FINAL PROJECT TEMPLATE

THREAT SUMMARY

- **Summary of Situation:** (Summarize the current threat situation)
3 hospitals (Hospital A , hospital B and Hospital C) can not access their centeralized log management systems, there was a message it shown on the screen asking for a ransom to unlock the system and file recovery (decrepit files that FIN4 have it) , It start when one of the employee of Technology department opens an email attachment resource.

- **Asset:** (What assets are being targeted?) the log management system was no longer accessible also the control system used to monitor patient state and doctor reports feature was inaccessible .

- **Impact:** (What part of the CIA triad is being impacted?) the whole CIA triad being impacted

- **Threat Actor:** (Identify potential threat actors) intentional external threat actors.

Intentional threat: the employee who interacted with the attachment unintentionally caused the incident.

External threat: a financially-motivated threat group called FIN4.

- **Threat Actor Motivation:** (Share potential motivations behind the attacks) motivated by financial gain

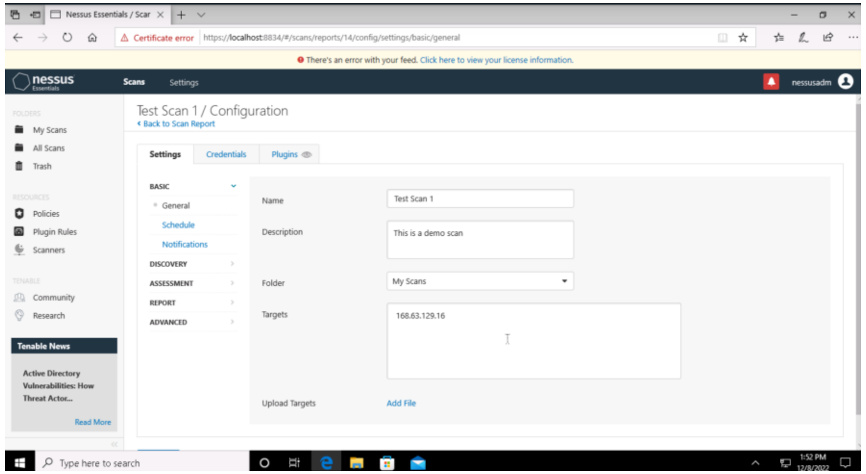
- **Common Threat Actor Techniques:** (Share attack methods commonly used by the threat actor.) Application Layer Protocol: Web Protocols, Proxy: Multi-hop Proxy and Phishing: Spearphishing Attachment etc.

- *Hint: Carefully check the ransom note for additional clues.*

VULNERABILITY SCANNING TARGETS

- **Summary of scan targets:**
  - Number of devices scanned: one device
  - Device type: (operating system and version) Microsoft windows 10
  - Primary purpose of device: (describe what the devices are used for and what kind of data might be on them) general purpose machine

(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)



Test Scan 1 / Configuration
‹ Back to Scan Report

Settings | Credentials | Plugins

BASIC
- General
- Schedule
- Notifications

DISCOVERY
ASSESSMENT
REPORT
ADVANCED

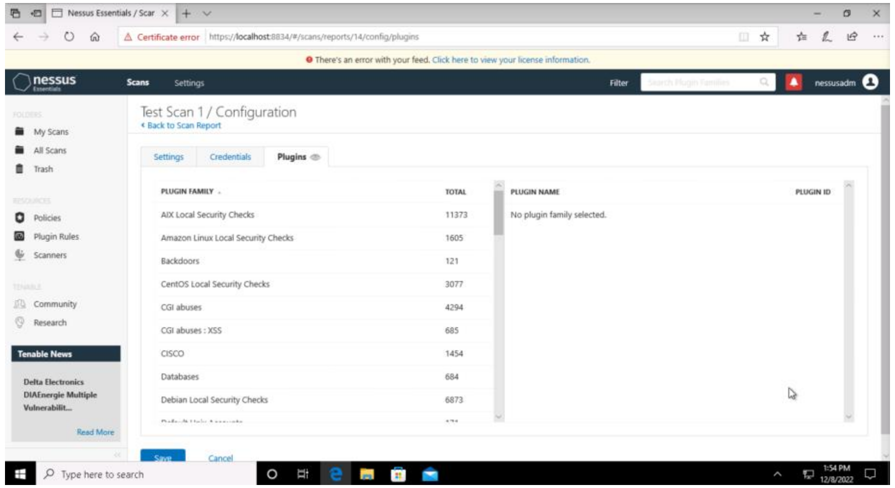
Name: Test Scan 1

Description: This is a demo scan

Folder: My Scans

Targets: 168.63.129.16

Upload Targets: Add File



Test Scan 1 / Configuration
‹ Back to Scan Report

Settings | Credentials | Plugins

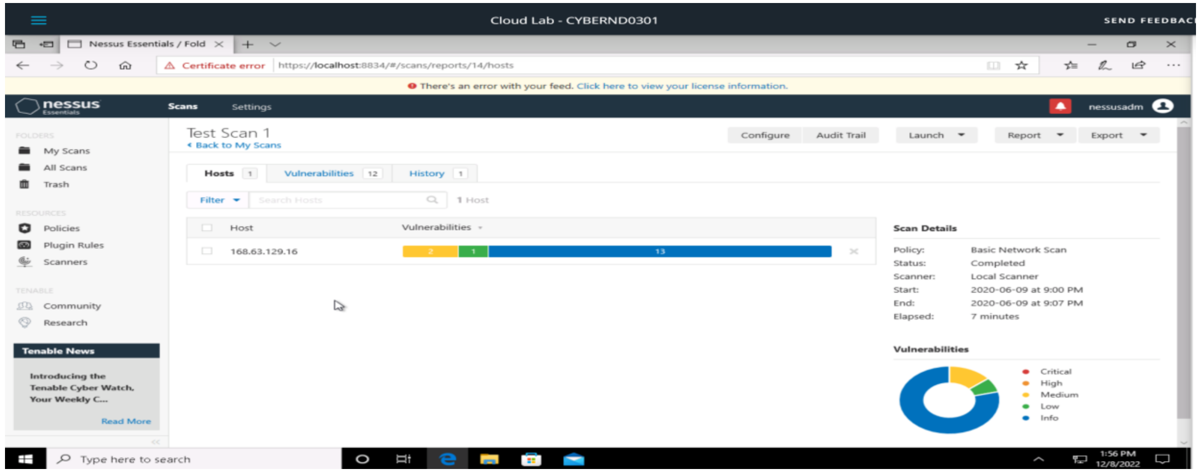
PLUGIN FAMILY	TOTAL
AIX Local Security Checks	11373
Amazon Linux Local Security Checks	1605
Backdoors	121
CentOS Local Security Checks	3077
CGI abuses	4294
CGI abuses : XSS	685
CISCO	1454
Databases	684
Debian Local Security Checks	6873

PLUGIN NAME	PLUGIN ID
No plugin family selected.	

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)



Cloud Lab - CYBERND0301

https://localhost:8834/#/scans/reports/14/hosts

There's an error with your feed. Click here to view your license information.

Test Scan 1

	Host	Vulnerabilities
□	168.63.129.16	2 1 13

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	2020-06-09 at 9:00 PM
End:	2020-06-09 at 9:07 PM
Elapsed:	7 minutes

Vulnerabilities

Tenable News

Introducing the Tenable Cyber Watch, Your Weekly C...

REMEDIATION RECOMMENDATION

- Fix within 30 days

Finding	Severity Rating	Recommended Fix
DNS server Request Amplification DDoS	medium	Restrict access to your DNS server from public network or configure it to reject such queries.
DNS cache poisoning	medium	Upgrade to the latest virion of bind.

- Fix within 60 days

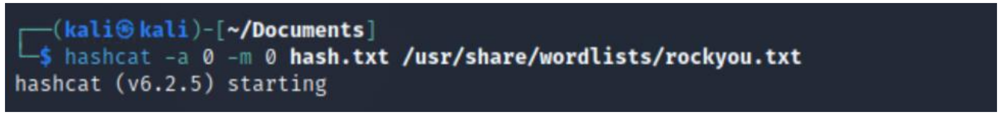
Finding	Severity Rating	Recommended Fix
DHCP server Detection	Low	Apply the filtering to keep this information off the network and remove any options that are not in use

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

PASSWORD PENETRATION TEST OUTCOME

- **Methodology:** (Summarize steps taken to test password security)

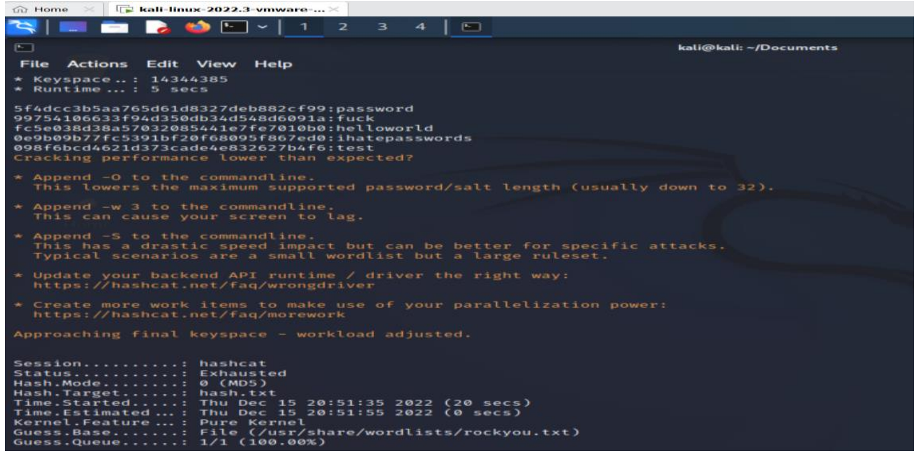
I used kali-linux and prepare hash file also used rockyou.txt .



```
┌──(kali㉿kali)-[~/Documents]
└─$ hashcat -a 0 -m 0 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.5) starting
```

Hashcat –a 0 –m 0 hash.txt /usr/share/wordlists/rockyou.txt
-a0 : means Dictionary attack
-m0 : means MD5 Algorithm

- **Number of passwords tested:** (insert number) 41
- **Number of passwords cracked:** (insert number) 5
- **Evidence of weak passwords:**



```
* Keyspace..: 14344385
* Runtime ...: 5 secs

5f4dcc3b5aa765d61d8327deb882cf99:password
99754106633f94d350db34d548d6091a:fuck
fc5e038d38a57032085441e7fe7010b0:helloworld
0e9b09b77fc5391bf20f68095f867ed0:ihatepasswords
098f6bcd4621d373cade4e832627b4f6:test
Cracking performance lower than expected?

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

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

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* 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

Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: hash.txt
Time.Started.....: Thu Dec 15 20:51:35 2022 (20 secs)
Time.Estimated ...: Thu Dec 15 20:51:55 2022 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
```

- **Recommended steps to improve passwords security:** (Summarize best practice recommendations to avoid brute force attacks in the future)

Uses a combination of symbols (@ # $ % & * - _) , upper&Lower case letters , Numbers and also I prefer to use phrases , make sure password length at least 10-12 , change your password Periodically (60 to 90 days).

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

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

  The system was hit by a ransomware attack , preventing administrators , doctors and nurses from accessing the system by encrypting of all system files .

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

- Step 1: the incident was discovered by the helpdesk and end-users.
- Step 2: the ransom message was the indicator of compromise, the impact that doctors cannot reach to patient reports so they cannot provide them the treatment, Name of system being targeted is(The control systems used to monitor patient stats)
- Step 3: the incident was confirmed, and we can not access to the system, and it is still in progress. It is a malware (ransomware)
- Step 4: human life at immediate risk
- Step 6: Category one - A threat to public safety or life.

(Add another slide if needed)

INCIDENT RESPONSE RECOMMENDED ACTION

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

  Starting by isolating the affected system because if they are in the same network will explore other system

  Delete the system and recover from backup system and restore the update which is missing that allow the attack happened .

  Finally document all steps and lessons to better respond in future.
- Documented actions and notes from the IR checklist

- Step 7: *(Tip: Select procedures you'd recommend for this type of incident) procedure that should the IR team follow is Malware response procedure*
- Step 8: ensuring business continuity by preparing temporary procedures may use digital forensic techniques, including reviewing system logs, checking computer activity
- Step 9:Re-install the affected system(s) from scratch and restore data from backups if necessary.
- Step 12: Document all steps and lessons to better respond in futures.

(Add another slide if needed)