Question #1 *Topic 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

Correct Answer: *D*

Community vote distribution

A (100%)

None

Question #2

Topic 1

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

Correct Answer: *B*

Reference:

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

None

Question #3 *Topic 1*

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

Correct Answer: *A*

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.

Community vote distribution

D (100%)

None

Question #4 *Topic 1*

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

Correct Answer: *A*

Community vote distribution

A (100%)

None

Question #5 *Topic 1*

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

Correct Answer: *C*

None

Question #6 *Topic 1*

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

A. A,B and C

B. A and C

C. C and D

D. C and D

Correct Answer: *C*

Community vote distribution

B (100%)

None

Question #7 *Topic 1*

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

Correct Answer: *D*

Community vote distribution

B (100%)

None

Question #8 *Topic 1*

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.

Correct Answer: *B*
Reference:
http://www.slashroot.in/what-ping-sweep-and-how-do-ping-sweep

None

Question #9 Topic 1

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.

Correct Answer: *D*

Community vote distribution

B (100%)

None

Question #10 *Topic 1*

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

Correct Answer: *C*

Community vote distribution

D (100%)

None

Question #11 *Topic 1*

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%

Correct Answer: *D*

Community vote distribution

D (100%)

None

Question #12 *Topic 1*

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

Correct Answer: *A*

Community vote distribution

A (100%)

None

Question #13 *Topic 1*

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

Correct Answer: *C*

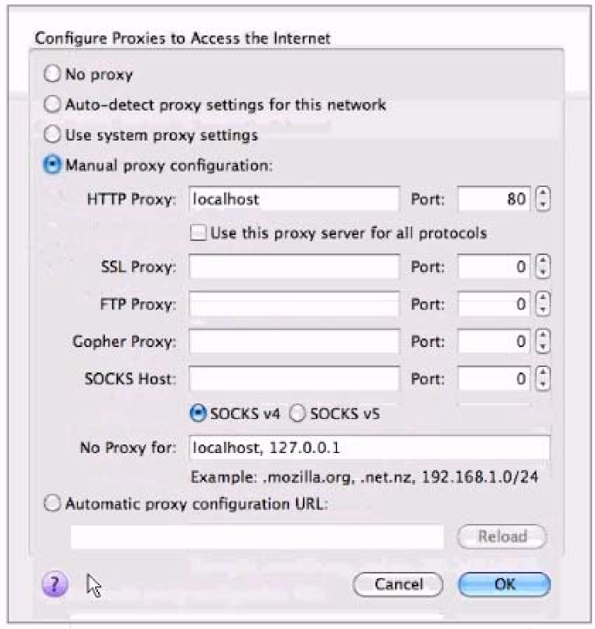
Community vote distribution

C (100%)

None

Question #14 *Topic 1*

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?



Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: localhost Port: 80

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

Gopher Proxy: Port: 0

SOCKS Host: Port: 0

● SOCKS v4 ○ SOCKS v5

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

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

Correct Answer: *A*

Community vote distribution

A (100%)

None

Question #15 *Topic 1*

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.

Correct Answer: *D*

Community vote distribution

C (100%)

None

Question #16 *Topic 1*

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

Correct Answer: *B*

Community vote distribution

B (100%)

None

Question #17 *Topic 1*

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

A. Browsercookie

B. Windowcookie

C. Document cookie

D. Session cookie

Correct Answer: *C*

Reference:

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

None

Question #18 *Topic 1*

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 I open and I closed port

Device type, general purpose -

Running: Microsoft Windows XP -
OS details: Microsoft Windows XP SP2

Network Distance : 1 hop -
Nmap done: I IP address (I host up) scanned in I .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.

Correct Answer: *D*

Community vote distribution

D (100%)

None

Question #19 *Topic 1*

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

Correct Answer: *D*

Reference:

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

None

Question #20 *Topic 1*

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

Correct Answer: *B*

Community vote distribution

C (100%)

None

Question #21 *Topic 1*

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

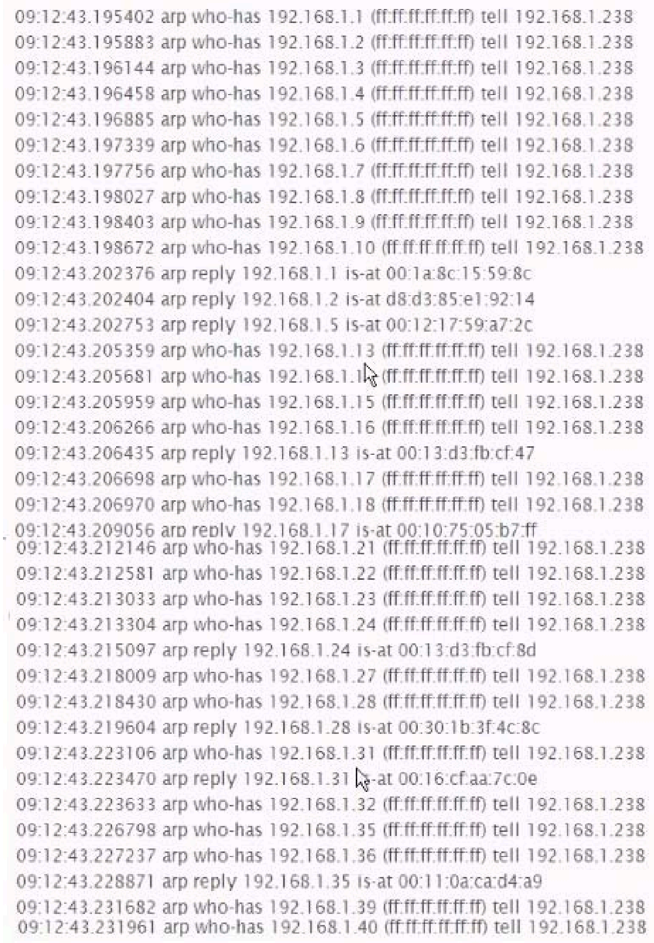
D. Your ISP Is blocking the traffic

Correct Answer: *C*

None

Question #22 *Topic 1*

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

Correct Answer: *A*

Community vote distribution

A (100%)

None

Question #23 *Topic 1*

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

Correct Answer: *D*

Community vote distribution

C (100%)

None

Question #24 *Topic 1*

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.

Correct Answer: *C*

None

Question #25 *Topic 1*

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.

Correct Answer: *B*

Community vote distribution

A (100%)

None

Question #26 *Topic 1*

You are done pen testing a Windows system and need to clean up some of the changes you have made. You created an account pentester on the system, what command would you use to delete that account?

A. Net user pentester /del

B. Net name pentester /del

C. Net localuser pentester /del

D. Net account pentester /del

Correct Answer: *A*

Community vote distribution

A (100%)

None

Question #27 *Topic 1*

Your company has decided that the risk of performing a penetration test Is too great. You would like to figure out other ways to find vulnerabilities on their systems, which of the following is MOST likely to be a valid alternative?

A. Network scope Analysis

B. Baseline Data Reviews

C. Patch Policy Review

D. Configuration Reviews

Correct Answer: *A*

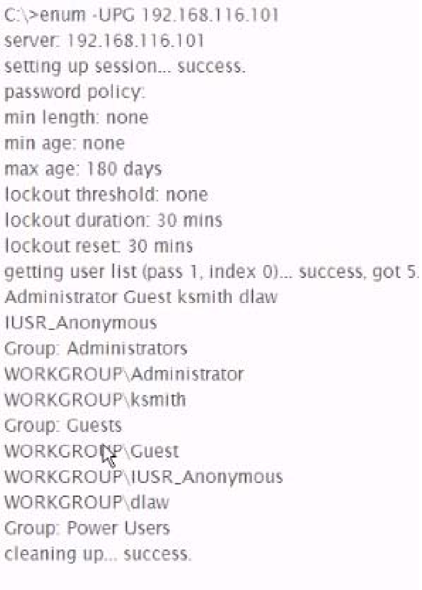
Community vote distribution

D (100%)

None

Question #28 *Topic 1*

Analyze the command output below, what action is being performed by the tester?



```
C:\>enum -UPG 192.168.116.101
server: 192.168.116.101
setting up session... success.
password policy:
min length: none
min age: none
max age: 180 days
lockout threshold: none
lockout duration: 30 mins
lockout reset: 30 mins
getting user list (pass 1, index 0)... success, got 5.
Administrator Guest ksmith dlaw
IUSR_Anonymous
Group: Administrators
WORKGROUP\Administrator
WORKGROUP\ksmith
Group: Guests
WORKGROUP\Guest
WORKGROUP\IUSR_Anonymous
WORKGROUP\dlaw
Group: Power Users
cleaning up... success.
```

A. Displaying a Windows SAM database

B. Listing available workgroup services

C. Discovering valid user accounts

D. Querying locked out user accounts

Correct Answer: *C*

None

Question #29 Topic 1

Raw netcat shells and telnet terminals share which characteristic?

A. Ability to send commands to a target machine.

B. Ability to adapt output to the size of display window

C. Shells and terminals are exactly the same.

D. Ability to process standard output control sequences.

Correct Answer: *D*

Reference:

http://tartarus.org/~simon/putty-snapshots/htmldoc/Chapter3.html

None

Question #30 *Topic 1*

How can a non-privileged user on a Unix system determine if shadow passwords are being used?

A. Read /etc/password and look for "x" or "II" in the second colon-delimited field

B. Read /etc/shadow and look for "x" or "II" in the second colon-delimited field

C. Verify that /etc/password has been replaced with /etc/shadow

D. Read /etc/shadow and look NULL values In the second comma delimited field

Correct Answer: *B*

Community vote distribution

A (100%)

None

Question #31 *Topic 1*

When DNS is being used for load balancing, why would a penetration tester choose to identify a scan target by its IP address rather than its host name?

A. Asingle IP may have multiple domains.

B. A single domain name can only have one IP address.

C. Scanning tools only recognize IP addresses

D. A single domain name may have multiple IP addresses.

Correct Answer: *C*
Reference:
http://www.flashcardmachine.com/sec-midterm.html

None

Question #32 *Topic 1*

What problem occurs when executing the following command from within a netcat raw shell? sudo cat /etc/shadow

A. Sudo does not work at all from a shell

B. Sudo works fine if the user and command are both in the /etc/sudoers file

C. The display blanks after typing the sudo command

D. You will not be able to type the password at the password prompt

Correct Answer: *A*

Community vote distribution

D (100%)

None

Question #33 *Topic 1*

You are pen testing a Windows system remotely via a raw netcat shell. You want to get a listing of all the local users in the administrators group, what command would you use?

A. Net account administrators

B. Net user administrators

C. Net localgroup administrators

D. Net localuser administrators

Correct Answer: *C*

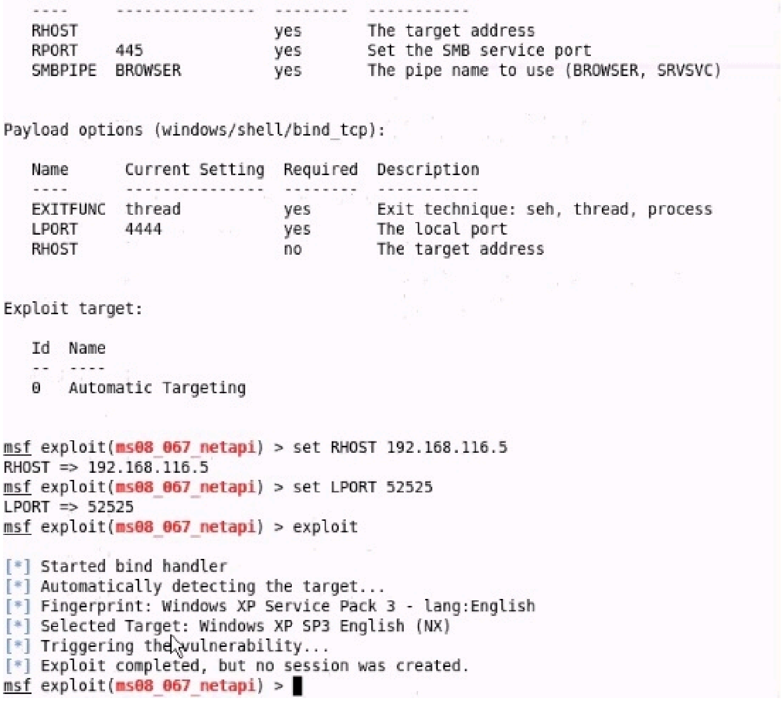
Community vote distribution

C (100%)

None

Question #34 *Topic 1*

Analyze the screenshot below. What type of vulnerability is being attacked?



```
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process
   LPORT     4444             yes       The local port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > set RHOST 192.168.116.5
RHOST => 192.168.116.5
msf exploit(ms08_067_netapi) > set LPORT 52525
LPORT => 52525
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (NX)
[*] Triggering the vulnerability...
[*] Exploit completed, but no session was created.
msf exploit(ms08_067_netapi) > █
```

A. Windows Server service

B. Internet Explorer

C. Windows Powershell

D. Local Security Authority

Correct Answer: *B*

Community vote distribution

A (100%)

None

Question #35 *Topic 1*

You have compromised a Windows workstation using Metasploit and have injected the Meterpreter payload into the smss process. You want to dump the SAM database of the remote system so you can crack it offline. Which Meterpreter module would you need to load in addition to the defaults so that you can accomplish this?

A. Core

B. Priv

C. Stdapi

D. Hashdump

Correct Answer: *C*

None

Question #36 *Topic 1*

Which of the following is the feature that separates the use of Rainbow Tables from other applications such as Cain or John the Ripper?

A. Salts are used to create massive password databases for comparison.

B. Applications take advantage of 64-bit CPU processor and multithread the crackingprocess.

C. Data Is aligned efficiently in the rainbow tables making the search process quicker

D. Raw hashed passwords are compared to pre-calculated hash tables.

Correct Answer: *B*

Community vote distribution

D (100%)

None

Question #37 *Topic 1*

You suspect that system administrators In one part of the target organization are turning off their systems during the times when penetration tests are scheduled, what feature could you add to the ' Rules of engagement' that could help your team test that part of the target organization?

A. Un announced test

B. Tell response personnel the exact lime the test will occur

C. Test systems after normal business hours

D. Limit tests to business hours

Correct Answer: *C*

None

Question #38 *Topic 1*

You are conducting a penetration test for a private contractor located in Singapore. The scope extends to all internal hosts controlled by the company, you have gathered necessary hold-harmless and nondisclosure agreements. Which action by your group can incur criminal liability under Chapter 50a, Computer Misuse
Act?

A. Exploiting vulnerable web services on internal hosts

B. Attempts at social engineering employees via telephone calls

C. Testing denial-of-service tolerance of the communications provider

D. Cracking password hashes on the corporate domain server

Correct Answer: *D*

None

Question #39 *Topic 1*

Which of the following is a WEP weakness that makes it easy to Inject arbitrary clear text packets onto a WEP network?

A. Reversible hashes use for IVs

B. Cryptographically weak CRC32 checksum

C. RC4 algorithm

D. Small key space

Correct Answer: *D*

None

Question #40 *Topic 1*

During a penetration test we determine that TCP port 22 is listening on a target host. Knowing that SSHD is the typical service that listens on that port we attempt to validate that assumption with an SSH client but our effort Is unsuccessful. It turns out that it is actually an Apache webserver listening on the port, which type of scan would have helped us to determine what service was listening on port 22?

A. Version scanning

B. Port scanning

C. Network sweeping

D. OS fingerprinting

Correct Answer: *A*

Community vote distribution

A (100%)

None

Question #41 *Topic 1*

Which type of Cross-Sire Scripting (XSS> vulnerability is hardest for automated testing tools to detect, and for what reason?

A. Stored XSS. because it may be located anywhere within static or dynamic sitecontent

B. Stored XSS. because it depends on emails and instant messaging systems.

C. Reflected XSS. because It can only be found by analyzing web server responses.

D. Reflected XSS: because it is difficult to find within large web server logs.

Correct Answer: *A*

None

Question #42 *Topic 1*

You are using the Nmap Scripting Engine and want detailed output of the script as it runs. Which option do you include in the command string?

A. Nmap --script-output -script-SSH-hostkey.nse 155.65.3.221 -p 22

B. Nmap --script-trace --script-ssh-hostkey.nse 155.65.3.221 -p 22

C. Nmap -script-verbose --scrlpr-ssh-hostkey.nse 155.65.3.221 -p 22

D. Nmap -v --script=ssh-hostkey.nse 155.65.3.221 -p 22

Correct Answer: *C*

None

Question #43

Topic 1

What is the purpose of the following command?

```
C:\>wmic /node:[target IP] /user:[admin-user]
/password:[password] process call create [command]
```

A. Running a command on a remote Windows machine

B. Creating a service on a remote Windows machine

C. Creating an admin account on a remote Windows machine

D. Listing the running processes on a remote windows machine

Correct Answer: *D*

None

Question #44 *Topic 1*

Approximately how many packets are usually required to conduct a successful FMS attack onWEP?

A. 250.000

B. 20.000

C. 10.000,000

D. I (with a weak IV)

Correct Answer: *B*

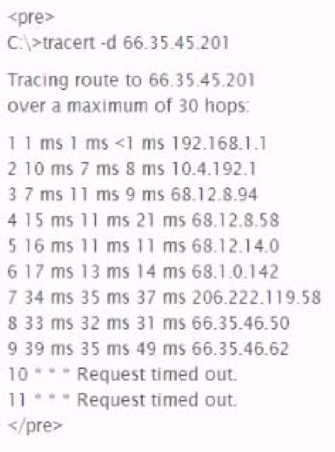
Community vote distribution

A (100%)

None

Question #45 *Topic 1*

What is the most likely cause of the responses on lines 10 and 11 of the output below?



```
<pre>
C:\>tracert -d 66.35.45.201

Tracing route to 66.35.45.201
over a maximum of 30 hops:

1 1 ms 1 ms <1 ms 192.168.1.1
2 10 ms 7 ms 8 ms 10.4.192.1
3 7 ms 11 ms 9 ms 68.12.8.94
4 15 ms 11 ms 21 ms 68.12.8.58
5 16 ms 11 ms 11 ms 68.12.14.0
6 17 ms 13 ms 14 ms 68.1.0.142
7 34 ms 35 ms 37 ms 206.222.119.58
8 33 ms 32 ms 31 ms 66.35.46.50
9 39 ms 35 ms 49 ms 66.35.46.62
10 * * * Request timed out.
11 * * * Request timed out.
</pre>
```

A. The device at hop 10 silently drops UDP packets with a high destination port.

B. The device at hop 10 is down and not forwarding any requests at all.

C. The host running the tracer utility lost its network connection during the scan

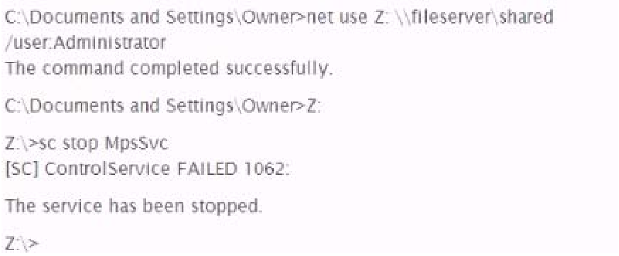
D. The devices at hops 10 and II did not return an "ICMP TTL Exceeded in Transit" message.

Correct Answer: *D*

None

Question #46 *Topic 1*

A penetration tester wishes to stop the Windows Firewall process on a remote host running Windows Vista She issues the following commands:



```
C:\Documents and Settings\Owner>net use Z: \\fileserver\shared
/user:Administrator
The command completed successfully.

C:\Documents and Settings\Owner>Z:

Z:\>sc stop MpsSvc
[SC] ControlService FAILED 1062:

The service has been stopped.

Z:\>
```

A check of the remote host indicates that Windows Firewall is still running. Why did the command fail?

A. The kernel prevented the command from being executed.

B. The user does not have the access level needed to stop the firewall.

C. The sc command needs to be passed the IP address of the target.

D. The remote server timed out and did not complete the command.

Correct Answer: *C*

None

Question #47 *Topic 1*

By default Active Directory Controllers store password representations in which file?

A. %system roots .system 32/ntds.dit

B. %System roots /ntds\ntds.dit

C. %System roots /ntds\sam.dat

D. %System roots /ntds\sam.dit

Correct Answer: *A*

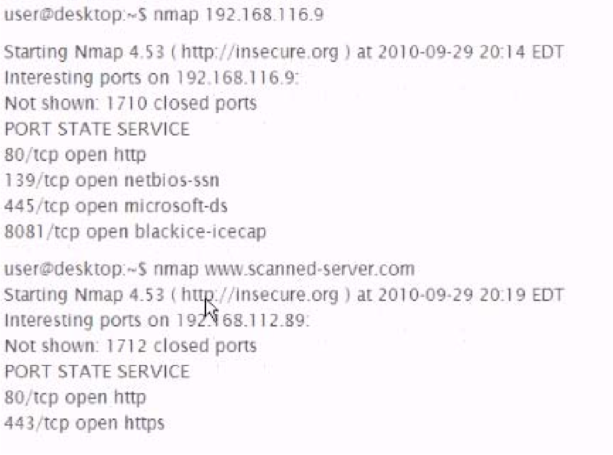
Reference:

http://www.scribd.com/doc/212238158/Windows-Administrator-L2-Interview-Question-System-Administrator#scribd

None

Question #48 *Topic 1*

192.168.116.9 Is an IP address forvvww.scanned-server.com. Why are the results from the two scans, shown below, different?



```
user@desktop:~$ nmap 192.168.116.9

Starting Nmap 4.53 ( http://insecure.org ) at 2010-09-29 20:14 EDT
Interesting ports on 192.168.116.9:
Not shown: 1710 closed ports
PORT STATE SERVICE
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
8081/tcp open blackice-icecap

user@desktop:~$ nmap www.scanned-server.com
Starting Nmap 4.53 ( http://insecure.org ) at 2010-09-29 20:19 EDT
Interesting ports on 192.168.112.89:
Not shown: 1712 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
```

A. John.pot

B. John conf

C. John.rec

D. John.ini

Correct Answer: *C*

None

Question #49 *Topic 1*

You have been contracted to perform a black box pen test against the Internet facing servers for a company. They want to know, with a high level of confidence, if their servers are vulnerable to external attacks. Your contract states that you can use all tools available to you to pen test the systems. What course of action would you use to generate a report with the lowest false positive rate?

A. Use a port scanner to find open service ports and generate a report listing allvulnerabilities associated with those listening services.

B. Use a vulnerability or port scanner to find listening services and then try to exploitthose services.

C. Use a vulnerability scanner to generate a report of vulnerable services.

D. Log into the system and record the patch levels of each service then generate areport that lists known vulnerabilities for all the running services.

Correct Answer: *B*

None

Question #50 *Topic 1*

You successfully compromise a target system's web application using blind command injection. The command you injected is ping-n 1 192.168.1.200. Assuming your machine is 192.168.1 200, which of the following would you see?

A. Ping-n 1 192.168.1 200 on the compromised system

B. A 'Destination host unreachable' error message on the compromised system

C. A packet containing 'Packets: Sent - 1 Received = 1, Loss = 0 (0% loss) on yoursniffer

D. An ICMP Echo packet on your sniffer containing the source address of the target

Correct Answer: *A*

None

Question #51 *Topic 1*

When a DNS server transfers its zone file to a remote system, what port does it typically use?

A. 53/TCP

B. 153/UDP

C. 35/TCP

D. 53/UDP

Correct Answer: *D*

Reference:

http://www.networkworld.com/article/2231682/cisco-subnet/cisco-subnet-allow-both-tcp-and-udp-port-53-to-your-dns-servers.html

None

Question #52 *Topic 1*

Which of the following modes describes a wireless interface that is configured to passively grab wireless frames from one wireless channel and pass them to the operating system?

A. Monitor Mode

B. Promiscuous Mode

C. Managed Mode

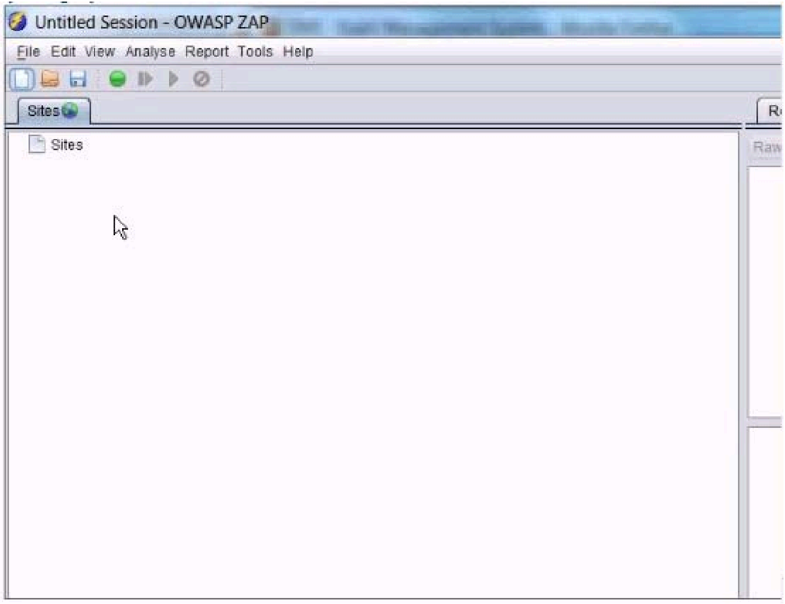
D. Master Mode

Correct Answer: *C*
Reference:
http://www.willhackforsushi.com/books/377_eth_2e_06.pdf

None

Question #53 *Topic 1*

In the screen shot below, which selections would you need click in order to intercept and alter all http traffic passing through OWASP ZAP?


Untitled Session - OWASP ZAP
File Edit View Analyse Report Tools Help
Sites
Sites
Raw

A. Trap response and continue

B. Set Break and Continue

C. Trap request and continue

D. Continue and drop

Correct Answer: *B*

None

Question #54 *Topic 1*

Which of the following file transfer programs will automatically convert end-of line characters between different platforms when placed in ASCII Mode?

A. ftp

B. nc

C. tftp

D. scp

Correct Answer: *A*

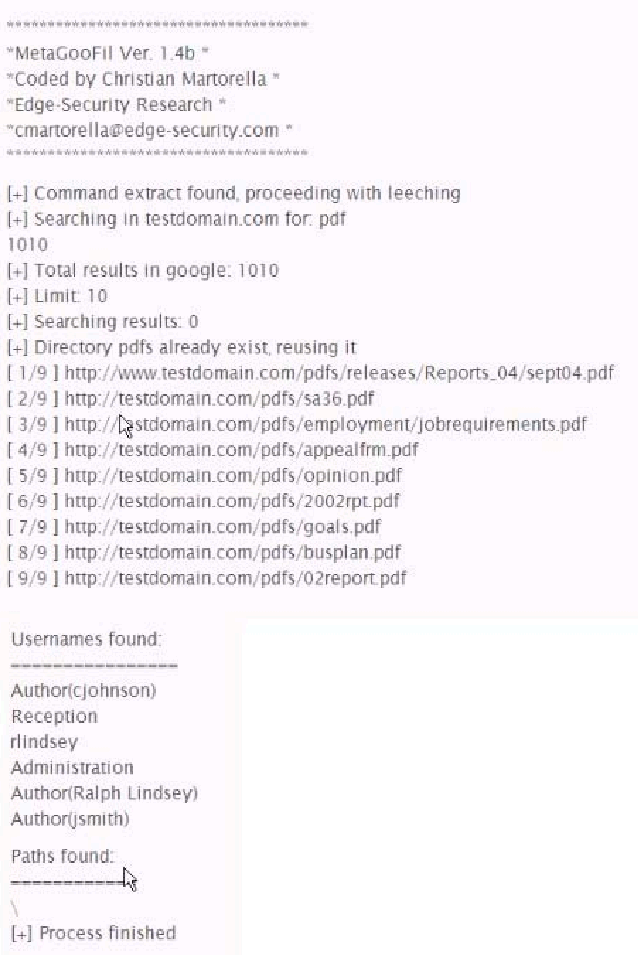
Reference:

https://wiki.filezilla-project.org/Data_Type

None

Question #55 *Topic 1*

Analyze the command output below. What information can the tester infer directly from the Information shown?



```
**************************************
*MetaGooFil Ver. 1.4b *
*Coded by Christian Martorella *
*Edge-Security Research *
*cmartorella@edge-security.com *
**************************************

[+] Command extract found, proceeding with leeching
[+] Searching in testdomain.com for: pdf
1010
[+] Total results in google: 1010
[+] Limit: 10
[+] Searching results: 0
[+] Directory pdfs already exist, reusing it
[ 1/9 ] http://www.testdomain.com/pdfs/releases/Reports_04/sept04.pdf
[ 2/9 ] http://testdomain.com/pdfs/sa36.pdf
[ 3/9 ] http://testdomain.com/pdfs/employment/jobrequirements.pdf
[ 4/9 ] http://testdomain.com/pdfs/appealfrm.pdf
[ 5/9 ] http://testdomain.com/pdfs/opinion.pdf
[ 6/9 ] http://testdomain.com/pdfs/2002rpt.pdf
[ 7/9 ] http://testdomain.com/pdfs/goals.pdf
[ 8/9 ] http://testdomain.com/pdfs/busplan.pdf
[ 9/9 ] http://testdomain.com/pdfs/02report.pdf

Usernames found:
================
Author(cjohnson)
Reception
rlindsey
Administration
Author(Ralph Lindsey)
Author(jsmith)

Paths found:
============
\
[+] Process finished
```

A. Usernames for the domain tesrdomain.com

B. Directory indexing is allowed on the web server

C. Vulnerable versions of Adobe software in use

D. Naming convention for public documents

Correct Answer: *D*

None

Question #56 *Topic 1*

All of the following are advantages of using the Metasploitpriv module for dumping hashes from a local Windows machine EXCEPT:

A. Doesn't require SMB or NetBIOS access to the target machine

B. Can run inside of a process owned by any user

C. Provides less evidence for forensics Investigators to recover

D. LSASS related reboot problems aren't an Issue

Correct Answer: *B*
Reference:
http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Security/Meetings/ISOAG/2012/2012_Jan_ISOAG.pdf

None

Question #57 *Topic 1*

What command will correctly reformat the Unix passwordcopy and shadowcopy Tiles for input to John The Ripper?

A. /Un shadow passwd copy shadowcopy > johnfile

B. /Unshadow passwdcopy shadowcopy > johnfile

C. /Unshadow shadowcopy passwdcopy >john file

D. /Unshadow passwdcopy shadowcopy > johnfile

Correct Answer: *C*

Reference:

https://books.google.co.in/books?id=SC-tAwAAQBAJ&pg=PA286&lpg=PA286&dq=/Unshadow+shadow+copy+passwd+copy+%3Ejohn+file&source=bl&ots=OnZK9atlc1&sig=co7EM5EHye96vO74W3wZxky3sXU&hl=en&sa=X&ei=FBuoVPLHDc-cugSDxYGYBA&ved=0CCwQ6AEwAg#v=onepage&q=%2FUnshadow%20shadow%20copy%20passwd%20copy%20%3Ejohn%20file&f=false

Community vote distribution

B (100%)

None

Question #58 Topic 1

Which of the following best explains why you would warn to clear browser slate (history. cache, and cookies) between examinations of web servers when you've been trapping and altering values with a non-transparent proxy?

A. Values trapped and stored in the browser will reveal the techniques you've used toexamine the web servers.

B. Trapping and changing response values is beneficial for web site testing but usingthe same cached values in your browser will prevent you from being able to changethose values.

C. Trapping and changing response values is beneficial for web site testing but willcause browser instability if not cleared.

D. Values trapped and changed in the proxy, such as a cookie, will be stored by thebrowser and may impact further testing.

Correct Answer: *D*

None

Question #59 *Topic 1*

You are performing a wireless penetration lest and are currently looking for rogue access points in one of their large facilities. You need to select an antenna that you can setup in a building and monitor the area for several days to see if any access points are turned on during the duration of the test. What type of antenna will you be selecting for this task?

A. High gain and Omni-Directional

B. High gain and Directional

C. Low gain and Omni-Directional

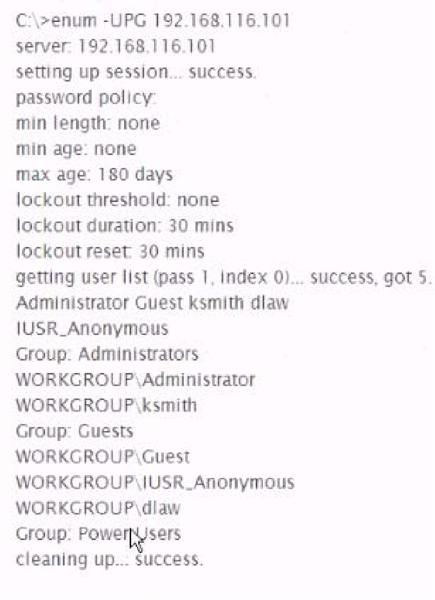
D. Low gain and Directional

Correct Answer: *B*

None

Question #60 *Topic 1*

Analyze the command output below. What information can the tester infer directly from the information shown?



```
C:\>enum -UPG 192.168.116.101
server: 192.168.116.101
setting up session... success.
password policy:
min length: none
min age: none
max age: 180 days
lockout threshold: none
lockout duration: 30 mins
lockout reset: 30 mins
getting user list (pass 1, index 0)... success, got 5.
Administrator Guest ksmith dlaw
IUSR_Anonymous
Group: Administrators
WORKGROUP\Administrator
WORKGROUP\ksmith
Group: Guests
WORKGROUP\Guest
WORKGROUP\IUSR_Anonymous
WORKGROUP\dlaw
Group: Power Users
cleaning up... success.
```

A. The administrator account has no password

B. Null sessions are enabled on the target

C. The target host is running Linux with Samba services

D. Account lockouts must be reset by the Administrator

Correct Answer: *C*

Community vote distribution

B (100%)

None

Question #61 *Topic 1*

What concept do Rainbow Tables use to speed up password cracking?

A. Fast Lookup Crack Tables

B. Memory Swap Trades

C. Disk Recall Cracking

D. Time-Memory Trade-off

Correct Answer: *D*

Reference:

http://en.wikipedia.org/wiki/Space%E2%80%93time_tradeoff

None

Question #62 *Topic 1*

When sniffing wireless frames, the interface mode plays a key role in successfully collecting traffic. Which of the mode or modes are best used for sniffing wireless traffic?

A. Master Ad-hoc

B. RFMON

C. RFMON. Ad-hoc

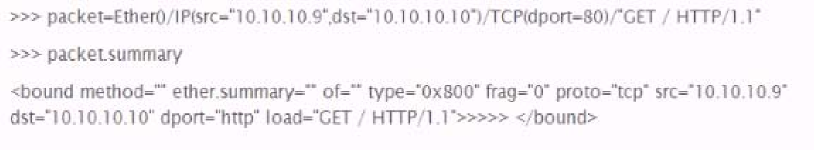
D. Ad-hoc

Correct Answer: *A*
Reference:
http://www.willhackforsushi.com/books/377_eth_2e_06.pdf

None

Question #63 *Topic 1*

Given the following Scapy information, how is default Layer 2 information derived?



```
>>> packet=Ether()/IP(src="10.10.10.9",dst="10.10.10.10")/TCP(dport=80)/"GET / HTTP/1.1"

>>> packet.summary

<bound method="" ether.summary="" of="" type="0x800" frag="0" proto="tcp" src="10.10.10.9"
dst="10.10.10.10" dport="http" load="GET / HTTP/1.1">>>>> </bound>
```

A. The default layer 2 information is contained in a local scapy.cfg configuration fileon the local system.

B. If not explicitly defined, the Ether type field value Is created using the hex value ofthe destination port, in this case 80

C. If not explicitly defined, pseudo-random values are generated for the Layer 2 defaultinformation.

D. Scapy relies on the underlying operating system to construct Layer 2 information touse as default.

Correct Answer: *C*

Community vote distribution

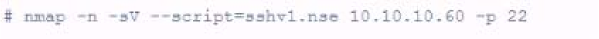
D (100%)

None

Question #64

Topic 1

A customer has asked for a scan or vulnerable SSH servers. What is the penetration tester attempting to accomplish using the following Nmap command?



```
# nmap -n -sV --script=sshv1.nse 10.10.10.60 -p 22
```

A. Checking operating system version

B. Running an exploit against the target

C. Checking configuration

D. Checking protocol version

Correct Answer: *D*

None

Question #65 *Topic 1*

While performing an assessment on a banking site, you discover the following link:
hnps://mybank.com/xfer.aspMer_toMaccount_number]&amount-[dollars]
Assuming authenticated banking users can be lured to your web site, which crafted html tag may be used to launch a XSRF attack?

A. <imgsrc-"java script alert ('document cookie'):">

B. <scripi>alert('hnps:/'mybank.com/xfer.a$p?xfer_io-[attacker_account]&amoutn-[dollars]')</script>

C. <scripr>document.\write('hTtp$://mybankxom/xfer.a$p?xfer_to-[attacker.accountl &amount-[dollars)</script>

D. <img src-'https/mybank.com/xfer.asp?xfer_to=[artacker_account]&amount= [dollars]">

Correct Answer: *C*

None

Question #66 *Topic 1*

You are conducting a penetration test for a private company located in the UK. The scope extends to all internal and external hosts controlled by the company.
You have gathered necessary hold-harmless and non-disclosure agreements. Which action by your group can incur criminal liability under the computer Misuse
Act of 1990?

A. Sending crafted packets to internal hosts in an attempt to fingerprint the operatingsystems

B. Recovering the SAM database of the domain server and attempting to crackpasswords

C. Installing a password sniffing program on an employee's personal computer withoutconsent

D. Scanning open ports on internal user workstations and exploiting vulnerableapplications

Correct Answer: *B*

None

Question #67 *Topic 1*

While performing a code audit, you discover a SQL injection vulnerability assuming the following vulnerable query, what user input could be injected to make the query true and return data? select * from widgets where name = '[user-input]';

A. 'or 1=1

B. ‘or l=l…

C. 'or 1=1--

D. ‘or l=1’

Correct Answer: *D*

None

Question #68 *Topic 1*

You have compromised a Windows XP system and Injected the Meterpreter payload into the lsass process. While looking over the system you notice that there is a popular password management program on the system. When you attempt to access the file that contains the password you find it is locked. Further investigation reveals that it is locked by the passmgr process. How can you use the Meterpreter to get access to this file?

A. Use the getuid command to determine the user context the process is runningunder, then use the imp command to impersonate that user.

B. use the getpid command to determine the user context the process is runningunder, then use the Imp command to impersonate that user.

C. Use the execute command to the passmgr executable. That will give you access to the file.

D. Use the migrate command to jump to the passmgr process. That will give you accessto the file.

Correct Answer: *C*

None

Question #69 *Topic 1*

When attempting to crack a password using Rainbow Tables, what is the output of the reduction function?

A. A new potential chain

B. A new potential table

C. A new potential password

D. A new potential hash

Correct Answer: *D*

Reference:

http://en.wikipedia.org/wiki/Rainbow_table

None

Question #70 *Topic 1*

You are performing a vulnerability assessment using Nessus and your clients printers begin printing pages of random text and showing error messages. The client is not happy with the situation. What is the best way to proceed?

A. Enable the "Skip all primers" option and re-scan

B. Ensure Safe Checks is enabled in Nessus scan policies

C. Remove primer IP addresses from your target list

D. Verify primers are in scope and tell the client In progress scans cannot be stopped

Correct Answer: *B*

None

Question #71 Topic 1

As pan or a penetration lest, your team is tasked with discovering vulnerabilities that could be exploited from an inside threat vector. Which of the following activities fall within that scope?

A. B, C, and D

B. A, B. and D

C. B and D

D. A and D

Correct Answer: *C*

None

Question #72 *Topic 1*

Which of the following is the number of bits of encryption that 64-bit Wired Equivalent Privacy (WEP) effectively provides?

A. 64

B. 40

C. 60

D. 44

Correct Answer: *A*

Reference:

http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

None

Question #73 *Topic 1*

Which of the following is a method of gathering user names from a Linux system?

A. Displaying the owner information of system-specific binaries

B. Reviewing the contents of the system log files

C. Gathering listening services from the xinetd configuration files

D. Extracting text strings from the system password file

Correct Answer: *C*

Reference:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf

None

Question #74

Topic 1

While scanning a remote system that is running a web server with a UDP scan and monitoring the scan with a sniffer, you notice that the target is responding with
ICMP Port Unreachable only once a second What operating system is the target likely running?

A. Linux

B. Windows

C. OpenBSD

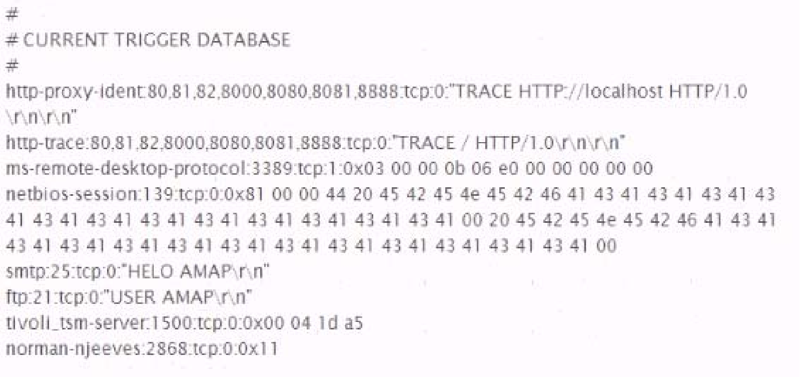
D. Mac OS X

Correct Answer: *A*

None

Question #75 *Topic 1*

Based on the partial appdefstrig rile listed below, which port scan signature is classified by AMap as harmful?



```
#
# CURRENT TRIGGER DATABASE
#
http-proxy-ident:80,81,82,8000,8080,8081,8888:tcp:0:"TRACE HTTP://localhost HTTP/1.0
\r\n\r\n"
http-trace:80,81,82,8000,8080,8081,8888:tcp:0:"TRACE / HTTP/1.0\r\n\r\n"
ms-remote-desktop-protocol:3389:tcp:1:0x03 00 00 0b 06 e0 00 00 00 00 00
netbios-session:139:tcp:0:0x81 00 00 44 20 45 42 45 4e 45 42 46 41 43 41 43 41 43 41 43
41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 00 20 45 42 45 4e 45 42 46 41 43 41
43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 00
smtp:25:tcp:0:"HELO AMAP\r\n"
ftp:21:tcp:0:"USER AMAP\r\n"
tivoli_tsm-server:1500:tcp:0:0x00 04 1d a5
norman-njeeves:2868:tcp:0:0x11
```

A. smtp

B. netbios-session

C. http-trace

D. ms-remote-desktop-protocol

Correct Answer: *C*

Community vote distribution

D (100%)

None

Question #76 *Topic 1*

Why is OSSTMM beneficial to the pen tester?

A. It provides a legal and contractual framework for testing

B. It provides in-depth knowledge on tools

C. It provides report templates

D. It includes an automated testing engine similar to Metasploit

Correct Answer: *C*

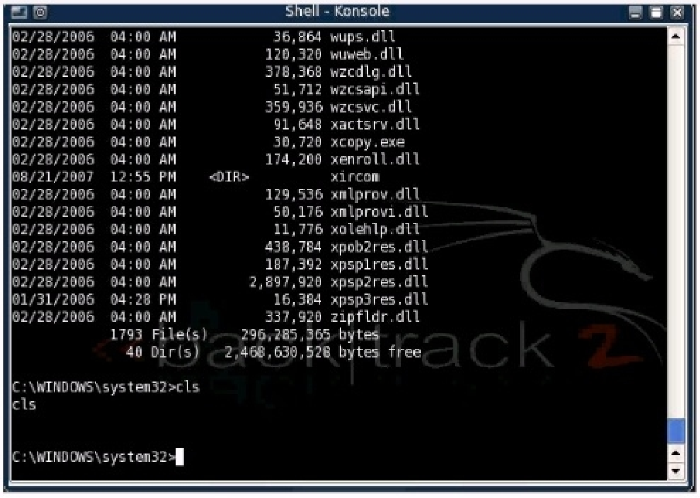
Reference:

http://www.pen-tests.com/open-source-security-testing-methodology-manual-osstmm.html

None

Question #77 Topic 1

You have connected to a Windows system remotely and have shell access via netcat. While connected to the remote system you notice that some Windows commands work normally while others do not An example of this is shown in the picture below Which of the following best describes why tins is happening?



```
02/28/2006  04:00 AM            36,864 wups.dll
02/28/2006  04:00 AM           120,320 wuweb.dll
02/28/2006  04:00 AM           378,368 wzcdlg.dll
02/28/2006  04:00 AM            51,712 wzcsapi.dll
02/28/2006  04:00 AM           359,936 wzcsvc.dll
02/28/2006  04:00 AM            91,648 xactsrv.dll
02/28/2006  04:00 AM            30,720 xcopy.exe
02/28/2006  04:00 AM           174,200 xenroll.dll
08/21/2007  12:55 PM    <DIR>          xircom
02/28/2006  04:00 AM           129,536 xmlprov.dll
02/28/2006  04:00 AM            50,176 xmlprovi.dll
02/28/2006  04:00 AM            11,776 xolehlp.dll
02/28/2006  04:00 AM           438,784 xpob2res.dll
02/28/2006  04:00 AM           187,392 xpsp1res.dll
02/28/2006  04:00 AM         2,897,920 xpsp2res.dll
01/31/2006  04:28 PM            16,384 xpsp3res.dll
02/28/2006  04:00 AM           337,920 zipfldr.dll
            1793 File(s)    296,285,365 bytes
              40 Dir(s)   2,468,630,528 bytes free

C:\WINDOWS\system32>cls
cls


C:\WINDOWS\system32>
```

A. Netcat cannot properly interpret certain control characters or Unicode sequences.

B. The listener executed command.com instead of cmd.exe.

C. Another application is already running on the port Netcat is listening on.

D. TheNetcat listener is running with system level privileges.

Correct Answer: *D*

None

Question #78 *Topic 1*

If the privacy bit is set in the 802.11 header, what does it indicate?

A. SSID cloaking is being used.

B. Some form of encryption is In use.

C. WAP is being used.

D. Some form of PEAP is being used.

Correct Answer: *C*

None

Question #79 *Topic 1*

You suspect that a firewall or IPS exists between you and the target machine. Which nmap option will elicit responses from some firewalls and IPSs while being silently dropped by the target, thus confirming the existence of a firewall or IPS?

A. –Traceroute

B. –Firewalk

C. –Badsum

D. --SF

Correct Answer: *B*

None

Question #80 *Topic 1*

A client has asked for a vulnerability scan on an internal network that does not have internet access. The rules of engagement prohibits any outside connection for the Nessus scanning machine. The customer has asked you to scan for a new critical vulnerability, which was released after the testing started, winch of the following methods of updating the Nessus plugins does not violate the rules of engagement?

A. Connect the scanning machine via wireless bridge and download the updateddirectly

B. Change the routing and connect through an alternative gateway

C. Proceed with the test and note the limitation of updating the plugins

D. Download the updates on an alternative machine and manually load on scanningmachine

Correct Answer: *D*

None

Question #81 *Topic 1*

You are pen testing a network and have shell access to a machine via Netcat. You try to use ssh to access another machine from the first machine. What is the expected result?

A. The ssh connection will succeed If you have root access on the intermediate machine

B. The ssh connection will fail

C. The ssh connection will succeed

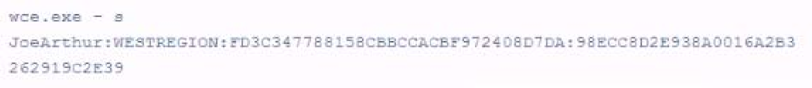
D. The ssh connection will succeed if no password required

Correct Answer: *C*

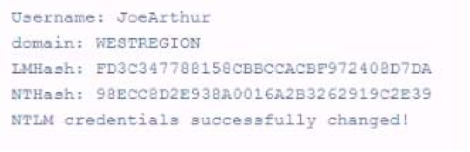
None

Question #82 Topic 1

A pen tester is able to pull credential information from memory on a Windows system. Based on the command and output below, what advantage does this technique give a penetration tester when trying to access another windows system on the network?



```
wce.exe - s
JoeArthur:WESTREGION:FD3C347788158CBBCCACBF972408D7DA:98ECC8D2E938A0016A2B3
262919C2E39
```



```
Username: JoeArthur
domain: WESTREGION
LMHash: FD3C347788158CBBCCACBF972408D7DA
NTHash: 98ECC8D2E938A0016A2B3262919C2E39
NTLM credentials successfully changed!
```

A. The technique is more effective through perimeter firewalls than otherauthentication attacks.

B. It allows the tester to escalate the privilege level of the account,

C. Access to the system can be gained without password guessing or cracking.

D. Salts are removed from the hashes to allow for faster, offline cracking

Correct Answer: *A*

Community vote distribution

C (100%)

None

Question #83 *Topic 1*

During a penetration test you discover a valid set of SSH credentials to a remote system. How can this be used to your advantage in a Nessus scan?

A. This information can be entered under the 'Hydra' tab to launch a brute-forcepassword attack.

B. There isn't an advantage as Nessus will ultimately discover this information.

C. The "SSH' box can be checked to let Nessus know the remote system is running

D. This information can be entered under the 'credentials' tab to allow Nessus to log into the system

Correct Answer: *C*

Community vote distribution

D (100%)

None

Question #84

Topic 1

Where are Netcat's own network activity messages, such as when a connection occurs, sent?

A. Standard Error

B. Standard input

C. Standard Logfile

D. Standard Output

Correct Answer: *A*

Reference:

http://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf

None

Question #85 *Topic 1*

You've been contracted by the owner of a secure facility to try and break into their office in the middle of the night. Your client requested photographs of any sensitive information found as proof of your accomplishments. The job you've been hired to perform is an example of what practice?

A. Penetration Testing

B. Ethical Hacking

C. Vulnerability Assessing

D. Security Auditing

Correct Answer: *B*

Community vote distribution

A (100%)

None

Question #86 *Topic 1*

Which of the following is possible in some SQL injection vulnerabilities on certain types of databases that affects the underlying server OS?

A. Database structure retrieval

B. Shell command execution

C. Data manipulation

D. Data query capabilities

Correct Answer: *A*

Reference:

http://www.darkmoreops.com/2014/08/28/use-sqlmap-sql-injection-hack-website-database/

None

Question #87

Topic 1

You are pen testing a system and want to use Metasploit 3.X to open a listening port on the system so you can access it via a netcat shell. Which stager would you use to have the system listen on TCP port 50000?

A. Reverse.tcp

B. Bind.tcp

C. Fincltag.ord

D. Passivex

Correct Answer: *B*

None

Question #88

Topic 1

Which of the following best describes a server side exploit?

A. Attack on the physical machine

B. Attack of a service listening on a network port

C. Attack that escalates user privilege to root or administrator

D. Attack of a client application that retrieves content from the network

Correct Answer: *C*

None

Question #89

Topic 1

You are conducting a penetration test for a private company located in Canada. The scope extends to all internal-facing hosts controlled by the company. You have gathered necessary hold-harmless and non-disclosure agreements. Which action by your group can incur criminal liability under Criminal Code of Canada
Sections 184 and 542 CC 184?

A. Analyzing internal firewall router software for vulnerabilities

B. Exploiting application vulnerabilities on end-user workstations

C. Attempting to crack passwords on a development server

D. Capturing a VoIP call to a third party without prior notice

Correct Answer: *D*

None

Question #90 *Topic 1*

What is the purpose of die following command:
nc.exe -l -p 2222 -e cmd.exe

A. It is used to start a persistent listener linked to cmd.exe on port 2222 TCP

B. It is used to start a listener linked to cmd.exe on port 2222 TCP

C. It is used to start a listener linked to cmd.exe on port 2222 UDP

D. It is used to start a persistent listener linked to cmd.exe on port 2222 UDP

Correct Answer: *C*

Community vote distribution

A (100%)

None

Question #91 *Topic 1*

A tester has been contracted to perform a penetration test for a corporate client. The scope of the test is limited to end-user workstations and client programs only.
Which of die following actions is allowed in this test?

A. Attempting to redirect the internal gateway through ARP poisoning

B. Activating bot clients and performing a denial-of-service against the gateway.

C. Sniffing and attempting to crack the Domain Administrators password hash.

D. Sending a malicious pdf to a user and exploiting a vulnerable Reader version.

Correct Answer: *D*

Community vote distribution

D (100%)

None

Question #92 *Topic 1*

Why is it important to have a cheat sheet reference of database system tables when performing SQL Injection?

A. This is where sites typically store sensitive information such as credit card numbers.

B. These tables contain a list of allowed database applications

C. The information in these tables will reveal details about the web application's code.

D. These tables contain metadata that can be queried to gain additional helpful information.

Correct Answer: *D*

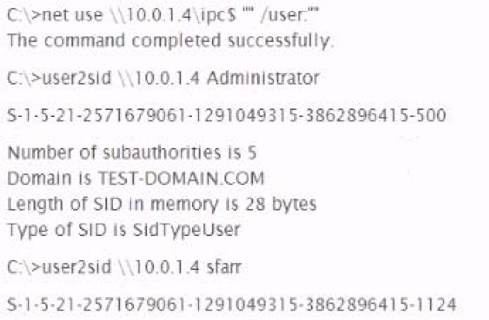
Reference:

http://www.rackspace.com/knowledge_center/article/sql-injection-in-mysql

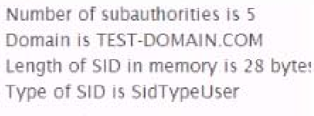
None

Question #93 Topic 1

Analyze the command output below. What action is being performed by the tester?



```
C:\>net use \\10.0.1.4\ipc$ "" /user:""
The command completed successfully.

C:\>user2sid \\10.0.1.4 Administrator

S-1-5-21-2571679061-1291049315-3862896415-500

Number of subauthorities is 5
Domain is TEST-DOMAIN.COM
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

C:\>user2sid \\10.0.1.4 sfarr

S-1-5-21-2571679061-1291049315-3862896415-1124
```



```
Number of subauthorities is 5
Domain is TEST-DOMAIN.COM
Length of SID in memory is 28 byte!
Type of SID is SidTypeUser
```

A. Creating user accounts on 10.0.1.4 and testing privileges

B. Collecting password hashes for users on 10.0.1.4

C. Attempting to exploit windows File and Print Sharing service

D. Gathering Security identifiers for accounts on 10.0.1.4

Correct Answer: *C*

Community vote distribution

D (100%)

None

Question #94 *Topic 1*

How does OWASP ZAP function when used for performing web application assessments?

A. It is a non-transparent proxy that sits between your web browser and the targetapplication.

B. It is a transparent policy proxy that sits between Java servers and |SP web pages.

C. It is a non-transparent proxy that passively sniffs network traffic for HTTPvulnerabilities.

D. It is a transparent proxy that sits between a target application and the backenddatabase.

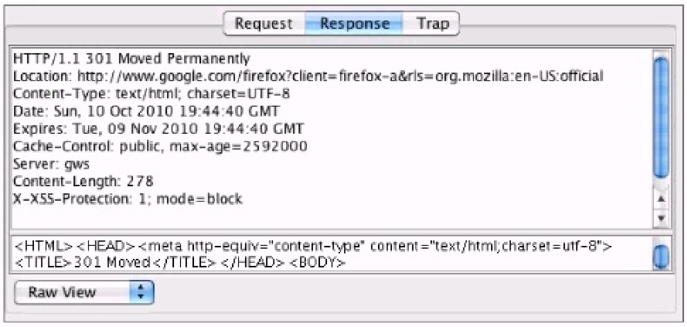
Correct Answer: *D*

None

Question #95 *Topic 1*

You've been asked to test a non-transparent proxy lo make sure it is working. After confirming the browser is correctly pointed at the proxy, you try to browse a web site. The browser indicates it is "loading" but never displays any part the page. Checking the proxy, you see a valid request in the proxy from your browser.

Checking the response to the proxy, you see the results displayed in the accompanying screenshot. Which of the following answers is the most likely reason the browser hasn't displayed the page yet?



```
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official
Content-Type: text/html; charset=UTF-8
Date: Sun, 10 Oct 2010 19:44:40 GMT
Expires: Tue, 09 Nov 2010 19:44:40 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 278
X-XSS-Protection: 1; mode=block
```

```
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
```

A. The proxy is likely hung and must be restarted.

B. The proxy is configured to trap responses.

C. The proxy is configured to trap requests.

D. The site you are trying to reach is currently down.

Correct Answer: *C*

None

Question #96 *Topic 1*

A penetration tester used a client-side browser exploit from metasploit to get an unprivileged shell prompt on the target Windows desktop. The penetration tester then tried using the getsystem command to perform a local privilege escalation which failed. Which of the following could resolve the problem?

A. Load priv module and try getsystem again

B. Run getuid command, then getpriv command, and try getsystem again

C. Run getuid command and try getsystem again

D. Use getprivs command instead of getsystem

Correct Answer: *B*

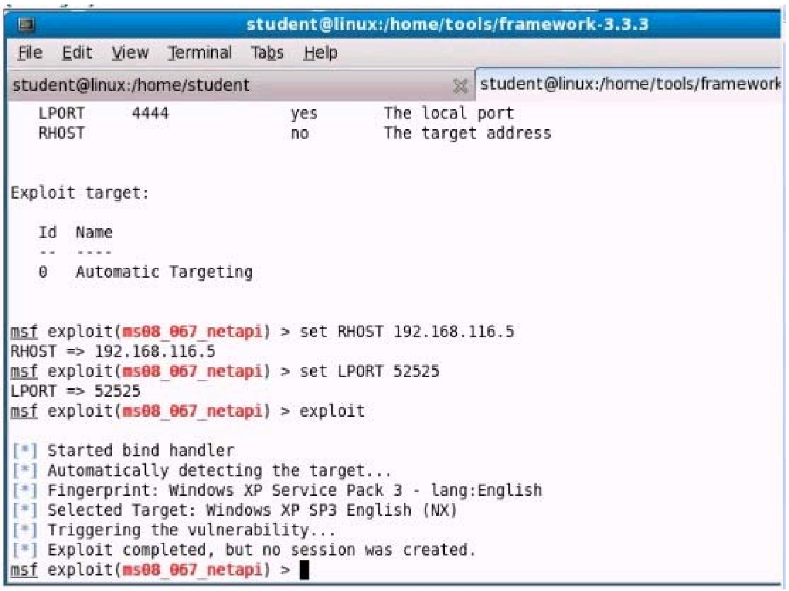
Community vote distribution

A (100%)

None

Question #97 Topic 1

Analyze the screenshot below. What event is depicted?



student@linux:/home/tools/framework-3.3.3
File Edit View Terminal Tabs Help
student@linux:/home/student
student@linux:/home/tools/framework

```
   LPORT    4444              yes       The local port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > set RHOST 192.168.116.5
RHOST => 192.168.116.5
msf exploit(ms08_067_netapi) > set LPORT 52525
LPORT => 52525
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (NX)
[*] Triggering the vulnerability...
[*] Exploit completed, but no session was created.
msf exploit(ms08_067_netapi) > 
```

A. An exploit that was attempted does not work against the target selected.

B. A payload was used that is not compatible with the chosen exploit.

C. The exploit is designed to work against the local host only.

D. The payload Is designed to create an interactive session.

Correct Answer: *A*

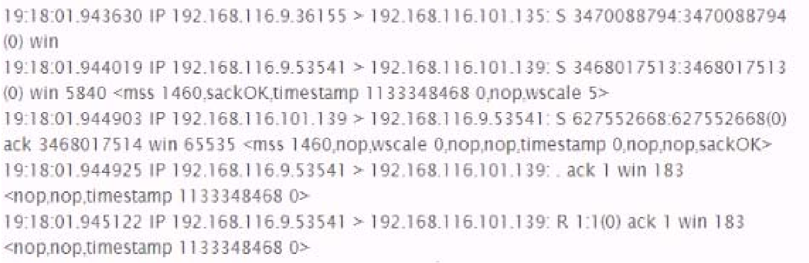
Community vote distribution

A (100%)

None

Question #98 Topic 1

Analyze the excerpt from a packet capture between the hosts 192.168.116.9 and 192.168.116.101. What factual conclusion can the tester draw from this output?



```
19:18:01.943630 IP 192.168.116.9.36155 > 192.168.116.101.135: S 3470088794:3470088794
(0) win
19:18:01.944019 IP 192.168.116.9.53541 > 192.168.116.101.139: S 3468017513:3468017513
(0) win 5840 <mss 1460,sackOK,timestamp 1133348468 0,nop,wscale 5>
19:18:01.944903 IP 192.168.116.101.139 > 192.168.116.9.53541: S 627552668:627552668(0)
ack 3468017514 win 65535 <mss 1460,nop,wscale 0,nop,nop,timestamp 0,nop,nop,sackOK>
19:18:01.944925 IP 192.168.116.9.53541 > 192.168.116.101.139: . ack 1 win 183
<nop,nop,timestamp 1133348468 0>
19:18:01.945122 IP 192.168.116.9.53541 > 192.168.116.101.139: R 1:1(0) ack 1 win 183
<nop,nop,timestamp 1133348468 0>
```

A. Port 135 is filtered, port 139 is open.

B. Pons 135 and 139 are filtered.

C. Ports 139 and 135 are open.

D. Port 139 is closed, port 135 is open

Correct Answer: *C*

Community vote distribution

A (100%)

None

Question #99 *Topic 1*

What is the main difference between LAN MAN and NTLMv1 challenge/responses?

A. NTLMv1 only pads IS bytes, whereas LANMAN pads to 21 bytes

B. NTLMv1 starts with the NT hash, whereas LANMAN starts with the LANMAN hash

C. NTLMv1utilizes DES, whereas LANMAN utilizes MD4

D. NTLMv1 splits the hash into 3 eight-byte pieces, whereas LAN MAN splits the hash Into 3 seven-byte pieces

Correct Answer: *A*

None

Question #100 *Topic 1*

You have been contracted to penetration test an e-mail server for a client that wants to know for sure if the sendmail service is vulnerable to any known attacks.
You have permission to run any type of test, how will you proceed to give the client the most valid answer?

A. Run all known sendmail exploits against the server and see if you can compromisethe service, even if it crashed the machine or service

B. Run a banner grabbing vulnerability checker to determine the sendmail version andpatch level, then look up and report all the vulnerabilities that exist for that versionand patch level

C. Run all sendmail exploits that will not crash the server and see if you cancompromise the service

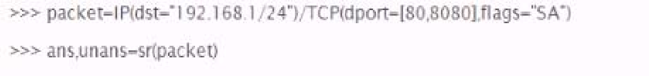
D. Log into the e-mail and determine the sendmail version and patch level, then lookup and report all the vulnerabilities that exist for that version and patch level

Correct Answer: *C*

None

Question #1 *Topic 2*

What will the following scapy commands do?



```
>>> packet=IP(dst="192.168.1/24")/TCP(dport=[80,8080],flags="SA")
>>> ans,unans=sr(packet)
```

A. Perform a SYN-ACK scan against TCP ports 80 and 3080 on host 192.168.1.24.

B. Perform a SYN scan against ports 80 through 8080 for all hosts on the192.168.1.0/24 network.

C. Combine the answered and unanswered results of a previous scan into the sr(packet)variable.

D. Perform a SYN-ACK scan against TCP ports 80 and 8080 for all hosts on the192.16S.1.0/24 network.

Correct Answer: *D*

None

Question #2 *Topic 2*

You want to find out what ports a system is listening on. What Is the correct command on a Linux system?

A. netstat nap

B. f port/p

C. tasklist/v

D. Isof -nao

Correct Answer: *A*

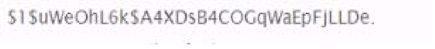
Reference:

http://cbl.abuseat.org/advanced.html

None

Question #3 *Topic 2*

You have obtained the hash below from the /etc/shadow file. What are you able to discern simply by looking at this hash?



```
$1$uWeOhL6k$A4XDsB4COGqWaEpFJLLDe.
```

A. A4XD$B4COCqWaEpFjLLDe. is a SHAI hash that was created using the salt $1 SuWeOhL6k$ 1

B. A4XD$B4COCqWaEpFjLLDe. is an MD5 hash that was created using the salt $1 SuWeOhL6k$

C. A4XDsB4COGqWaEpFjLLDe. is an MD5 hash that was created using the salt uWeOhL6k

D. A4XDsB4COCqWaEpFjLLDe. is a SHAI hash that was created using the salt

Correct Answer: *C*

None

Question #4 *Topic 2*

What difference would you expect to result from running the following commands;
(I). S dig ns domain.com target.com -t AXFR
and
(2). S dig ns.domain.com target.com -t IXFR=1002200301

A. Command (I) will display incremental information about a domain and command (2) will provide only 1002200301 bytes of information

B. Command (1) will display all information about a domain and command (2) willprovide only incremental updates from SOA 1002200301

C. Command (I) will display all information about a domain and command (2) willprovide only incremental updates up to SOA 1002200301

D. Command (I) will display all information about a domain and command (2) willprovide only 1002200301 bytes of information

Correct Answer: *B*

None

Question #5 *Topic 2*

The scope of your engagement is to include a target organization located in California with a /24 block of addresses that they claim to completely own. Which site could you utilize to confirm that you have been given accurate information before starting reconnaissance activities?

A. www.whois.net

B. www.arin.nei

C. www.apnic.net

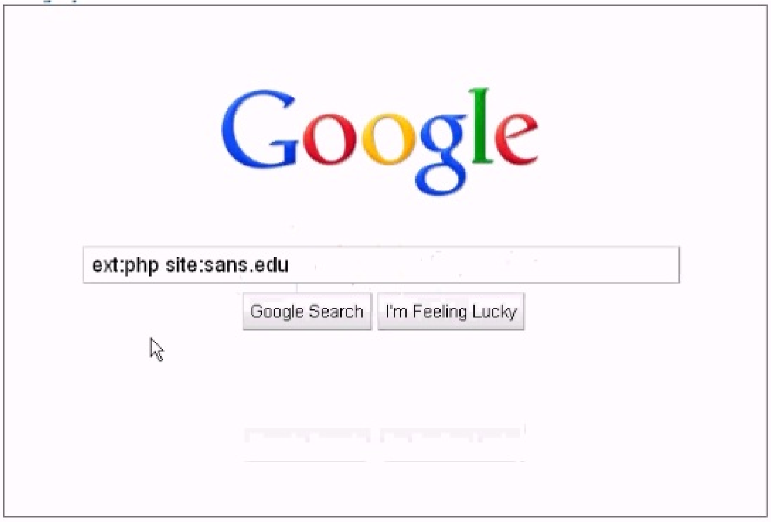
D. www.ripe.net

Correct Answer: *B*

None

Question #6 Topic 2

Analyze the screenshot below, which of the following sets of results will be retrieved using this search?



ext:php site:sans.edu

A. Pages from the domain sans.edu that have external links.

B. Files of type .php from the domain sans.edu.

C. Pages that contain the term ext:php and slte.sans.edu.

D. Files of type .php that redirect to the sans.edu domain.

Correct Answer: *B*

Community vote distribution

B (100%)

None

Question #7 *Topic 2*

Which of the following United States laws protects stored electronic information?

A. Title 18, Section 1029

B. Title 18, Section 1362

C. Title 18, Section 2701

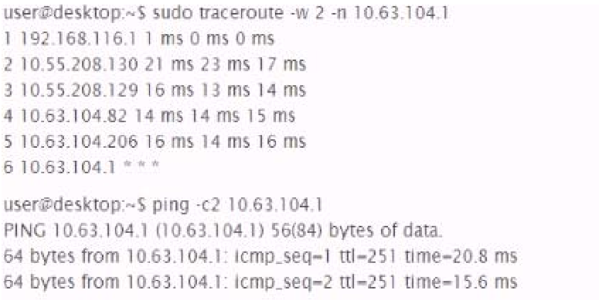
D. Title 18, Section 2510

Correct Answer: *D*

None

Question #8 *Topic 2*

Analyze the output of the two commands below:



```
user@desktop:~$ sudo traceroute -w 2 -n 10.63.104.1
1 192.168.116.1 1 ms 0 ms 0 ms
2 10.55.208.130 21 ms 23 ms 17 ms
3 10.55.208.129 16 ms 13 ms 14 ms
4 10.63.104.82 14 ms 14 ms 15 ms
5 10.63.104.206 16 ms 14 ms 16 ms
6 10.63.104.1 * * *

user@desktop:~$ ping -c2 10.63.104.1
PING 10.63.104.1 (10.63.104.1) 56(84) bytes of data.
64 bytes from 10.63.104.1: icmp_seq=1 ttl=251 time=20.8 ms
64 bytes from 10.63.104.1: icmp_seq=2 ttl=251 time=15.6 ms
```

Which of the following can be factually inferred from the results of these commands?

A. The router 192.16S.U6.1 is filtering UDP traceroute.

B. The host 10.63.104.1 is silently dropping UDP packets.

C. The host 10.63.104.1 is not issuing ICMP packets.

D. The router 10 63.104 206 is dropping ICMP traceroute.

Correct Answer: *C*

None

Question #9 *Topic 2*

Which protocol would need to be available on a target in order for Nmap to identify services like IMAPS and POP3S?

A. HTTPS

B. SSL

C. LDAP

D. TLS

Correct Answer: *A*

Reference:

http://nmap.org/book/vscan.html

Community vote distribution

B (100%)

None

Question #10 *Topic 2*

What is the sequence in which packets are sent when establishing a connection to a secured network?

A. Auth, Associate and Probe

B. Probe, Auth and Associate

C. Associate, Probe and Auth

D. Probe. Associate and Auth

Correct Answer: *C*

None

Question #11 *Topic 2*

You work as a Network Administrator in the Secure Inc. You often need to send PDF documents that contain secret information, such as, client password, their credit card details, email passwords, etc. through email to your customers. However, you are making PDFs password protected you are getting complaints from customers that their secret information is being misused. When you analyze this complaint you get that however you are applying the passwords on PDFs, they are not providing the maximum protection. What may be the cause of this security hole?

A. PDFs can be read easily in the plain-text form by applying a sniffer.

B. PDFs are sent in email in the plain-text form.

C. PDF passwords can easily be cracked by brute force attacks.

D. You are applying easily guessed passwords.

Correct Answer: *C*

None

Question #12 *Topic 2*

Which of the following tasks can be performed by using netcat utility?
Each correct answer represents a complete solution. Choose all that apply.

A. Firewall testing

B. Creating a Backdoor

C. Port scanning and service identification

D. Checking file integrity

Correct Answer: *ABC*

None

Question #13 *Topic 2*

You work as a Network Penetration tester in the Secure Inc. Your company takes the projects to test the security of various companies. Recently, Secure Inc. has assigned you a project to test the security of the Bluehill Inc. For this, you start monitoring the network traffic of the Bluehill Inc. In this process, you get that there are too many FTP packets traveling in the Bluehill Inc. network.

Now, you want to sniff the traffic and extract usernames and passwords of the FTP server. Which of the following tools will you use to accomplish the task?

A. Ettercap

B. L0phtcrack

C. NetStumbler

D. SARA

Correct Answer: *A*

None

Question #14 *Topic 2*

Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends large number of unsolicited commercial e-mail (UCE) messages on these addresses. Which of the following e-mail crimes is Peter committing?

A. E-mail spoofing

B. E-mail Spam

C. E-mail bombing

D. E-mail Storm

Correct Answer: *B*

None

Question #15 *Topic 2*

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully performed the following steps of the preattack phase to check the security of the We-are-secure network: l Gathering information l Determining the network range l Identifying active systems
Now, he wants to find the open ports and applications running on the network. Which of the following tools will he use to accomplish his task?

A. APNIC

B. SuperScan

C. RIPE

D. ARIN

Correct Answer: *B*

None

Question #16 *Topic 2*

Which of the following is the most common method for an attacker to spoof email?

A. Back door

B. Replay attack

C. Man in the middle attack

D. Open relay

Correct Answer: *D*

None

Question #17 *Topic 2*

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure. com Web site. For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value. What may be the reason?

A. The zombie computer is not connected to the we-are-secure.com Web server.

B. The zombie computer is the system interacting with some other system besides your comp uter.

C. Hping does not perform idle scanning.

D. The firewall is blocking the scanning process.

Correct Answer: *B*

None

Question #18 *Topic 2*

Joseph works as a Network Administrator for WebTech Inc. He has to set up a centralized area on the network so that each employee can share resources and documents with one another. Which of the following will he configure to accomplish the task?

A. WEP

B. VPN

C. Intranet

D. Extranet

Correct Answer: *C*

None

Question #19 *Topic 2*

Adam works as a professional Computer Hacking Forensic Investigator. He works with the local police. A project has been assigned to him to investigate an iPod, which was seized from a student of the high school. It is suspected that the explicit child pornography contents are stored in the iPod. Adam wants to investigate the iPod extensively. Which of the following operating systems will Adam use to carry out his investigations in more extensive and elaborate manner?

A. Windows XP

B. Mac OS

C. MINIX 3

D. Linux

Correct Answer: *B*

None

Question #20 *Topic 2*

Which of the following tools is an automated tool that is used to implement SQL injections and to retrieve data from Web server databases?

A. Fragroute

B. Absinthe

C. Stick

D. ADMutate

Correct Answer: *B*

None

Question #21 *Topic 2*

)?

A. Implement WEP.

B. Disabling SSID broadcast.

C. Change hub with switch.

D. Deploying a powerful antenna.

Correct Answer: *B*

None

Question #22 *Topic 2*

Which of the following is a passive information gathering tool?

A. Whois

B. Snort

C. Ettercap

D. Nmap

Correct Answer: *A*

None

Question #23 *Topic 2*

SIMULATION -

Fill in the blank with the appropriate tool name.

__________is a wireless network cracking tool that exploits the vulnerabilities in the RC4 Algorithm, which comprises the WEP security parameters.

Correct Answer: *WEPcrack*

None

Question #24 Topic 2

SIMULATION -

Write the appropriate attack name to fill in the blank.

In a _____________ DoS attack, the attacker sends a spoofed TCP SYN packet in which the IP address of the target is filled in both the source and destination fields.

Correct Answer: *land*

None

Question #25 *Topic 2*

Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 Active Directory domain-based network. The domain consists of a domain controller, two Windows 2003 member servers, and one hundred client computers. The company employees use laptops with Windows XP Professional.

These laptops are equipped with wireless network cards that are used to connect to access points located in the Marketing department of the company. The company employees log on to the domain by using a user name and password combination. The wireless network has been configured with WEP in addition to

802.1x. Mark wants to provide the best level of security for the kind of authentication used by the company. What will Mark do to accomplish the task?

A. Use EAP-TLS

B. Use MD5

C. Use PEAP

D. Use IPSec

Correct Answer: *C*

None

Question #26 *Topic 2*

You work as a professional Ethical Hacker. You are assigned a project to perform blackhat testing on www.we-are-secure.com. You visit the office of we-are- secure.com as an air-condition mechanic. You claim that someone from the office called you saying that there is some fault in the air-conditioner of the server room. After some inquiries/arguments, the Security Administrator allows you to repair the air-conditioner of the server room.

When you get into the room, you found the server is Linux-based. You press the reboot button of the server after inserting knoppix Live CD in the CD drive of the server. Now, the server promptly boots backup into Knoppix. You mount the root partition of the server after replacing the root password in the /etc/shadow file with a known password hash and salt. Further, you copy the netcat tool on the server and install its startup files to create a reverse tunnel and move a shell to a remote server whenever the server is restarted. You simply restart the server, pull out the Knoppix Live CD from the server, and inform that the air-conditioner is working properly.

After completing this attack process, you create a security auditing report in which you mention various threats such as social engineering threat, boot from Live

CD, etc. and suggest the countermeasures to stop booting from the external media and retrieving sensitive data. Which of the following steps have you suggested to stop booting from the external media and retrieving sensitive data with regard to the above scenario?

Each correct answer represents a complete solution. Choose two.

A. Setting only the root level access for sensitive data.

B. Encrypting disk partitions.

C. Placing BIOS password.

D. Using password protected hard drives.

Correct Answer: *BD*

None

Question #27

Topic 2

What happens when you scan a broadcast IP address of a network?
Each correct answer represents a complete solution. Choose all that apply.

A. It may show smurf DoS attack in the network IDS of the victim.

B. It leads to scanning of all the IP addresses on that subnet at the same time.

C. It will show an error in the scanning process.

D. Scanning of the broadcast IP address cannot be performed.

Correct Answer: *AB*

None

Question #28 *Topic 2*

Which of the following tools can be used to perform Windows password cracking, Windows enumeration, and VoIP session sniffing?

A. Cain

B. L0phtcrack

C. Pass-the-hash toolkit

D. John the Ripper

Correct Answer: *A*

None

Question #29 *Topic 2*

John works as a Professional Penetration Tester. He has been assigned a project to test the Website security of www.we-are-secure Inc. On the We-are-secure

Website login page, he enters='or''=' as a username and successfully logs on to the user page of the Web site. Now, John asks the we-are-secure Inc. to improve the login page PHP script. Which of the following suggestions can John give to improve the security of the we-are-secure Website login page from the SQL injection attack?

A. Use the session_regenerate_id() function

B. Use the escapeshellcmd() function

C. Use the mysql_real_escape_string() function for escaping input

D. Use the escapeshellarg() function

Correct Answer: *C*

None

Question #30 *Topic 2*

Which of the following attacks can be overcome by applying cryptography?

A. Buffer overflow

B. Web ripping

C. DoS

D. Sniffing

Correct Answer: *D*

None

Question #31 *Topic 2*

Which of the following tools uses exploits to break into remote operating systems?

A. Nessus

B. Metasploit framework

C. Nmap

D. John the Ripper

Correct Answer: *B*

None

Question #32 *Topic 2*

Which of the following penetration testing phases involves gathering data from whois, DNS, and network scanning, which helps in mapping a target network and provides valuable information regarding the operating system and applications running on the systems?

A. Post-attack phase

B. Attack phase

C. Pre-attack phase

D. On-attack phase

Correct Answer: *C*

None

Question #33 *Topic 2*

John works as a Penetration Tester in a security service providing firm named you-are-secure Inc.
Recently, John's company has got a project to test the security of a promotional Website www.missatlanta.com and assigned the pen-testing work to John. When
John is performing penetration testing, he inserts the following script in the search box at the company home page:
<script>alert('Hi, John')</script>
After pressing the search button, a pop-up box appears on his screen with the text - "Hi, John."
Which of the following attacks can be performed on the Web site tested by john while considering the above scenario?

A. Replay attack

B. Buffer overflow attack

C. CSRF attack

D. XSS attack

Correct Answer: *D*

None

Question #34 *Topic 2*

Which of the following is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards and also detects wireless networks marking their relative position with a GPS?

A. NetStumbler

B. Tcpdump

C. Kismet

D. Ettercap

Correct Answer: *A*

None

Question #35 *Topic 2*

Which of the following tools is used for vulnerability scanning and calls Hydra to launch a dictionary attack?

A. Whishker

B. Nmap

C. Nessus

D. SARA

Correct Answer: *C*

None

Question #36 *Topic 2*

Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

A. Man-in-the-middle

B. ARP spoofing

C. Port scanning

D. Session hijacking

Correct Answer: *B*

None

Question #37 *Topic 2*

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure. com Web site. For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value. What may be the reason?

A. The zombie computer is the system interacting with some other system besides your comp uter.

B. The firewall is blocking the scanning process.

C. The zombie computer is not connected to the we-are-secure.com Web server.

D. Hping does not perform idle scanning.

Correct Answer: *A*

None

Question #38

Topic 2

You execute the following netcat command:

```
c:\target\nc -1 -p 53 -d -e cmd.exe
```

What action do you want to perform by issuing the above command?

A. Capture data on port 53 and performing banner grabbing.

B. Capture data on port 53 and delete the remote shell.

C. Listen the incoming traffic on port 53 and execute the remote shell.

D. Listen the incoming data and performing port scanning.

Correct Answer: *C*

None

Question #39 *Topic 2*

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure. com Website. The we-are-secure.com Web server is using Linux operating system. When you port scanned the we-are- secure.com Web server, you got that TCP port 23, 25, and 53 are open. When you tried to telnet to port 23, you got a blank screen in response. When you tried to type the dir, copy, date, del, etc. commands you got only blank spaces or underscores symbols on the screen. What may be the reason of such unwanted situation?

A. The we-are-secure.com server is using honeypot.

B. The we-are-secure.com server is using a TCP wrapper.

C. The telnet service of we-are-secure.com has corrupted.

D. The telnet session is being affected by the stateful inspection firewall.

Correct Answer: *B*

None

Question #40

Topic 2

Which of the following tools is used to verify the network structure packets and confirm that the packets are constructed according to specification?

A. snort_inline

B. EtherApe

C. Snort decoder

D. AirSnort

Correct Answer: *C*

None

Question #41 *Topic 2*

You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement?
Each correct answer represents a complete solution. Choose two.

A. MAC filtering the router

B. Using WPA encryption

C. Using WEP encryption

D. Not broadcasting SSID

Correct Answer: *BC*

None

Question #42 *Topic 2*

You work as an Administrator for Bluesky Inc. The company has 145 Windows XP Professional client computers and eighty Windows 2003 Server computers.

You want to install a security layer of WAP specifically designed for a wireless environment. You also want to ensure that the security layer provides privacy, data integrity, and authentication for client-server communications over a wireless network. Moreover, you want a client and server to be authenticated so that wireless transactions remain secure and the connection is encrypted. Which of the following options will you use to accomplish the task?

A. Wired Equivalent Privacy (WEP)

B. Virtual Private Network (VPN)

C. Wireless Transport Layer Security (WTLS)

D. Recovery Console

Correct Answer: *C*

None

Question #43 *Topic 2*

You run the following PHP script:

```
<?php $name = mysql_real_escape_string($_POST["name"]);
$password = mysql_real_escape_string($_POST["password"]);?>
```

What is the use of the mysql_real_escape_string() function in the above script.

Each correct answer represents a complete solution. Choose all that apply

A. It escapes all special characters from strings $_POST["name"] and $_POST["password"].

B. It escapes all special characters from strings $_POST["name"] and $_POST["password"] except ' and ".

C. It can be used to mitigate a cross site scripting attack.

D. It can be used as a countermeasure against a SQL injection attack.

Correct Answer: *AD*

None

Question #44 *Topic 2*

You run the following bash script in Linux:
for i in 'cat hostlist.txt' ;do nc -q 2 -v $i 80 < request.txt done where, hostlist.txt file contains the list of IP addresses and request.txt is the output file.
Which of the following tasks do you want to perform by running this script?

A. You want to perform port scanning to the hosts given in the IP address list.

B. You want to transfer file hostlist.txt to the hosts given in the IP address list.

C. You want to perform banner grabbing to the hosts given in the IP address list.

D. You want to put nmap in the listen mode to the hosts given in the IP address list.

Correct Answer: *C*

None

Question #45 *Topic 2*

You want to perform an active session hijack against Secure Inc. You have found a target that allows Telnet session. You have also searched an active session due to the high level of traffic on the network. What should you do next?

A. Use a sniffer to listen network traffic.

B. Use macoff to change MAC address.

C. Guess the sequence numbers.

D. Use brutus to crack telnet password.

Correct Answer: *C*

None

Question #46 *Topic 2*

Which of the following statements are true about firewalking?
Each correct answer represents a complete solution. Choose all that apply.

A. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall.

B. Firewalking works on the UDP packets.

C. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.

D. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.

Correct Answer: *ACD*

None

Question #47 *Topic 2*

Which of the following Web attacks is performed by manipulating codes of programming languages such as SQL, Perl, Java present in the Web pages?

A. Command injection attack

B. Cross-Site Scripting attack

C. Cross-Site Request Forgery

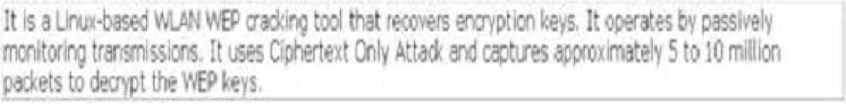
D. Code injection attack

Correct Answer: *D*

None

Question #48 *Topic 2*

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:



It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

Which of the following tools is John using to crack the wireless encryption keys?

A. AirSnort

B. PsPasswd

C. Cain

D. Kismet

Correct Answer: *A*

None

Question #49 *Topic 2*

What happens when you scan a broadcast IP address of a network?
Each correct answer represents a complete solution. Choose all that apply.

A. It will show an error in the scanning process.

B. Scanning of the broadcast IP address cannot be performed.

C. It may show smurf DoS attack in the network IDS of the victim.

D. It leads to scanning of all the IP addresses on that subnet at the same time.

Correct Answer: *CD*

None

Question #50 *Topic 2*

You have forgotten your password of an online shop. The web application of that online shop asks you to enter your email so that they can send you a new password. You enter your email you@gmail.com' and press the submit button. The Web application displays the server error.
What can be the reason of the error?

A. The remote server is down.

B. You have entered any special character in email.

C. Your internet connection is slow.

D. Email entered is not valid.

Correct Answer: *B*

None

Question #51 *Topic 2*

You want to run the nmap command that includes the host specification of 202.176.56-57.*. How many hosts will you scan?

A. 512

B. 64

C. 1024

D. 256

Correct Answer: *A*

None

Question #52 *Topic 2*

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He enters the following command on the

Linux terminal:chmod 741 secure.c

Considering the above scenario, which of the following statements are true?

Each correct answer represents a complete solution. Choose all that apply.

A. John is restricting a guest to only write or execute the secure.c file.

B. John is providing all rights to the owner of the file.

C. By the octal representation of the file access permission, John is restricting the group members to only read the secure.c file.

D. The textual representation of the file access permission of 741 will be -rwxr--rw-.

Correct Answer: *BC*

None

Question #53 *Topic 2*

John works as a Professional Penetration Tester. He has been assigned a project to test the Website security of www.we-are-secure Inc. On the We-are-secure
Website login page, he enters ='or''=' as a username and successfully logs on to the user page of the Web site. Now, John asks the we-are-secure Inc. to improve the login page PHP script. Which of the following suggestions can John give to improve the security of the we-are-secure Website login page from the SQL injection attack?

A. Use the escapeshellarg() function

B. Use the session_regenerate_id() function

C. Use the mysql_real_escape_string() function for escaping input

D. Use the escapeshellcmd() function

Correct Answer: *C*

None

Question #54 *Topic 2*

Which of the following Web authentication techniques uses a single sign-on scheme?

A. NTLM authentication

B. Microsoft Passport authentication

C. Basic authentication

D. Digest authentication

Correct Answer: *B*

None

Question #55 *Topic 2*

Which of the following tools is spyware that makes Windows clients send their passwords as clear text?

A. Pwddump2

B. SMBRelay

C. KrbCrack

D. C2MYAZZ

Correct Answer: *D*

None

Question #56 | *Topic 2*

Which of the following tools allow you to perform HTTP tunneling?
Each correct answer represents a complete solution. Choose all that apply.

A. BackStealth

B. Tunneled

C. Nikto

D. HTTPort

Correct Answer: *ABD*

None

Question #57 *Topic 2*

You want to create a binary log file using tcpdump. Which of the following commands will you use?

A. tcpdump -B

B. tcpdump -dd

C. tcpdump -w

D. tcpdump –d

Correct Answer: *C*

None

Question #58 *Topic 2*

Which of the following standards is used in wireless local area networks (WLANs)?

A. IEEE 802.4

B. IEEE 802.3

C. IEEE 802.11b

D. IEEE 802.5

Correct Answer: *C*

None

Question #59 *Topic 2*

Anonymizers are the services that help make a user's own Web surfing anonymous. An anonymizer removes all the identifying information from a user's computer while the user surfs the Internet. It ensures the privacy of the user in this manner. After the user anonymizes a Web access with an anonymizer prefix, every subsequent link selected is also automatically accessed anonymously. Which of the following are limitations of anonymizers?

Each correct answer represents a complete solution. Choose all that apply.

A. Java applications

B. Secure protocols

C. ActiveX controls

D. JavaScript

E. Plugins

Correct Answer: *ABCDE*

None

Question #60 *Topic 2*

), you implement WEP. Now you want to connect your client computer to the WLAN. Which of the following is the required information that you will need to configure the client computer?
Each correct answer represents a part of the solution. Choose two.

A. WEP key

B. MAC address of the router

C. IP address of the router

D. SSID of the WLAN

Correct Answer: *AD*

None

Question #61 *Topic 2*

Which of the following vulnerability scanner scans from CGI, IDA, Unicode, and Nimda vulnerabilities?

A. Hackbot

B. SARA

C. Nessus

D. Cgichk

Correct Answer: *A*

None

Question #62 *Topic 2*

You want to scan your network quickly to detect live hosts by using ICMP ECHO Requests. What type of scanning will you perform to accomplish the task?

A. Idle scan

B. TCP SYN scan

C. Ping sweep scan

D. XMAS scan

Correct Answer: *C*

None

Question #63 *Topic 2*

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with a lot of requests. Which of the following tools can an attacker use to perform a DNS zone transfer?
Each correct answer represents a complete solution. Choose all that apply.

A. NSLookup

B. Host

C. DSniff

D. Dig

Correct Answer: *ABD*

None

Question #64 *Topic 2*

This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:

It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.

It is commonly used for the following purposes:

a. War driving

b. Detecting unauthorized access points

c. Detecting causes of interference on a WLAN

d. WEP ICV error tracking

e. Making Graphs and Alarms on 802.11 Data, including Signal Strength

This tool is known as __________.

A. Absinthe

B. THC-Scan

C. NetStumbler

D. Kismet

Correct Answer: *C*

None

Question #65

Topic 2

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following pre-attack phases while testing the security of the server:
Footprinting Scanning Now he wants to conduct the enumeration phase. Which of the following tools can John use to conduct it?
Each correct answer represents a complete solution. Choose all that apply.

A. PsFile

B. PsPasswd

C. UserInfo

D. WinSSLMiM

Correct Answer: *ABC*

None

Question #66 *Topic 2*

You want to search the Apache Web server having version 2.0 using google hacking. Which of the following search queries will you use?

A. intitle:"Test Page for Apache Installation" "You are free"

B. intitle:"Test Page for Apache Installation" "It worked!"

C. intitle:test.page "Hey, it worked !" "SSl/TLS aware"

D. intitle:Sample.page.for.Apache Apache.Hook.Function

Correct Answer: *D*

None

Question #67 *Topic 2*

The employees of EWS Inc. require remote access to the company's Web servers. In order to provide solid wireless security, the company uses EAP-TLS as the authentication protocol. Which of the following statements are true about EAP-TLS?
Each correct answer represents a complete solution. Choose all that apply.

A. It provides a moderate level of security.

B. It uses password hash for client authentication.

C. It uses a public key certificate for server authentication.

D. It is supported by all manufacturers of wireless LAN hardware and software.

Correct Answer: *CD*

None

Question #68 Topic 2

SIMULATION -

Fill in the blank with the appropriate tool.

____scans IP networks for NetBIOS name information and works in the same manner as nbtstat, but it operates on a range of addresses instead of just one.

Correct Answer: *NBTscan*

None

Question #69 Topic 2

Which of the following tools can be used as a Linux vulnerability scanner that is capable of identifying operating systems and network services? Each correct answer represents a complete solution. Choose all that apply.

A. Cheops

B. Fport

C. Elsave

D. Cheops-ng

Correct Answer: *AD*

None

Question #70 *Topic 2*

In which of the following attacks does an attacker use packet sniffing to read network traffic between two parties to steal the session cookie?

A. Cross-site scripting

B. Session fixation

C. Session sidejacking

D. ARP spoofing

Correct Answer: *C*

None

Question #71 *Topic 2*

Which of the following Nmap commands is used to perform a UDP port scan?

A. nmap -sS

B. nmap -sY

C. nmap -sN

D. nmap –sU

Correct Answer: *D*

None

Question #72 *Topic 2*

SIMULATION -
Fill in the blank with the appropriate act name.
The___ act gives consumers the right to ask emailers to stop spamming them.

Correct Answer: *CAN-SPAM*

None

Question #73 *Topic 2*

John works as an Ethical Hacker for uCertify Inc. He wants to find out the ports that are open in uCertify's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?

A. TCP FIN

B. Xmas tree

C. TCP SYCK

D. TCP SYN

Correct Answer: *D*

None

Question #74 Topic 2

Which of following tasks can be performed when Nikto Web scanner is using a mutation technique?
Each correct answer represents a complete solution. Choose all that apply.

A. Guessing for password file names.

B. Sending mutation payload for Trojan attack.

C. Testing all files with all root directories.

D. Enumerating user names via Apache.

Correct Answer: *ACD*

None

Question #75 *Topic 2*

You are sending a file to an FTP server. The file will be broken into several pieces of information packets (segments) and will be sent to the server. The file will again be reassembled and reconstructed once the packets reach the FTP server. Which of the following information should be used to maintain the correct order of information packets during the reconstruction of the file?

A. Acknowledge number

B. TTL

C. Checksum

D. Sequence number

Correct Answer: *D*

None

Question #76

Topic 2

Which of the following is the frequency range to tune IEEE 802.11a network?

A. 1.15-3.825 GHz

B. 5.15-5.825 GHz

C. 5.25-9.825 GHz

D. 6.25-9.825 GHz

Correct Answer: *B*

None

Question #77

Topic 2

Which of the following tools monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools?

A. IDS

B. Firewall

C. Snort

D. WIPS

Correct Answer: *D*

None

Question #78 *Topic 2*

Adam works as a professional Computer Hacking Forensic Investigator. He wants to investigate a suspicious email that is sent using a Microsoft Exchange server.
Which of the following files will he review to accomplish the task?
Each correct answer represents a part of the solution. Choose all that apply.

A. Checkpoint files

B. cookie files

C. Temporary files

D. EDB and STM database files

Correct Answer: *ACD*

None

Question #79 *Topic 2*

You work as a Web developer in the IBM Inc. Your area of proficiency is PHP. Since you have proper knowledge of security, you have bewared from rainbow attack. For mitigating this attack, you design the PHP code based on the following algorithm: key = hash(password + salt) for 1 to 65000 do key = hash(key + salt)

Which of the following techniques are you implementing in the above algorithm?

A. Key strengthening

B. Hashing

C. Sniffing

D. Salting

Correct Answer: *A*

None

Question #80 *Topic 2*

You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

A. Implement WEP

B. Implement MAC filtering

C. Don't broadcast SSID

D. Implement WPA

Correct Answer: *C*

None

Question #81 *Topic 2*

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using the Linux operating system. He wants to use a wireless sniffer to sniff the We-are-secure network. Which of the following tools will he use to accomplish his task?

A. NetStumbler

B. Snadboy's Revelation

C. WEPCrack

D. Kismet

Correct Answer: *D*

None

Question #82 Topic 2

You work as a Network Penetration tester in the Secure Inc. Your company takes the projects to test the security of various companies. Recently, Secure Inc. has assigned you a project to test the security of a Web site. You go to the Web site login page and you run the following SQL query:
SELECT email, passwd, login_id, full_name

FROM members -
WHERE email = 'attacker@somehwere.com'; DROP TABLE members; --'
What task will the above SQL query perform?

A. Performs the XSS attacks.

B. Deletes the entire members table.

C. Deletes the rows of members table where email id is 'attacker@somehwere.com' given.

D. Deletes the database in which members table resides.

Correct Answer: *B*

None

Question #83 *Topic 2*

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server.

The output of the scanning test is as follows:

```
C:\whisker.pl -h target_IP_address
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - =
= Host: target_IP_address
= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1
mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22
+ 200 OK: HEAD /cgi-bin/printenv
```

John recognizes /cgi-bin/printenv vulnerability ('Printenv' vulnerability) in the We_are_secure server. Which of the following statements about 'Printenv' vulnerability are true?

Each correct answer represents a complete solution. Choose all that apply.

A. 'Printenv' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.

B. The countermeasure to 'printenv' vulnerability is to remove the CGI script.

C. This vulnerability helps in a cross site scripting attack.

D. With the help of 'printenv' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

Correct Answer: *BCD*

None

Question #84 *Topic 2*

Ryan wants to create an ad hoc wireless network so that he can share some important files with another employee of his company. Which of the following wireless security protocols should he choose for setting up an ad hoc wireless network?
Each correct answer represents a part of the solution. Choose two.

A. WPA2 -EAP

B. WPA-PSK

C. WPA-EAP

D. WEP

Correct Answer: *BD*

None

Question #85 *Topic 2*

Which of the following statements are true about NTLMv1?
Each correct answer represents a complete solution. Choose all that apply.

A. It uses the LANMAN hash of the user's password.

B. It is mostly used when no Active Directory domain exists.

C. It is a challenge-response authentication protocol.

D. It uses the MD5 hash of the user's password.

Correct Answer: *ABC*

None

Question #86

Topic 2

Which of the following can be used as a countermeasure against the SQL injection attack?
Each correct answer represents a complete solution. Choose two.

A. mysql_real_escape_string()

B. Prepared statement

C. mysql_escape_string()

D. session_regenerate_id()

Correct Answer: *AB*

None

Question #87 *Topic 2*

You send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024 using hping2 utility. This attack is known as
__________.

A. Port scanning

B. Spoofing

C. Cloaking

D. Firewalking

Correct Answer: *D*

None

Question #88 *Topic 2*

Which of the following tools connects to and executes files on remote systems?

A. Spector

B. Hk.exe

C. PsExec

D. GetAdmin.exe

Correct Answer: *C*

None

Question #89 *Topic 2*

You are concerned about rogue wireless access points being connected to your network. What is the best way to detect and prevent these?

A. Site surveys

B. Protocol analyzers

C. Network anti-spyware software

D. Network anti-virus software

Correct Answer: *A*

None

Question #90

Topic 2

How many bits encryption does SHA-1 use?

A. 140

B. 512

C. 128

D. 160

Correct Answer: *D*

None

Question #91 *Topic 2*

You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company.

The suspected employee is using an online e-mail system such as Hotmail or Yahoo. Which of the following folders on the local computer will you review to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. History folder

B. Temporary Internet Folder

C. Cookies folder

D. Download folder

Correct Answer: *ABC*

None

Question #92 *Topic 2*

You run the rdisk /s command to retrieve the backup SAM file on a computer. Where should you go on the computer to find the file?

A. %systemroot%\password\sam._

B. %systemroot%\sam._

C. %systemroot%\repair\sam._

D. %systemroot%\backup\sam._

Correct Answer: *C*

None