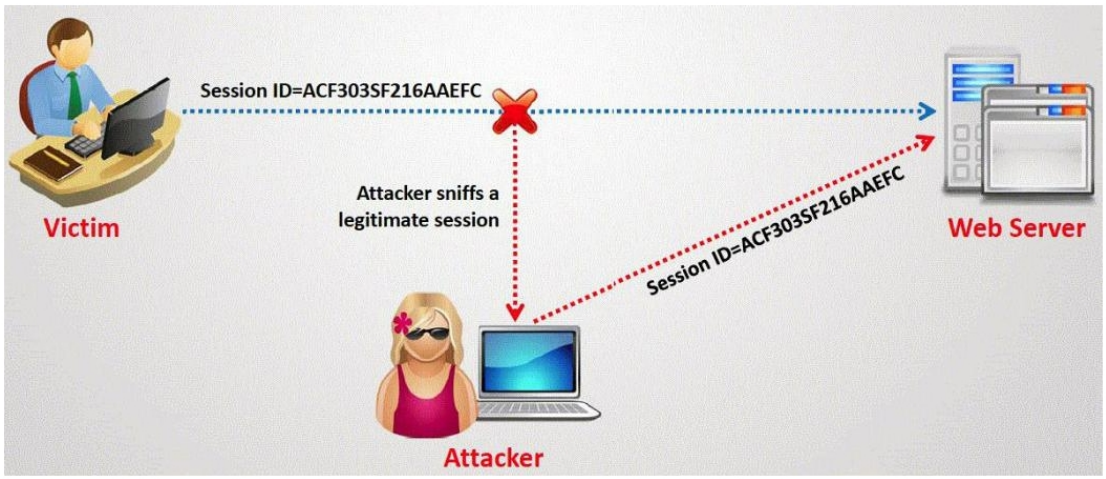
QUESTION 155

What type of session hijacking attack is shown in the exhibit?



A. Session Sniffing Attack
B. Cross-site scripting Attack
C. SQL Injection Attack
D. Token sniffing Attack

Correct Answer: A

QUESTION 156

What is the default Password Hash Algorithm used by NTLMv2?

A. MD4
B. DES
C. SHA-1
D. MD5

Correct Answer: D

QUESTION 157

Gerald, the Systems Administrator for Hyped Enterprises, has just discovered that his network has been breached by an outside attacker. After performing routine maintenance on his servers, he discovers numerous remote tools were installed that no one claims to have knowledge of in his department. Gerald logs onto the management console for his IDS and discovers an unknown IP address that scanned his network constantly for a week and was able to access his network through a high-level port that was not closed. Gerald traces the IP address he found in the IDS log to a proxy server in Brazil. Gerald calls the company that owns the proxy server and after searching through their logs, they trace the source to another proxy server in Switzerland. Gerald

calls the company in Switzerland that owns the proxy server and after scanning through the logs again, they trace the source back to a proxy server in China. What proxy tool has Gerald's attacker used to cover their tracks?

A. ISA proxy
B. IAS proxy
C. TOR proxy
D. Cheops proxy

Correct Answer: C

QUESTION 158

Frederickson Security Consultants is currently conducting a security audit on the networks of Hawthorn Enterprises, a contractor for the Department of Defense. Since Hawthorn Enterprises conducts business daily with the federal government, they must abide by very stringent security policies. Frederickson is testing all of Hawthorn's physical and logical security measures including biometrics, passwords, and permissions. The federal government requires that all users must utilize random, non-dictionary passwords that must take at least 30 days to crack. Frederickson has confirmed that all Hawthorn employees use a random password generator for their network passwords. The Frederickson consultants have saved off numerous SAM files from Hawthorn's servers using Pwdump6 and are going to try and crack the network passwords. What method of attack is best suited to crack these passwords in the shortest amount of time?

A. Brute force attack
B. Birthday attack
C. Dictionary attack
D. Brute service attack

Correct Answer: A

QUESTION 159

You want to know whether a packet filter is in front of 192.168.1.10. Pings to 192.168.1.10 don't get answered. A basic nmap scan of 192.168.1.10 seems to hang without returning any information. What should you do next?

A. Run NULL TCP hping2 against 192.168.1.10.
B. Run nmap XMAS scan against 192.168.1.10.
C. The firewall is blocking all the scans to 192.168.1.10.
D. Use NetScan Tools Pro to conduct the scan.

Correct Answer: A

QUESTION 160

An Attacker creates a zuckerjournals.com website by copying and mirroring HACKERJOURNALS.COM site to spread the news that Hollywood actor Jason Jenkins died in a car accident. The attacker then submits his fake site for indexing in major search engines. When users search for "Jason Jenkins", attacker's fake site shows up and dupes victims by the fake news.

This is another great example that some people do not know what URL's are. Real website: Fake website: http://www.zuckerjournals.com

The website is clearly not WWW.HACKERJOURNALS.COM. It is obvious for many, but unfortunately some people still do not know what an URL is. It's the address that you enter into the address bar at the top your browser and this is clearly not legit site, its www.zuckerjournals.com How would you verify if a website is authentic or not?

A. Visit the site using secure HTTPS protocol and check the SSL certificate for authenticity.
B. Navigate to the site by visiting various blogs and forums for authentic links.
C. Enable Cache on your browser and lookout for error message warning on the screen.
D. Visit the site by clicking on a link from Google search engine.

Correct Answer: D

QUESTION 161
A digital signature is simply a message that is encrypted with the public key instead of the private key.

A. true
B. false

Correct Answer: B

QUESTION 162

Blane is a network security analyst for his company. From an outside IP, Blane performs an XMAS scan using Nmap. Almost every port scanned does not illicit a response. What can he infer from this kind of response?

A. These ports are open because they do not illicit a response.
B. He can tell that these ports are in stealth mode.
C. If a port does not respond to an XMAS scan using NMAP, that port is closed.
D. The scan was not performed correctly using NMAP since all ports, no matter what their state, will illicit some sort of response from an XMAS scan.

Correct Answer: A

QUESTION 163

In TCP communications there are 8 flags; FIN, SYN, RST, PSH, ACK, URG, ECE, CWR. These flags have decimal numbers assigned to them:

- FIN = 1
- SYN = 2
- RST = 4
- PSH = 8
- ACK = 16
- URG = 32
- ECE = 64
- CWR =128

Example: To calculate SYN/ACK flag decimal value, add 2 (which is the decimal value of the SYN flag) to 16 (which is the decimal value of the ACK flag), so the result would be 18. Based on the above calculation, what is the decimal value for XMAS scan?

A. 23
B. 24
C. 41
D. 64

Correct Answer: C

QUESTION 164

A simple compiler technique used by programmers is to add a terminator 'canary word' containing four letters NULL (0x00), CR (0x0d), LF (0x0a) and EOF (0xff) so that most string operations are terminated. If the canary word has been altered when the function returns, and the program responds by emitting an intruder alert into syslog, and then halts what does it