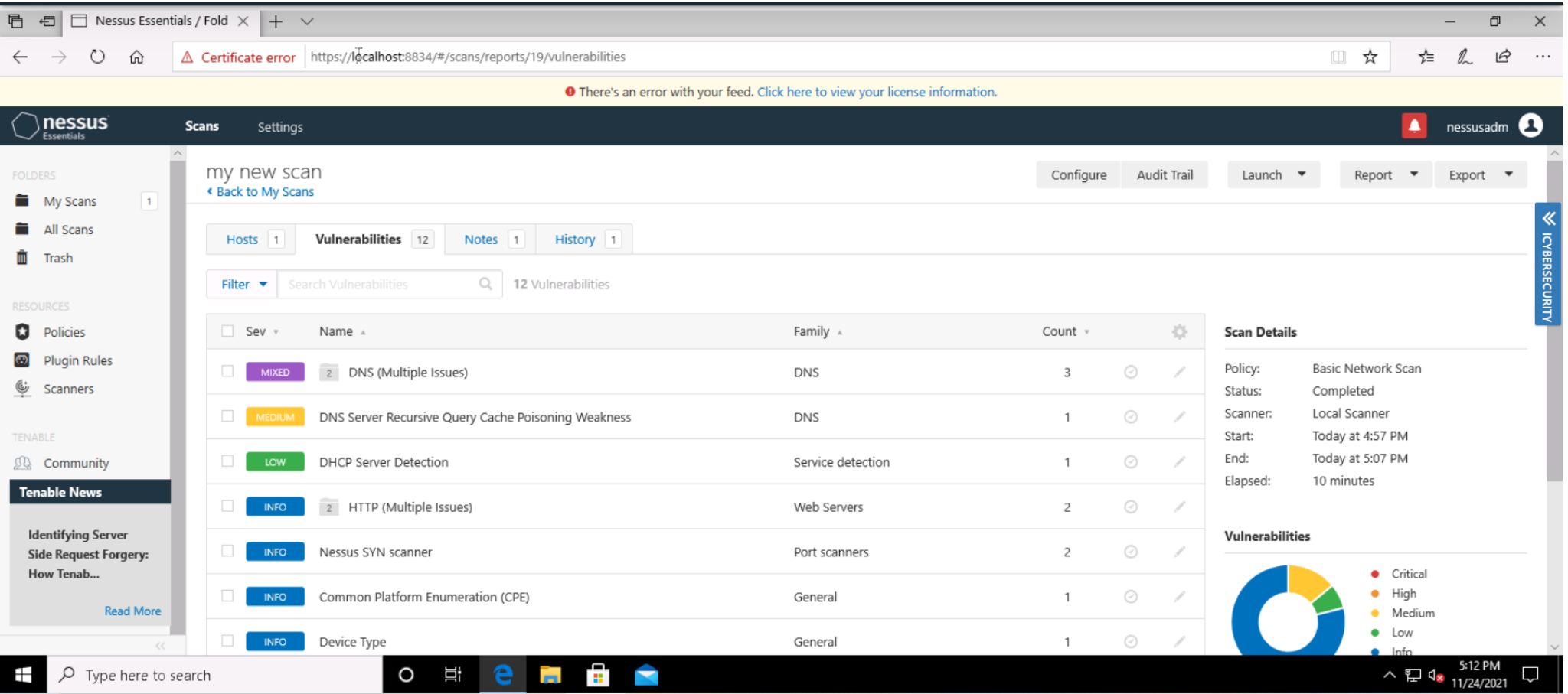
- **Summary of scan targets:**
  - Number of devices scanned: 1
  - Device type: windows 10 virtual machine
  - Primary purpose of device: general purpose





VULNERABILITY SCAN RESULTS

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



REMEDIATION RECOMMENDATION

- Fix within 7 days

Finding	Severity Rating	Recommended Fix
Fortunately, there isn't neither critical nor high risks available		

- Fix within 30 days

Finding	Severity Rating	Recommended Fix
DNS Server Recursive Query cache Poisoning Weakness	Medium	Recursive queries need to be restricted

- Fix within 60 days

Finding	Severity Rating	Recommended Fix
DHCP server detection	Medium	Remove any unused options and filter information

PASSWORD PENETRATION TEST OUTCOME

- **Methodology:** create two txt files, one contained the hashes and one contains the password list. Open command prompt and use cd to go to the hashcat file location, then type “hashcat –m 0 –a 0 hashes.txt my_cracked_passwords.txt”. Where “-m” is the type of the hash and “-a” is mode of the attack.
- **Number of passwords tested:** 35
- **Number of passwords cracked:** 5
- **Evidence of weak passwords:** cracked easily
- **Recommended steps to improve passwords security:** passwords must contain minimum of 12 characters including special characters, and to be updated each 2 months

```
C:\Users\karee\Downloads\hashcat-6.2.5>hashcat -m 0 -a 0 hashes.txt my_cracked_passwords.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.1 ) - Platform #1 [Intel(R) Corporation]
============================================================
* Device #1: Intel(R) UHD Graphics, 3200/6472 MB (1618 MB allocatable), 24MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

Administrator: Command Prompt

```
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 421 MB

Dictionary cache built:
* Filename..: my_cracked_passwords.txt
* Passwords.: 35
* Bytes.....: 299
* Keyspace..: 35
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

5f4dcc3b5aa765d61d8327deb882cf99:password
098f6bcd4621d373cade4e832627b4f6:test
fc5e038d38a57032085441e7fe7010b0:helloworld
8743b52063cd84097a65d1633f5c74f5:hashcat
0e9b09b77fc5391bf20f68095f867ed0:ihatepasswords

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: hashes.txt
Time.Started.....: Fri Nov 26 14:26:53 2021 (0 secs)
Time.Estimated...: Fri Nov 26 14:26:53 2021 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (my_cracked_passwords.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    18204 H/s (0.04ms) @ Accel:128 Loops:1 Thr:64 Vec:1
Recovered........: 5/5 (100.00%) Digests
Progress.........: 35/35 (100.00%)
Rejected.........: 0/35 (0.00%)
Restore.Point....: 0/35 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
```

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

■**Summarize ongoing incident:** all personal files of doctors, nurses and administrators are encrypted by an attacker who wants a ransom of 1 million dollars in bitcoins to decrypt their personal files. no one can access toe log analysis tool. The patient status can't be monitored anymore, and the doctors can't render any treatment. this is a critical security incident

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

- Step 1: cyber security professionals' team must be available right now
- Step 2: don't fulfil the attacker requirements and never pay him the 1 million dollar as he can use you again and again and ask more
- Step 3: use your backups that was done the last month to restore the personal files of the staff and the server
- Step 4: the incident source must be identified
- Step 5: the incident source must be isolated
- Step 6: think how to avoid paying ransom in a professional way that would not cause any additional harm to the organization
- Step 7: after solving the issue, a cybersecurity training must be done to all staff to make them aware from upcoming threats and to reduce the probability of the existence of a victim employee who has no security awareness
- Step 8: backups must be made on weekly basis

INCIDENT RESPONSE RECOMMENDED ACTION

Summarize recommendation to contain, eradicate, and recover:
search for the source incident. delete the email attachment and use backups to restore the personal files and the server. if the software is deleted then any remaining trace must be eliminated. the incident severity is high. doctors can't render treatments for patients because their status can't be accessed. many patients might die from this types of incidents. Therefore, the organization must ensure that all staff members have enough security awareness to deal with social engineering and such threats. and a weekly backup must be done to ensure the data availability

Documented actions and notes from the IR checklist

- Step 9: response for denial of service and malwares
- Step 10: determine the incident cause to take efficient actions and eliminate that incident from occurring again, also check if it is done intentionally or not
- Step 11: make sure that all patches are up to date
- Step 12: document what happened and recommendations to avoid these types of incident in the future