QUESTION 182

Yancey is a network security administrator for a large electric company. This company provides power for over 100, 000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him. What would Yancey be considered?

A. Yancey would be considered a Suicide Hacker.
B. Since he does not care about going to jail, he would be considered a Black Hat.
C. Because Yancey works for the company currently; he would be a White Hat.
D. Yancey is a Hacktivist Hacker since he is standing up to a company that is downsizing.

Correct Answer: A

QUESTION 183

You receive an e-mail like the one shown below. When you click on the link contained in the mail, you are redirected to a website seeking you to download free Anti-Virus software.

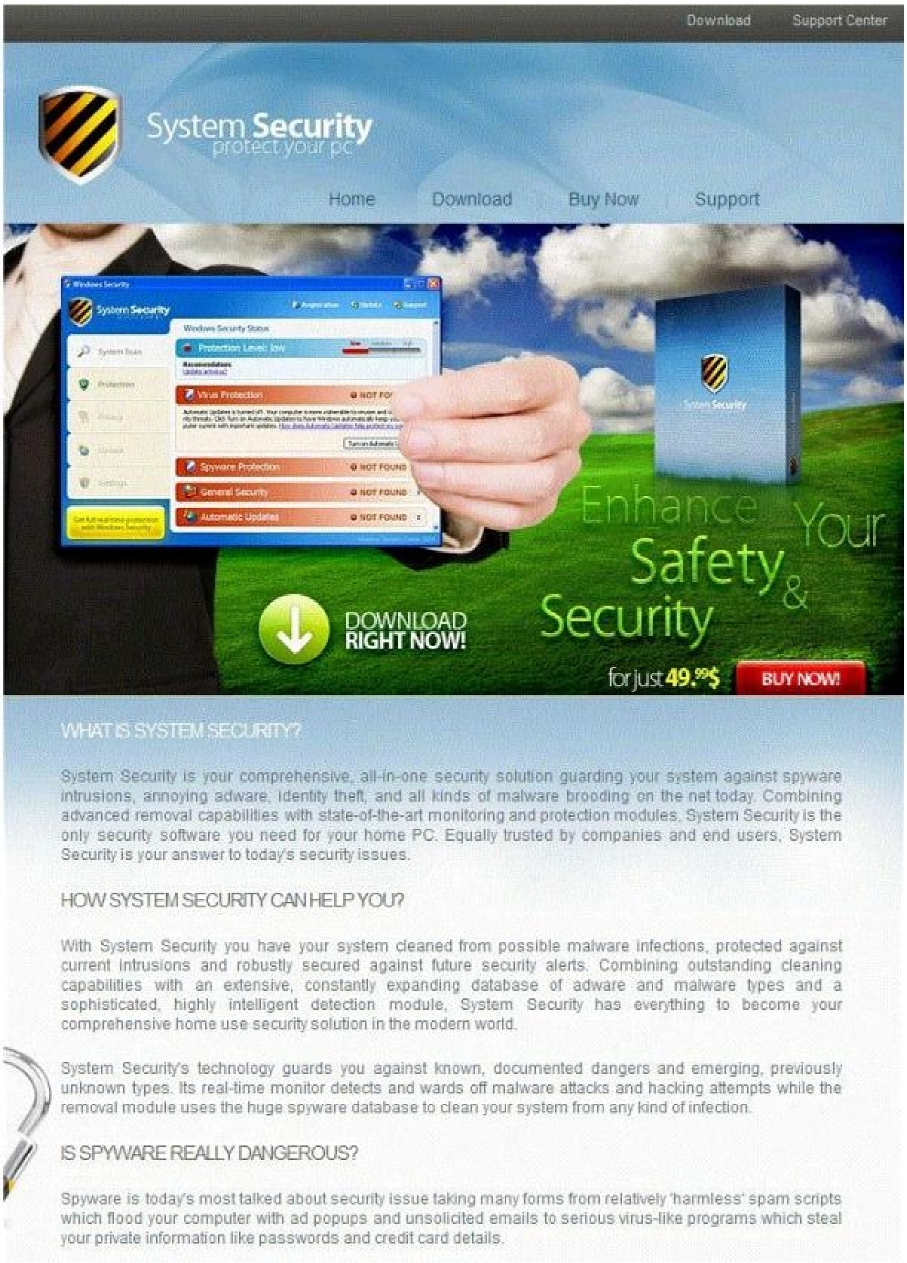
Dear valued customers,

We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:

Antivirus code: 5014
http://www.juggyboy/virus/virus.html
Thank you for choosing us, the worldwide leader Antivirus solutions.
Mike Robertson
PDF Reader Support
Copyright Antivirus 2010 © All rights reserved
If you want to stop receiving mail, please go to:
http://www.juggyboy.com

Or you may contact us at the following address:
Media Internet Consultants, Edif. Neptuno, Planta Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama

How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?



WHAT IS SYSTEM SECURITY?

System Security is your comprehensive, all-in-one security solution guarding your system against spyware intrusions, annoying adware, identity theft, and all kinds of malware brooding on the net today. Combining advanced removal capabilities with state-of-the-art monitoring and protection modules, System Security is the only security software you need for your home PC. Equally trusted by companies and end users, System Security is your answer to today's security issues.

HOW SYSTEM SECURITY CAN HELP YOU?

With System Security you have your system cleaned from possible malware infections, protected against current intrusions and robustly secured against future security alerts. Combining outstanding cleaning capabilities with an extensive, constantly expanding database of adware and malware types and a sophisticated, highly intelligent detection module, System Security has everything to become your comprehensive home use security solution in the modern world.

System Security's technology guards you against known, documented dangers and emerging, previously unknown types. Its real-time monitor detects and wards off malware attacks and hacking attempts while the removal module uses the huge spyware database to clean your system from any kind of infection.

IS SPYWARE REALLY DANGEROUS?

Spyware is today's most talked about security issue taking many forms from relatively 'harmless' spam scripts which flood your computer with ad popups and unsolicited emails to serious virus-like programs which steal your private information like passwords and credit card details.

A. Look at the website design, if it looks professional then it is a Real Anti-Virus website.

B. Connect to the site using SSL, if you are successful then the website is genuine.

C. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site.

D. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware.

E. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware.

Correct Answer: C

QUESTION 184

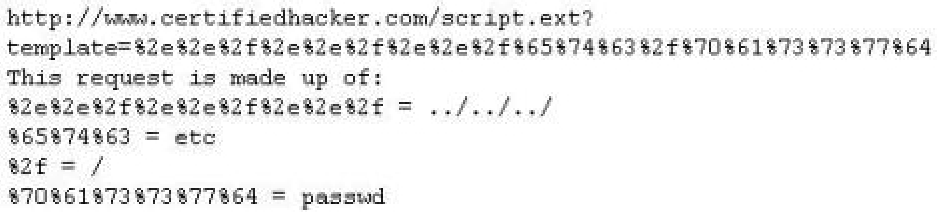
Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms. What is this document called?

A. Information Audit Policy (IAP)
B. Information Security Policy (ISP)
C. Penetration Testing Policy (PTP)
D. Company Compliance Policy (CCP)

Correct Answer: B

QUESTION 185

Take a look at the following attack on a Web Server using obstructed URL:



```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2e%2f%2e%2e%2f = ../../../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

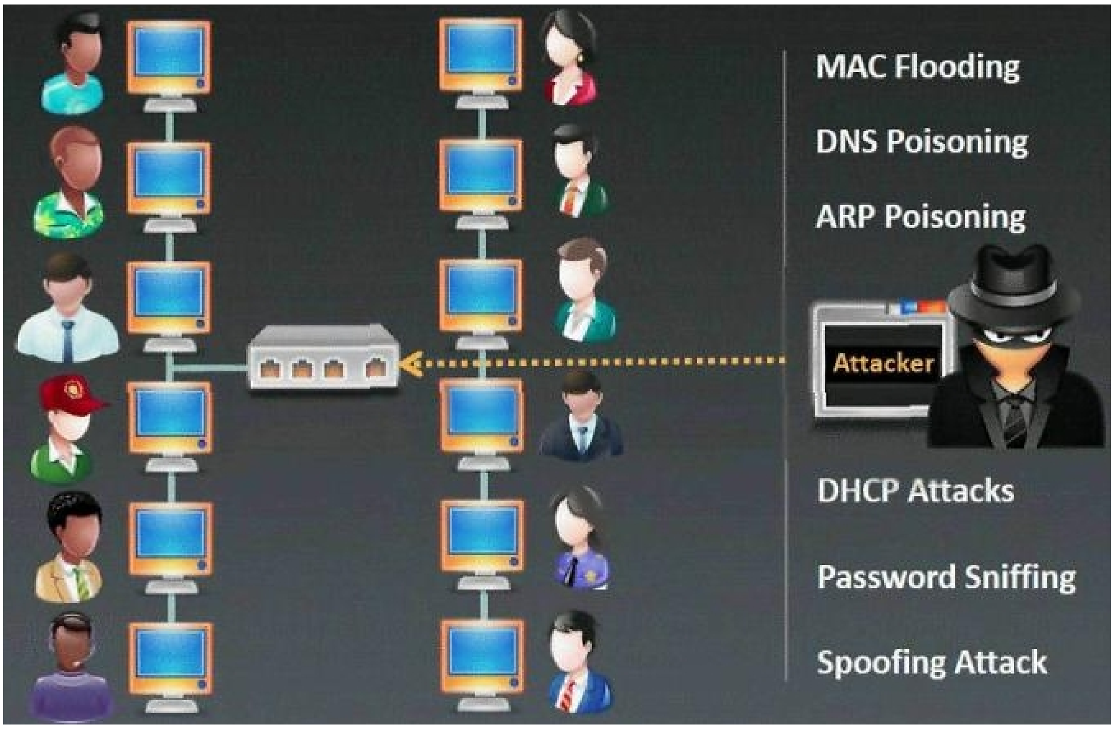
How would you protect from these attacks?

A. Configure the Web Server to deny requests involving "hex encoded" characters.
B. Create rules in IDS to alert on strange Unicode requests.
C. Use SSL authentication on Web Servers.
D. Enable Active Scripts Detection at the firewall and routers.

Correct Answer: B

QUESTION 186

Which type of sniffing technique is generally referred as MiTM attack?

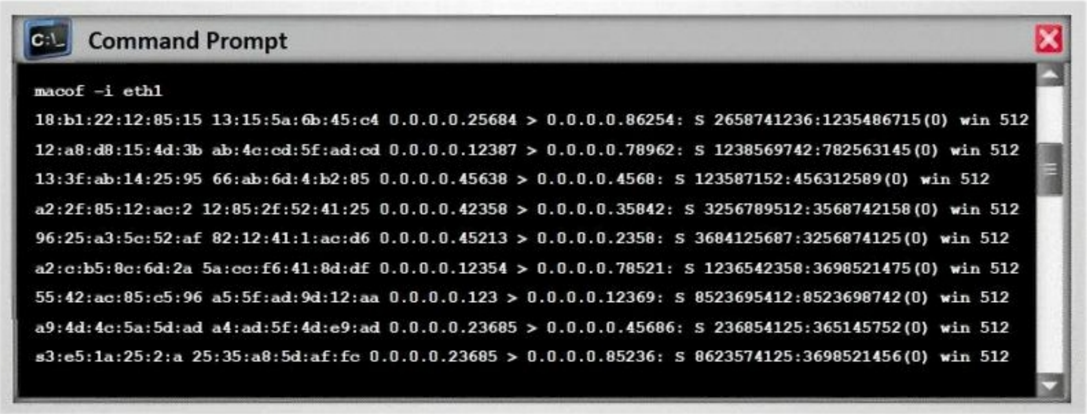


A. Password Sniffing
B. ARP Poisoning
C. Mac Flooding
D. DHCP Sniffing

Correct Answer: B

QUESTION 187

Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.



```
macof -i eth1
18:b1:22:12:85:15 13:15:5a:6b:45:c4 0.0.0.0.25684 > 0.0.0.0.86254: S 2658741236:1235486715(0) win 512
12:a8:d8:15:4d:3b ab:4c:cd:5f:ad:cd 0.0.0.0.12387 > 0.0.0.0.78962: S 1238569742:782563145(0) win 512
13:3f:ab:14:25:95 66:ab:6d:4:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: S 123587152:456312589(0) win 512
a2:2f:85:12:ac:2 12:85:2f:52:41:25 0.0.0.0.42358 > 0.0.0.0.35842: S 3256789512:3568742158(0) win 512
96:25:a3:5c:52:af 82:12:41:1:ac:d6 0.0.0.0.45213 > 0.0.0.0.2358: S 3684125687:3256874125(0) win 512
a2:c:b5:8c:6d:2a 5a:cc:f6:41:8d:df 0.0.0.0.12354 > 0.0.0.0.78521: S 1236542358:3698521475(0) win 512
55:42:ac:85:c5:96 a5:5f:ad:9d:12:aa 0.0.0.0.123 > 0.0.0.0.12369: S 8523695412:8523698742(0) win 512
a9:4d:4c:5a:5d:ad a4:ad:5f:4d:e9:ad 0.0.0.0.23685 > 0.0.0.0.45686: S 236854125:365145752(0) win 512
s3:e5:1a:25:2:a 25:35:a8:5d:af:fc 0.0.0.0.23685 > 0.0.0.0.85236: S 8623574125:3698521456(0) win 512
```

In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various MAC addresses to physical ports. What happens when the CAM table becomes full?

A. Switch then acts as hub by broadcasting packets to all machines on the network.
B. The CAM overflow table will cause the switch to crash causing Denial of Service.
C. The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF.
D. Every packet is dropped and the switch sends out SNMP alerts to the IDS port.

Correct Answer: A

QUESTION 188

You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place. Your peer, Peter Smith who works at the same department disagrees with you. He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain. What is Peter Smith talking about?

A. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain.
B. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks.
C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks.
D. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway.

Correct Answer: A

QUESTION 189

How does a denial-of-service attack work?

A. A hacker prevents a legitimate user (or group of users) from accessing a service.
B. A hacker uses every character, word, or letter he or she can think of to defeat authentication.
C. A hacker tries to decipher a password by using a system, which subsequently crashes the network.
D. A hacker attempts to imitate a legitimate user by confusing a computer or even another person.