FINAL PROJECT TEMPLATE

THREAT SUMMARY

- **Summary of Situation:** Hospitals A,B and C got a message says: "all personal documents and files are encrypted" and the only way to decrypt them if the payment done. The incident has started with user in technology department opening an email attachment resource.
- **Asset:** Centralized log files and backups, Windows systems, The control systems, Doctors report, patients' information and log analysis tool.
- **Impact:** Confidentiality, Integrity and Availability.
- **Threat Actor:** An External threat actor (Cybercriminals). Internal threat actor (user in technology department).
- **Threat Actor Motivation:** Cybercriminals are financially motivated individuals who carry out attacks mainly for monetary reasons.

Disgruntled insiders are employees who are unhappy with the organization and seek to retaliate often through digital resources and exploitation.

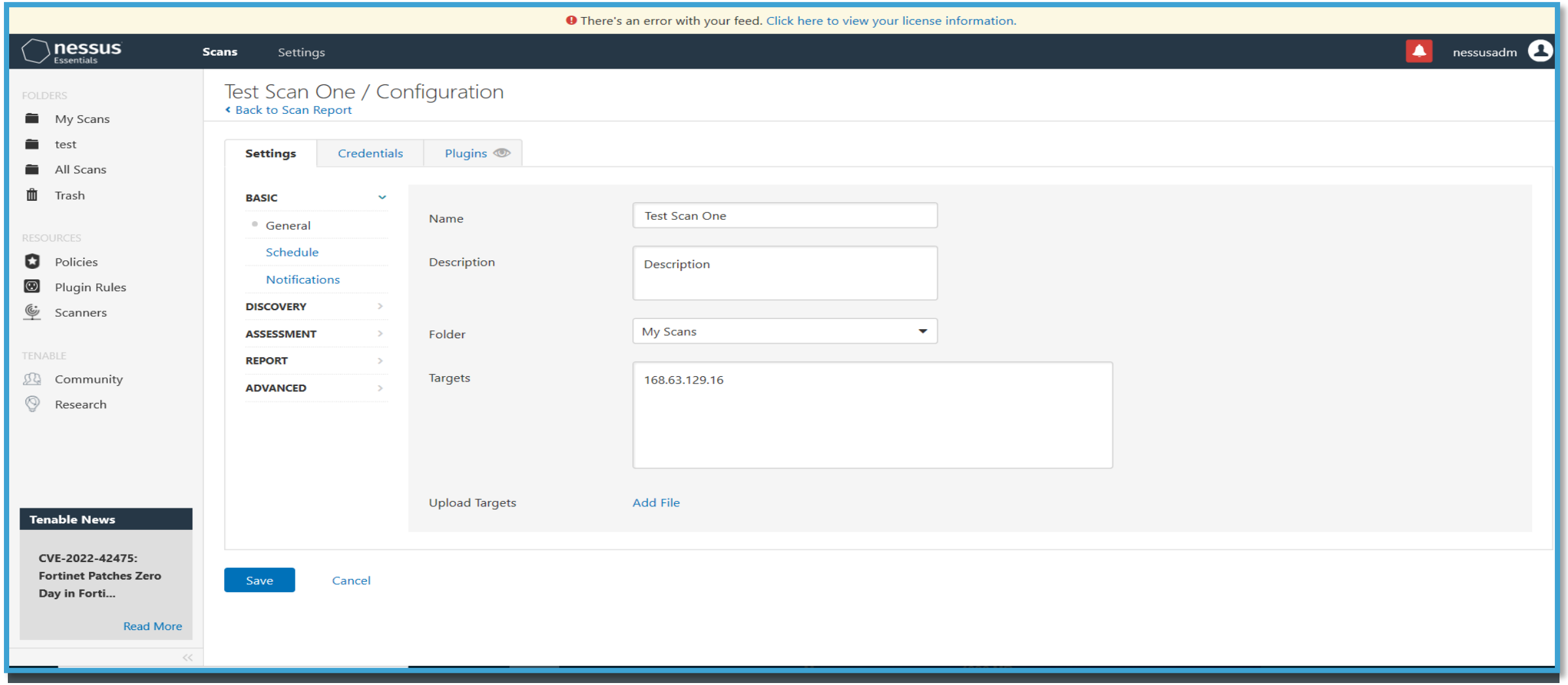
- **Common Threat Actor Techniques:** : Intentional threats: Phishing: Spearphishing Attachment used to acquire sensitive data using an email attachment.
- Unintentional threats: Could cause by an employee who unaware of security practices.

VULNERABILITY SCANNING TARGETS

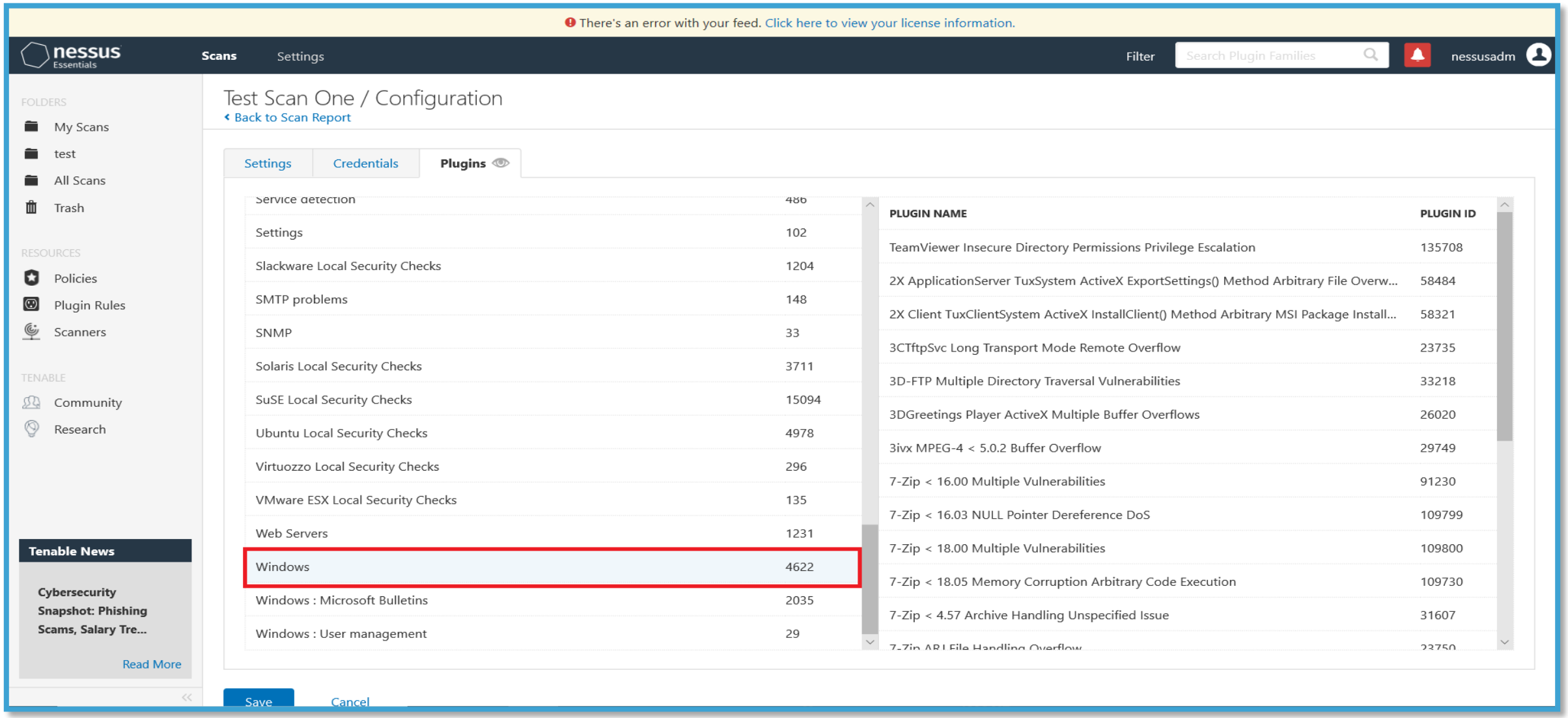
- **Summary of scan targets:**
  - Number of devices scanned: One (1) host.
  - Device type: (operating system and version) Microsoft Windows 10
  - Primary purpose of device: (describe what the devices are used for and what kind of data might be on them) general-purpose computer it used to store personal documents and files.

(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)

Settings tab:



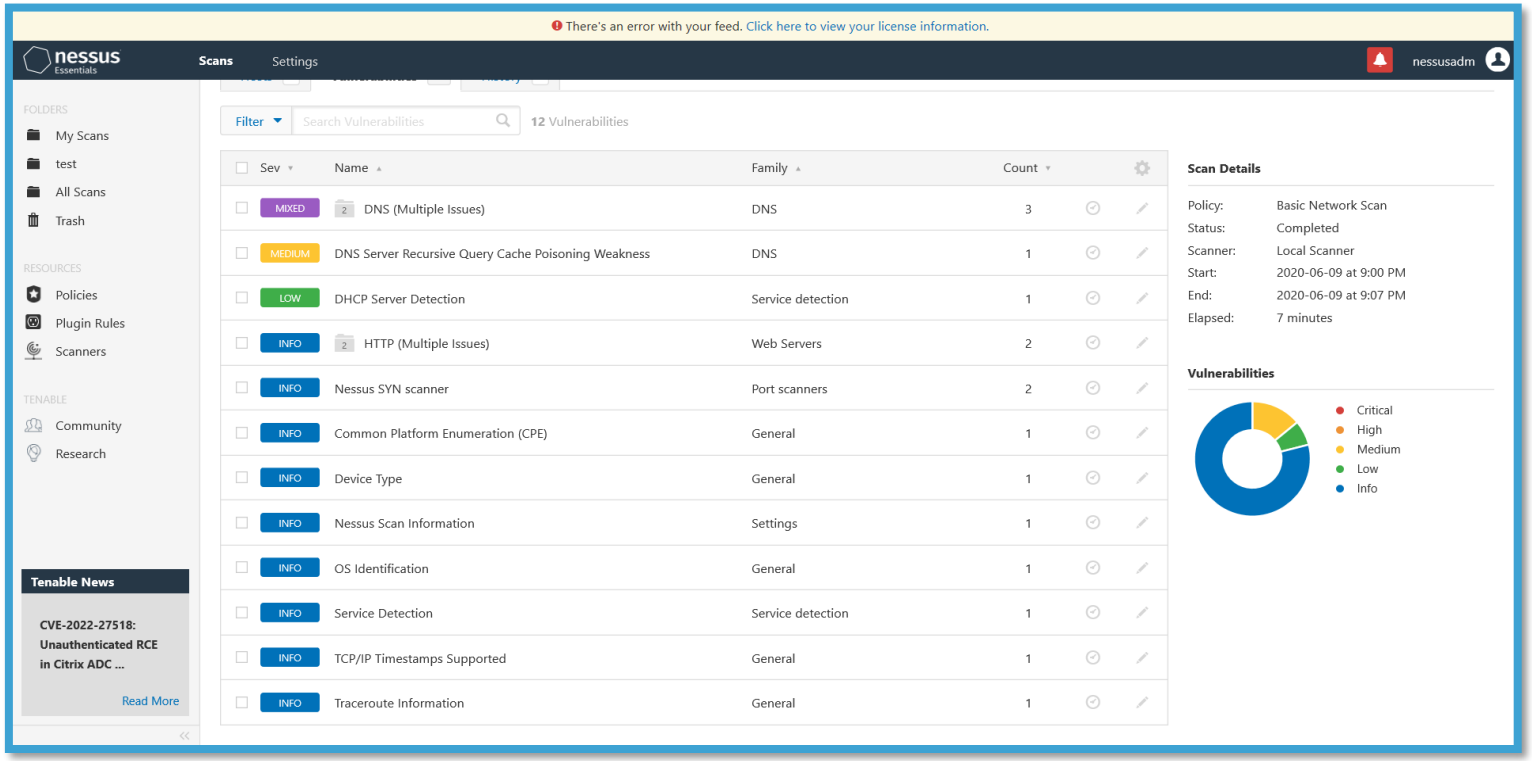
Plugins tab:


There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
Filter
Search Plugin Families
nessusadm
FOLDERS
My Scans
test
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
Cybersecurity Snapshot: Phishing Scams, Salary Tre...
Read More
Test Scan One / Configuration
Back to Scan Report
Settings
Credentials
Plugins
Service detection 486
Settings 102
Slackware Local Security Checks 1204
SMTP problems 148
SNMP 33
Solaris Local Security Checks 3711
SuSE Local Security Checks 15094
Ubuntu Local Security Checks 4978
Virtuozzo Local Security Checks 296
VMware ESX Local Security Checks 135
Web Servers 1231
Windows 4622
Windows : Microsoft Bulletins 2035
Windows : User management 29
PLUGIN NAME
PLUGIN ID
TeamViewer Insecure Directory Permissions Privilege Escalation 135708
2X ApplicationServer TuxSystem ActiveX ExportSettings() Method Arbitrary File Overw... 58484
2X Client TuxClientSystem ActiveX InstallClient() Method Arbitrary MSI Package Install... 58321
3CTftpSvc Long Transport Mode Remote Overflow 23735
3D-FTP Multiple Directory Traversal Vulnerabilities 33218
3DGreetings Player ActiveX Multiple Buffer Overflows 26020
3ivx MPEG-4 < 5.0.2 Buffer Overflow 29749
7-Zip < 16.00 Multiple Vulnerabilities 91230
7-Zip < 16.03 NULL Pointer Dereference DoS 109799
7-Zip < 18.00 Multiple Vulnerabilities 109800
7-Zip < 18.05 Memory Corruption Arbitrary Code Execution 109730
7-Zip < 4.57 Archive Handling Unspecified Issue 31607
Save
Cancel

VULNERABILITY SCAN RESULTS

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

(insert screenshot from scan results dashboard)



REMEDIATION RECOMMENDATION

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

- Fix within 7 days: There are no "**Critical**" or "**High**" vulnerabilities.

Finding	Severity Rating	Recommended Fix

- Fix within 14 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 the DNS server from public network or reconfigure it to reject such queries.

- Fix within 30 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.

CSV report:

4	10539	CVE-1999-0024	5	Medium	168.63.129.16	udp	53	DNS Server Recursive Query Cache Poisoning Weakness	The remote name server allows recursive queries to be performed	It is possible to query the	Restrict	http://www.nessus.org/u?c4dcf24a
5	10663		3.3	Low	168.63.129.16	udp	67	DHCP Server Detection	The remote DHCP server may expose information about the associated	This script contacts the	Apply	
6	11002			None	168.63.129.16	tcp	53	DNS Server Detection	A DNS server is listening on the remote host.	The remote service is a	Disable this	https://en.wikipedia.org/wiki/Domain_Name_System
7	11002			None	168.63.129.16	udp	53	DNS Server Detection	A DNS server is listening on the remote host.	The remote service is a	Disable this	https://en.wikipedia.org/wiki/Domain_Name_System
8	11219			None	168.63.129.16	tcp	53	Nessus SYN scanner	It is possible to determine which TCP ports are open.	This plugin is a SYN 'half-	Protect your target with an IF	Port 53/tcp was found to be open
9	11219			None	168.63.129.16	tcp	80	Nessus SYN scanner	It is possible to determine which TCP ports are open.	This plugin is a SYN 'half-	Protect your target with an IF	Port 80/tcp was found to be open
10	11936			None	168.63.129.16	tcp	0	OS Identification	It is possible to guess the remote operating system.	Using a combination of	n/a	
11	19506			None	168.63.129.16	tcp	0	Nessus Scan Information	This plugin displays information about the Nessus scan.	This plugin displays, for	n/a	Information
12	22964			None	168.63.129.16	tcp	80	Service Detection	The remote service could be identified.	Nessus was able to identify	n/a	A web server is running on this port.
13	24260			None	168.63.129.16	tcp	80	HyperText Transfer Protocol (HTTP) Information	Some information about the remote HTTP configuration can be extracted.	This test gives some	n/a	
14	25220			None	168.63.129.16	tcp	0	TCP/IP Timestamps Supported	The remote service implements TCP timestamps.	The remote host	n/a	http://www.ietf.org/rfc/rfc1323.txt
15	35450	CVE-2006-0987	5	Medium	168.63.129.16	udp	53	DNS Server Spoofed Request Amplification DDoS	The remote DNS server could be used in a distributed denial of service	The remote DNS server	Restrict	https://isc.san
16	45590			None	168.63.129.16	tcp	0	Common Platform Enumeration (CPE)	It was possible to enumerate CPE names that matched on the remote	By using information	n/a	http://cpe.mit
17	54615			None	168.63.129.16	tcp	0	Device Type	It is possible to guess the remote device type.	Based on the remote	n/a	Remote
18												
19												
20												
21												
22												
23												
24												
25												
26												
27												
28												
29												
30												
31												
32												
33												
34												
35												
36												
37												
38												
39												
40												
41												

PASSWORD PENETRATION TEST OUTCOME

- **Methodology:**

1. Download the hashes file "hashed.txt" (From **Udacity**).
2. Download the wordlist "rockyou.txt" (From **GitHub**).
3. Open **CMD.**
4. Run the following command:

hashcat.exe -m 0 -a 0 (Hash file) (Wordlist)

Where **-m**: "Hash type" = "MD5"

-a: "Attack-mode" = "Straight"

- **Number of passwords tested:** 41
- **Number of passwords cracked:** 4
- **Evidence of weak passwords:**

```
PS C:\Users\antub\Desktop\hashcat-6.2.6> .\hashcat.exe -m 0 -a 0 C:\Users\antub\Desktop\Hashed.txt C:\Users\antub\Desktop\rockyou.txt
hashcat (v6.2.6) starting


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

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

- Passwords should be at least 8 characters.
- Passwords should changed every 90 days.
- Users Account should be locked out after 10 failed attempts.

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

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

    The attack encrypts all personal documents and files. The attacker set an amount to pay to decrypt these files. The staff (Doctors, Administration) has no access to the control system, and they are not able to access the information of their patients

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

  - Step 1: Gather incident response team.
  - Step 2: Review the logs to see what is the source of the incident.
  - Step 3: Contain and isolate the source of the incident.
  - Step 4: Remove malware from all affected systems and take action to prevent similar attacks in the future.
  - Step 5: Bring affected systems back online.
  - Step 6: Once the incident is over conducting proper cybersecurity training to all the staff members.

(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

The email attachment must be deleted or isolated.

The Malware which (FIN4 Bit Cryptor) will be deleted

Then restore the files and documents from backups.

Documented actions and notes from the IR checklist

- Step 7: *Malware response procedure , Insider threat procedure and g) Database or file denial of service response procedure*
- Step 8: Ensure the system is fully patched.
- Step 9: Be sure real time virus protection and intrusion detection is running.
- Step 12: Be sure the system is logging the correct events and to the proper level.

(Add another slide if needed)