ECCouncil

Exam EC0-350

Ethical Hacking and Countermeasures V8

Version: 5.1

[Total Questions: 878]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	100
Topic 4: Volume D	100
Topic 5: Volume E	100
Topic 6: Volume F	100
Topic 7: Volume G	100
Topic 8: Volume H	178

Topic 1, Volume A

Question No : 1 - (Topic 1)

What port number is used by Kerberos protocol?

A. 88
B. 44
C. 487
D. 419

Answer: A

Question No : 2 - (Topic 1)

Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices, which would otherwise be unable to communicate a means to notify administrators of problems or performance.

System Messages from the previous week

Thursday, July 20, 2006 12:21:25 PM CDT

Lists all system messages reported during the past 7 days

Number of records reported: 5

▼TimeStamp	ID	Severity	Server	Component	Error Co
Monday, July 17, 2006 2:49:30 PM CDT	870ef3dd1c10e5c6:19ee8a:10c7e0883f7:-7ff8	Fatal	dhcp-uaus09-147-76	Logging	ERROR
Monday, July 17, 2006 12:36:59 PM CDT	870ef3dd1c10e5c6:1983ad7:10c7d8ece05:-7ffb	Fatal	dhcp-uaus09-147-76	Logging	ERROR
Thursday, July 20, 2006 12:20:46 PM CDT	2fe1c4f202a318cd:15ad36d:10c8c6040be:-7fc0	Fatal	dhcp-uaus09-147-110	Logging	ERROR
Thursday, July 20, 2006 9:43:14 AM CDT	2fe1c4f202a318cd:15ad36d:10c8c6040be:-7fdd	Fatal	dhcp-uaus09-147-110	Logging	ERROR

What default port Syslog daemon listens on?

A. 242
B. 312
C. 416
D. 514

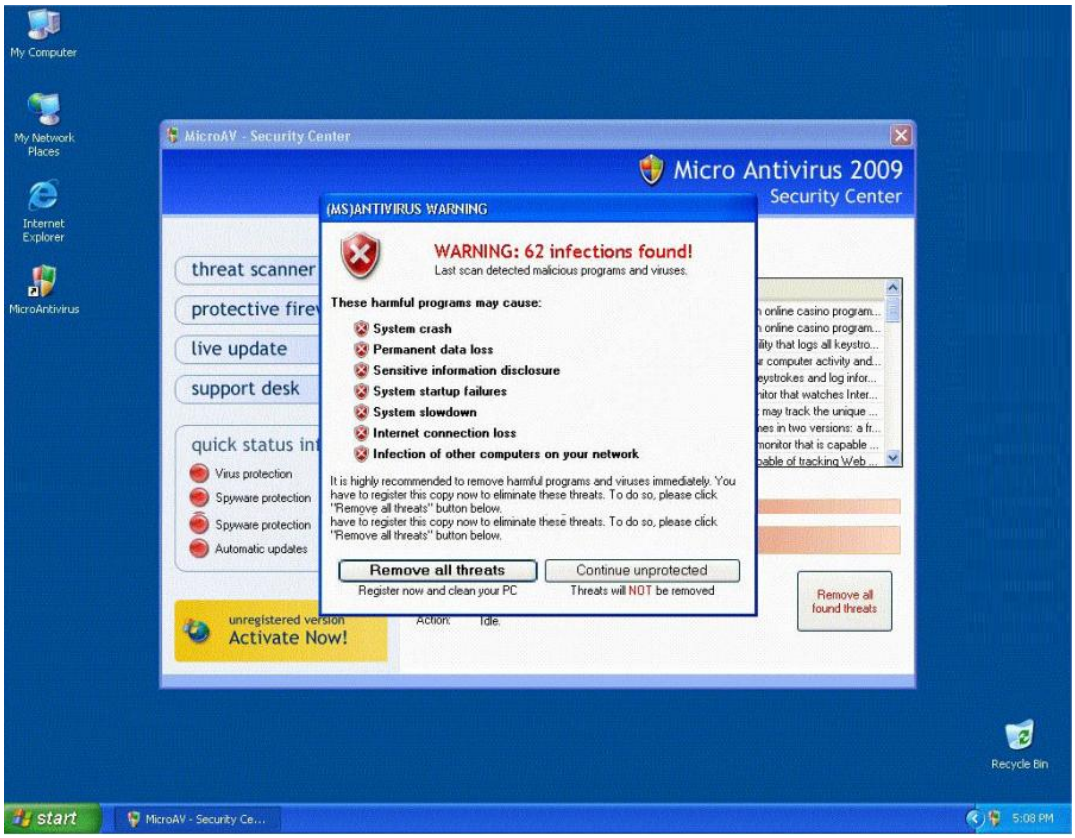
Answer: D

Question No : 3 - (Topic 1)

Fake Anti-Virus, is one of the most frequently encountered and persistent threats on the web. This malware uses social engineering to lure users into infected websites with a technique called Search Engine Optimization.

Once the Fake AV is downloaded into the user's computer, the software will scare them into believing their system is infected with threats that do not really exist, and then push users to purchase services to clean up the non-existent threats.

The Fake AntiVirus will continue to send these annoying and intrusive alerts until a payment is made.



What is the risk of installing Fake AntiVirus?

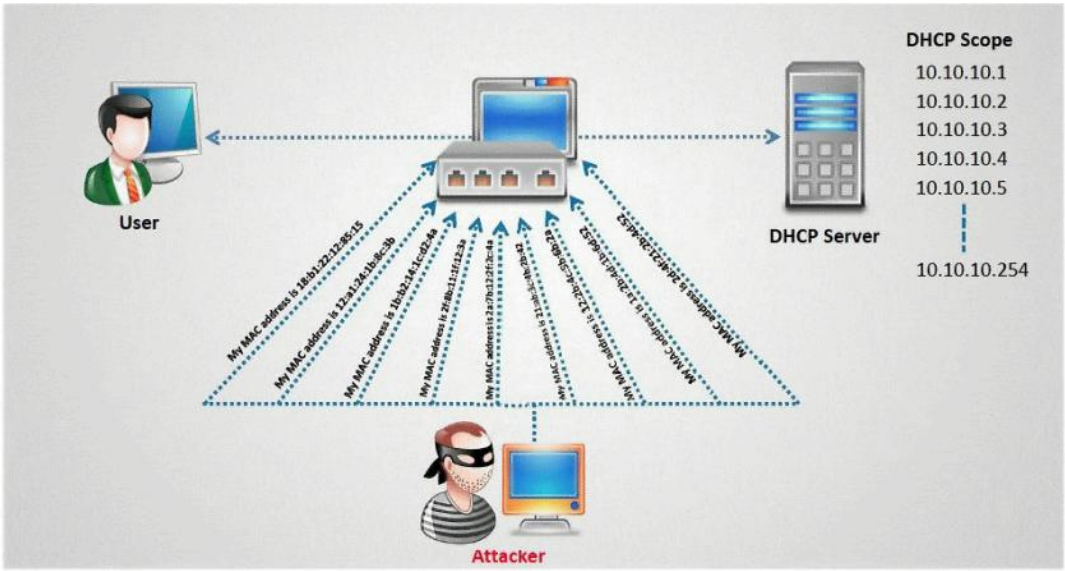
A. Victim's Operating System versions, services running and applications installed will be published on Blogs and Forums
B. Victim's personally identifiable information such as billing address and credit card details, may be extracted and exploited by the attacker
C. Once infected, the computer will be unable to boot and the Trojan will attempt to format the hard disk
D. Denial of Service attack will be launched against the infected computer crashing other

machines on the connected network

Answer: B

Question No : 4 - (Topic 1)

How do you defend against DHCP Starvation attack?



A. Enable ARP-Block on the switch
B. Enable DHCP snooping on the switch
C. Configure DHCP-BLOCK to 1 on the switch
D. Install DHCP filters on the switch to block this attack

Answer: B

Question No : 5 - (Topic 1)

Attacking well-known system defaults is one of the most common hacker attacks. Most software is shipped with a default configuration that makes it easy to install and setup the application. You should change the default settings to secure the system.

Which of the following is NOT an example of default installation?

A. Many systems come with default user accounts with well-known passwords that

administrators forget to change
B. Often, the default location of installation files can be exploited which allows a hacker to retrieve a file from the system
C. Many software packages come with "samples" that can be exploited, such as the sample programs on IIS web services
D. Enabling firewall and anti-virus software on the local system

Answer: D

Question No : 6 - (Topic 1)

Bret is a web application administrator and has just read that there are a number of surprisingly common web application vulnerabilities that can be exploited by unsophisticated attackers with easily available tools on the Internet. He has also read that when an organization deploys a web application, they invite the world to send HTTP requests. Attacks buried in these requests sail past firewalls, filters, platform hardening, SSL, and IDS without notice because they are inside legal HTTP requests. Bret is determined to weed out vulnerabilities.

What are some of the common vulnerabilities in web applications that he should be concerned about?

A. Non-validated parameters, broken access control, broken account and session management, cross-site scripting and buffer overflows are just a few common vulnerabilities
B. Visible clear text passwords, anonymous user account set as default, missing latest security patch, no firewall filters set and no SSL configured are just a few common vulnerabilities
C. No SSL configured, anonymous user account set as default, missing latest security patch, no firewall filters set and an inattentive system administrator are just a few common vulnerabilities
D. No IDS configured, anonymous user account set as default, missing latest security patch, no firewall filters set and visible clear text passwords are just a few common vulnerabilities

Answer: A

Question No : 7 - (Topic 1)

Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator

working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company.

She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks down the actual emails sent and upon opening them, only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture.

What technique was used by the Kiley Innovators employee to send information to the rival marketing company?

A. The Kiley Innovators employee used cryptography to hide the information in the emails sent
B. The method used by the employee to hide the information was logical watermarking
C. The employee used steganography to hide information in the picture attachments
D. By using the pictures to hide information, the employee utilized picture fuzzing

Answer: C

Question No : 8 - (Topic 1)

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 verify her password with him "just to double check our records." Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.'s computers with a valid user name and password, to steal the cookie recipe. What kind of attack is being illustrated here?

A. Reverse Psychology
B. Reverse Engineering
C. Social Engineering
D. Spoofing Identity

E. Faking Identity

Answer: C

Question No : 9 - (Topic 1)

You just purchased the latest DELL computer, which comes pre-installed with Windows 7, McAfee antivirus software and a host of other applications. You want to connect Ethernet wire to your cable modem and start using the computer immediately. Windows is dangerously insecure when unpacked from the box, and there are a few things that you must do before you use it.

A. New installation of Windows should be patched by installing the latest service packs and hotfixes
B. Key applications such as Adobe Acrobat, Macromedia Flash, Java, Winzip etc., must have the latest security patches installed
C. Install a personal firewall and lock down unused ports from connecting to your computer
D. Install the latest signatures for Antivirus software
E. Configure "Windows Update" to automatic
F. Create a non-admin user with a complex password and logon to this account
G. You can start using your computer as vendors such as DELL, HP and IBM would have already installed the latest service packs.

Answer: A,C,D,E,F

Question No : 10 - (Topic 1)

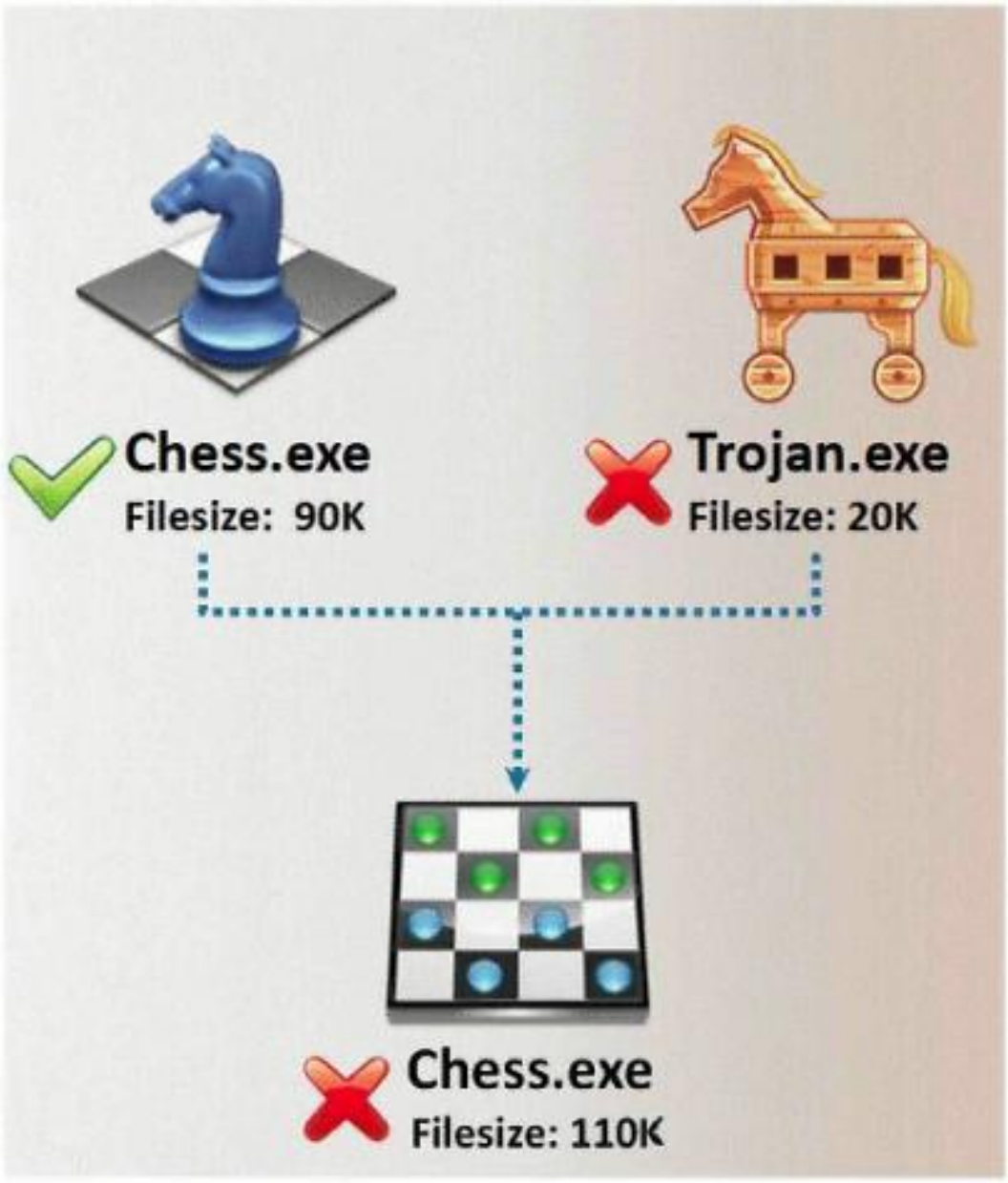
What does FIN in TCP flag define?

A. Used to abort a TCP connection abruptly
B. Used to close a TCP connection
C. Used to acknowledge receipt of a previous packet or transmission
D. Used to indicate the beginning of a TCP connection

Answer: B

Question No : 11 - (Topic 1)

In Trojan terminology, what is required to create the executable file chess.exe as shown below?



A. Mixer
B. Converter
C. Wrapper
D. Zipper

Answer: C

Question No : 12 - (Topic 1)

Peter extracts the SID list from Windows 2008 Server machine using the hacking tool "SIDExtracter". Here is the output of the SIDs:

```
S-1-5-21-1125394485-807628933-549785860-100 John
S-1-5-21-1125394485-807628933-549785860-652 Rebecca
S-1-5-21-1125394485-807628933-549785860-412 Sheela
S-1-5-21-1125394485-807628933-549785860-999 Shawn
S-1-5-21-1125394485-807628933-549785860-777 Somia
S-1-5-21-1125394485-807628933-549785860-500 Chang
S-1-5-21-1125394485-807628933-549785860-555 Micah
```

From the above list identify the user account with System Administrator privileges?

A. John
B. Rebecca
C. Sheela
D. Shawn
E. Somia
F. Chang
G. Micah

Answer: F

Question No : 13 - (Topic 1)

Shayla is an IT security consultant, specializing in social engineering and external penetration tests. Shayla has been hired on by Treks Avionics, a subcontractor for the Department of Defense. Shayla has been given authority to perform any and all tests necessary to audit the company's network security.

No employees for the company, other than the IT director, know about Shayla's work she will be doing. Shayla's first step is to obtain a list of employees through company website contact pages. Then she befriends a female employee of the company through an online chat website. After meeting with the female employee numerous times, Shayla is able to gain her trust and they become friends. One day, Shayla steals the employee's access badge and uses it to gain unauthorized access to the Treks Avionics offices.

What type of insider threat would Shayla be considered?

A. She would be considered an Insider Affiliate