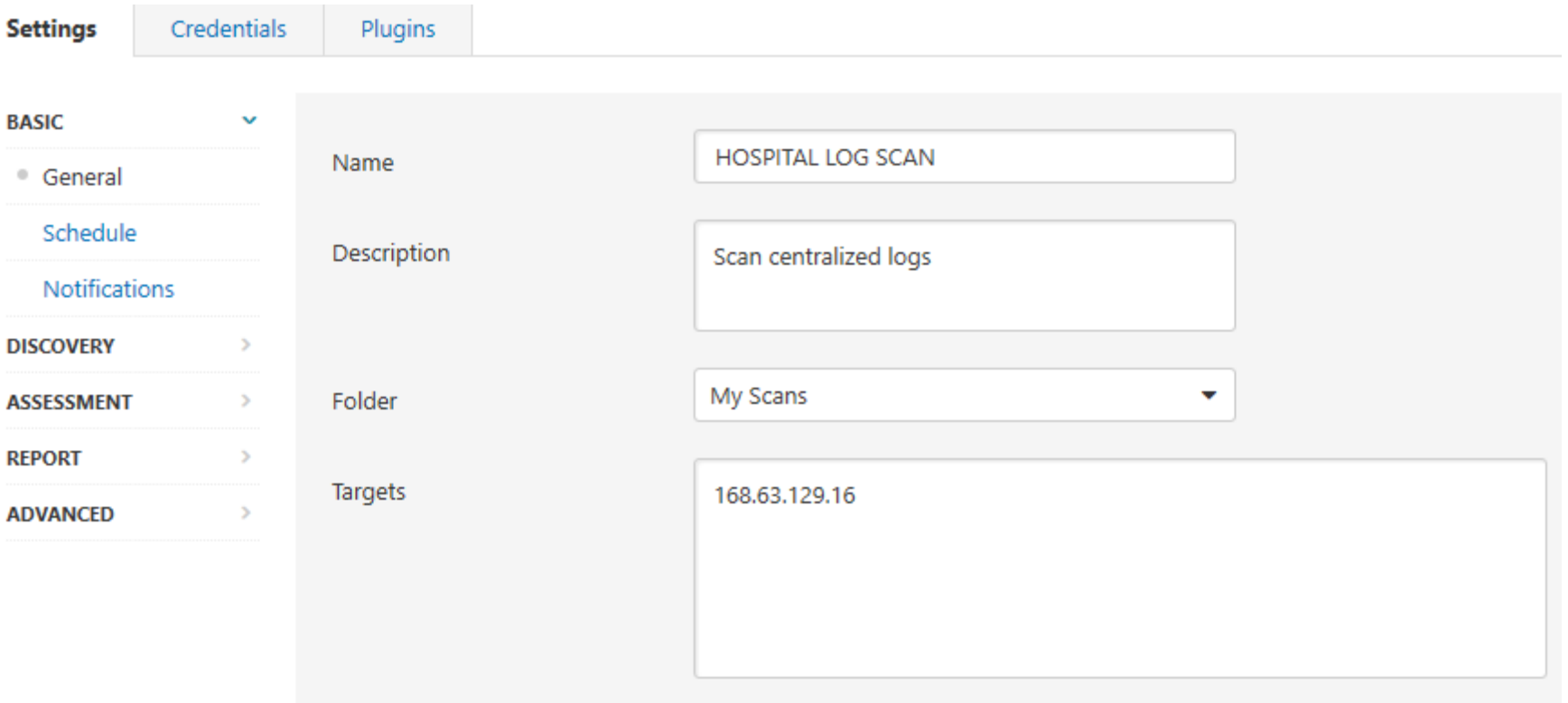
FINAL PROJECT TEMPLATE

THREAT SUMMARY

- **Summary of Situation:** (Summarize the current threat situation)
  - Hospital A, Hospital B, and Hospital C have reported ransomware attack when logging into their centralized log management system
  - Hospital X has not experienced this ransomware attack.
  - These hospitals reported that information was disclosed by an user in the technology department opening an email attachment resource
- **Asset: Target confidential information related to public financial market, particularly healthcare companies**
- **Impact: Confidentiality, Authentication**
- **Threat Actor: FIN4**
- **Threat Actor Motivation: Financially motivated group**
- **Common Threat Actor Techniques:** (Share attack methods commonly used by the threat actor.)
  - **Email Collection: Remote Email Collection**: FIN4 has accessed and hijacked online email communications using stolen credentials.
  - **Hide Artifacts: Email Hiding Rules:** FIN4 has created rules in victim's Microsoft Outlook accounts to automatically delete emails containing words such as "hacked", "phish", and "malware" in a likely attempt to prevent organizations from communicating about their activities.
  - **Phishing: Spear phishing Attachment:** FIN4 has used spearphising emails containing attachments with embedded malicious macros.
  - **User Execution: Malicious Link**: FIN4 has lured victims to click malicious links delivered via spearphising emails.
  - **Common and Scripting Interpreter: Visual Basic**: FIN4 used VBA macros to display a dialogue box and collect victim credentials.

VULNERABILITY SCANNING TARGETS

- **Summary of scan targets:**
  - Number of devices scanned: 1
  - Device type: (operating system and version) Windows 10 Pro Version
  - Primary purpose of device: The devices are servers and used to contain data such as patient information.


Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
HOSPITAL LOG SCAN
Description
Scan centralized logs
Folder
My Scans
Targets
168.63.129.16

Plugins

ENABLED	Web Servers	1231
ENABLED	Windows	4622
ENABLED	Windows : Microsoft Bulletins	2035
ENABLED	Windows : User management	29

VULNERABILITY SCAN RESULTS

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

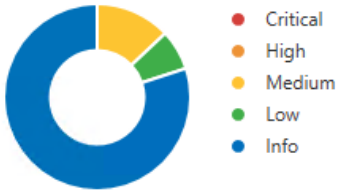
Scan Results

Host	Vulnerabilities
168.63.129.16	2 / 1 / 14

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v2.0
Scanner:	Local Scanner
Start:	Today at 1:02 AM
End:	Today at 1:08 AM
Elapsed:	5 minutes

Vulnerabilities



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

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 (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 }'

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:** (Summarize steps taken to test password security)

1. Use and downloaded Hashcat
2. Using GitHub to downloaded rockyou.txt which is list of passwords.
3. Created a folder within the Hashcat-6.2.5 folder called wordlists
4. Created to 2 text documents: new password and hash. The newpassword.txt had 3 passwords obtained from the rockyou.txt. Using MD5 hash converter via internet, I obtained the hashes for the 3 passwords. I placed these hashes in hash.txt.
5. Using the Command Prompt (CMD), cracked the password using the dictionary file and specify this command **-m 0 -a 0 hash.txt file.txt** which translates into the following arguments:
   - Hash type: - m 0
   - Attack mode: -a 0
   - Hash file: hash.txt
   - Dictionary file: file.dict
   - -m 0 represents the hash type MD5
   - -a 0 represents to dictionary attack mode

- **Number of passwords tested:** 3
- **Number of passwords cracked:** 3
- **Evidence of weak passwords: refer to Slide #11 and Slide #12**
- **Recommended steps to improve passwords security:**
- Setting the Password Policy:

1. ▪ Local Security Policy>Account Policies>Password Policy>Password must meet complexity requirements>change to Enable
2. ▪ Local Security Policy>Account Policies>Password Policy>Minimum password length>8 characters
3. ▪ Local Security Policy>Account Policies>Password Policy>Minimum password age>120 days
4. ▪ Local Security Policy>Account Policies>Password Policy>Enforce password history>change to 5 passwords remembered.

PASSWORD PENETRATION TEST OUTCOME

- Multi-factor Authentication

Setting the Account Lockout Policy:
1. ▪ Local Security Policy>Account Policies>Account Lockout Policy>Account Lockout Threshold>change to 5 invalid logon attempt

```
C:\Users\cyberadmin\Desktop\hashcat-6.2.5>hashcat.exe -m 0 -a 0 C:\Users\cyberadmin\Desktop\hashcat-6.2.5\hash.txt C:\Tools\hashcat-6.2.5\wordlists\newpassword.txt --force
hashcat (v6.2.5) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 2.1 WINDOWS) - Platform #1 [Intel(R) Corporation]
====================================================================
* Device #1: Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz, 1759/3583 MB (447 MB allocatable), 1MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 3 digests; 3 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

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

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: C:\Tools\hashcat-6.2.5\wordlists\newpassword.txt
* Passwords.: 3
* Bytes.....: 29
* Keyspace..: 3
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.
```

```
f25a2fc72690b780b2a14e140ef6a9e0:iloveyou
dc0fa7df3d07904a09288bd2d2bb5f40:7777777
25f9e794323b453885f5181f1b624d0b:123456789

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: C:\Users\cyberadmin\Desktop\hashcat-6.2.5\hash.txt
Time.Started.....: Tue Feb 15 02:57:08 2022, (0 secs)
Time.Estimated...: Tue Feb 15 02:57:08 2022, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (C:\Tools\hashcat-6.2.5\wordlists\newpassword.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    21802 H/s (0.01ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 3/3 (100.00%) Digests
Progress.........: 3/3 (100.00%)
Rejected.........: 0/3 (0.00%)
Restore.Point....: 0/3 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: iloveyou -> 123456789

Started: Tue Feb 15 02:56:56 2022
Stopped: Tue Feb 15 02:57:14 2022
```

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- Summarize ongoing incident:
  - This is the 3rd update.
  - Several hospital staff are not able to access systems unless they pay one million dollars in Bitcoin.
- Document actions or notes from the following steps of the initial incident response checklist

- Step 1: The Help Desk provide a note that the End Users(Doctors, Nurses, and Administrative Staff) discovered that they were asked to pay billion dollars in Bitcoin to access their systems.
- Step 2: The incident team gathers and using the incident checklist, determines that this incident should be escalated to a critical incident. Based upon:
  - Some doctors report being unable to render treatments because they cannot view detailed information about patient status.
  - The control systems used to monitor patient stats are no longer available through the standard user interface.
  - attempt to log into the log analysis tool, but that's no longer accessible.
- Step 3: The following questions on triage are asked:
  - Is the incident confirmed: Yes
  - Is the incident contained already or still in progress? Still in progress
  - What type of incident is this? Malware, Ransomware
- Step 4: Is safety or human like at immediate risk?
  - Yes, patient safety is at risk due the reasons outlined in Step 2
- Step 6: An incident ticket should be created by the Incident Response (IR) team. The category ticket should be opened to:
  - Category one-A threat to public safety or life. The reason for this category is outlined in Step 2.

INCIDENT RESPONSE RECOMMENDED ACTION

- Summarize recommendation to contain, eradicate, and recover:
  - Containment Strategy
    - Redirect the attacker to a sandbox so they can monitor the attacker's activity, to help gather additional evidence.
    - Discuss this strategy with the legal department if possible.
    - Gather evidence during an incident is to resole the incident, it may need for legal proceedings. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed fromo previous discussion with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court.
  - Eradication and Recovery Strategy
    - Eradication is necessary to eliminate the incident such as malware, disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited.
    - Identify the all the affected hosts within the hospitals so they can be remediated.
    - Incident Response (IR) team and administrators restore systems to normal operations, confirm that the systems are functioning normally
    - Remediate vulnerabilities to prevent similar incidents.
- Documented actions and notes from the IR checklist
  - Step 7: Which applicable procedure should the IR team follow based on their understanding of the incident:
    - Database or file denial of service response procedure
  - Step 8: Since not able to log into the log analysis tool, you can try the following:
    - Profile Networks and Systems: measure the characteristics of expected activity so that changes to it can be easily identified.
    - Understand Normal Behaviors. The Incident Response (IR) team should study the networks, systems and applications to understand the normal behaviors is so that abnormal behavior is easily recognized.
    - Evidence of an incident may be captured in several logs:
      - Firewall logs may have the source IP address that was used
      - Network IDPS may detect that an attack was launched against a particular host.
  - Step 9: IR team should make the following changes to prevent the occurrence from happening again or infecting other systems:
    - Re-install the affected system form scratch and restore data from backups. 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.
    - Ensure the system has been hardened by turning off or uninstalling unused services.