

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

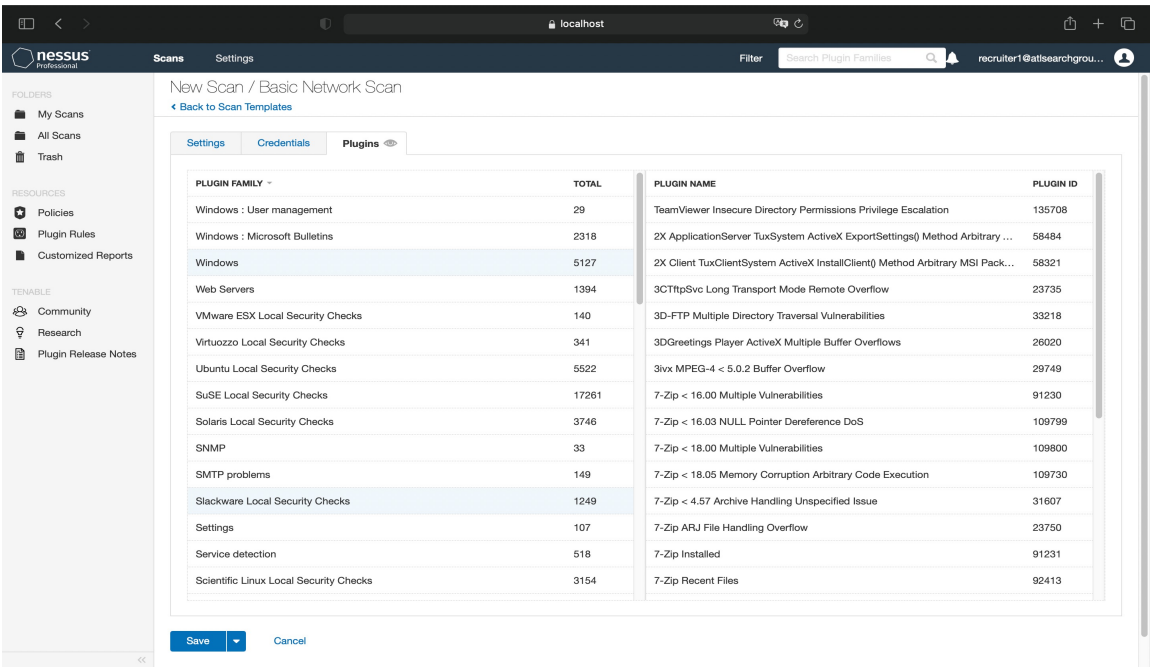
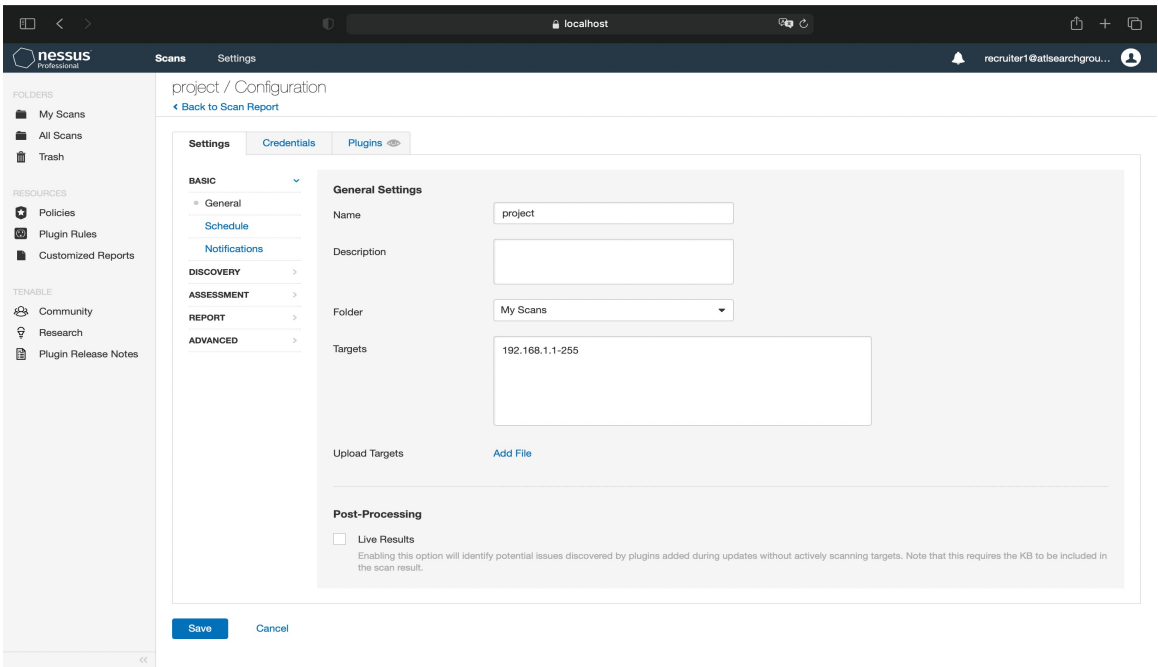
Summary of scan targets:

Number of devices scanned: (5) devices were scanned

Device type: Traget:(Windows I0 Pro) / Others: MACOS, Windows I0 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:

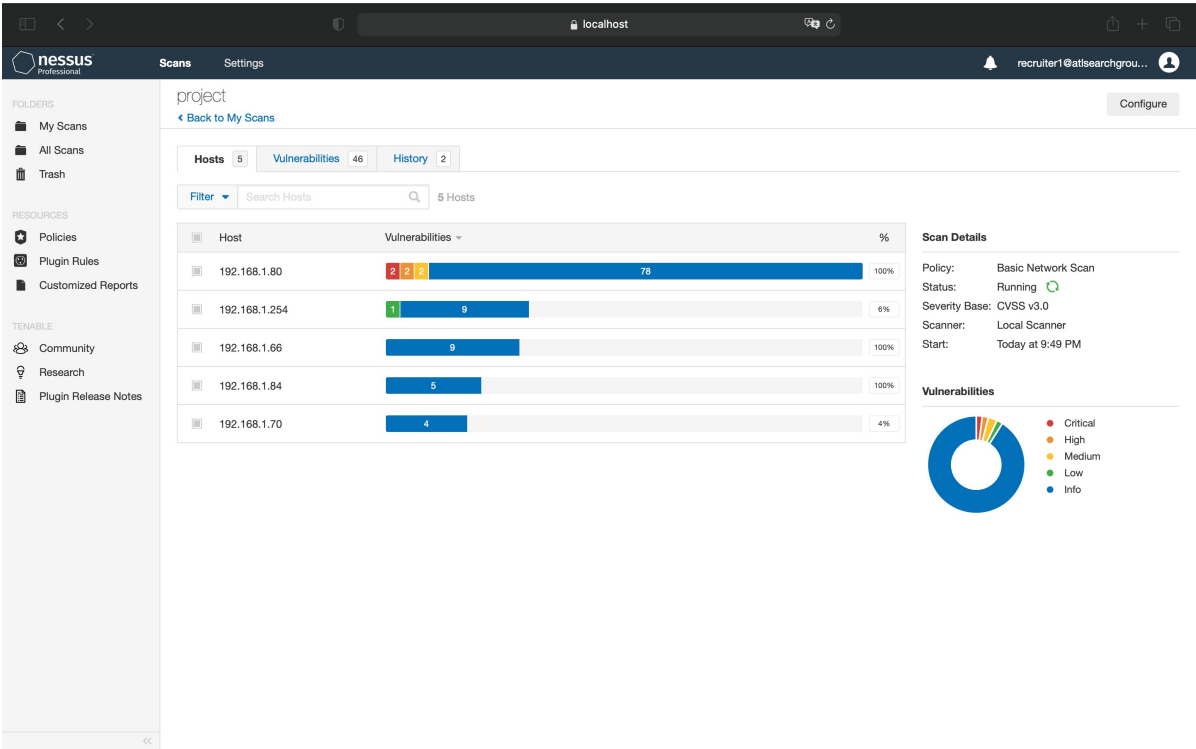
Critical: 1

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

```
Kali (1) - [REDACTED]
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Temporary
Hash 'hashes.txt': Token length exception
No hashes loaded.

Started: Sat Jun 26 21:55:24 2021
Stopped: Sat Jun 26 21:55:25 2021

[REDACTED]@kali:~$ hashcat -m 0 -a 0 '/home/[REDACTED]/Desktop/hashes.txt' '/home/[REDACTED]/Desktop/rockyou.txt'
hashcat (v6.11.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz, 2884/2948 MB (1024 MB allocatable), 2MCU

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

Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 6 (5f4dcc3b5aa765d61d8327deb882cf99) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 7 (e10a1c3949ba59abbe560057f20f883e) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 8 (25d5ead283aa400af46476d713c07ad) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 9 (81dc1b5b52d04dc200361bd8313ed055) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 10 (d85'8edf8458ce06fbc1bb76a58c5ca4) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 11 (8271cb0eea8a706c4c3a16891f84e7b) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 12 (8621f1dbc5698829397d97767ac13db3) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 13 (acc6f2779b808637d04c71e3d8360eeb) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 14 (276f8db0b86edaa7fc805516c852c889) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 15 (37b4e2d82900d5e94b8da524fbeb33c0) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 16 (0d107d09f5bbe40cade3de5c71e9e9b7) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 17 (d0763edaa9d9bd2a9516280e9044d885) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 18 (7d0710824ff191f6a0086a7e3891641e) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 19 (e99a18c428cb38d5f260853678922e03) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 20 (bee783ee2974595487357e195ef38ca2) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 21 (0ac4f539a14b3aa27deeb4cbdf6e989f) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 22 (3bf1114a986ba87ed28fc1b5884fc2f8) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 23 (eb0a191797624dd3a48fa681d3061212) : Token length exception
Hashfile '/home/[REDACTED]/Desktop/hashes.txt' on line 24 (1600fe5c81c4ce6a261149c439e1ba) : Token length exception
```

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:i hate passwords

098f6bcd4621d373cade4e832627b4f6:test

```
Applications | Knowledge - Udcity - M... | Terminal | 09:57 PM EN
File Edit View Terminal Tabs Help
Hashes: 41 Digests: 5 unique digests, 1 unique salts
Himemory: 26 bits, 65536 entries, 0x0000ffff mask, 202144 bytes, 5/13 rotates
Poles: 1

Applicable optimizers applied:
+ Zero
+ EarlyExit
+ No-Salt
+ No-1000000
+ Single-Salt
+ No-Mem

ATTENTION: Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

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

Host memory required for this attack: 64 MB
Storage
Dictionary Cache built:
+ Files: 1 /home/[REDACTED]/Desktop/rockyou.txt
+ Passwords: 14344391
+ Bytes: 1: 33922497
+ KeySpace: 14344394
+ Runtime: 1: 2 secs

5f4dcc3b5aa765d61d8327deb882cf99:password
fc5e038d38a57032085441e7fe7010b0:helloworld
0e9b09b77fc5391bf20f68095f867ed0:i hate passwords
098f6bcd4621d373cade4e832627b4f6:test
Approaching final keypace - workload adjusted.

Session: [REDACTED] hashcat
Status: [REDACTED] Exhausted
Hash Name: [REDACTED]
Hash File: [REDACTED] /home/[REDACTED]/Desktop/hashes.txt
Time Started: Sat Jun 26 21:57:05 2021 (6 secs)
Time Estimated: Sat Jun 26 21:57:11 2021 (6 secs)
Guess Base: [REDACTED] File (/home/[REDACTED]/Desktop/rockyou.txt)
Crack Speed: 171 (100.00%)
Loaded: [REDACTED] 2238.8 MiB/s (8.40ms) @ Accel:1024 Loops:1 Thr1: Vec:10
Recovered: [REDACTED] 4/5 (80.00%) Digests
Progress: [REDACTED] 14344394/14344394 (100.00%)
Rejected: [REDACTED] 0/14344394 (0.00%)
Restore Point: [REDACTED] 14344384/14344384 (100.00%)
Restore Sum: [REDACTED]
Candidate #1: [REDACTED] 5HEX[2908060531030303] -> 0MX[84240337c2a15681066732103]

Started: Sat Jun 26 21:56:56 2021
Stopped: Sat Jun 26 21:57:11 2021
```

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, nurses 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.