FINAL PROJECT TEMPLATE

Event Summarization

The incidents reported by Hospital A, Hospital B, and Hospital C indicate a ransomware attack and a System Disruption. The infiltration was done using Phishing method – as an attachment emailed to an Technologic employee. Ransomware is a type of malicious software that Blocks access to key components of the network and demands a ransom payment, in Bitcoin, in exchange for the decryption key. The attackers gain unauthorized access to the hospitals' centralized log management systems, encrypt the files, and display a ransom message demanding payment for the decryption key

- **Asset:** All files from servers
- **Impact:** Confidentiality and Availability of data
- **Threat Actor:** Cybercriminal groups FIN4 that attach healthcare establishment.
- **Threat Actor Motivation:** Financial Motivation.
- **Common Threat Actor Techniques:** (Phishing Emails, encryption of files, Ransom Demands, Untraceable payment option, Time constraint.

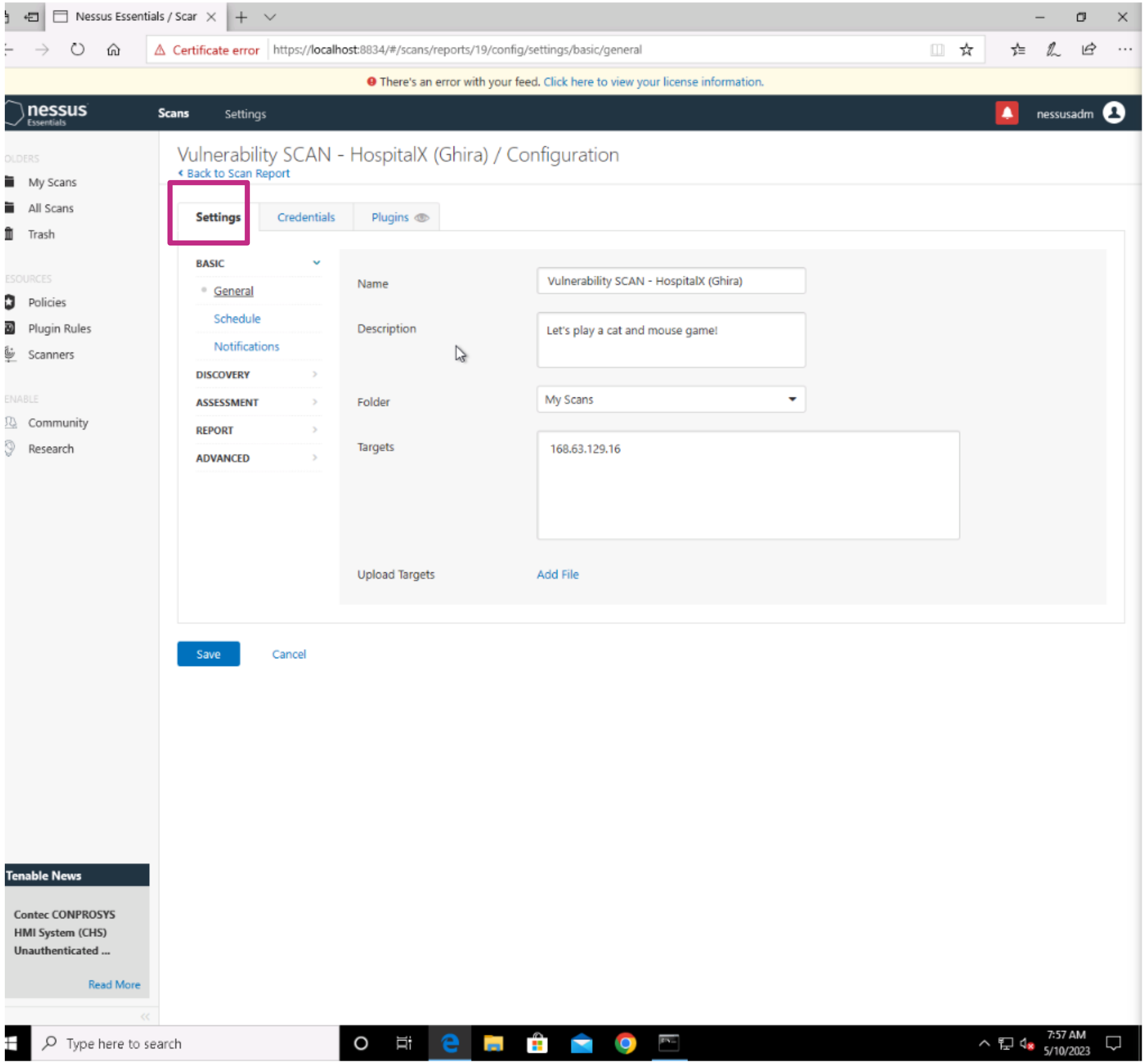
Threat profile

- Goals and Intent: fraud, theft of intellectual property (IP), and potentially espionage. The attackers aim to exploit vulnerabilities in the hospitals' systems to gain financial benefits
- Consequences: Financial Impact: Hospitals may suffer financial losses due to ransom payments, and disruption to operations and patient care. Also reputational Impact
- Target: Hospitals.
- Capabilities: The threat group behind the attack have the technical expertise necessary to conduct targeted and persistent attacks.
- Tactics: The threat group is known to employ various tactics, including: Spearphishing:
- Credential Theft: The attackers gain broader access to critical systems and data.
- Exploiting Vulnerabilities: The attackers take advantage of unpatched vulnerabilities in Windows systems,
- Timeframe: The timeframe for the attack is undetermined.

VULNERABILITY SCANNING TARGETS

- **Summary of scan targets:**
  - Number of devices scanned: 1
  - Device type: Remote device type
  - Primary purpose of device: general purpose computer

(insert 2 screenshots from scan configuration window – one of the settings tab and one of the plugins tab- see next slide)



Vulnerability SCAN - HospitalX (Ghira) / Configuration

‹ Back to Scan Report

Name: Vulnerability SCAN - HospitalX (Ghira)

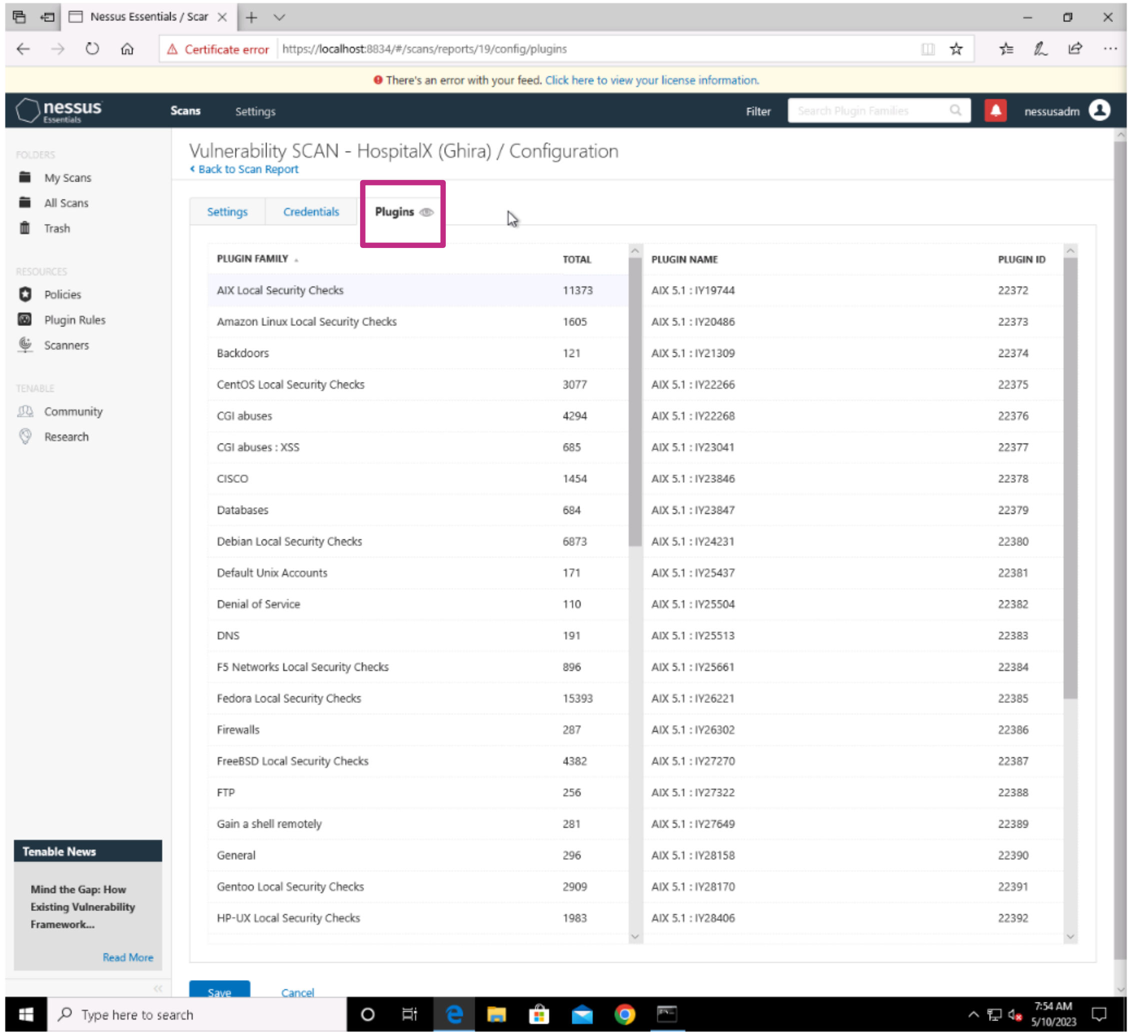
Description: Let's play a cat and mouse game!

Folder: My Scans

Targets: 168.63.129.16

Upload Targets: Add File

CYBERND0301



Vulnerability SCAN - HospitalX (Ghira) / Configuration

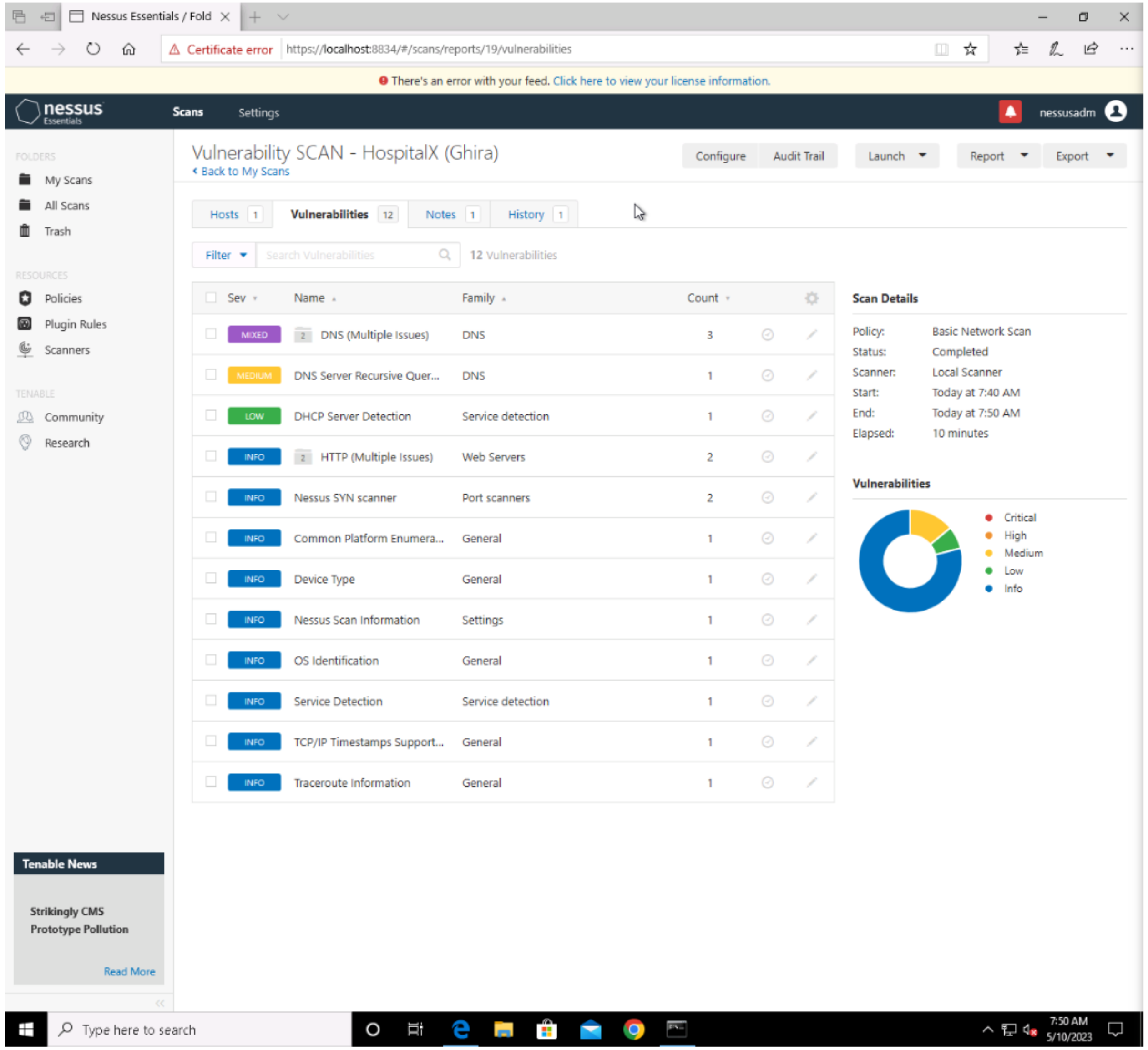
‹ Back to Scan Report

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
Gain a shell remotely	281
General	296
Gentoo Local Security Checks	2909
HP-UX Local Security Checks	1983

PLUGIN NAME	PLUGIN ID
AIX 5.1 : IY19744	22372
AIX 5.1 : IY20486	22373
AIX 5.1 : IY21309	22374
AIX 5.1 : IY22266	22375
AIX 5.1 : IY22268	22376
AIX 5.1 : IY23041	22377
AIX 5.1 : IY23846	22378
AIX 5.1 : IY23847	22379
AIX 5.1 : IY24231	22380
AIX 5.1 : IY25437	22381
AIX 5.1 : IY25504	22382
AIX 5.1 : IY25513	22383
AIX 5.1 : IY25661	22384
AIX 5.1 : IY26221	22385
AIX 5.1 : IY26302	22386
AIX 5.1 : IY27270	22387
AIX 5.1 : IY27322	22388
AIX 5.1 : IY27649	22389
AIX 5.1 : IY28158	22390
AIX 5.1 : IY28170	22391
AIX 5.1 : IY28406	22392

CYBERND0301

Cloud Lab – CYBERNDU001



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

Vulnerability SCAN - HospitalX (Ghira)

‹ Back to My Scans

12 Vulnerabilities

Sev	Name	Family	Count
MIXED	2 DNS (Multiple Issues)	DNS	3
MEDIUM	DNS Server Recursive Quer...	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 Enumera...	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 Support...	General	1
INFO	Traceroute Information	General	1

Scan Details

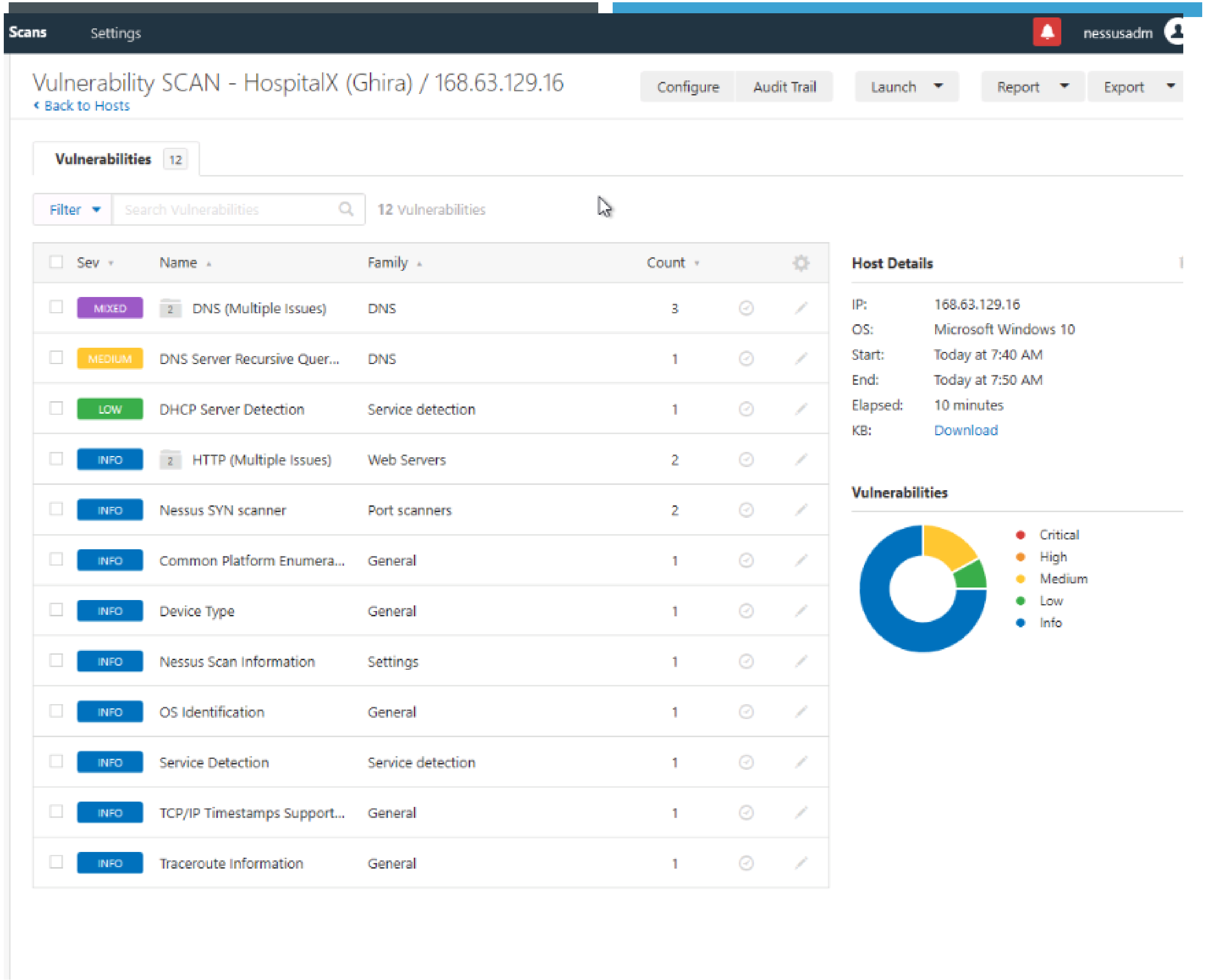
Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 7:40 AM
End:	Today at 7:50 AM
Elapsed:	10 minutes

Vulnerabilities

VULNERABILITY SCAN RESULTS

- **Summary of findings:**
  - Total number of actionable findings:
    - Critical: 0 %
    - High: 0 %
    - Medium: 17 %
    - Low: 8%
    - Info 75 %

(insert screenshot from scan results dashboard – see next slide)



Vulnerability SCAN - HospitalX (Ghira) / 168.63.129.16

‹ Back to Hosts

Vulnerabilities 12

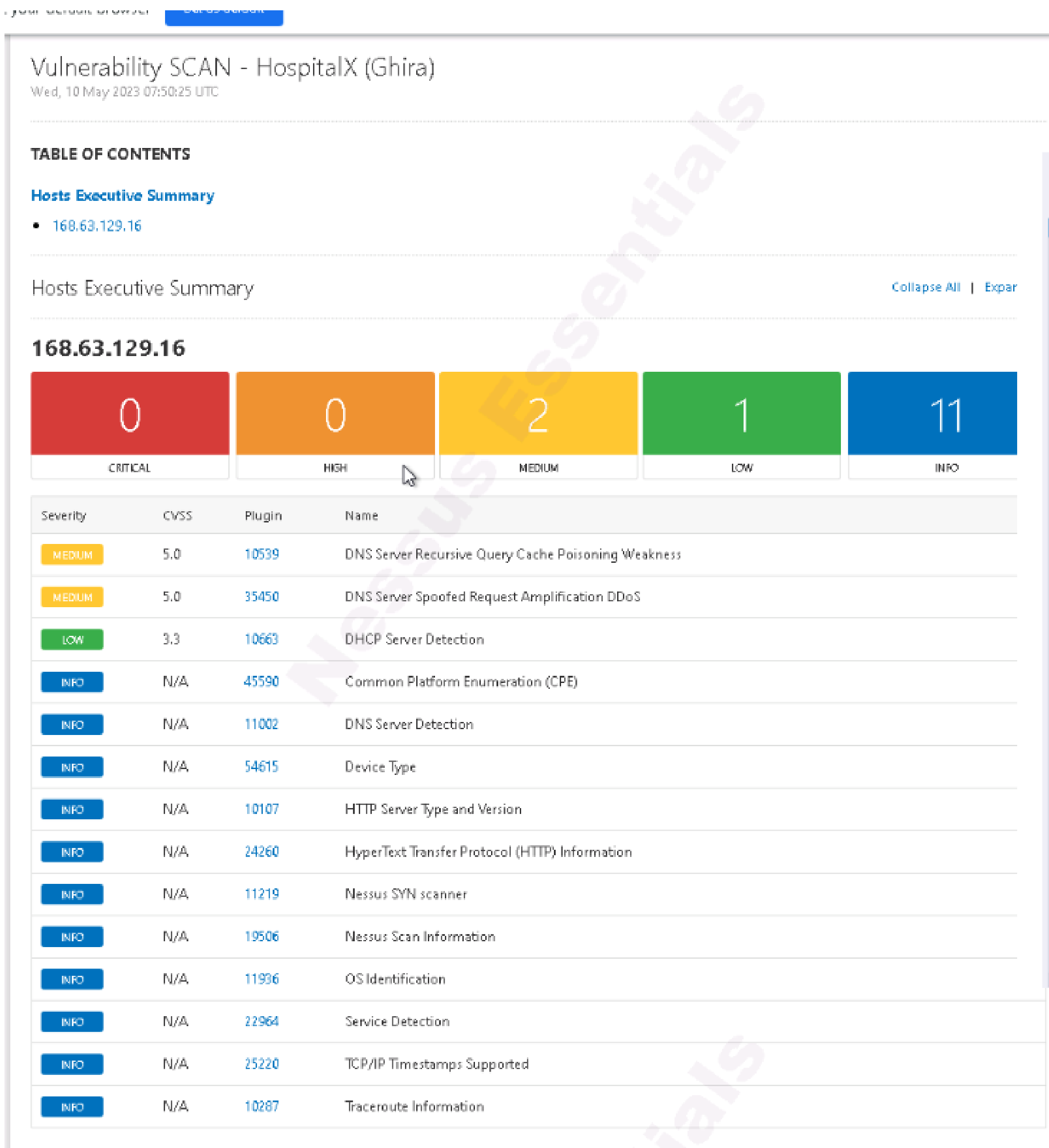
12 Vulnerabilities

Sev	Name	Family	Count
MIXED	2 DNS (Multiple Issues)	DNS	3
MEDIUM	DNS Server Recursive Quer...	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 Enumera...	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 Support...	General	1
INFO	Traceroute Information	General	1

Host Details

IP:	168.63.129.16
OS:	Microsoft Windows 10
Start:	Today at 7:40 AM
End:	Today at 7:50 AM
Elapsed:	10 minutes
KB:	Download

Vulnerabilities



Vulnerability SCAN - HospitalX (Ghira)

Wed, 10 May 2023 07:50:25 UTC

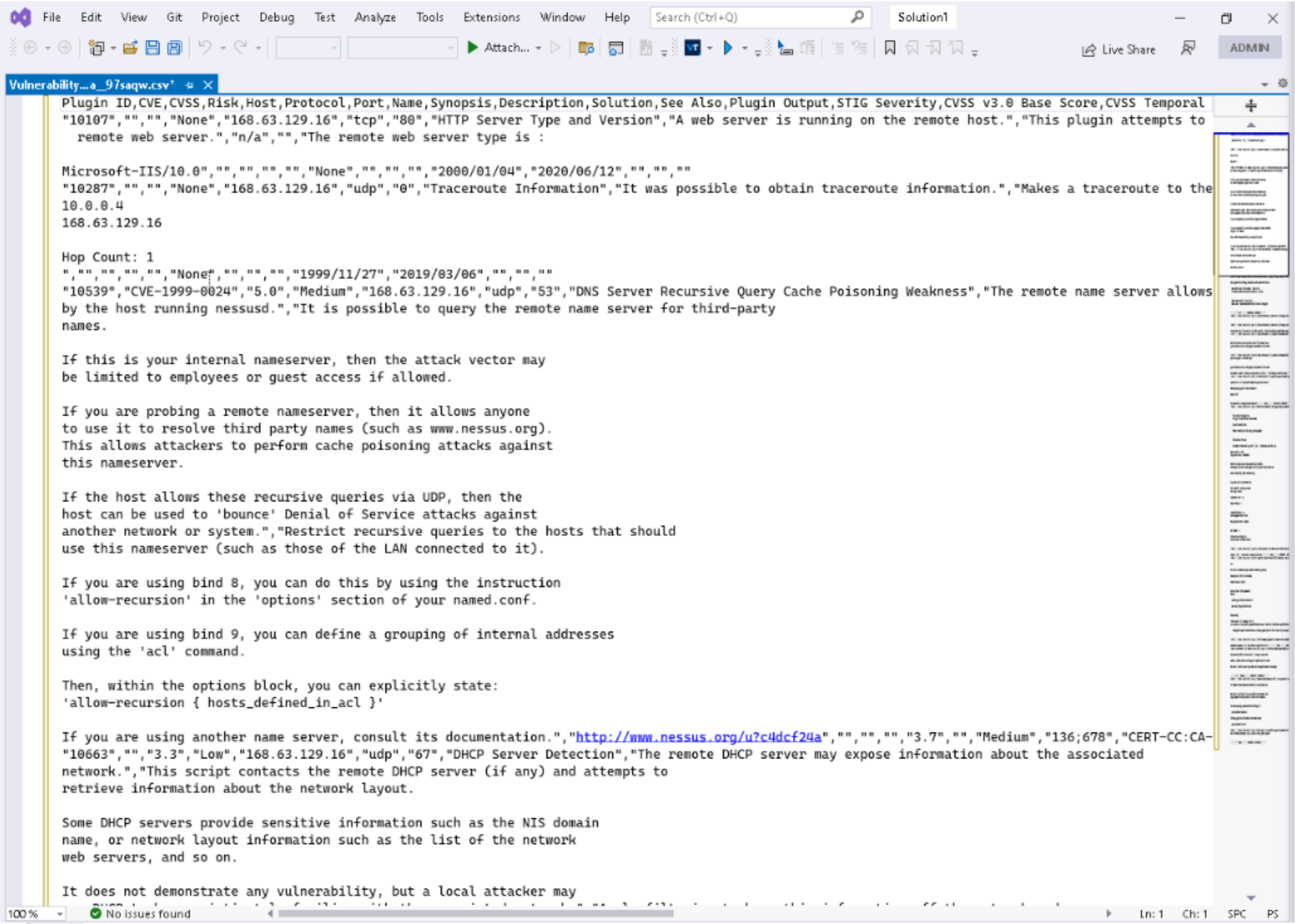
TABLE OF CONTENTS

Hosts Executive Summary

168.63.129.16

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	1	11

Severity	CVSS	Plugin	Name
MEDIUM	5.0	10539	DNS Server Recursive Query Cache Poisoning Weakness
MEDIUM	5.0	35450	DNS Server Spoofed Request Amplification DDoS
LOW	3.3	10663	DHCP Server Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	11002	DNS Server Detection
INFO	N/A	54615	Device Type
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information



```
Plugin ID,CVE,CVSS,Risk,Host,Protocol,Port,Name,Synopsis,Description,Solution,See Also,Plugin Output,STIG Severity,CVSS v3.0 Base Score,CVSS Temporal
"10107","","","None","168.63.129.16","tcp","80","HTTP Server Type and Version","A web server is running on the remote host.","This plugin attempts to
  remote web server.","n/a","","The remote web server type is :

Microsoft-IIS/10.0","","","","","None","","","","2000/01/04","2020/06/12","","",""
"10287","","","None","168.63.129.16","udp","0","Traceroute Information","It was possible to obtain traceroute information.","Makes a traceroute to the
10.0.0.4
168.63.129.16

Hop Count: 1
","","","","","None","","","","1999/11/27","2019/03/06","","",""
"10539","CVE-1999-0024","5.0","Medium","168.63.129.16","udp","53","DNS Server Recursive Query Cache Poisoning Weakness","The remote name server allows
by the host running nessusd.","It is possible to query the remote name server for third-party
names.

If this is your internal nameserver, then the attack vector may
be limited to employees or guest access if allowed.

If you are probing a remote nameserver, then it allows anyone
to use it to resolve third party names (such as www.nessus.org).
This allows attackers to perform cache poisoning attacks against
this nameserver.

If the host allows these recursive queries via UDP, then the
host can be used to 'bounce' Denial of Service attacks against
another network or system.","Restrict recursive queries to the hosts that should
use this nameserver (such as those of the LAN connected to it).

If you are using bind 8, you can do this by using the instruction
'allow-recursion' in the 'options' section of your named.conf.

If you are using bind 9, you can define a grouping of internal addresses
using the 'acl' command.

Then, within the options block, you can explicitly state:
'allow-recursion { hosts_defined_in_acl }'

If you are using another name server, consult its documentation.","http://www.nessus.org/u?c4dcf24a","","","","3.7","","Medium","136;678","CERT-CC:CA-
"10663","","3.3","Low","168.63.129.16","udp","67","DHCP Server Detection","The remote DHCP server may expose information about the associated
network.","This script contacts the remote DHCP server (if any) and attempts to
retrieve information about the network layout.

Some DHCP servers provide sensitive information such as the NIS domain
name, or network layout information such as the list of the network
web servers, and so on.

It does not demonstrate any vulnerability, but a local attacker may
```

REMEDIATION RECOMMENDATION

- Fix within 7 days

Finding	Severity Rating	Recommended Fix
DNS Server Spoofed Request Amplification DDos	Medium	Restrict access to your DNS server from public network or reconfigure it to reject such queries
DNS server Recursive query cache poisoning windows	Medium	Restrict recursive queries to the host that should use this nameserver
DHCP Server Detection	Low	Apply filtering to keep this information off the network and remove any option that is not in use

- Fix within 30 days

Finding	Severity Rating	Recommended Fix
DNS Server Detection	Info	Disable this service if it is not needed / restrict access to internal hosts only if the service is available externally.

- Fix within 60 days

Finding	Severity Rating	Recommended Fix
HTTP Information	Info	N/A

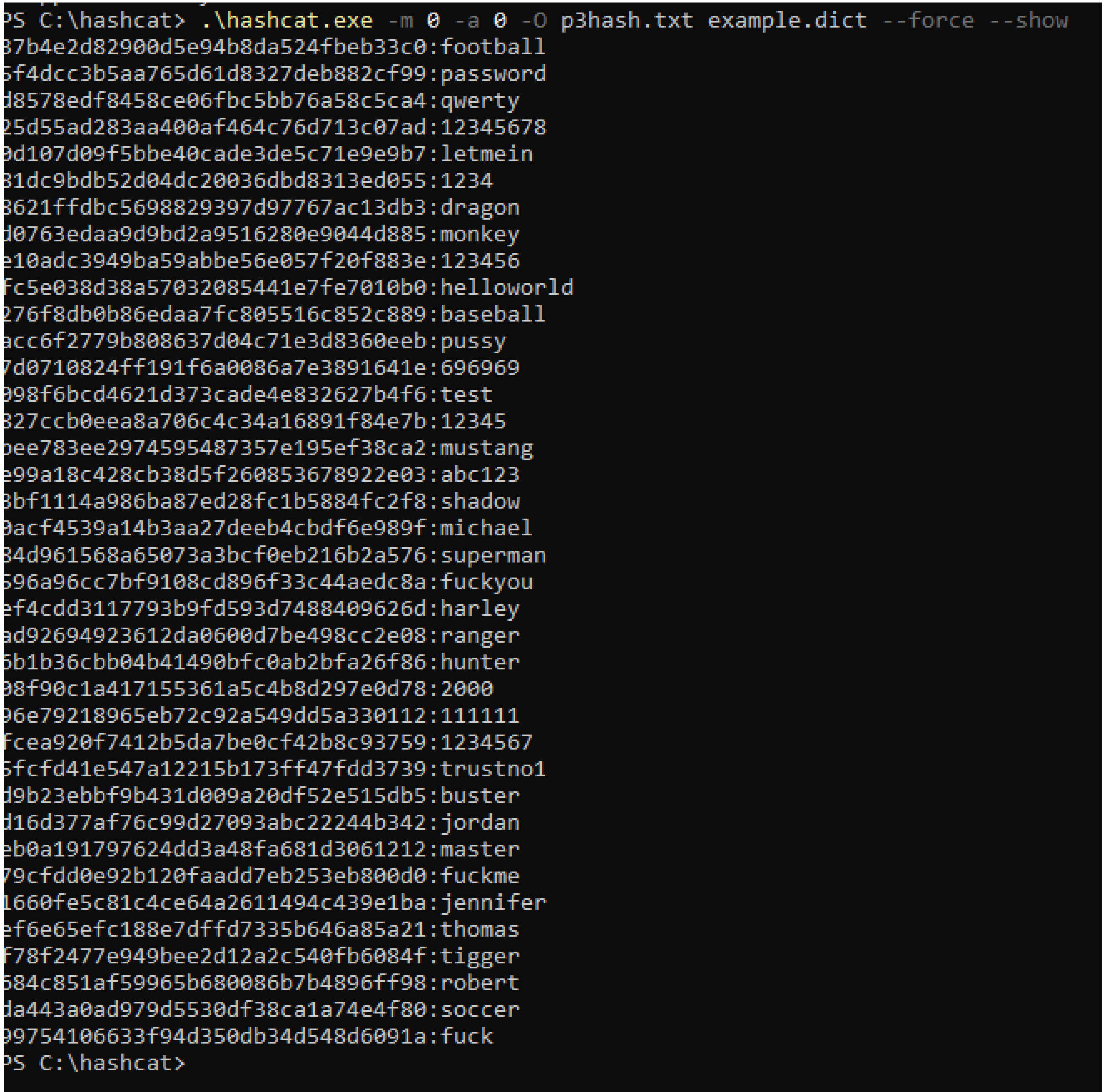
PASSWORD PENETRATION TEST OUTCOME

- **Methodology:**
- In order to determine the values for the hash, the hashcat was instaled on my personal computer.
- Was runed from Powershell using `cd C:\hashcat .\hashcat.exe –I`

- One commands was tried in order to find the values for the hash:
- **`PS C:\hashcat> .\hashcat.exe -m 0 -a 0 -O p3hash.txt example.dict --force –show`**

- **Number of passwords tested: 41**
- **Number of passwords cracked:** 38
- **Evidence of weak passwords: 38 (MD5 encryption type)**

See next slide



```
PS C:\hashcat> .\hashcat.exe -m 0 -a 0 -O p3hash.txt example.dict --force --show
37b4e2d82900d5e94b8da524fbeb33c0:football
5f4dcc3b5aa765d61d8327deb882cf99:password
d8578edf8458ce06fbc5bb76a58c5ca4:qwerty
25d55ad283aa400af464c76d713c07ad:12345678
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
81dc9bdb52d04dc20036dbd8313ed055:1234
8621ffdbc5698829397d97767ac13db3:dragon
d0763edaa9d9bd2a9516280e9044d885:monkey
e10adc3949ba59abbe56e057f20f883e:123456
fc5e038d38a57032085441e7fe7010b0:helloworld
276f8db0b86edaa7fc805516c852c889:baseball
acc6f2779b808637d04c71e3d8360eeb:pussy
7d0710824ff191f6a0086a7e3891641e:696969
098f6bcd4621d373cade4e832627b4f6:test
827ccb0eea8a706c4c34a16891f84e7b:12345
bee783ee2974595487357e195ef38ca2:mustang
e99a18c428cb38d5f260853678922e03:abc123
3bf1114a986ba87ed28fc1b5884fc2f8:shadow
0acf4539a14b3aa27deeb4cbdf6e989f:michael
84d961568a65073a3bcf0eb216b2a576:superman
596a96cc7bf9108cd896f33c44aedc8a:fuckyou
ef4cdd3117793b9fd593d7488409626d:harley
ad92694923612da0600d7be498cc2e08:ranger
6b1b36cbb04b41490bfc0ab2bfa26f86:hunter
08f90c1a417155361a5c4b8d297e0d78:2000
96e79218965eb72c92a549dd5a330112:111111
fcea920f7412b5da7be0cf42b8c93759:1234567
5fcfd41e547a12215b173ff47fdd3739:trustno1
d9b23ebbf9b431d009a20df52e515db5:buster
d16d377af76c99d27093abc22244b342:jordan
eb0a191797624dd3a48fa681d3061212:master
79cfdd0e92b120faadd7eb253eb800d0:fuckme
1660fe5c81c4ce64a2611494c439e1ba:jennifer
ef6e65efc188e7dffd7335b646a85a21:thomas
f78f2477e949bee2d12a2c540fb6084f:tigger
684c851af59965b680086b7b4896ff98:robert
da443a0ad979d5530df38ca1a74e4f80:soccer
9975410663 3f94d350db34d548d6091a:fuck
PS C:\hashcat>
```

- **Recommended steps to improve passwords security:**

1. Use Strong and Complex Passwords: A strong password should be at least 12 characters long and + uppercase and lowercase letters, +numbers + special characters.
2. Regularly Update Passwords: Update their passwords, preferably every 90 days.
3. Implement Password Managers like OKTA password manager.

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- Summarize ongoing incident:

  Multiple hospitals, including Hospital A, Hospital B, Hospital C, and five additional hospitals, have been targeted by a ransomware attack. The attack has resulted in the encryption of files, including centralized log files and backups, affecting the hospitals' ability to access critical systems and patient information. The attackers are taking advantage of an unpatched Windows vulnerability to execute the attack. The hospitals share the commonality of endorsing a recently passed healthcare law. This incident is considered a critical security incident.

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

- Step 1: The entities that discovered the incident are similar establishments (Hospital A B C).
- Step 2: The indicator of compromise is system unavailability, and the potential impact of incident might be the full loss of data and system disruption. The system being affect is centralized log management systems, running on Windows with IP address …..
- Step 3: The confirmation of incident comes from the initial 3 Hospitals and other 5 hospitals that faced the same incident, as well as members from Hospital X. The incident is in progress. The response must be urgent. We do not care if any response will alert the attacker. This is an intrusion incident.
- Step 4: The incident affect a hospital and when the operation is being stopped, then life of some patience who are at ER, Surgery, Intensive Care, might be at immediate risk.
- Step 6: Category one. This is because of the disruption of operation in the hospital. (see step 4)

(Add another slide if needed)

INCIDENT RESPONSE RECOMMENDED ACTION

- Summarize recommendation to contain, eradicate, and recover:

To contain, eradicate, and recover from the intrusion, the following recommendations are summarized:

Contain:

- Isolate affected computers from the network to prevent further spread of the ransomware and limit the impact on othes.
- Identify and disconnect any compromised server/computer/router/printer/etc

Eradicate:

- Conduct a thorough cyber-forensic analysis to identify the exact ransomware used.
- Patch and update systems to resolve the vulnerabilities used by the cyber-criminals.

Recover:

- Restore systems and data from clean backups
- Verify the integrity and security of backups to ensure they are not affected or infected.
- Prioritize the restoration of critical systems and patient care functionalities to minimize the impact on healthcare operations.

Documented actions and notes from the IR checklist

Step 7:

Malware response procedure. IR needs to isolate affected systems, and to determine the impact of the infection, identify the ransomware used, and restore the systems and data from back-up.

Step 8:

Unable to check the logs, document the reason because of the technical issues, such as log server failure or data corruption, document these limits. When the logs have been deleted by the attacker, note the absence of logs and any indications of unauthorized access.

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 is fully patched.
Be sure real time virus protection and intrusion detection is running.

Step 12:

- The incident response was not fast, as from the first news of the incident, until the Hospital X was affected 4 hours passed, yet in this time, the staff was not informed about the incident, the network was not isolated, nor scanned, the system wasn't updated.
- Change all passwords and all all users structure accounts. Change response procedure.
- To enable stronger firewall, to conduct data protection lessons to the staff. To migrate to a cloud based solution.