FINAL PROJECT TEMPLATE

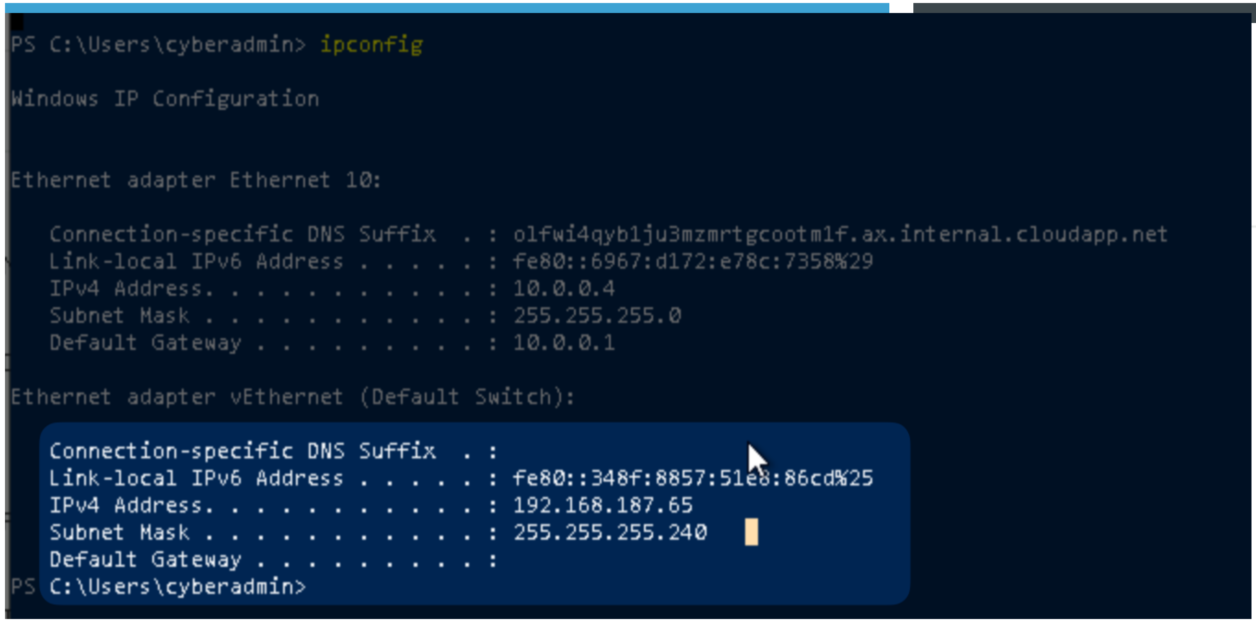
THREAT SUMMARY

- **Summary of Situation:** Hospital A, Hospital B and Hospital C have fallen victim to a cyber attack led by what appears to be a group of cyber activists who oppose the new health law that has just been approved. All of the hospitals that were affected had declared their support for the law before being attacked. Our hospital also supports the law and we fear the possibility of a similar attack on us.
- **Asset:** Systems, Control Systems, Patient stats, Doctor reports, Log Analysis tool
- **Impact:** Availability
- **Threat Actor:**
  - **External Threat Actors:** Cyber activists motivated by political or social opposition to the new health law. These actors are likely to be organized groups or individuals outside the hospital who seek to disrupt operations as a form of protest.
  - **Internal Threat Actors:** Hospital staff who may unintentionally aid the attackers through actions such as falling for phishing scams or other forms of social engineering. There is also the possibility of intentional insider threats from staff members who oppose the law.
- **Threat Actor Motivation:**
  - • **Political/Social Ends:** The primary motivation for these attacks is opposition to the newly approved health regulation. The activists aim to disrupt hospital operations to make a political statement or to sway public opinion against the law.

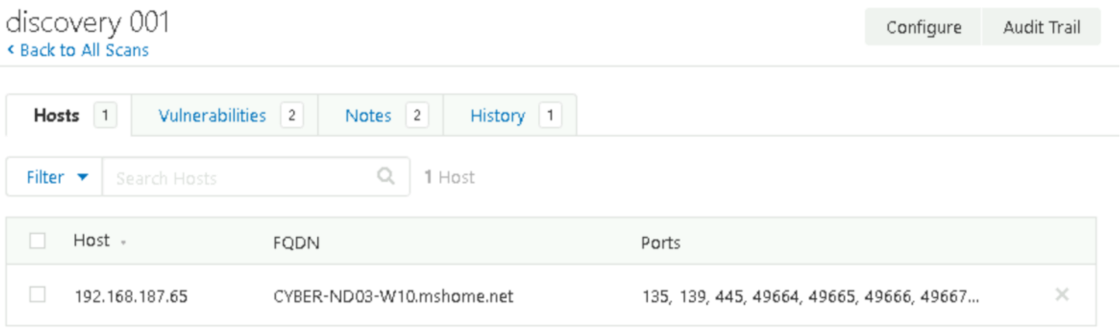
    • **Financial Gains:** Although the current evidence points to hacktivism, the possibility of financially motivated actors should not be dismissed. Groups such as **FIN4**—a well-known cybercriminal organization—are motivated by financial gain and are known for targeting healthcare institutions to steal sensitive information or deploy ransomware. FIN4 has been particularly active in exploiting vulnerabilities for profit, which could include holding hospital systems hostage until a ransom is paid.
- **Common Threat Actor Techniques:**
  - **Intentional Threats:**
    - **Phishing:** Cyber activists and malicious insiders may use phishing emails to trick hospital staff into revealing sensitive information or downloading malicious software.
    - **Social Engineering:** Techniques such as impersonation or manipulation of staff to gain unauthorized access to hospital systems.
    - **Insider Threats:** Staff members who may intentionally support the attack due to personal beliefs or financial incentive.
  - **Unintentional Threats:**
    - **Human Error:** Unintentional actions by staff, such as clicking on malicious links or mishandling sensitive information, which can facilitate an attack.
    - **Social Engineering:** Even well-meaning staff can be manipulated into actions that compromise security through sophisticated social engineering tactics.

VULNERABILITY SCANNING TARGETS

- **Summary of scan targets:**
  - Number of devices scanned: Network scan over the entire subnet. **Found 1 device**
  - Device type: **PC/Server - Windows 10 Pro**
  - Primary purpose of device: **Log Server – Personal patients' information**



```
PS C:\Users\cyberadmin> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 10:

   Connection-specific DNS Suffix  . : olfwi4qyb1ju3mzmrtgcootm1f.ax.internal.cloudapp.net
   Link-local IPv6 Address . . . . . : fe80::6967:d172:e78c:7358%29
   IPv4 Address. . . . . . . . . . . : 10.0.0.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::348f:8857:51e8:86cd%25
   IPv4 Address. . . . . . . . . . . : 192.168.187.65
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . :
PS C:\Users\cyberadmin>
```

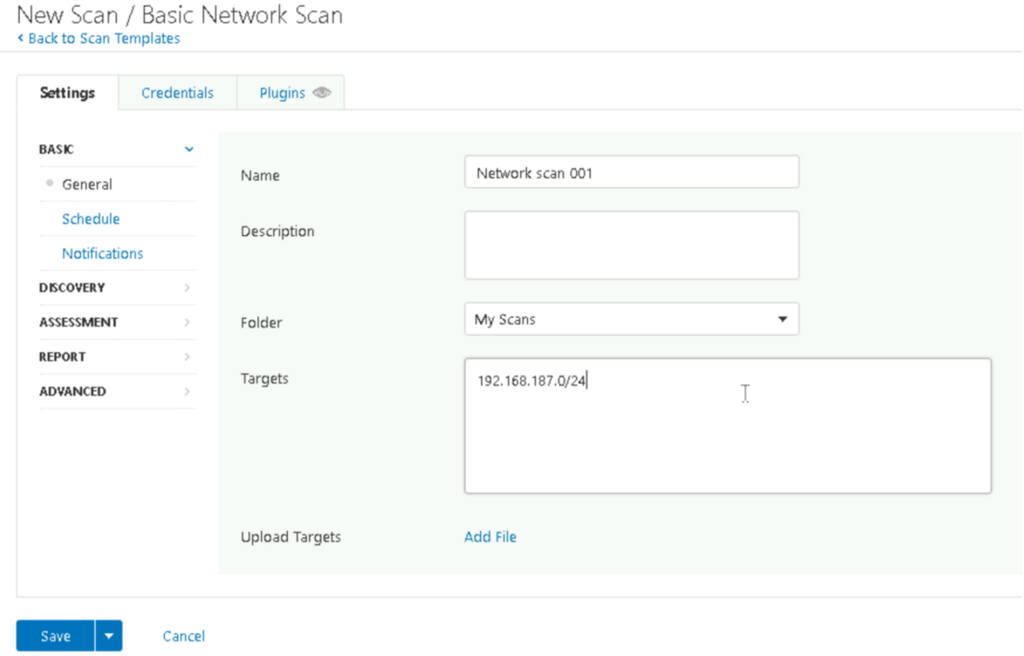


discovery 001

‹ Back to All Scans

1 Host

□	Host	FQDN	Ports
□	192.168.187.65	CYBER-ND03-W10.mshome.net	135, 139, 445, 49664, 49665, 49666, 49667...



New Scan / Basic Network Scan

‹ Back to Scan Templates

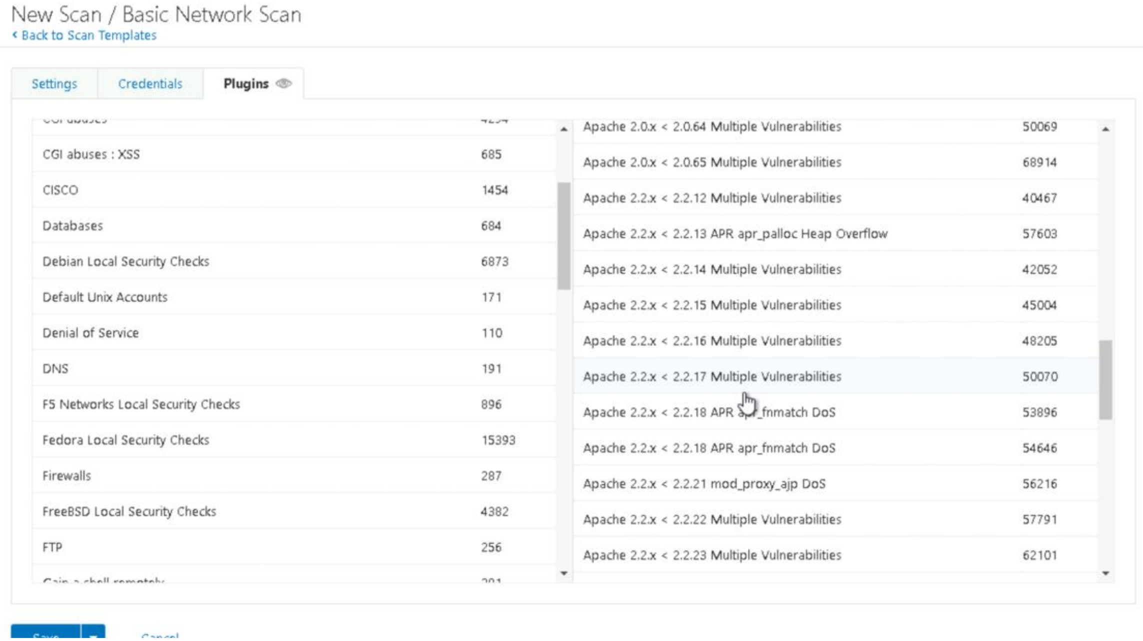
Name: Network scan 001

Description:

Folder: My Scans

Targets: 192.168.187.0/24

Upload Targets: Add File



New Scan / Basic Network Scan

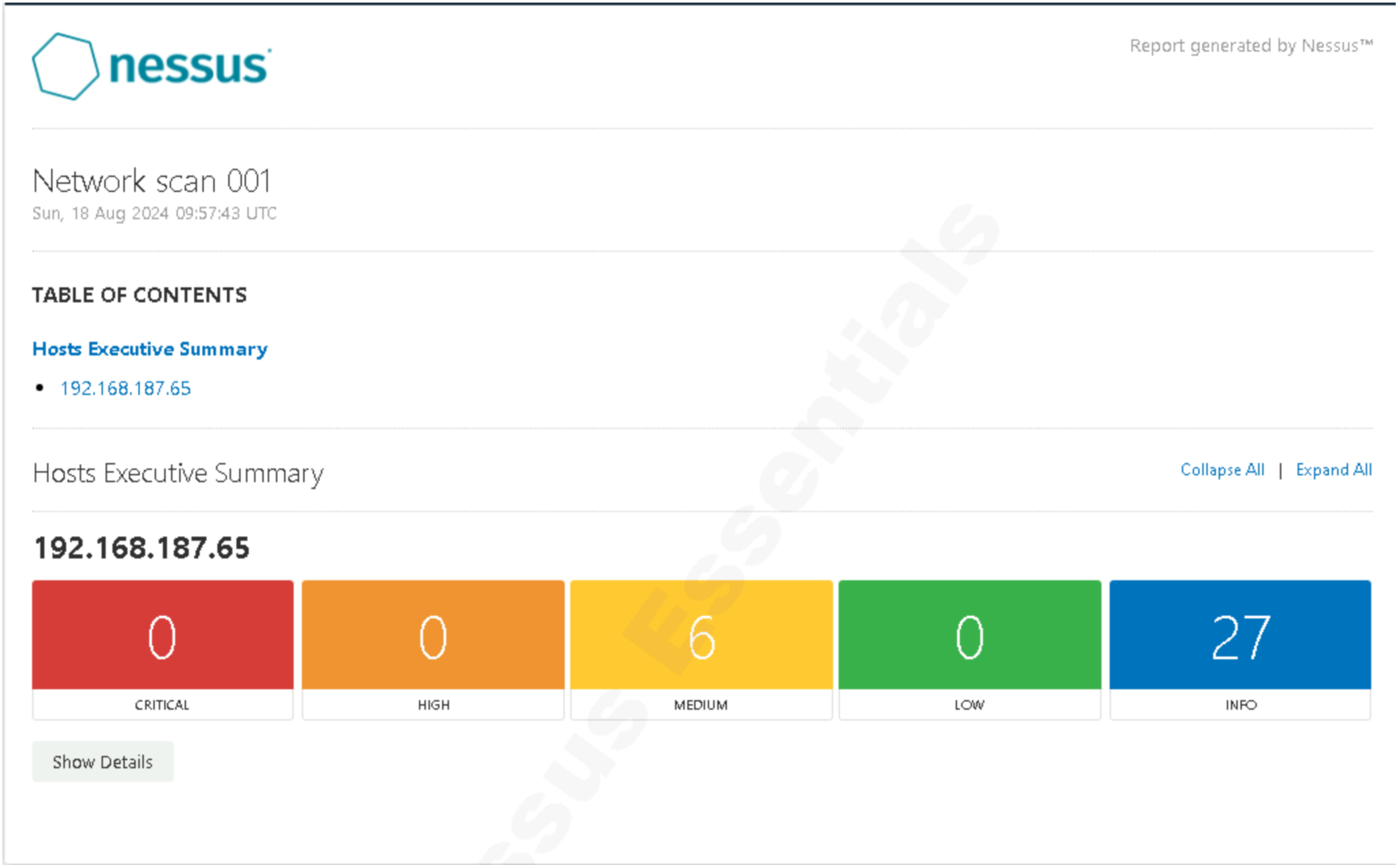
‹ Back to Scan Templates

CGI abuses	4254
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	201

Apache 2.0.x < 2.0.64 Multiple Vulnerabilities	50069
Apache 2.0.x < 2.0.65 Multiple Vulnerabilities	68914
Apache 2.2.x < 2.2.12 Multiple Vulnerabilities	40467
Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow	57603
Apache 2.2.x < 2.2.14 Multiple Vulnerabilities	42052
Apache 2.2.x < 2.2.15 Multiple Vulnerabilities	45004
Apache 2.2.x < 2.2.16 Multiple Vulnerabilities	48205
Apache 2.2.x < 2.2.17 Multiple Vulnerabilities	50070
Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS	53896
Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS	54646
Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS	56216
Apache 2.2.x < 2.2.22 Multiple Vulnerabilities	57791
Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	62101

VULNERABILITY SCAN RESULTS

- **Summary of findings:**
  - Total number of actionable findings:
    - Critical: 0
    - High: 0
    - Medium: 6
    - Low: 0



Report generated by Nessus™

Network scan 001

Sun, 18 Aug 2024 09:57:43 UTC

TABLE OF CONTENTS

Hosts Executive Summary

192.168.187.65

0	0	6	0	27
CRITICAL	HIGH	MEDIUM	LOW	INFO

REMEDIATION RECOMMENDATION

- Fix within 7 days

Finding	Severity Rating	Recommended Fix
SMB Signin not required	MEDIUM	Implement SMB server signing – Microsoft sign communications (always)

- Fix within 30 days

Finding	Severity Rating	Recommended Fix
TLS Version 1.0 detected	Medium	Disable support for
TLS Version 1.1 detected	Medium	Disable support for

- Fix within 60 days

Finding	Severity Rating	Recommended Fix
Certificate cannot be trusted	Medium	Generate a signed certificate for msrdp
SSL Self signed Certificate	Medium	Generate a signed certificate for msrdp
SSL Medium Strength Suites Supported	Medium	Reconfigure msrdp to avoid use of m.s.c.

PASSWORD PENETRATION TEST OUTCOME

- **Methodology:**

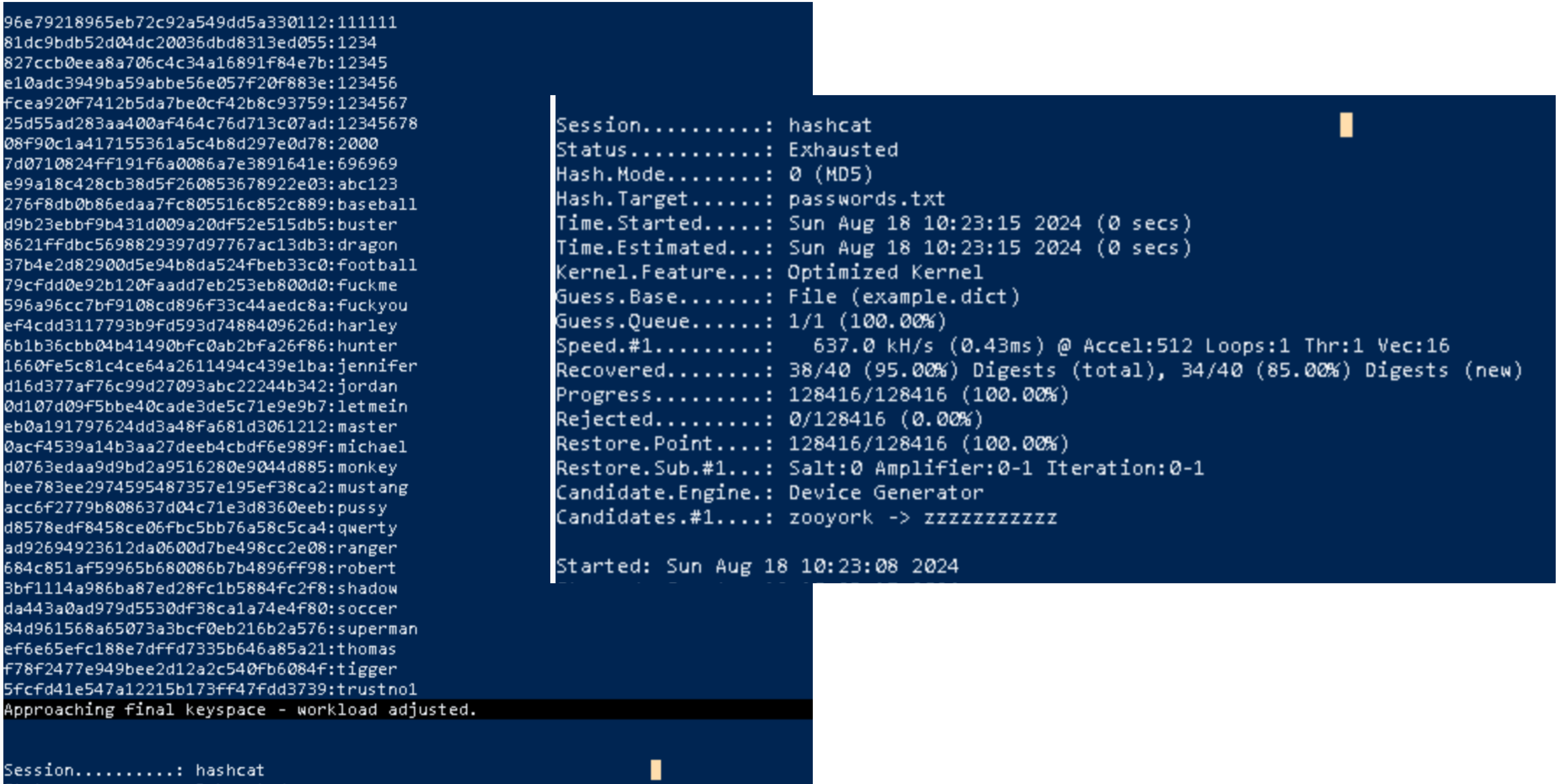
  1. Collected MD5 Hash for passwords

  2. Tested MD5 Hash over hashcat dictionary

  3.
  ```
  .\hashcat.exe -m 0 -a 0 -D 1,2 -O
  passwords.txt example.dict
  ```

- **Number of passwords tested:** 40
- **Number of passwords cracked:** 34
- **Evidence of weak passwords:** **<u>Next slide</u>**

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



```
96e79218965eb72c92a549dd5a330112:111111
81dc9bdb52d04dc20036dbd8313ed055:1234
827ccb0eea8a706c4c34a16891f84e7b:12345
e10adc3949ba59abbe56e057f20f883e:123456
fcea920f7412b5da7be0cf42b8c93759:1234567
25d55ad283aa400af464c76d713c07ad:12345678
08f90c1a417155361a5c4b8d297e0d78:2000
7d0710824ff191f6a0086a7e3891641e:696969
e99a18c428cb38d5f260853678922e03:abc123
276f8db0b86edaa7fc805516c852c889:baseball
d9b23ebbf9b431d009a20df52e515db5:buster
8621ffdbc5698829397d97767ac13db3:dragon
37b4e2d82900d5e94b8da524fbeb33c0:football
79cfdd0e92b120faadd7eb253eb800d0:fuckme
596a96cc7bf9108cd896f33c44aedc8a:fuckyou
ef4cdd3117793b9fd593d7488409626d:harley
6b1b36cbb04b41490bfc0ab2bfa26f86:hunter
1660fe5c81c4ce64a2611494c439e1ba:jennifer
d16d377af76c99d27093abc22244b342:jordan
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
eb0a191797624dd3a48fa681d3061212:master
0acf4539a14b3aa27deeb4cbdf6e989f:michael
d0763edaa9d9bd2a9516280e9044d885:monkey
bee783ee2974595487357e195ef38ca2:mustang
acc6f2779b808637d04c71e3d8360eeb:pussy
d8578edf8458ce06fbc5bb76a58c5ca4:qwerty
ad92694923612da0600d7be498cc2e08:ranger
684c851af59965b680086b7b4896ff98:robert
3bf1114a986ba87ed28fc1b5884fc2f8:shadow
da443a0ad979d5530df38ca1a74e4f80:soccer
84d961568a65073a3bcf0eb216b2a576:superman
ef6e65efc188e7dffd7335b646a85a21:thomas
f78f2477e949bee2d12a2c540fb6084f:tigger
5fcfd41e547a12215b173ff47fdd3739:trustno1
Approaching final keyspace - workload adjusted.


Session..........: hashcat
```

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: passwords.txt
Time.Started.....: Sun Aug 18 10:23:15 2024 (0 secs)
Time.Estimated...: Sun Aug 18 10:23:15 2024 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (example.dict)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   637.0 kH/s (0.43ms) @ Accel:512 Loops:1 Thr:1 Vec:16
Recovered........: 38/40 (95.00%) Digests (total), 34/40 (85.00%) Digests (new)
Progress.........: 128416/128416 (100.00%)
Rejected.........: 0/128416 (0.00%)
Restore.Point....: 128416/128416 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: zooyork -> zzzzzzzzzzz

Started: Sun Aug 18 10:23:08 2024
```

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- Summarize ongoing incident:

  A ransomware attack has been reported, affecting multiple systems used by doctors, nurses, and administrative staff. The ransomware demands a payment of one million dollars in Bitcoin to restore access. Critical systems for patient monitoring and treatment have been compromised, and the log analysis tool is no longer accessible. This situation has been declared a critical security incident by the security leader.

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

- Step 1: Document that end users discovered the issue
- Step 2:
  - Systems not available anymore
  - Critical impact
  - Windows 10 PRO, 192.168.187.65, CYBER-ND03-W10
- Step 3:
  - Incident is confirmed
  - Incident is still in progress
  - Response is urgent
  - Not sure. We don’t care.
  - Ransomware
- Step 4: The lives of the staff are not at risk. The lives of the patients could be at risk.
- Step 6: Category A "A threat to public safety or life." The attack compromises access to clinical care for hospital patients. The other categories, while all true, are of lesser relevance.

INCIDENT RESPONSE RECOMMENDED ACTION

- Summarize recommendation to contain, eradicate, and recover:

1. **Containment:**

- **Isolate Affected Systems:** Immediately disconnect infected systems from the network to prevent further spread of the ransomware.
- **Shutdown Non-Essential Systems:** Temporarily shut down other vulnerable systems to avoid additional infections.
- **Activate the Incident Response Team:** Mobilize the team to handle the situation, ensuring roles and responsibilities are clearly defined.

2. **Eradication:**

- **Remove the Ransomware:** Utilize antivirus and anti-malware tools to thoroughly clean the infected systems.
- **Patch Vulnerabilities:** Identify and fix any vulnerabilities that the ransomware exploited to ensure it doesn’t reoccur.
- **Secure Systems:** Ensure that all traces of the ransomware are eradicated before reconnecting systems to the network.

3. **Recovery:**

- **Restore from Clean Backups:** Use the most recent, unaffected backups to restore critical systems.
- **Validate System Integrity:** Verify that restored systems are functioning properly and are free from ransomware.
- **Monitor for Recurrence:** Implement enhanced monitoring to detect any signs of lingering threats or re-infection.

INCIDENT RESPONSE RECOMMENDED ACTION

- Documented actions and notes from the IR checklist
- Step 7: *Malware procedure. According to the IR document it is required to wipe affected devices clean and fully restore from backup*
- Step 8:
  - Authorization status: At this time, I have not received explicit authorization to review system logs related to the ransomware attack. Without access to these logs, I am unable to directly analyze the sequence of events or identify potential indicators of compromise within the system.
  - Alternative Actions:
    - **Engage Authorized Personnel:** I recommend that authorized members of the Incident Response (IR) team, who have the necessary permissions, perform a thorough review of the system logs. This will include checking security logs, event logs, and any other relevant logs on affected systems and network devices.
    - **Request a Summary:** If direct access to logs is not granted, I will request a summary report from the authorized personnel detailing key findings from their log review.
- 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 weak passwords (view slide 9)
  - Fix SMB vulnerability discovered (view slide 7)
  - Be sure real time malware protection is enabled on all devices
- Step 12:
  - I suggest implementing a SIEM system like Wazuh with the application of appropriate active response criteria.
  - The response was appropriate. The procedure included an explicit reference to the possibility of Ransomware attacks, supported by an operational procedure for removing the infection.
  - We have learned that Ransomware attacks can occur very quickly and cause the Availability of computer systems to fail in very short time frames.