FINAL PROJECT TEMPLATE

THREAT SUMMARY

- **Summary of Situation:**

Ransomware is a form of malicious software that locks up the files on the computer, encrypts them, and demands that you pay to get your files back. When a system is infected, a pop up window appears, prompting you to pay to recover all your files ,with a countdown timer on the left of the window. It adds that if you fail to pay within that time, the fee will be doubled, and if you don’t pay you will lose the files forever.

The incident start with user in technology department installing email attachment,its occur to hospital A, B and C, it didn't reach hospital x at 9:00 am monday

at 11:00 am monday we receive report that five more hospital been hit by the same attack , All hospitals have a few things in common, they all endorsed the new healthcare law, we notice that the attacker targeting windows system unpatched that contain centralized log files and backups

at 1:00pm monday, we receive that doctors and administrative staff have been asked to pay ransom to access the systems , both control system and log analysis tool are no longer available

THREAT SUMMARY

Asset:

Hospitals data and patient personal information,patient control systems and log management servers

- **Impact:**

  its effect all of CIA tride , for availability its deny the access to data ,for confidentiality loss and theft of personal info if not pay ransom, for integrity as hackers could access and change data such as patient health records

- **Threat Actor:**

  Cyber criminals , Criminal insiders, Oblivious insiders،FIN4 criminal group

- **Threat Actor Motivation:**

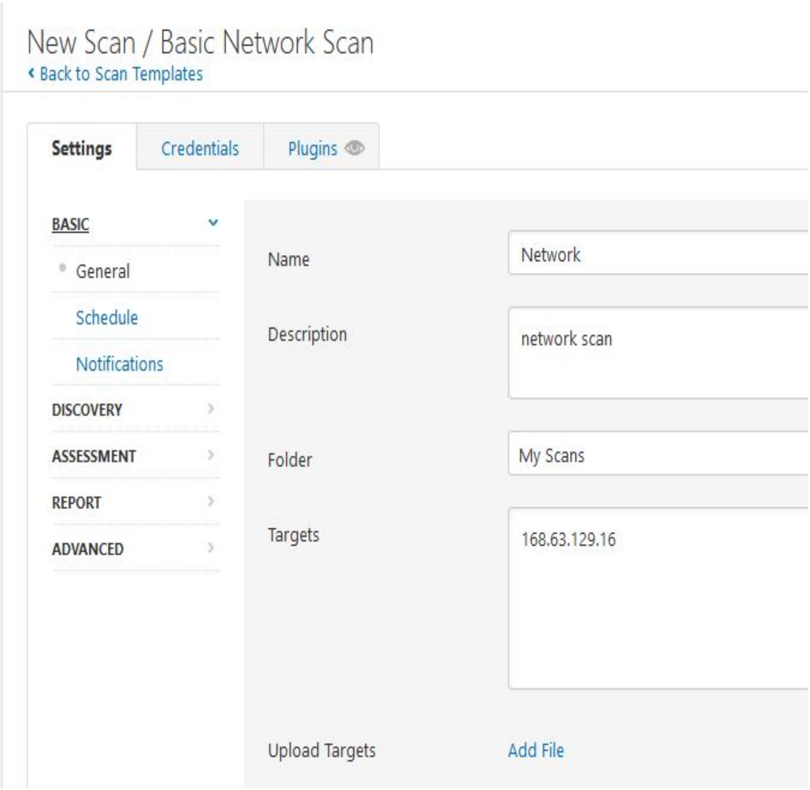
  financially motivated and hacktivists

- **Common Threat Actor Techniques:**

  Email accounts - T1586 , Spearphishing Attachment - T1193 ,Service Execution -T1035, File and Directory Discovery -T1083,FIN4 criminal group,Data Encrypted for Impact -T1486

VULNERABILITY SCANNING TARGETS

- **Summary of scan targets:**
  - Number of devices scanned: one
  - Device type: windows
  - Primary purpose of device: log files and backups



New Scan / Basic Network Scan

‹ Back to Scan Templates

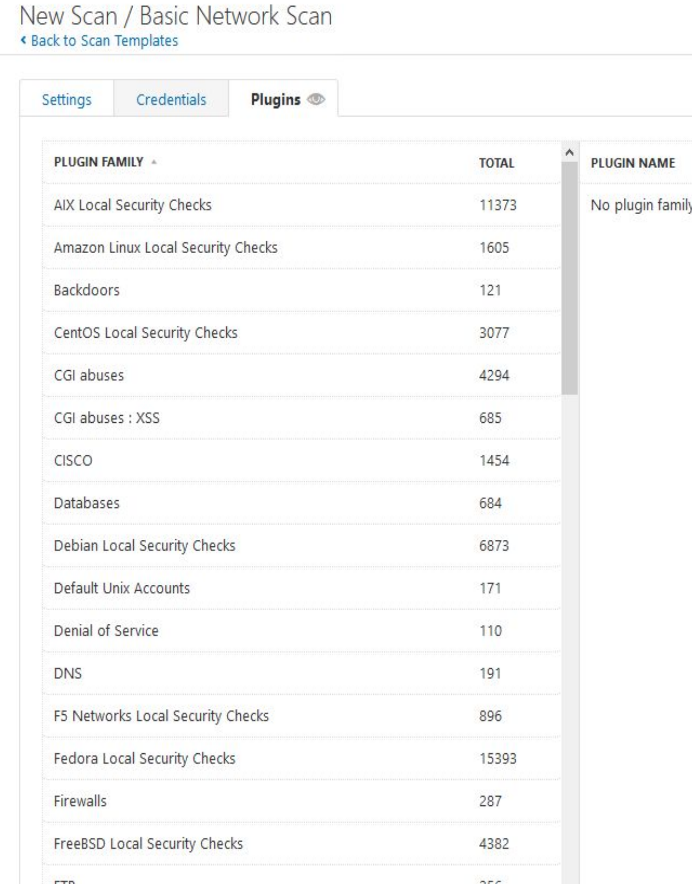
Name: Network

Description: network scan

Folder: My Scans

Targets: 168.63.129.16

Upload Targets: Add File



New Scan / Basic Network Scan

‹ Back to Scan Templates

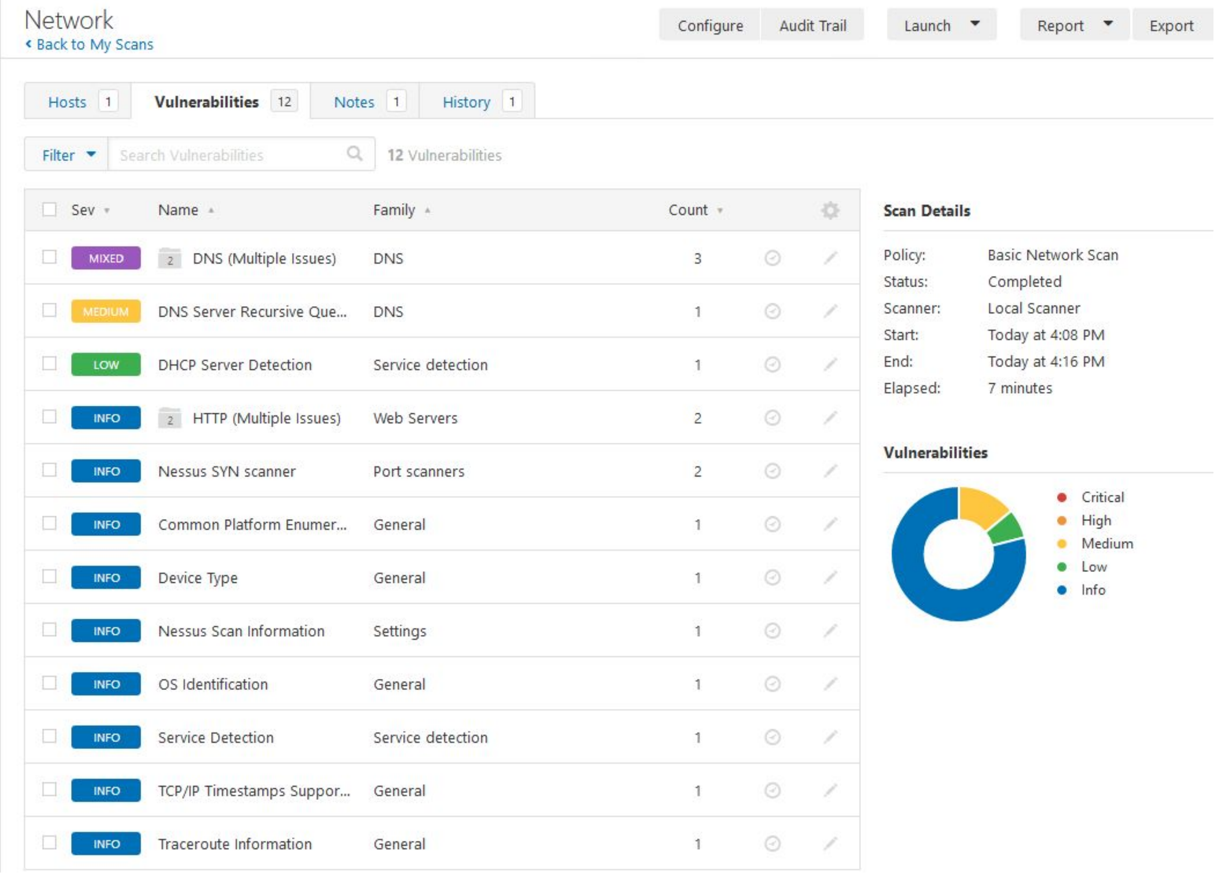
PLUGIN FAMILY	TOTAL
AIX Local Security Checks	11373
Amazon Linux Local Security Checks	1605
Backdoors	121
CentOS Local Security Checks	3077
CGI abuses	4294
CGI abuses : XSS	685
CISCO	1454
Databases	684
Debian Local Security Checks	6873
Default Unix Accounts	171
Denial of Service	110
DNS	191
F5 Networks Local Security Checks	896
Fedora Local Security Checks	15393
Firewalls	287
FreeBSD Local Security Checks	4382
FTP	256

PLUGIN NAME

No plugin family

VULNERABILITY SCAN RESULTS

- **Summary of findings:**
  - Total number of actionable findings:
    - Critical: 0
    - High: no high
    - Medium:2
    - Low:1



Network

‹ Back to My Scans

12 Vulnerabilities

☐	Sev	Name	Family	Count
☐	MIXED	2 DNS (Multiple Issues)	DNS	3
☐	MEDIUM	DNS Server Recursive Que...	DNS	1
☐	LOW	DHCP Server Detection	Service detection	1
☐	INFO	2 HTTP (Multiple Issues)	Web Servers	2
☐	INFO	Nessus SYN scanner	Port scanners	2
☐	INFO	Common Platform Enumer...	General	1
☐	INFO	Device Type	General	1
☐	INFO	Nessus Scan Information	Settings	1
☐	INFO	OS Identification	General	1
☐	INFO	Service Detection	Service detection	1
☐	INFO	TCP/IP Timestamps Suppor...	General	1
☐	INFO	Traceroute Information	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 4:08 PM
End:	Today at 4:16 PM
Elapsed:	7 minutes

Vulnerabilities

REMEDIATION RECOMMENDATION

- Fix within 7 days

Finding	Severity Rating	Recommended Fix

- Fix within 30 days

Finding	Severity Rating	Recommended Fix
DNS Server Spoofed Request Amplification DDoS CVE-2006-0987	Medium	Restrict access to your DNS server from public network or reconfigure it to reject such queries.

- Fix within 60 days

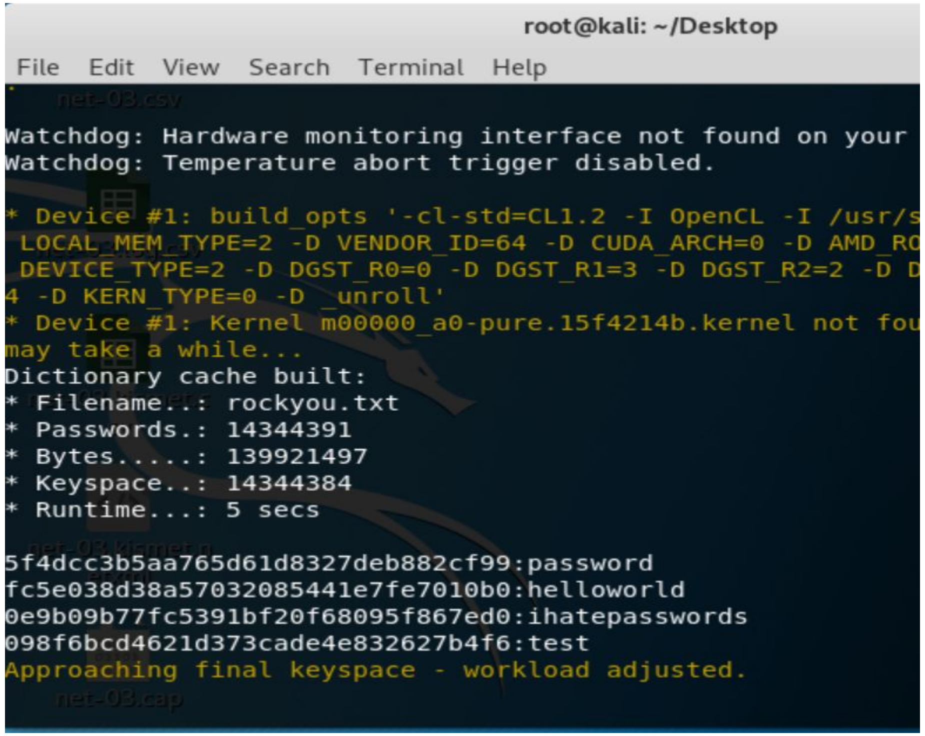
Finding	Severity Rating	Recommended Fix
DNS cache poisoning via BIND CVE-1999-0024	Medium	Restrict recursive queries to the hosts that should use this nameserver
optional : **DHCP Server Detection**	Low	Apply filtering to keep this information off the network and remove any options that are not in use

PASSWORD PENETRATION TEST OUTCOME

- **Methodology:** Dictionary Attack Mode
- **Number of passwords tested:** 14344391 **:** rockyou.txt
- **Number of passwords cracked:** 4
- **Recommended steps to improve passwords security:**

  Capital and small letters , Sepicail symbol , Avoid Personal Information.

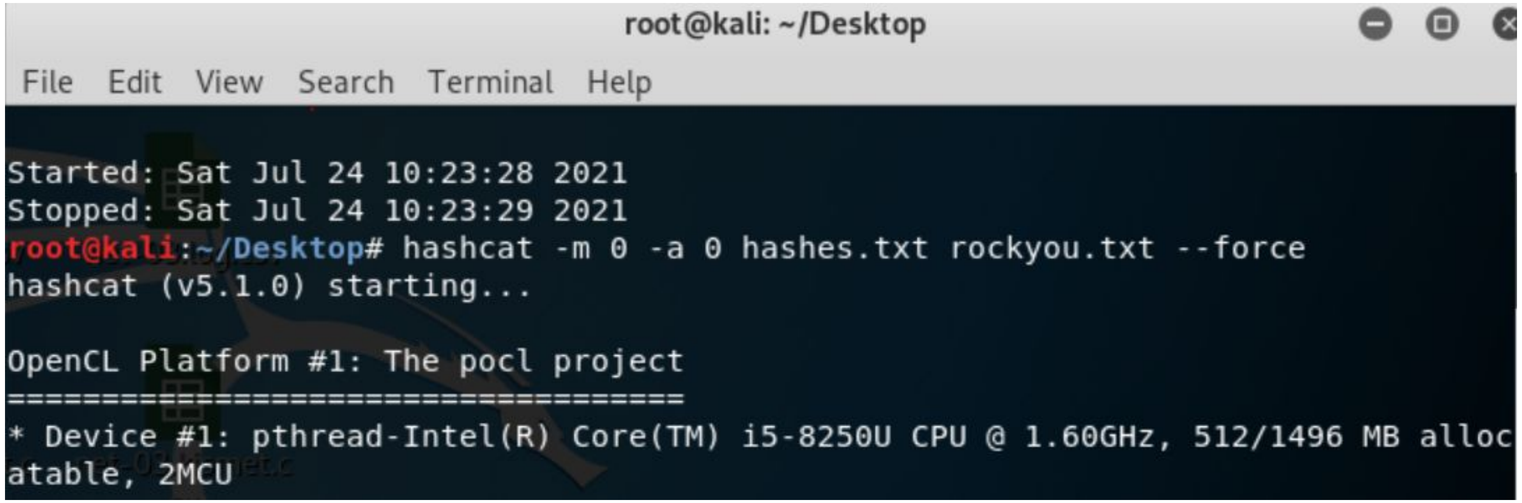
  - **Evidence of weak passwords:**



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

* Device #1: build_opts '-cl-std=CL1.2 -I OpenCL -I /usr/s
 LOCAL_MEM_TYPE=2 -D VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_RO
 DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R1=3 -D DGST_R2=2 -D D
4 -D KERN_TYPE=0 -D _unroll'
* Device #1: Kernel m00000_a0-pure.15f4214b.kernel not fou
may take a while...
Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 5 secs

5f4dcc3b5aa765d61d8327deb882cf99:password
fc5e038d38a57032085441e7fe7010b0:helloworld
0e9b09b77fc5391bf20f68095f867ed0:ihatepasswords
098f6bcd4621d373cade4e832627b4f6:test
Approaching final keyspace - workload adjusted.
```



```
Started: Sat Jul 24 10:23:28 2021
Stopped: Sat Jul 24 10:23:29 2021
root@kali:~/Desktop# hashcat -m 0 -a 0 hashes.txt rockyou.txt --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 512/1496 MB alloc
atable, 2MCU
```

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- Summarize ongoing incident:
  - ransomware attack preventing from accessing the data
- Document actions or notes from the following steps of the initial incident response checklist

❑ Step 1:

Helpdesk team

❑ Step 2:

Temporary denied access or permanent loss of sensitive information,disruption to regular operations and financial losses incurred to restore systems and files.

Hospital X , windows 10 , 20.57.54.121

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- Step 3:

  the incident it's confirmed and still in progress , and it's urgent to respond carefully to not alert the attacker its called ransomware

- Step 4:

  its doesnt affect any human life risk

- Step 6:

  category two - a threat to sensitive data , cause its block the access to data in computer

INCIDENT RESPONSE RECOMMENDED ACTION

- Summarize recommendation to contain, eradicate, and recover:
  - Prevent the infection from spreading by separating all infected computers from each other, shared storage, and the network.,Report to the authorities to support and coordinate measures to counter attack,Use safe backups and program and software sources to restore,Make an assessment of how the infection occurred and what you can do to put measures into place that will prevent it from happening again
- Documented actions and notes from the IR checklist
  - Step 7: *Malware response procedure*
  - Step 8: multiple attempt failed to login
  - Step 9 : Rise security awareness training and Data backup and recovery
  -

INCIDENT RESPONSE RECOMMENDED ACTION

- Step 12:
- employee security training policy and spread awareness to end user will definitely prevent the incident from happening . and patching the system regularly to prevent any exploit.
- The incident response could be improved by focusing at the end user security awareness and training