WIAM ALMOKHTAR

FINAL PROJECT TEMPLATE

THREAT SUMMARY

- **Summary of Situation:** (Summarize the current threat situation)
two hospitals' management system files have been encrypted by an attacker and the attacker is asking for an amount of bitcoin in order to decrypt the files. The price gets higher as more time passes.

- **Asset:** (What assets are being targeted?)
patient data like medical records.
Other data like employees' information, doners' information, and visitors' information depending on the digital records the hospital keeps

- **Impact:** (What part of the CIA triad is being impacted?)
Confidentiality: the files have been exposed to a party that is not intended to use the system
Integrity: the form of the files has been changed and may be modified since a malicious actor has access to the files
Availability: The authorized parties (hospital employees) are unable to access the system

- **Threat Actor:** (Identify potential threat actors)
External threat: the attacker who sent the email and encrypted the files
Internal threat: the employee who opened the email attachment sent by the attacker. This may be intentional or unintentional

- **Threat Actor Motivation:** (Share potential motivations behind the attacks)
Financially motivated: the cybercriminal is a financially motivated individual who's carrying the attack mainly for money.
Political: the threat actor may be against the recently endorsed law and the attack is a form of protest (hacktivism)
A terminated employee who still holds a grudge against the hospital

- **Common Threat Actor Techniques:** (Share attack methods commonly used by the threat actor)
Phishing: using email attachments to initiate the attack
Ransomware: the unencrypted files are held hostage until the bitcoin amount is paid

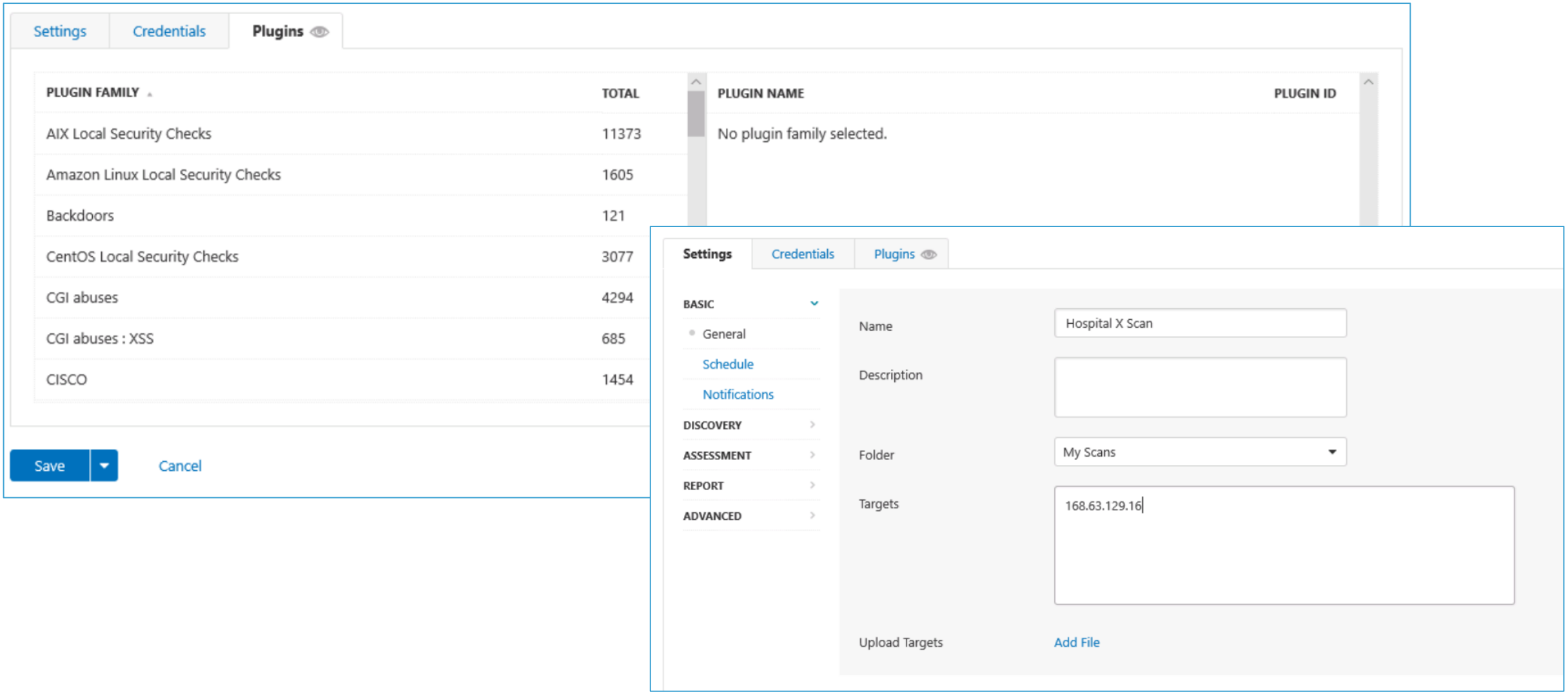
VULNERABILITY SCANNING TARGETS

- **Summary of scan targets:**
  - Number of devices scanned: 1
  - Device type: windows machine
  - Primary purpose of device: (describe what the devices are used for and what kind of data might be on them)

  General purpose PC. It may contain personal/ work data. Used as centralized device for logs, files and backups

(insert 2 screenshots from scan configuration window – one of the settings tab and one of the plugins tab) : **inserted in the next slide**

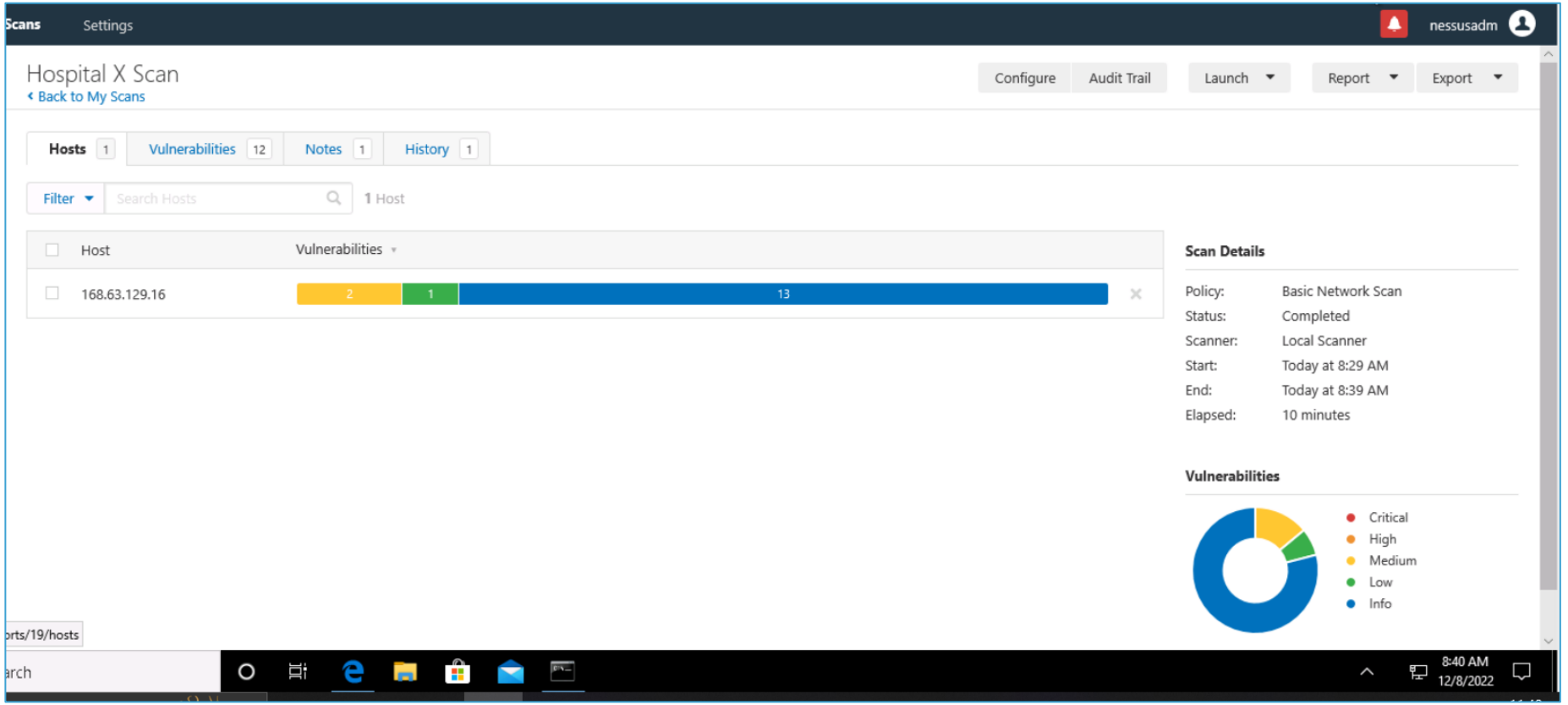
VULNERABILITY SCANNING



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

- Fix within 7 days **(no critical vulnerabilities found)**
- Fix within 30 days

Finding	Severity Rating	Recommended Fix
CVE-1999-0024 DNS cache poisoning via BIND, by predictable query IDs	Medium (5.0)	• use a router to filter all name-based authentication services instead of relying on DNS information for authentication • Upgrade to the latest version of BIND
CVE-2006-0987 DNS server spoofed request amplification DDoS	Medium (5.0)	• Restrict access to DNS server from public networks • Reconfigure DNS server to reject queries that reveal too much information

- Fix within 60 days

Finding	Severity Rating	Recommended Fix
DHCP Server Detection (attempts to retrieve information about network layout)	Low (3.3)	Apply filtering to keep this information off the network

PASSWORD PENETRATION TEST OUTCOME

- **Methodology:** (Summarize steps taken to test password security)
  1- downloaded hashcat
  2- downloaded rockyoufile (dictionary)
  3- placed the given password hashes in a text file hashes.txt
  4- run the command hashcat.exe -m 0 (MD5) -a 0 (attack mode) hashes.txt (target) rockyou.txt
- **Number of passwords tested:** 41
- **Number of passwords cracked:** 39
- **Evidence of weak passwords:** common words/phrases, use of characters a-z only, use of numbers only

(insert screenshot of cracked passwords and command used to launch attack)
next slide

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

- Use characters other than just a-z, 0-9
- Choose long passwords (12 characters minimum)
- Avoid using actual words and names
- Make the password as random as possible
- Use a password management tool to generate variety of strong passwords and manage them

```
C:\Users\Wiama\Desktop\Udacity Course\hashcat-6.2.6>hashcat.exe -m 0 -a 0 hashes.txt rockyou.txt
hashcat (v6.2.6) starting
```

```
Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

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

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: hashes.txt
Time.Started.....: Thu Dec 08 14:29:19 2022 (2 secs)
Time.Estimated...: Thu Dec 08 14:29:21 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2881.2 kH/s (6.35ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Speed.#3.........:  5817.2 kH/s (9.20ms) @ Accel:128 Loops:1 Thr:64 Vec:1
Speed.#*.........:  8698.4 kH/s
Recovered........: 39/40 (97.50%) Digests (total), 39/40 (97.50%) Digests (new)
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 0/14344384 (0.00%)
Restore.Point....: 14306260/14344384 (99.73%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 011038 -> *CHUVI*
Candidates.#3....: $HEX[2a4348554c412a] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 56c Util: 63% Core:1824MHz Mem:3494MHz Bus:4
Hardware.Mon.#3..: N/A

Started: Thu Dec 08 14:29:18 2022
Stopped: Thu Dec 08 14:29:23 2022
```

INCIDENT RESPONSE PRELIMINARY ASSESSMENT

- Summarize ongoing incident:
  - Number of hospitals including my hospital are attacked with ransomware
  - all the files are held hostage by being encrypted until 1 million dollars worth of bitcoin is paid
  - Doctors are no longer able to treat patients due to the unavailability of patient records
  - Audit log can't be accessed
- Document actions or notes from the following steps of the initial incident response checklist

- **Step 1:** inform all employees of the incident and to avoid paying any amount of money
- **Step 2:** gather with the IT team to start investigating the incident and finding the source (the employee who opened the attachment)
- **Step 3:** check if all data can be restored from backup
- **Step 4:** consult legal and finance teams for the right decision in the case that not all data can be restored from backup (pay ransom or sacrifice the missing data)
- **Step 6:** contact the management team to establish a temporary plan to continue seeing patients whose treatment can be managed without referring to the system

INCIDENT RESPONSE RECOMMENDED ACTION

- Summarize recommendation to contain, eradicate, and recover:
  - After discovering the source, all employees need to be educated about the dangers of opening untrusted email attachments to avoid any similar incidents in the future
  - Restore data from backup
  - Remove the ransomware software after restoring data
  - Enable/start using real-time malware protection software to avoid installing any suspicious files from the internet
  - Document the source of the incident, its type, what was done in response, and the effectiveness of the response.

- Documented actions and notes from the IR checklist
  - **Step 7:** *(Tip: Select procedures you'd recommend for this type of incident)*
    - malware response procedure (removing the ransomware)
    - System failure procedure
  - **Step 8:** interview employees to determine who caused the incident and whether it was intentional or unintentional.
  - **Step 9:** reconfigure firewall to prevent any traffic from the IP address that sent the email
  - **Step 10:** restore data from backup
  - **Step 11:** enable/obtain a real-time malware detection/prevention system
  - **Step12:** Raise employees' awareness regarding phishing emails and other common attacks
  - **Step13:** Document all the steps followed to respond to the incident