GCIH$^{Q\&As}$

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

QUESTION 1

Which of the following will best protect your network from being mapped by untrusted, external sources, while still allowing trusted sources to verify network connectivity with ping requests and replies?

A. Use settings on a network mapping tool to limit inbound ICMP and protect your network

B. Establish an IDS on the DMZ to alert on all inbound ICMP requests

C. Shut down ICMP and traceroute on your internal servers

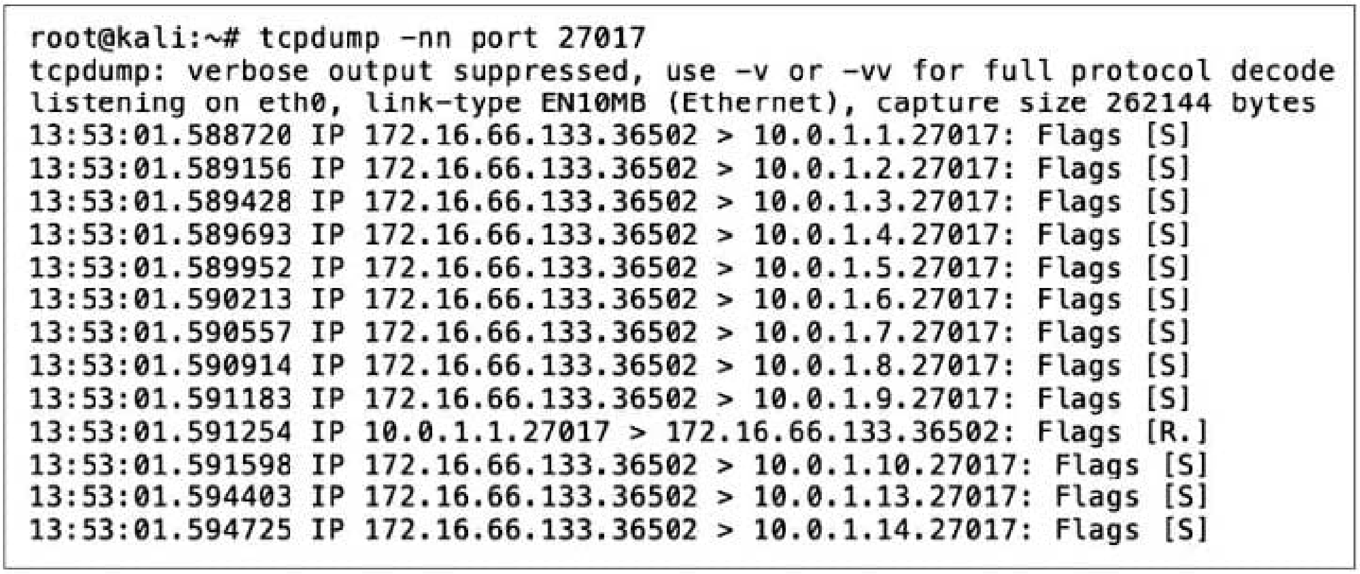
D. Filter ICMP at the perimeter, allowing ICMP only from trusted sources

Correct Answer: D

Creating a filter on your perimeter firewall is an easy way to restrict inbound ICMP requests. You can specify certain IP addresses that can legitimately ping you and drop all others. An IDS can be configured to inform you of ping sweep activity, but establishing one on your DMZ to report all ICMP requests will create an overwhelming number of alerts ?far too many to be an effective security measure. Shutting down ICMP on your internal servers does nothing to protect the perimeter. Finally, if the bad guys are the ones using the network mapping tools against your perimeter, it is unlikely that they will configure their mapping tools to allow protection of your network.

QUESTION 2

During which phase of incident response would an analyst review the data below?



```
root@kali:~# tcpdump -nn port 27017
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:53:01.588720 IP 172.16.66.133.36502 > 10.0.1.1.27017: Flags [S]
13:53:01.589156 IP 172.16.66.133.36502 > 10.0.1.2.27017: Flags [S]
13:53:01.589428 IP 172.16.66.133.36502 > 10.0.1.3.27017: Flags [S]
13:53:01.589693 IP 172.16.66.133.36502 > 10.0.1.4.27017: Flags [S]
13:53:01.589952 IP 172.16.66.133.36502 > 10.0.1.5.27017: Flags [S]
13:53:01.590213 IP 172.16.66.133.36502 > 10.0.1.6.27017: Flags [S]
13:53:01.590557 IP 172.16.66.133.36502 > 10.0.1.7.27017: Flags [S]
13:53:01.590914 IP 172.16.66.133.36502 > 10.0.1.8.27017: Flags [S]
13:53:01.591183 IP 172.16.66.133.36502 > 10.0.1.9.27017: Flags [S]
13:53:01.591254 IP 10.0.1.1.27017 > 172.16.66.133.36502: Flags [R.]
13:53:01.591598 IP 172.16.66.133.36502 > 10.0.1.10.27017: Flags [S]
13:53:01.594403 IP 172.16.66.133.36502 > 10.0.1.13.27017: Flags [S]
13:53:01.594725 IP 172.16.66.133.36502 > 10.0.1.14.27017: Flags [S]
```

A. Preparation

B. Reconnaissance

C. Detection

D. Enumeration

Correct Answer: A

Reference: https://www.securitymetrics.com/blog/6-phases-incident-response-plan

QUESTION 3

An attacker sends a large number of packets to a target computer that causes denial of service. Which of the following type of attacks is this?

A. Spoofing

B. Snooping

C. Phishing

D. Flooding

Correct Answer: D

QUESTION 4

Assuming you use each program listed, of the choices listed below, which represents the BEST defense against protocol parser vulnerabilities?

A. Disable scripts in Internet Explorer

B. Disable the Outlook preview pane

C. Keep Nmap fully patched

D. Keep tcpdump fully patched

Correct Answer: D

But, pay extra special attention to your sniffer tools and their associated analysis programs, such as Wireshark, Snort, tcpdump, Netmon, or any others. These tools must be carefully patched on a frequent basis, as vendors release fixes. These sniffing programs are often installed on sensitive networks, such as DMZs, data centers, and so on, because these locations are where you want to monitor traffic. Therefore, we have an application type that often has vulnerabilities, and is located on or near sensitive machines. An unpatched sniffer system is akin to asking for trouble on your network.

QUESTION 5

John works as a Professional Ethical Hacker for NetPerfect Inc. The company has a Linux-based network. All client computers are running on Red Hat 7.0 Linux. The Sales Manager of the company complains to John that his system contains an unknown package named as tar.gz and his documents are exploited. To resolve the problem, John uses a Port scanner to enquire about the open ports and finds out that the HTTP server service port on 27374 is open. He suspects that the other computers on the network are also facing the same problem. John discovers that a malicious application is using the synscan tool to randomly generate IP addresses.

Which of the following worms has attacked the computer?

A. Code red

B. Ramen

C. LoveLetter

D. Nimda

Correct Answer: B

QUESTION 6

You work as a Network Administrator for InformSec Inc. You find that the TCP port number 23476 is open on your server. You suspect that there may be a Trojan named Donald Dick installed on your server. Now you want to verify whether Donald Dick is installed on it or not. For this, you want to know the process running on port 23476, as well as the process id, process name, and the path of the process on your server. Which of the following applications will you most likely use to accomplish the task?

A. Tripwire

B. SubSeven

C. Netstat

D. Fport

Correct Answer: D

QUESTION 7

You have responded to the breach of an internal file server that contains highly confidential strategic information. The attacker compromised the server and created a local administrator. The compromise was discovered quickly, and the

network cable was disconnected from the server.

Management has decided that they do not want to risk any bad publicity and will not seek prosecution of the attacker.

IT management will allow you to rebuild the server over the weekend. Until then, you create a plan to lock the administrator account, block RDP traffic with a firewall rule, and create email alerts on network traffic and from the affected server.

What phase of the incident response process is addressed by your plan?

A. Recovery

B. Containment

C. Eradication

D. Identification

Correct Answer: B

You are in the containment phase of the incident handling process. The eradication phase will kick in once you remove the administrative account and any remnants of the attack and isolate the cause of the compromise, and the recovery phase will occur when the system is brought back online. The identification phase has already occurred when the compromise was discovered.

QUESTION 8

An attacker has used an infected USB thumb drive to compromise an internal host. The host is firewalled, blocking all inbound ports and protocols, and allowing tcp port 8080 outbound through an internal proxy. Which covert method would the attacker use to control the remote host?

A. Ptunnel

B. Passive FTP

C. Reverse HTTP shell

D. Covert_TCP

Correct Answer: C

A reverse HTTP shell allows an attacker to connect outbound over HTTP (regardless of port) and this will work through proxies as well. Ptunnel requires ICMP. Covert_TCP will not facilitate remote control. Passive FTP is not a covert method nor does it facilitate remote control.

QUESTION 9

You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are working as a root user on the Linux operating system. Your company is facing an IP spoofing attack.

Which of the following tools will you use to get an alert saying that an upcoming IP packet is being spoofed?

A. Despoof

B. Dsniff

C. ethereal

D. Neotrace

Correct Answer: A

QUESTION 10

Which of the following would allow you to automatically close connections or restart a server or service when a DoS attack is detected?

A. Signature-based IDS

B. Network-based IDS

C. Passive IDS

D. Active IDS

Correct Answer: D

QUESTION 11

Which of the following commands would set up an administrative session with a remote system and mount "one" on your system?

A. mount \\10.0.0.1\one adminpassword /u:adminuser

B. net use \\10.0.0.1\one adminpassword /u:adminuser

C. net mount \\10.0.0.1\one /p:adminpassword /u:adminuser

D. net use \\10.0.0.1\one adminpassword adminuser

Correct Answer: B

QUESTION 12

You want to connect to your friend\\'s computer and run a Trojan on it. Which of the following tools will you use to accomplish the task?

A. PSExec

B. Remoxec

C. Hk.exe

D. GetAdmin.exe

Correct Answer: A

QUESTION 13

OutGuess is used for ___________ attack.

A. Steganography

B. Web password cracking

C. SQL injection

D. Man-in-the-middle

Correct Answer: A

QUESTION 14

You work as a System Administrator for Happy World Inc. Your company has a server named uC1 that runs Windows Server 2008. The Windows Server virtualization role service is installed on the uC1 server which hosts one virtual machine that also runs Windows Server 2008. You are required to install a new application on the virtual machine. You need to ensure that in case of a failure of the application installation, you are able to quickly restore the virtual machine to its original state.

Which of the following actions will you perform to accomplish the task?

A. Use the Virtualization Management Console to save the state of the virtual machine.

B. Log on to the virtual host and create a new dynamically expanding virtual hard disk.

C. Use the Virtualization Management Console to create a snapshot of the virtual machine.

D. Use the Edit Virtual Hard Disk Wizard to copy the virtual hard disk of the virtual machine.

Correct Answer: C

QUESTION 15

Which of the following would be a recommended containment measure taken to prevent a bot infected system from communicating over command and control channels?

A. Configuring a host IPS to block incoming web traffic

B. Updating the system to the current patch level

C. Setting an egress firewall rule at the host\\'s subnet perimeter

D. Changing the system\\'s DNS pointer to a different IP address

Correct Answer: C

Bot infected systems communicate with CandC servers via outbound connections over many types of protocols and applications. The best way to prevent these communications during containment would be an egress firewall rule. Changing the host\\'s DNS pointer, patching the already infected host, and using host IPS to block incoming web traffic wouldn\\'t prevent CandC outbound connections.