GIAC

GPEN Exam

GIAC Certified Penetration Tester

[Questions & Answers Demo]

Version: 9.0

Question: 1

ACME corporation has decided to setup wireless (IEEE 802.11) network in it's sales branch at Tokyo and found that channels 1, 6, 9,11 are in use by the neighboring offices. Which is the best channel they can use?

A. 4
B. 5
C. 10
D. 2

Answer: D

Question: 2

Which Metasploitvncinject stager will allow VNC communications from the attacker to a listening port of the attacker's choosing on the victim machine?

A. Vncinject/find.lag
B. Vncinject/reverse.tcp
C. Vncinject/reverse-http
D. Vncinject /bind.tcp

Answer: B

Explanation:
Reference:
http://www.rapid7.com/db/modules/payload/windows/vncinject/reverse_tcp

Question: 3

What is the MOST important document to obtain before beginning any penetration testing?

A. Project plan
B. Exceptions document
C. Project contact list
D. A written statement of permission

Answer: A

Explanation:
Reference:

Before starting a penetration test, all targets must be identified. These targets should be obtained from the customer during the initial questionnaire phase. Targets can be given in the form of specific IP addresses, network ranges, or domain names by the customer. In some instances, the only target the customer provides is the name of the organization and expects the testers be able to identify the rest on their own. It is important to define if systems like firewalls and IDS/IPS or networking equipment that are between the tester and the final target are also part of the scope. Additional elements such as upstream providers, and other 3rd party providers should be identified and defined whether they are in scope or not.

Question: 4

While reviewing traffic from a tcpdump capture, you notice the following commands being sent from a remote system to one of your web servers:
C:\>sc winternet.host.com create ncservicebinpath- "c:\tools\ncexe -I -p 2222 -e cmd.exe"
C:\>sc vJnternet.host.com query ncservice.
What is the intent of the commands?

A. The first command creates a backdoor shell as a service. It is being started on TCP2222 using cmd.exe. The second command verifies the service is created and itsstatus.
B. The first command creates a backdoor shell as a service. It is being started on UDP2222 using cmd.exe. The second command verifies the service is created and itsstatus.
C. This creates a service called ncservice which is linked to the cmd.exe command andits designed to stop any instance of nc.exe being run. The second command verifiesthe service is created and its status.
D. The first command verifies the service is created and its status. The secondcommand creates a backdoor shell as a service. It is being started on TCP 2222connected to cmd.exe.

Answer: C

Question: 5

Which of the following best describes a client side exploit?

A. Attack of a client application that retrieves content from the network
B. Attack that escalates user privileged to root or administrator
C. Attack of a service listening on a client system
D. Attack on the physical machine

Answer: C

Question: 6

Which of the following TCP packet sequences are common during a SYN (or half-open) scan?

A. The source computer sends SYN and the destination computer responds with RST
B. The source computer sends SYN-ACK and no response Is received from the destination computer
C. The source computer sends SYN and no response is received from the destination computer

D. The source computer sends SYN-ACK and the destination computer responds with RST-ACK
A. A,B and C
B. A and C
C. C and D
D. C and D

Answer: C

Question: 7

Which of the following describes the direction of the challenges issued when establishing a wireless (IEEE 802.11) connection?

A. One-way, the client challenges the access point
B. One-way, the access point challenges the client
C. No challenges occur (or wireless connection
D. Two-way, both the client and the access point challenge each other

Answer: D

Question: 8

You have gained shell on a Windows host and want to find other machines to pivot to, but the rules of engagement state that you can only use tools that are already available. How could you find other machines on the target network?

A. Use the "ping" utility to automatically discover other hosts
B. Use the "ping" utility in a for loop to sweep the network.
C. Use the "edit" utility to read the target's HOSTS file.
D. Use the "net share" utility to see who is connected to local shared drives.

Answer: B

Explanation:
Reference:
http://www.slashroot.in/what-ping-sweep-and-how-do-ping-sweep

Question: 9

A penetration tester obtains telnet access to a target machine using a captured credential. While trying to transfer her exploit to the target machine, the network intrusion detection systems keeps detecting her exploit and terminating her connection. Which of the following actions will help the penetration tester transfer an exploit and compile it in the target system?

A. Use the http service's PUT command to push the file onto the target machine.
B. Use the scp service, protocol SSHv2 to pull the file onto the target machine.

C. Use the telnet service's ECHO option to pull the file onto the target machine
D. Use the ftp service in passive mode to push the file onto the target machine.

Answer: D

Question: 10

What section of the penetration test or ethical hacking engagement final report is used to detail and prioritize the results of your testing?

A. Methodology
B. Conclusions
C. Executive Summary
D. Findings

Answer: C

Question: 11

You are pen testing a Windows system remotely via a raw netcat shell. You want to quickly change directories to where the Windows operating system resides, what command could you use?

A. cd systemroot
B. cd-
C. cd /systemroot/
D. cd %systemroot%

Answer: B

Question: 12

A client with 7200 employees in 14 cities (all connected via high speed WAN connections) has suffered a major external security breach via a desktop which cost them more than SI 72.000 and the loss of a high profile client. They ask you to perform a desktop vulnerability assessment to identify everything that needs to be patched. Using Nessus you find tens of thousands of vulnerabilities that need to be patched. In the report you find workstations running several Windows OS versions and service pack levels, anti-virus software from multiple vendors several major browser versions and different versions of Acrobat Reader. Which of the following recommendations should you provide with the report?

A. The client should standardize their desktop software
B. The client should eliminate workstations to reduce workload
C. The client should hire more people to catch up on patches
D. The client should perform monthly vulnerability assessments

Answer: C

Question: 13

Which Metasploit payload includes simple upload and download functionality for moving files to and from compromised systems?

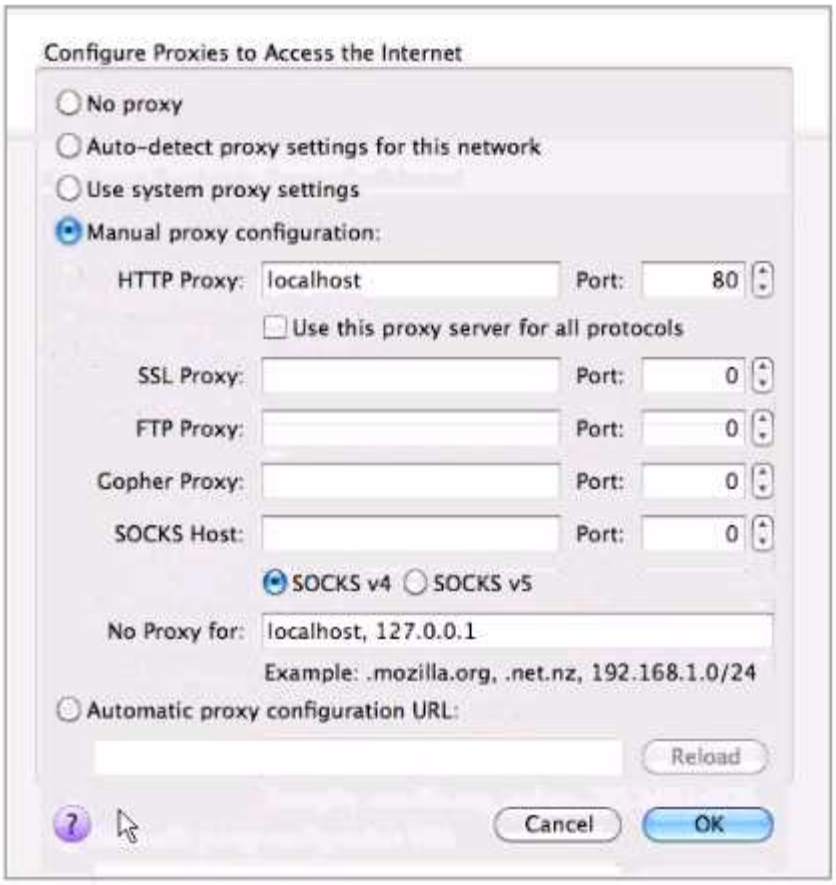
A. DLL inject
B. Upexec
C. Meterpreter
D. Vncinject

Answer: D

Explanation:
Reference:
http://www.opensourceforu.com/2011/02/metasploit-meterpreter-payload/

Question: 14

A junior penetration tester at your firm is using a non-transparent proxy for the first time to test a web server. He sees the web site In his browser but nothing shows up In the proxy. He tells you that he just installed the non-transparent proxy on his computer and didn't change any defaults. After verifying the proxy is running, you ask him to open up his browser configuration, as shown in the figure, which of the following recommendations will correctly allow him to use the transparent proxy with his browser?



A. He should change the PORT: value to match the port used by the non-transparentproxy.
B. He should select the checkbox "use this proxy server for all protocols" for theproxy to function correctly.
C. He should change the HTTP PROXY value to 127.0.0.1 since the non-transparentproxy is running on the same machine as the browser.
D. He should select NO PROXY instead of MANUAL PROXY CONFIGURATION as thissetting is only necessary to access the Internet behind protected networks.

Answer: C

Question: 15

Which of the following describe the benefits to a pass-the-hash attack over traditional password cracking?

A. No triggering of IDS signatures from the attack privileges at the level of theacquired password hash and no corruption of the LSASS process.
B. No triggering of IDS signatures from the attack, no account lockout and use ofnative windows file and print sharing tools on the compromised system.
C. No account lockout, privileges at the level of the acquired password hash and useof native windows file and print Sharif tools on the compromised system.

D. No account lockout, use of native file and print sharing tools on the compromisedsystem and no corruption of the LSASS process.

Answer: D

Question: 16

You are pen testing a Linux target from your windows-based attack platform. You just moved a script file from the windows system to the Linux target, but it will not execute properly. What is the most likely problem?

A. The byte length is different on the two machines
B. End of-line characters are different on the two machines
C. The file must have become corrupt during transfer
D. ASCII character sets are different on the two machines

Answer: A

Question: 17

Which of the following is the JavaScript variable used to store a cookie?

A. Browsercookie
B. Windowcookie
C. Document cookie
D. Session cookie

Answer: C

Explanation:
Reference:
http://www.w3schools.com/js/js_cookies.asp

Question: 18

Analyze the command output below. Given this information, which is the appropriate next step for the tester?
Starting Nmap4.53 (hnp://insecure.org I at2010-09-30 19:13 EDT interesting ports on 192.163.116.101:
PORT STATE SERVICE
130/tcp filtered cisco-fna
131/tcp filtered cisco-tna
132/tcp filtered cisco-sys
133/tcp filtered statsrv
134/tcp filtered Ingres-net
135/tcp filtered msrpc

136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp open netbios-ssn
140/tcp filtered emfis-data
MAC Address: 00:30:1&:B8:14:8B (Shuttle)
warning: OSS can results may be unreliable because we could not find at least l open and l closed port
Device type, general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2
Network Distance : 1 hop
Nmap done: l IP address (I host up) scanned in l .263 seconds

A. Determine the MAC address of the scanned host.
B. Send a single SYN packet to port 139/tcp on the host.
C. Send spoofed packets to attempt to evade any firewall
D. Request a list of shares from the scanned host.

Answer: B

Question: 19

The resulting business impact, of the penetration test or ethical hacking engagement is explained in what section of the final report?

A. Problems
B. Findings
C. Impact Assessment
D. Executive Summary

Answer: D

Explanation:
Reference:
http://www.frost.com/upld/get-data.do?id=1568233

Question: 20

You have been contracted to map me network and try to compromise the servers for a client. Which of the following would be an example of scope creep' with respect to this penetration testing project?

A. Disclosing information forbidden in the NDA
B. Compromising a server then escalating privileges
C. Being asked to compromise workstations
D. Scanning network systems slowly so you are not detected

Answer: B

Question: 21

You are running a vulnerability scan on a remote network and the traffic Is not making It to the target system. You investigate the connection issue and determine that the traffic is making it to the internal interface of your network firewall, but not making. It to the external Interface or to any systems outside your firewall. What is the most likely problem?

A. Your network firewall is blocking the traffic
B. The NAT or pat tables on your network based firewall are filling up and droppingthe traffic
C. A host based firewall is blocking the traffic
D. Your ISP Is blocking the traffic

Answer: C

Question: 22

Identify the network activity shown below;

```
09:12:43.195402 arp who-has 192.168.1.1 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.195883 arp who-has 192.168.1.2 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.196144 arp who-has 192.168.1.3 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.196458 arp who-has 192.168.1.4 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.196885 arp who-has 192.168.1.5 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.197339 arp who-has 192.168.1.6 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.197756 arp who-has 192.168.1.7 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.198027 arp who-has 192.168.1.8 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.198403 arp who-has 192.168.1.9 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.198672 arp who-has 192.168.1.10 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.202376 arp reply 192.168.1.1 is-at 00:1a:8c:15:59:8c
09:12:43.202404 arp reply 192.168.1.2 is-at d8:d3:85:e1:92:14
09:12:43.202753 arp reply 192.168.1.5 is-at 00:12:17:59:a7:2c
09:12:43.205359 arp who-has 192.168.1.13 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.205681 arp who-has 192.168.1.14 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.205959 arp who-has 192.168.1.15 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.206266 arp who-has 192.168.1.16 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.206435 arp reply 192.168.1.13 is-at 00:13:d3:fb:cf:47
09:12:43.206698 arp who-has 192.168.1.17 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.206970 arp who-has 192.168.1.18 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.209056 arp reply 192.168.1.17 is-at 00:10:75:05:b7:ff
09:12:43.212146 arp who-has 192.168.1.21 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.212581 arp who-has 192.168.1.22 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.213033 arp who-has 192.168.1.23 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.213304 arp who-has 192.168.1.24 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.215097 arp reply 192.168.1.24 is-at 00:13:d3:fb:cf:8d
09:12:43.218009 arp who-has 192.168.1.27 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.218430 arp who-has 192.168.1.28 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.219604 arp reply 192.168.1.28 is-at 00:30:1b:3f:4c:8c
09:12:43.223106 arp who-has 192.168.1.31 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.223470 arp reply 192.168.1.31 is-at 00:16:cf:aa:7c:0e
09:12:43.223633 arp who-has 192.168.1.32 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.226798 arp who-has 192.168.1.35 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.227237 arp who-has 192.168.1.36 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.228871 arp reply 192.168.1.35 is-at 00:11:0a:ca:d4:a9
09:12:43.231682 arp who-has 192.168.1.39 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
09:12:43.231961 arp who-has 192.168.1.40 (ff:ff:ff:ff:ff:ff) tell 192.168.1.238
```

A. A sweep of available hosts on the local subnet
B. A flood of the local switch's CAM table.
C. An attempt to disassociate wireless clients.
D. An attempt to impersonate the local gateway

Answer: D

Question: 23

You have compromised a Windows workstation using Metasploit and have injected the Meterpreter payload into the svchost process. After modifying some files to set up a persistent backdoor you realize that you will need to change the modified and access times of the files to ensure that the administrator can't see the changes you made. Which Meterpreter module would you need to load in order to do this?

A. Core
B. Priv
C. Stdapi
D. Browser

Answer: D

Question: 24

How can web server logs be leveraged to perform Cross-Site Scripting (XSSI?

A. Web logs containing XSS may execute shell scripts when opened In a GUI textbrowser
B. XSS attacks cause web logs to become unreadable and therefore are an effective DOS attack.
C. If web logs are viewed in a web-based console, log entries containing XSS mayexecute on the browser.
D. When web logs are viewed in a terminal. XSS can escape to the shell and executecommands.

Answer: C

Question: 25

What is the impact on pre-calculated Rainbow Tables of adding multiple salts to a set of passwords?

A. Salts increases the time to crack the original password by increasing the number oftables that must be calculated.
B. Salts double the total size of a rainbow table database.
C. Salts can be reversed or removed from encoding quickly to produce unsaltedhashes.
D. Salts have little effect because they can be calculated on the fly with applicationssuch as Ophcrack.

Answer: B