FINAL PROJECT TEMPLATE

THREAT SUMMARY

Summary of Situation: Multiple hospital in the area have been reached by hackers and now are under ransomware attacks.

Asset: Hospitals data**.**

Impact: What part of the CIA triad is being impacted?: *Confidentiality and Avialability.

Threat Actor: FIN4, that has targeted confidential information related to the public financial market, particularly regarding healthcare and pharmaceutical companies, since at least 2013.

Threat Actor Motivation: is a financially motivated threat group

Common Threat Actor Techniques: : Layer Protocol: Web Protocols, Command and Scripting Interpreter: Visual Basic , Email Collection: Remote Email Collection, Input Capture: Keylogging , Phishing: Spearphishing Attachment, User Execution: Malicious File

Hint: Carefully check the ransom note for additional clues.

VULNERABILITY SCANNING TARGETS

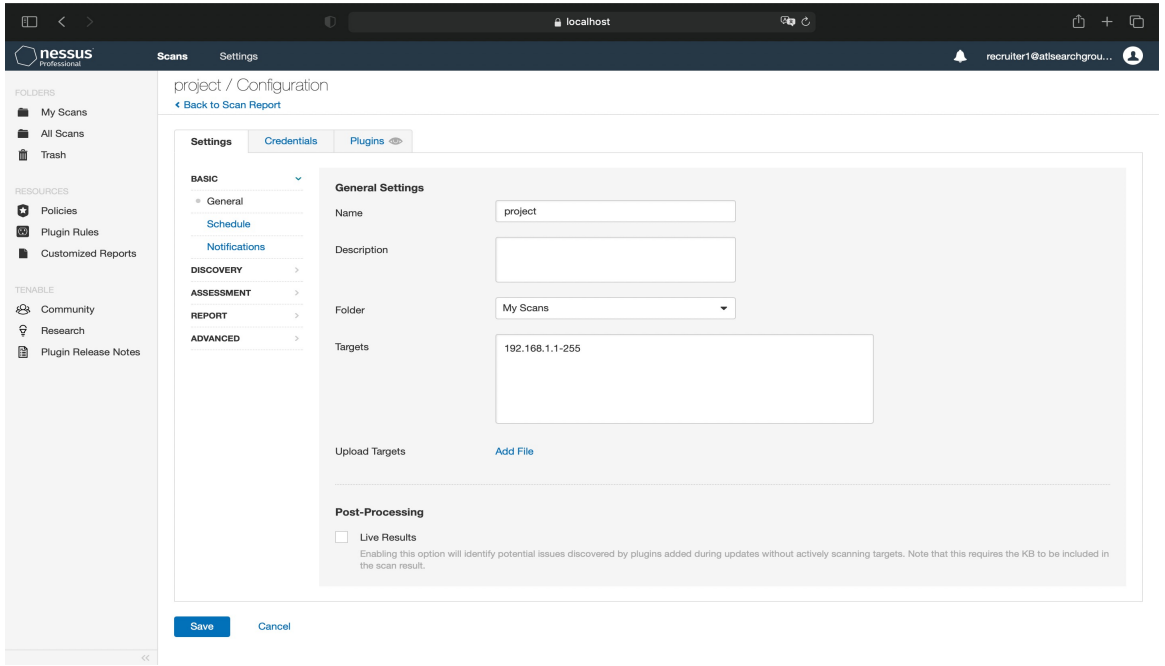
Summary of scan targets:

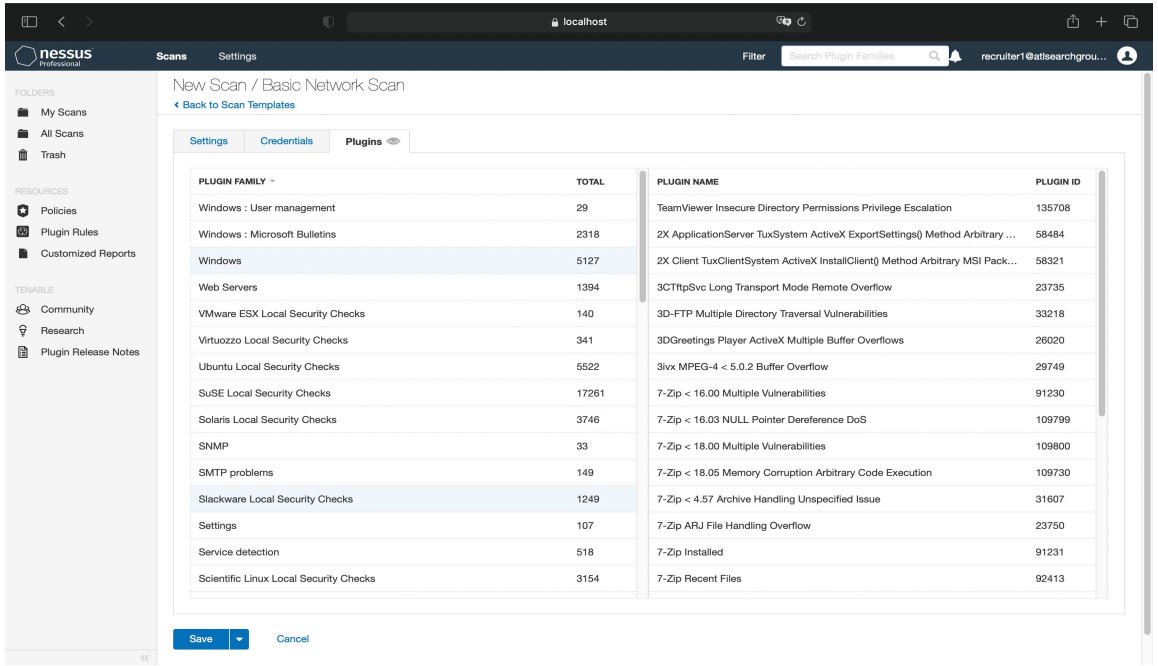
Number of devices scanned: (5) devices were scanned

Device type: Traget:(Windows 10 Pro) / Others: MACOS, Windows 10 Home.

Primary purpose of device: (Store Logs and backups)

(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:

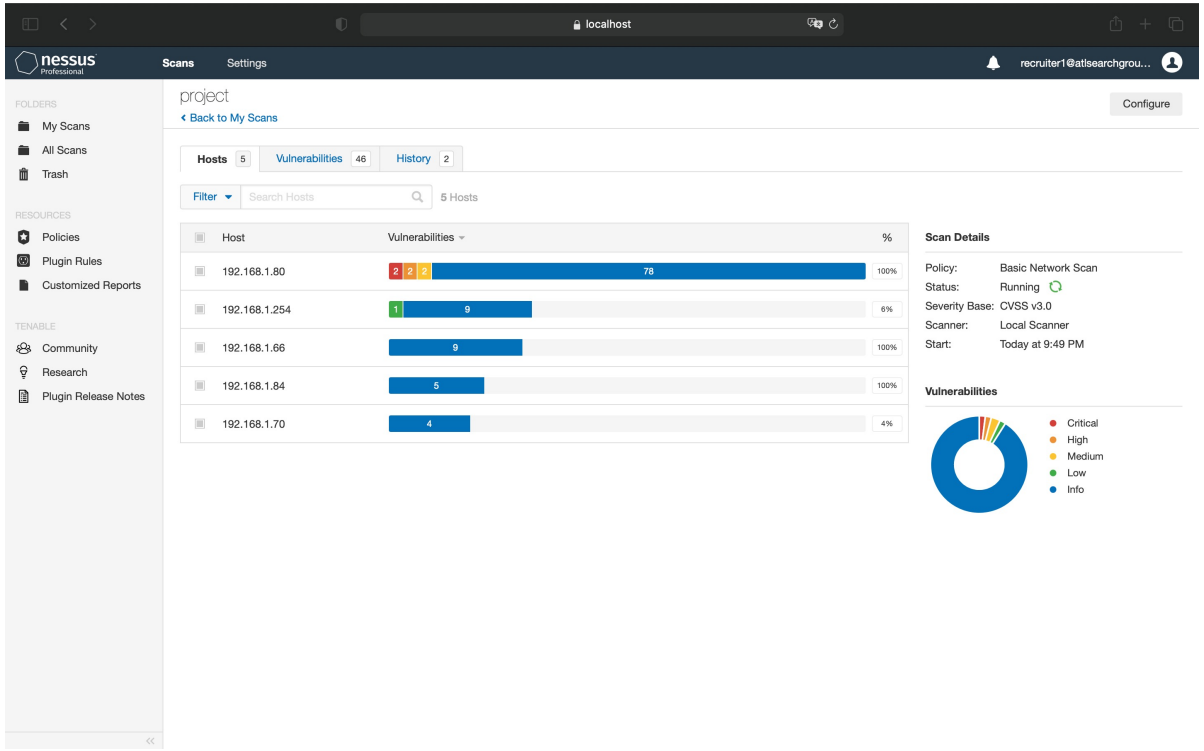
Critical: 1

High: 1

Medium: 2

Low: 0

(insert screenshot from scan results dashboard)



REMEDIATION RECOMMENDATION

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

Fix within 7 days

Finding	Severity Rating	Recommended Fix
Apache version 2.4.46	CVSS v3.0 Base Score 9.8	Upgrade to Apache version 2.4.47 or later.
Apache version 2.4.46	CVSS v3.0 Base Score 7.5	Upgrade to Apache version 2.4.48 or later.
server's X.509 certificate cannot be trusted	CVSS v3.0 Base Score 6.5	Purchase or generate a proper SSL certificate for this service

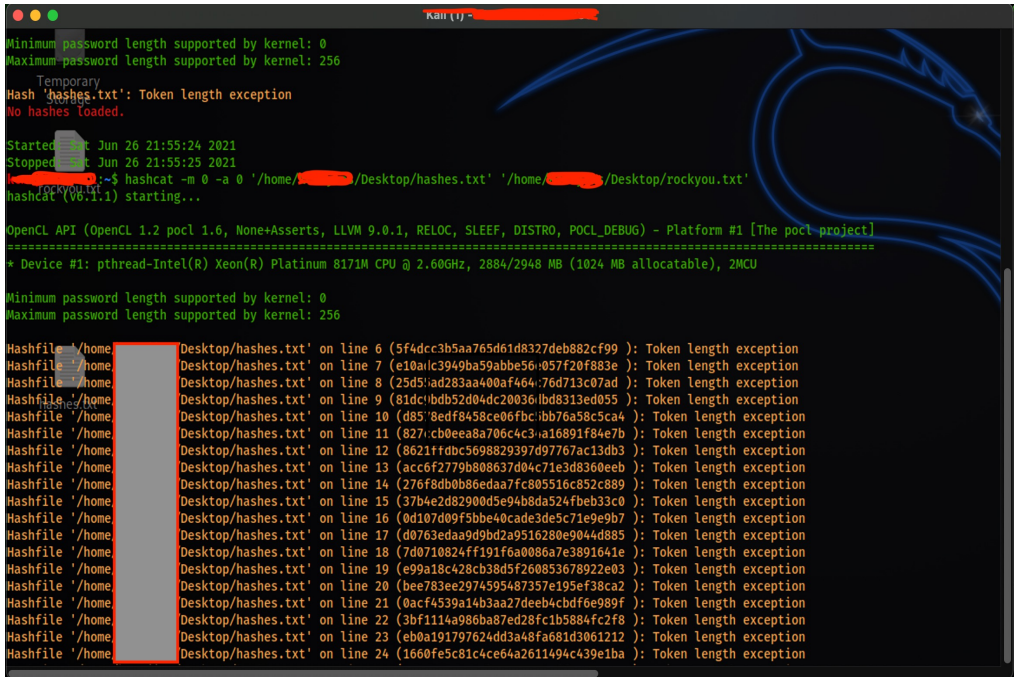
Fix within 30 days

Finding	Severity Rating	Recommended Fix
version of MySQL is 8.0.x prior to 8.0.24	CVSS v3.0 Base Score 5.5	MySQL version 8.0.24 or later

Fix within 60 days

Finding	Severity Rating	Recommended Fix

PASSWORD PENETRATION TEST OUTCOME



RECOMENDATIONS

- Configure a minimum password length.
- Enforce password history policy with at least 10 previous passwords remembered.
- Use passwords generators
- Enable the setting that requires passwords to meet complexity requirements. ...
- Reset local admin passwords every 180 days.

Methodology: (Created a Kali Linux VM> Used Hashcat> used hashes list> used Rockyou.txt list as a reference)

Number of passwords tested: (41)

Number of passwords cracked: (4)

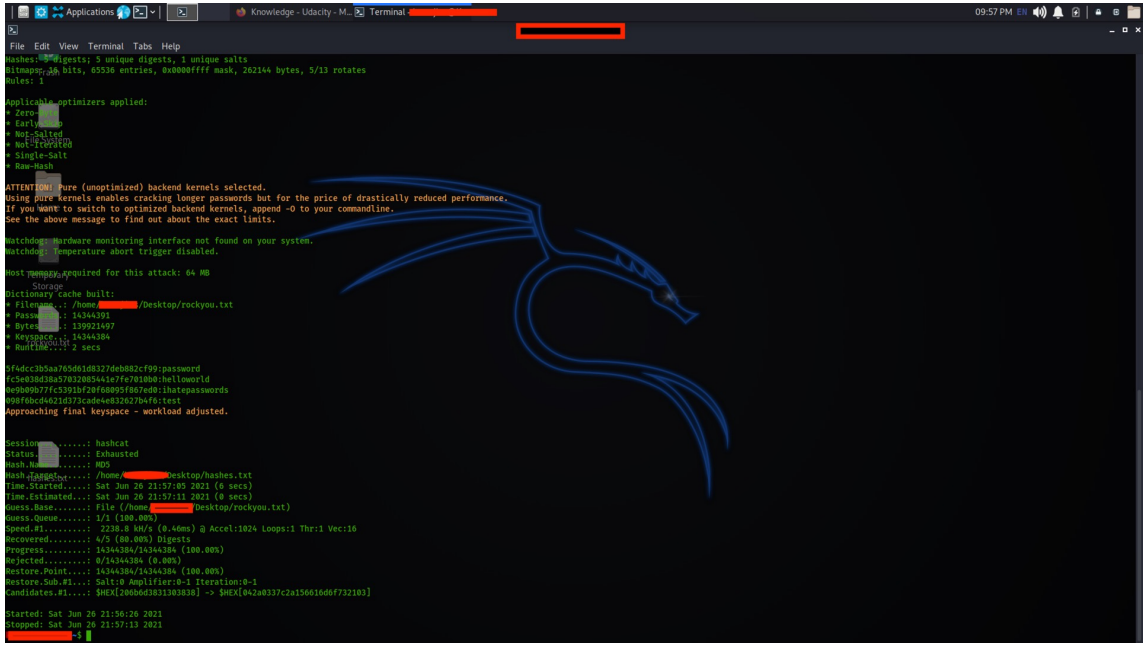
Evidence of weak passwords:

5f4dcc3b5aa765d61d8327deb882cf99:password

fc5e038d38a57032085441e7fe7010b0:helloworld

0e9b09b77fc5391bf20f68095f867ed0:ihatepasswords

098f6bcd4621d373cade4e832627b4f6:test



INCIDENT RESPONSE PRELIMINARY ASSESSMENT

Summarize ongoing incident:

What do you know so far?

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

- Step 1: End Users
- Step 2: Incident has a huge impact, doctors, nursers and hospitals personal aren't able to do their jobs, causing delays on treatments and even deaths due to lack of information and communication caused by the attack.

  The targeted systems are Windows machines/ 10.0.0.4
- Step 3: Incident is Confirmed.

  Incident is still in progress

  response is Urgent

  Responses will not alert attacker if so, it will not affect procedures

  This is Ransomware Attack (Virus)
- Step 4: Safety and human life is at risk, the IR team will make everything possible to ensure patients survival.
- Step 6: Ticket Category One(1) A treat to public safety or life

INCIDENT RESPONSE RECOMMENDED ACTION

Step 12:
-Consider whether an additional policy or technology could have prevented the intrusion:
Better Privileges Policies, firewall and malware protection and intrusion detections

-Was the incident response appropriate? How could it be improved? :
Incident response was appropriate but we could learn more from this event and improve procedures

-Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
They were detailed and covered the situation.

-What changes can be made to prevent a re-infection?
Update and improve Security policies.

-What lessons have been learned from this experience
Immediate and effective procedures following a ransomware attack.

Summarize recommendation to contain, eradicate, and recover:

Describe the overall recommended containment, eradication, and recovery plan

Documented actions and notes from the IR checklist

- Step 7: *Malware response procedure(ransomware) Isolate the systems infected by the malware, wipe the clean and restore systems fully from backups.*
- Step 8: IR team couldn't have access to logs
- Step 9: -Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
  -Make users change passwords if passwords may have been sniffed.
  -Ensure the system has been hardened by turning off or uninstalling unused services.
  -Ensure the system is fully patched.
  -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.