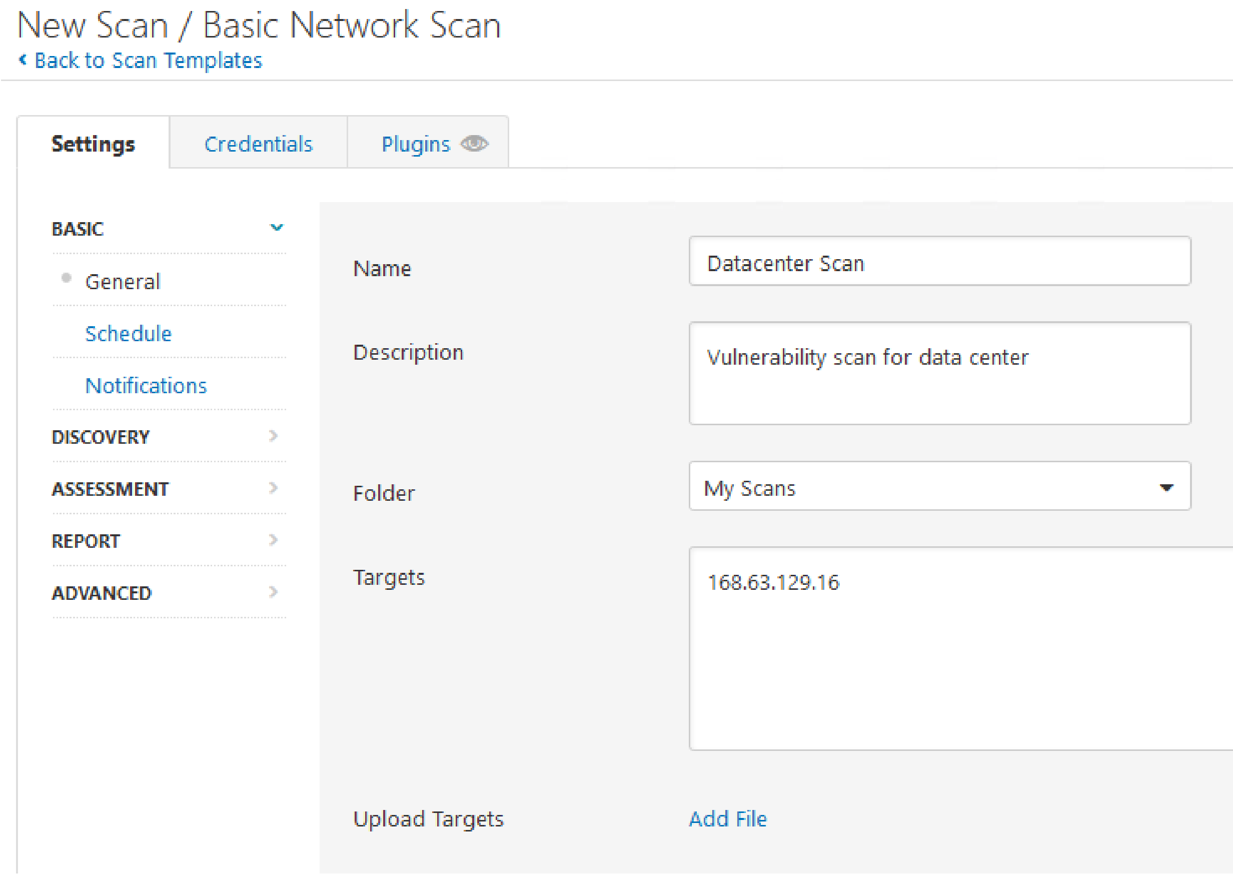
Hospital X Incident Report

THREAT SUMMARY

- **Summary of Situation:** A new healthcare legislation was announced this morning that negatively impacts millions of patients around the world, and masses are outraged. Soon after the announcement, 3 different hospitals called A, B and C in our partner network were hit with ransomware attacks that shut down their entire operations. FBI believes that this is not the last in the string of hits. The hospitals 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:** Personal documents and files of the centralized log management system, control systems used to monitor patient stats
- **Impact:** Confidentiality, Integrity, Availability
- **Threat Actor:**
  - **FIN4 – Financially-motivated threat group that has targeted confidential information related to the public financial market, particularly regarding healthcare and pharmaceutical companies, since at least 2013.**
  - External Threat – Cyber Criminal, Hacktivists
  - Insider Threat – Criminal, Oblivious, Third-party, Disgruntled, Terminated
- **Threat Actor Motivation:** It’s likely an attack on hospitals in favor of new healthcare legislation for advanced political or social causes. It could be a financial attack disguised as a hacktivist. In case of Insider threat motivations, it could be diverse. It could be intentional or unintentional. Just by mistake or premediated for money or disgruntled employee clicked intentionally even they knew its suspicious.
- **Common Threat Actor Techniques**
  - Intentional threats – Phishing, Spear phishing, Ransomware, Keylogger, Valid accounts
  - Unintentional threats – Using human error by social engineering security unaware employees to make them open email attachment which is malicious program or to gain passwords or credentials.

VULNERABILITY SCANNING TARGETS

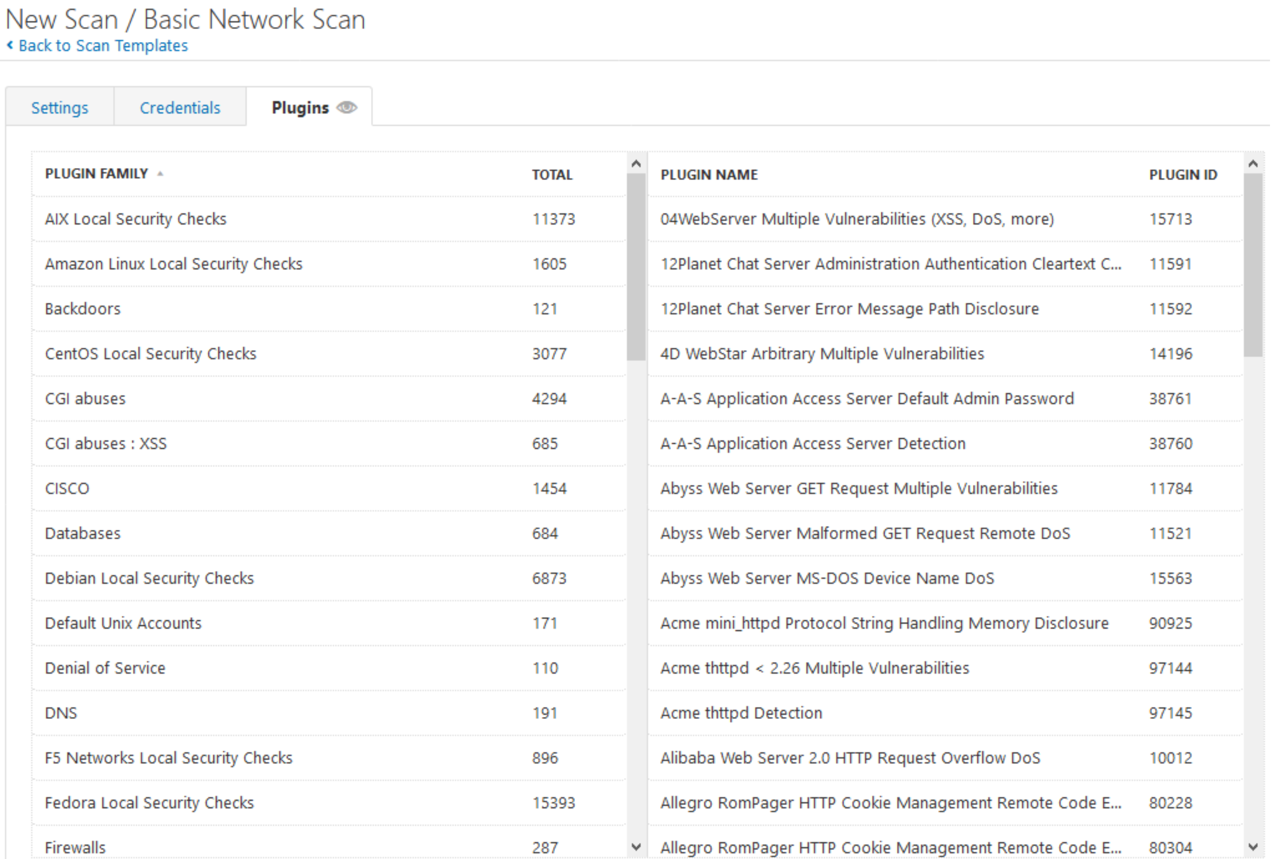
- **Summary of scan targets:**
  - Number of devices scanned: 1
  - Device type: VM(Virtual Machine)
  - Primary purpose of device: The device is used for data center that contain centralized log files and backups



New Scan / Basic Network Scan

‹ Back to Scan Templates

Name	Datacenter Scan
Description	Vulnerability scan for data center
Folder	My Scans
Targets	168.63.129.16
Upload Targets	Add File



New Scan / Basic Network Scan

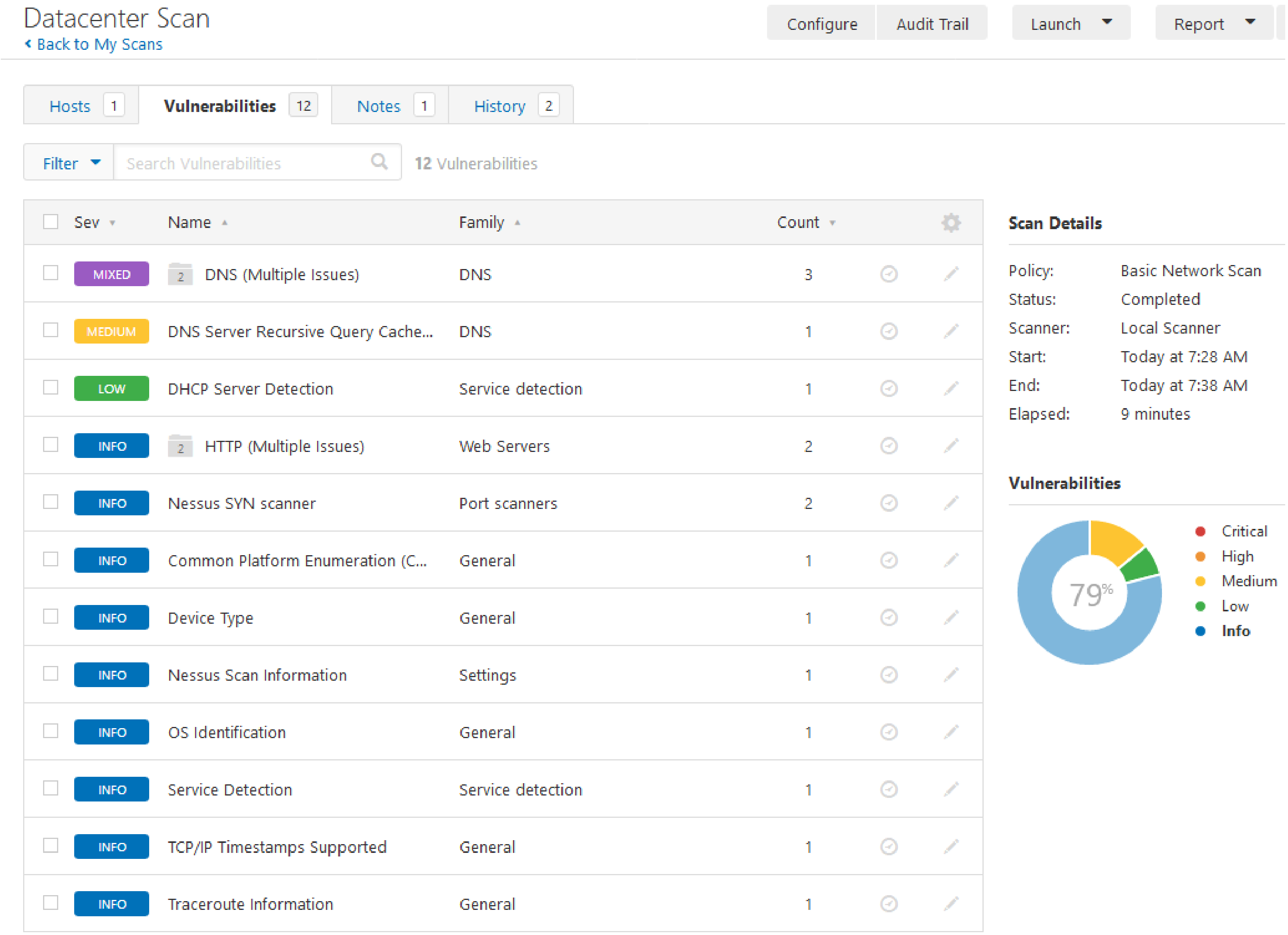
‹ Back to Scan Templates

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

PLUGIN NAME	PLUGIN ID
04WebServer Multiple Vulnerabilities (XSS, DoS, more)	15713
12Planet Chat Server Administration Authentication Cleartext C...	11591
12Planet Chat Server Error Message Path Disclosure	11592
4D WebStar Arbitrary Multiple Vulnerabilities	14196
A-A-S Application Access Server Default Admin Password	38761
A-A-S Application Access Server Detection	38760
Abyss Web Server GET Request Multiple Vulnerabilities	11784
Abyss Web Server Malformed GET Request Remote DoS	11521
Abyss Web Server MS-DOS Device Name DoS	15563
Acme mini_httpd Protocol String Handling Memory Disclosure	90925
Acme thttpd < 2.26 Multiple Vulnerabilities	97144
Acme thttpd Detection	97145
Alibaba Web Server 2.0 HTTP Request Overflow DoS	10012
Allegro RomPager HTTP Cookie Management Remote Code E...	80228
Allegro RomPager HTTP Cookie Management Remote Code E...	80304

VULNERABILITY SCAN RESULTS

- **Summary of findings:**
  - Total number of actionable findings: 12
    - Critical: 0
    - High: 0
    - Medium: 2
    - Low: 1



Sev	Name	Family	Count
MIXED	2 DNS (Multiple Issues)	DNS	3
MEDIUM	DNS Server Recursive Query Cache...	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 Enumeration (C...	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 Supported	General	1
INFO	Traceroute Information	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 7:28 AM
End:	Today at 7:38 AM
Elapsed:	9 minutes

Vulnerabilities

REMEDIATION RECOMMENDATION

- Fix within 7 days

Finding	Severity Rating	Recommended Fix
No Critical or high vulnerabilities found		

- Fix within 30 days

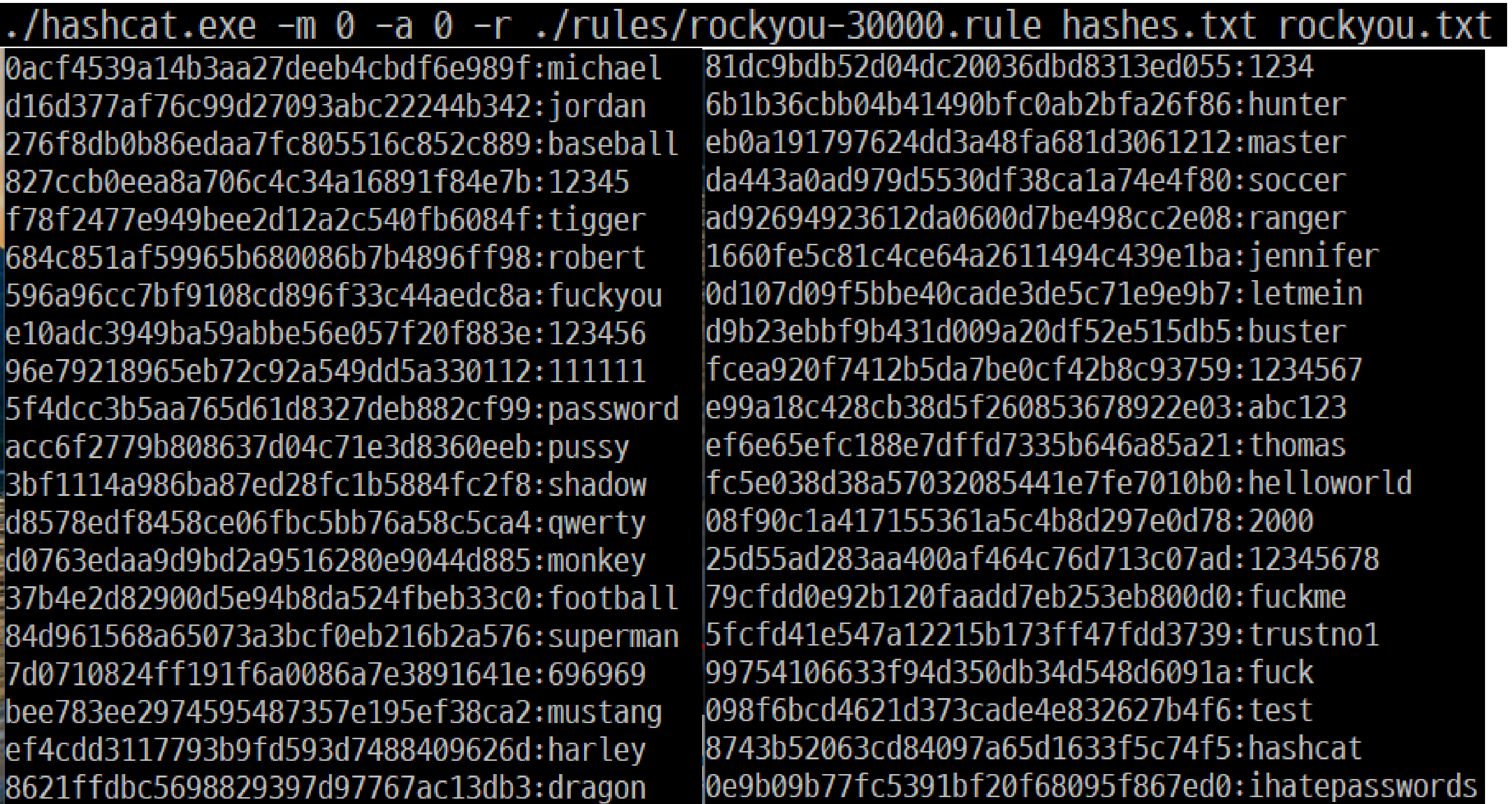
Finding	Severity Rating	Recommended Fix
DNS Server Recursive Query Cache Poisoning Weakness	Medium	Restrict recursive queries to the hosts that should use this nameserver
DNS Server Spoofed Request Amplification DDoS	Medium	Restrict access to your DNS server from public network or reconfigure it to reject such queries

- Fix within 60 days

Finding	Severity Rating	Recommended Fix
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:** Processed at WSL(Window subsystem for Linux). Hash information of passwords are placed in hashes.txt file. Downloaded cleartext passwords list called **rockyou** as txt file. Used **hashcat.exe** file to crack password hashes with options **md5**, **straight** attack type feeding rockyou.txt. Additionally used rule-based attack with the rule supported by hashcat program itself called **rockyou-30000.rule**.
- **Number of passwords tested:** 40
- **Number of passwords cracked:** 40
- **Evidence of weak passwords:** All password has been cracked under 10 seconds. Using md5 hashing algorithm. Most of the passwords are under 10 characters.



```
./hashcat.exe -m 0 -a 0 -r ./rules/rockyou-30000.rule hashes.txt rockyou.txt
0acf4539a14b3aa27deeb4cbdf6e989f:michael   81dc9bdb52d04dc20036dbd8313ed055:1234
d16d377af76c99d27093abc22244b342:jordan    6b1b36cbb04b41490bfc0ab2bfa26f86:hunter
276f8db0b86edaa7fc805516c852c889:baseball  eb0a191797624dd3a48fa681d3061212:master
827ccb0eea8a706c4c34a16891f84e7b:12345     da443a0ad979d5530df38ca1a74e4f80:soccer
f78f2477e949bee2d12a2c540fb6084f:tigger    ad92694923612da0600d7be498cc2e08:ranger
684c851af59965b680086b7b4896ff98:robert    1660fe5c81c4ce64a2611494c439e1ba:jennifer
596a96cc7bf9108cd896f33c44aedc8a:fuckyou   0d107d09f5bbe40cade3de5c71e9e9b7:letmein
e10adc3949ba59abbe56e057f20f883e:123456    d9b23ebbf9b431d009a20df52e515db5:buster
96e79218965eb72c92a549dd5a330112:111111    fcea920f7412b5da7be0cf42b8c93759:1234567
5f4dcc3b5aa765d61d8327deb882cf99:password  e99a18c428cb38d5f260853678922e03:abc123
acc6f2779b808637d04c71e3d8360eeb:pussy     ef6e65efc188e7dffd7335b646a85a21:thomas
3bf1114a986ba87ed28fc1b5884fc2f8:shadow    fc5e038d38a57032085441e7fe7010b0:helloworld
d8578edf8458ce06fbc5bb76a58c5ca4:qwerty    08f90c1a417155361a5c4b8d297e0d78:2000
d0763edaa9d9bd2a9516280e9044d885:monkey    25d55ad283aa400af464c76d713c07ad:12345678
37b4e2d82900d5e94b8da524fbeb33c0:football  79cfdd0e92b120faadd7eb253eb800d0:fuckme
84d961568a65073a3bcf0eb216b2a576:superman  5fcfd41e547a12215b173ff47fdd3739:trustno1
7d0710824ff191f6a0086a7e3891641e:696969    99754106633f94d350db34d548d6091a:fuck
bee783ee2974595487357e195ef38ca2:mustang   098f6bcd4621d373cade4e832627b4f6:test
ef4cdd3117793b9fd593d7488409626d:harley    8743b52063cd84097a65d1633f5c74f5:hashcat
8621ffdbc5698829397d97767ac13db3:dragon    0e9b09b77fc5391bf20f68095f867ed0:ihatepasswords
```

- Recommended steps to improve passwords security:
  - Use password more than 12 words
  - Use Upper / Lowercase letters, numbers, symbols both to make password hard to crack
  - Approximately with above it took 34k years to crack with combination of letter, numbers, symbols
  - Change password every 6 month
  - Use salt to prevent usage of rainbow table
  - Use more stronger hashing algorithm like sha256 to prevent hash collision as possible

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- Summarize ongoing incident:
  - 3 Hospitals A, B, and C were hit by Ransomware and now our hospital is contaminated by ransomware also and currently hackers are asking to pay one million dollars to access the system. The control systems used to monitor patient stats are no longer available through the standard user interface. Some doctors report being unable to render treatments because they cannot view detailed information about patient status. Log analysis tool is down, and security leader has declared this a critical security incident.
- Document actions or notes from the following steps of the initial incident response checklist

- Step 1: Several doctors, nurses, and administrative staff discovered the incident and contacted the help desk team for help.
- Step 2: Indicators of compromise is very clear that log analysis systems, control system used to monitor patient stats are down, and already attacked by Ransomware. This potential impact is to lost all the personal documents and files of the centralized log management system; patient's life might be threatened due to doctors are unable to render treatments. Currently control system and the data center that is used as centralized log management system is targeted. OS is window 10 pro, and the IP address is 52.251.118.221
- Step 3: The incident type is ransomware and security leader has confirmed as critical security incident and its on progress. The response should be urgent. Not sure is there are alerts embedded in the ransomware but assumed that hackers would not mind decrypting as they seem confidence. They are sure we cannot decrypt without this ransomware and allowing to delete the software. It is unlikely that action will be taken from hackers when we try to decrypt it. So, we don't care.

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- Step 4: While the control system is down doctors are unable to render treatments because they cannot view detailed information about patient status. Potentially, emergency patients may be in a dangerous situation because they are not properly treated. IR team and staff has no issue with safety, but patients' life could be at immediate risk.
- Step 5: All security team coordinate communications with necessary internal and external stakeholders. Doctor, nurse, staff, legal, IT support, media and PR, human resources team should know this situation immediately and plan to ensure the business continuity.
- Step 6: This incident should be categorized to a “Threat to public safety or life” with the highest applicable level. Even this is ransomware so likely to categorize into “Threat to sensitive data” but this is including human life problem so it should be categorized into “Threat to public safety or life” to be able to be prioritized compared to other “Threat to sensitive data” problem.
- Step 10: Incident is discovered by doctors, nurses, and administrative staff. It is intentional external threat which is ransomware, phishing, spear phishing, whaling. It happened by user opening an email attachment resource with is ransomware. Attack is coming from the group FIN4. They seem to be hacktivist unhappy with the hospital’s endorsement of the healthcare legislation or financially motivated attackers.

INCIDENT RESPONSE RECOMMENDED ACTION

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

  Eradication and recovering is the urgent thing because human life is at stake. Isolate the systems infected by ransomware, wipe them clean, and restore systems fully from backups. This will take time so in the meantime patients should be prioritized to select urgent patients. After that contact other hospital that might have the record of the urgent patient. If no records are possible re-check the patient as fast as possible.

  Containment follows next. Ransomware response procedure should be added to Step 7 of checklist. System that checks Email attachment to detect malicious programs should be conducted. Also, education of security to all staff inside the hospital must be done to prevent oblivious insider threat.

- Documented actions and notes from the IR checklist

- Step 7: IR team should follow Ransomware response procedure. Team should recover from the incident by isolating the systems infected by the ransomware, wipe them clean, and restore systems fully from backups.
- Step 8: Currently checking the logs for digital forensic is not possible. We need to investigate employees who opened emails infected with ransomware and find out if they are intentional and how this incident was caused.

INCIDENT RESPONSE RECOMMENDED ACTION

- Step 9:
  - Malicious program detection system for email should be conducted.
  - Ensure there is a backup server isolated from network
  - Least privilege should be conducted for file permission. Modifying the files should be able by only special process for example by hospital’s specific program. In other case, the user won’t be able to modify the files, and this will prevent ransomware because even user execute the program the program won’t be able to encrypt the files due to permission.
- Step 10: The response plan is to follow the checklist and recover the affected hospital’s system fast as possible. We will see this response plan is effective or not and will document every details after the incident is closed
- Step 11: Preserve every emails and records and the logs which is encrypted currently. This evidence should be preserved and kept as long as necessary to complete prosecution and beyond in case of an appeal.
- Step 12: Auto-backup system could be useful to prevent ransomware. The incident response was appropriate but currently there is no ransomware specific response plan so it could be good to add detailed plan for ransomware. Currently the recovery process is undergoing and need to talk about how could this be improved after the incident is closed.

  The changes of computer system side, human side should be made to prevent the re-infection. Mostly education of security to all staff inside the hospital must be done to prevent oblivious insider threat.

  Hospital systems are directly connected to the patient's life. We must make the main system more secure following least privilege, auto-updating patches, and auto-backup. We should strictly follow the security policy especially for the main server that affects the business continuity.