GCIH$^{\text{Q\&As}}$

GIAC Certified Incident Handler

QUESTION 1

Which of the following would be exposed to an attacker as a result of a remote employee attempting to connect to company resources without a VPN?

A. The employee\\'s private key

B. The employee\\'s domain credentials

C. The laptop\\'s private key

D. The laptop\\'s encryption password

Correct Answer: B

QUESTION 2

What is the best practice for analyzing network traffic in a production environment to minimize the risks associated with such activities?

A. Use a passive monitoring tool like p0f to capture and analyze the traffic as a privileged user

B. Use the wireshark tool for both capturing and analyzing the traffic as a privileged user

C. Capture the traffic with tcpdump, then analyze the traffic with wireshark using an unprivileged account

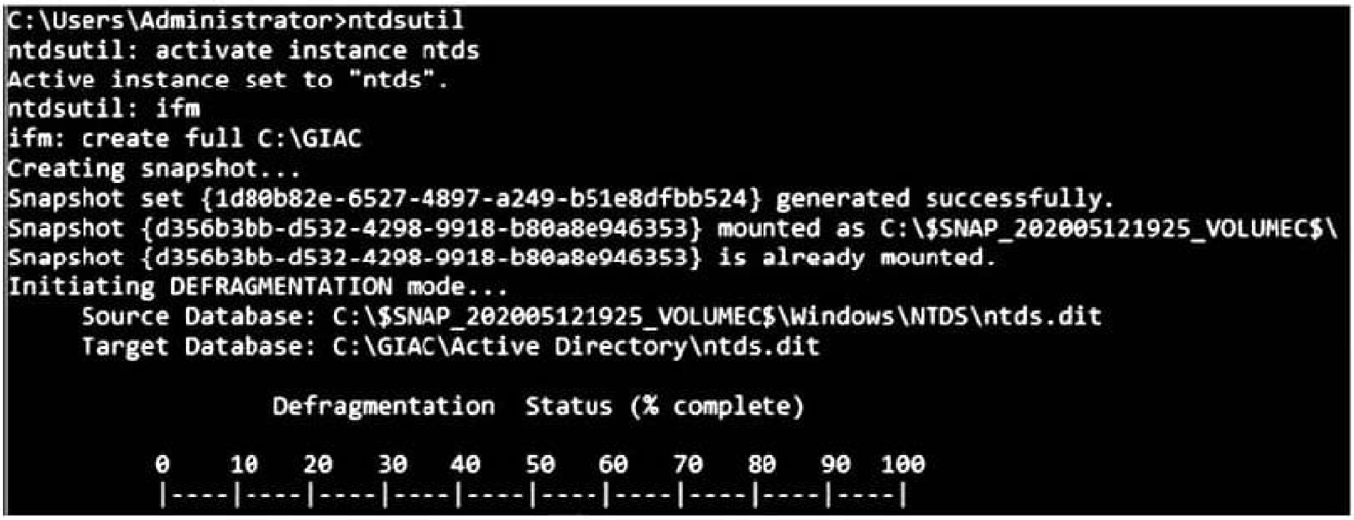
D. Capture the traffic with wireshark, then analyze the traffic with tcpdump using an unprivileged account

Correct Answer: C

Tools which parse data from the network are susceptible to buffer overflows. And wireshark especially has a long history of having issues with buffer overflows. Sniffing traffic as a privileged user would give an attacker administrative access on the machine the network administrator was running on if the attacker were able to take advantage of a buffer overflow. The safest way to sniff traffic from a network is to use tcpdump to capture the data, as tcpdump has not had the many buffer overflow problems which wireshark has had over the years. After capturing the packets, the network administrator could analyze the pcap file offline using a wireshark as a non-privileged user. The p0f tool is used to identify and fingerprint systems, not identify unusual traffic.

QUESTION 3

What is the goal of an attacker who has entered the commands shown in the screenshot?



```
C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: create full C:\GIAC
Creating snapshot...
Snapshot set {1d80b82e-6527-4897-a249-b51e8dfbb524} generated successfully.
Snapshot {d356b3bb-d532-4298-9918-b80a8e946353} mounted as C:\$SNAP_202005121925_VOLUMEC$\
Snapshot {d356b3bb-d532-4298-9918-b80a8e946353} is already mounted.
Initiating DEFRAGMENTATION mode...
     Source Database: C:\$SNAP_202005121925_VOLUMEC$\Windows\NTDS\ntds.dit
     Target Database: C:\GIAC\Active Directory\ntds.dit

                  Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
```

A. Enumerate listening ports on the target machine

B. Create a mountable snapshot to access older versions of the filesystem

C. Gather password and hash data for off-line cracking

D. Corrupt system backups

Correct Answer: C

QUESTION 4

Stacy is the lead of the network services team. She suspects that Keith, one of the network administrators, is not spending as much time working as he states he is. She suspects he is spending time researching the screenplay he is writing about the office. She asks a security analyst to track Keith\\'s web usage to verify what he is doing. What should the security analyst do next?

A. Direct Stacy to discuss her concerns with Keith regarding his work habits

B. Monitor his web browsing and let Stacy know if anything is suspicious

C. Email the logs from the web content filter to Stacy

D. Direct Stacy to contact Human Resources to start an investigation

Correct Answer: D

All requests for employee monitoring should come from Human Resources. No further actions should be taken from a technical standpoint without a formal request from Human Resources.

QUESTION 5

You are concerned about rootkits on your network communicating with attackers outside your network. Without using an IDS how can you detect this sort of activity?

A. By examining your domain controller server logs.

B. You cannot, you need an IDS.

C. By examining your firewall logs.

D. By setting up a DMZ.

Correct Answer: C