Exam : **EC1-350**

Title : Ethical Hacking and
Countermeasures V7

Version : Demo

1.Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?
A. Configure Port Security on the switch
B. Configure Port Recon on the switch C.
Configure Switch Mapping
D. Configure Multiple Recognition on the switch
Answer: A

2.Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database. What technique does Jimmy use to compromise a database.?
A. Jimmy can submit user input that executes an operating system command to compromise a target system
B. Jimmy can gain control of system to flood the target system with requests, preventing legitimate users from gaining access
C. Jimmy can utilize an incorrect configuration that leads to access with higher-than expected privilege of the database
D. Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system
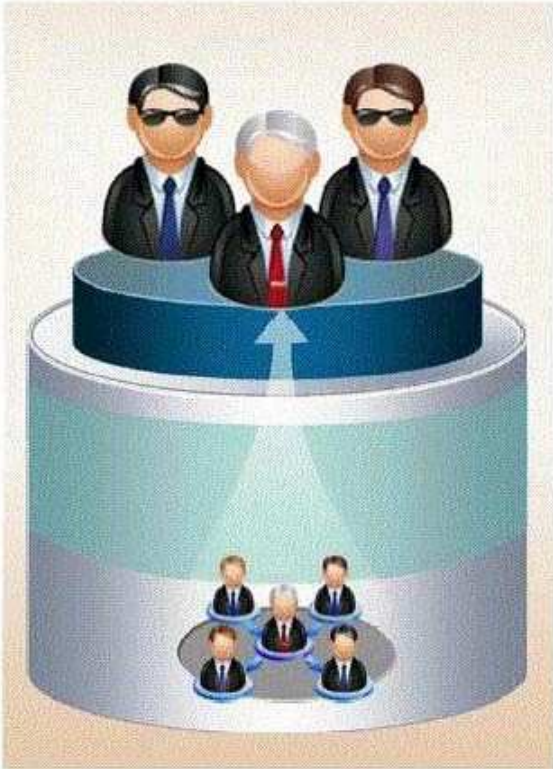**Answer:** D

3.This IDS defeating technique works by splitting a datagram (or packet) into multiple fragments and the IDS will not spot the true nature of the fully assembled datagram. The datagram is not reassembled until it reaches its final destination. It would be a processor-intensive task for IDS to reassemble all fragments itself, and on a busy system the packet will slip through the IDS onto the network. What is this technique called?
A. IP Routing or Packet Dropping
B. IDS Spoofing or Session Assembly
C. IP Fragmentation or Session Splicing
D. IP Splicing or Packet Reassembly
Answer: C

4.If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.
How would you prevent such type of attacks?

A. It is impossible to block these attacks

B. Hire the people through third-party job agencies who will vet them for you

C. Conduct thorough background checks before you engage them

D. Investigate their social networking profiles

Answer: C

5.This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.

A. UDP Scanning

B. IP Fragment Scanning

C. Inverse TCP flag scanning

D. ACK flag scanning

Answer: B

6.Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate. How would you call this type of activity?

A. Dumpster Diving

B. Scanning

C. CI Gathering

D. Garbage Scooping

Answer: A

7.Anonymizer sites access the Internet on your behalf, protecting your personal information from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you,

enabling you to remain at least one step removed from the sites you visit.

You can visit Web sites without allowing anyone to gather information on sites visited by you. Services that provide anonymity disable pop-up windows and cookies, and conceal visitor's IP address.

These services typically use a proxy server to process each HTTP request. When the user requests a Web page by clicking a hyperlink or typing a URL into their browser, the service retrieves and displays the information using its own server. The remote server (where the requested Web page resides) receives information on the anonymous Web surfing service in place of your information.

In which situations would you want to use anonymizer? (Select 3 answers)

A. Increase your Web browsing bandwidth speed by using Anonymizer

B. To protect your privacy and Identity on the Internet

C. To bypass blocking applications that would prevent access to Web sites or parts of sites that you want to visit.

D. Post negative entries in blogs without revealing your IP identity

Answer: B,C,D

8.What type of attack is shown in the following diagram?
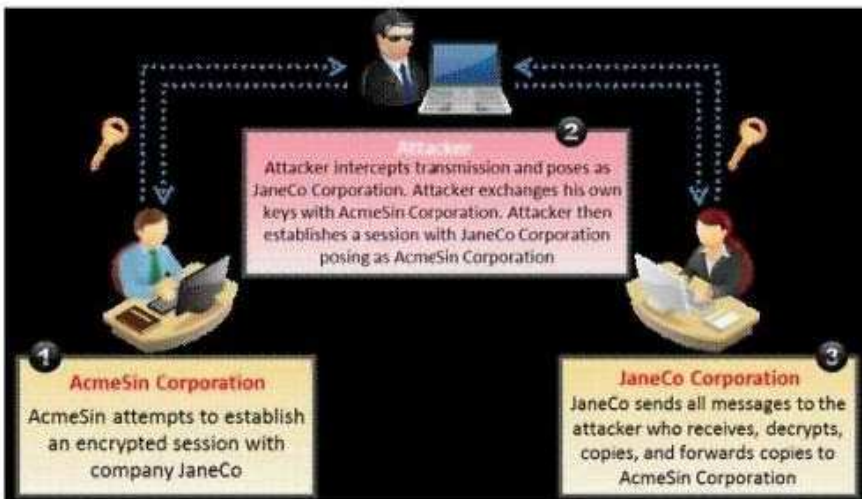
A. Man-in-the-Middle (MiTM) Attack

B. Session Hijacking Attack

C. SSL Spoofing Attack

D. Identity Stealing Attack

Answer: A

9.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

10.How do you defend against ARP Spoofing?

A. Use ARPWALL system and block ARP spoofing attacks

B. Tune IDS Sensors to look for large amount of ARP traffic on local subnets

C. Use private VLANS

D. Place static ARP entries on servers, workstation and routers

Answer: B,C,D

11.TCP SYN Flood attack uses the three-way handshake mechanism.

1. An attacker at system A sends a SYN packet to victim at system B.

2. System B sends a SYN/ACK packet to victim A.

3. As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.

This status of client B is called _____

A. "half-closed"

B. "half open"

C. "full-open"

D. "xmas-open"

Answer: B

12.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

13.You run nmap port Scan on 10.0.0.5 and attempt to gain banner/server information from services running on ports 21, 110 and 123.
Here is the output of your scan results:

```
PORT        STATE      SERVICE      VERSION
21/tcp      open       ftp          vsftpd 2.0.7
110/tcp     open       pop3         Courier pop3d
123/tcp     closed     ntp

Device type: general purpose
Running: Linux 2.8.X

OS details: Linux 2.8.18, Linux 2.8.20 - 2.8.24
Uptime: 65.658 days (since Mon Jun 19 00:43:29 2011)
Network Distance: 0 hops
Service Info: OS: Unix
```

Which of the following nmap command did you run?
A. nmap -A -sV -p21,110,123 10.0.0.5
B. nmap -F -sV -p21,110,123 10.0.0.5
C. nmap -O -sV -p21,110,123 10.0.0.5
D. nmap -T -sV -p21,110,123 10.0.0.5
Answer: C

14.How do you defend against Privilege Escalation?
A. Use encryption to protect sensitive data
B. Restrict the interactive logon privileges
C. Run services as unprivileged accounts
D. Allow security settings of IE to zero or Low
E. Run users and applications on the least privileges
Answer: A,B,C,E

15.What does ICMP (type 11, code 0) denote?
A. Source Quench
B. Destination Unreachable
C. Time Exceeded
D. Unknown Type
Answer: C

16.You are the security administrator of Jaco Banking Systems located in Boston. You are setting up e-banking website (http://www.ejacobank.com) authentication system. Instead of issuing banking customer with a single password, you give them a printed list of 100 unique passwords. Each time the customer needs to log into the e-banking system website, the customer enters the next password on the list. If someone sees them type the password using shoulder surfing, MiTM or keyloggers, then no damage is done because the password will not be accepted a second time.
Once the list of 100 passwords is almost finished, the system automatically sends out a new password list

by encrypted e-mail to the customer.

You are confident that this security implementation will protect the customer from password abuse.

Two months later, a group of hackers called "HackJihad" found a way to access the one-time password list issued to customers of Jaco Banking Systems. The hackers set up a fake website (http://www.e-jacobank.com) and used phishing attacks to direct ignorant customers to it. The fake website asked users for their e-banking username and password, and the next unused entry from their one-time password sheet. The hackers collected 200 customer's username/passwords this way. They transferred money from the customer's bank account to various offshore accounts.

Your decision of password policy implementation has cost the bank with USD 925,000 to hackers.

You immediately shut down the e-banking website while figuring out the next best security solution What effective security solution will you recommend in this case?

A. Implement Biometrics based password authentication system. Record the customers face image to the authentication database

B. Configure your firewall to block logon attempts of more than three wrong tries

C. Enable a complex password policy of 20 characters and ask the user to change the password immediately after they logon and do not store password histories

D. Implement RSA SecureID based authentication system

Answer: D

17.More sophisticated IDSs look for common shellcode signatures. But even these systems can be bypassed, by using polymorphic shellcode. This is a technique common among virus writers ?it basically hides the true nature of the shellcode in different disguises.

How does a polymorphic shellcode work?

A. They encrypt the shellcode by XORing values over the shellcode, using loader code to decrypt the shellcode, and then executing the decrypted shellcode

B. They convert the shellcode into Unicode, using loader to convert back to machine code then executing them

C. They reverse the working instructions into opposite order by masking the IDS signatures

D. They compress shellcode into normal instructions, uncompress the shellcode using loader code and then executing the shellcode

Answer: A

18.SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains: A. The source and destination address having the same value

B. A large number of SYN packets appearing on a network without the corresponding reply packets

C. The source and destination port numbers having the same value

D. A large number of SYN packets appearing on a network with the corresponding reply packets

Answer: B

19.Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?

A. Port Scanning

B. Single Scanning

C. External Scanning
D. Vulnerability Scanning
Answer: D

20.The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user:

```
var Shipcity;
ShipCity = Request.form ("ShipCity");
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:
SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'
How will you delete the OrdersTable from the database using SQL Injection?
A. Chicago'; drop table OrdersTable -B.
Delete table'blah'; OrdersTable -C.
EXEC; SELECT * OrdersTable > DROP -D.
cmdshell'; 'del c:\sql\mydb\OrdersTable' //
Answer: A

21.What are the limitations of Vulnerability scanners? (Select 2 answers)
A. There are often better at detecting well-known vulnerabilities than more esoteric ones
B. The scanning speed of their scanners are extremely high
C. It is impossible for any, one scanning product to incorporate all known vulnerabilities in a timely manner
D. The more vulnerabilities detected, the more tests required
E. They are highly expensive and require per host scan license
Answer: A,C

22.Stephanie works as senior security analyst for a manufacturing company in Detroit. Stephanie manages network security throughout the organization. Her colleague Jason told her in confidence that he was able to see confidential corporate information posted on the external website http://www.jeansclothesman.com. He tries random URLs on the company's website and finds confidential information leaked over the web. Jason says this happened about a month ago. Stephanie visits the said URLs, but she finds nothing. She is very concerned about this, since someone should be held accountable if there was sensitive information posted on the website.
Where can Stephanie go to see past versions and pages of a website?
A. She should go to the web page Samspade.org to see web pages that might no longer be on the website
B. If Stephanie navigates to Search.com; she will see old versions of the company website
C. Stephanie can go to Archive.org to see past versions of the company website
D. AddressPast.com would have any web pages that are no longer hosted on the company's website
Answer: C

23.Dan is conducting penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting vulnerability. Dan wants to replay this token. However,

the session ID manager (on the server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?

A. Dan cannot spoof his IP address over TCP network

B. The scenario is incorrect as Dan can spoof his IP and get responses

C. The server will send replies back to the spoofed IP address

D. Dan can establish an interactive session only if he uses a NAT

Answer: C

24.Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company's largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason's client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor.

Without any proof, Jason's company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason's company can finish the project. Once again, Jason says that he had nothing to do with it and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on.

Jason's supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing else. Jason's supervisor opens the picture files, but cannot find anything out of the ordinary with them.

What technique has Jason most likely used?

A. Stealth Rootkit Technique

B. ADS Streams Technique

C. Snow Hiding Technique

D. Image Steganography Technique

Answer: D

25.What type of Virus is shown here?

A. Cavity Virus

B. Macro Virus

C. Boot Sector Virus

D. Metamorphic Virus

E. Sparse Infector Virus

Answer: E

26.An attacker finds a web page for a target organization that supplies contact information for the company. Using available details to make the message seem authentic, the attacker drafts e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator.

The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming.
Google's Gmail was hacked using this technique and attackers stole source code and sensitive data from Google servers. This is highly sophisticated attack using zero-day exploit vectors, social engineering and malware websites that focused on targeted individuals working for the company.
What is this deadly attack called?
A. Spear phishing attack
B. Trojan server attack
C. Javelin attack
D. Social networking attack
Answer: A

27.Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfigurations of hosts. They also provide information regarding mitigating discovered vulnerabilities.
Which of the following statements is incorrect?
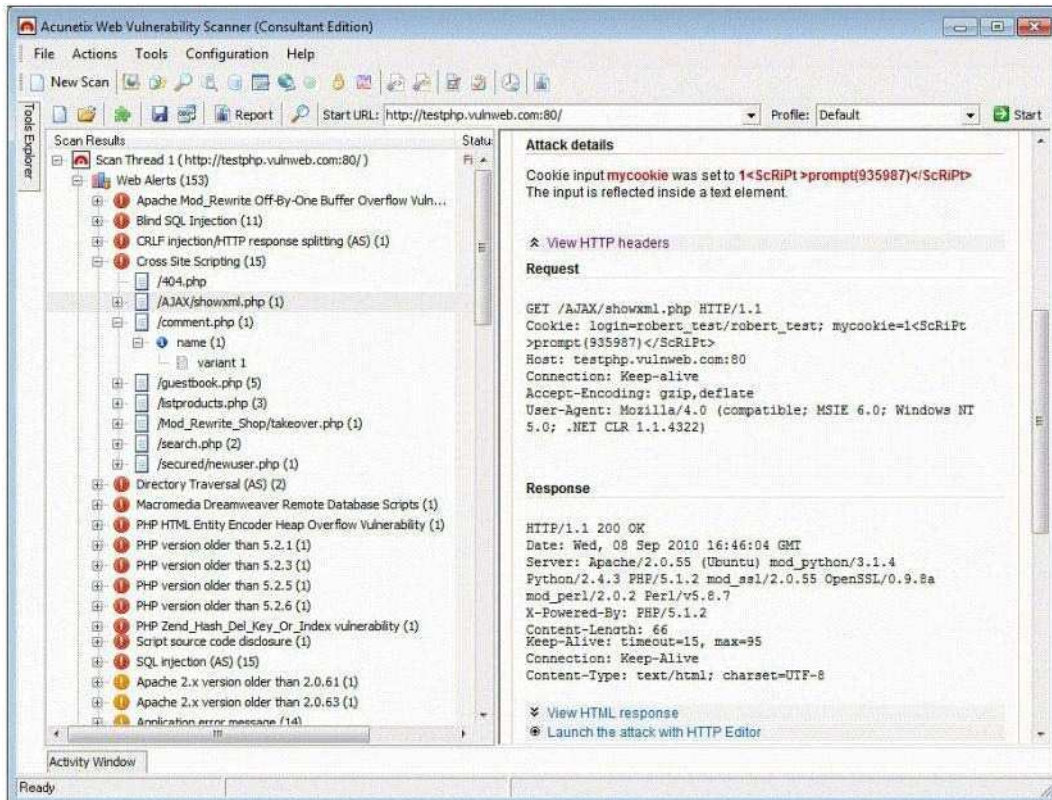
A. Vulnerability scanners attempt to identify vulnerabilities in the hosts scanned.

B. Vulnerability scanners can help identify out-of-date software versions, missing patches, or system upgrades

C. They can validate compliance with or deviations from the organization's security policy

D. Vulnerability scanners can identify weakness and automatically fix and patch the vulnerabilities without user intervention
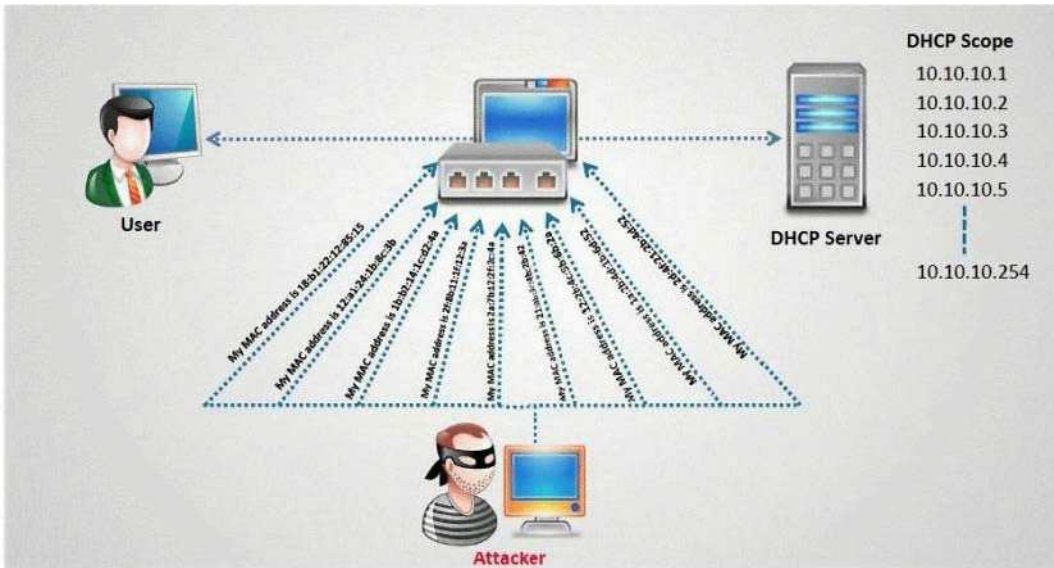
Answer: D

28.How does traceroute map the route a packet travels from point A to point B?

A. Uses a TCP timestamp packet that will elicit a time exceeded in transit message

B. Manipulates the value of the time to live (TTL) within packet to elicit a time exceeded in transit message

C. Uses a protocol that will be rejected by gateways on its way to the destination

D. Manipulates the flags within packets to force gateways into generating error messages

Answer: B

29.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

30.What type of session hijacking attack is shown in the exhibit?
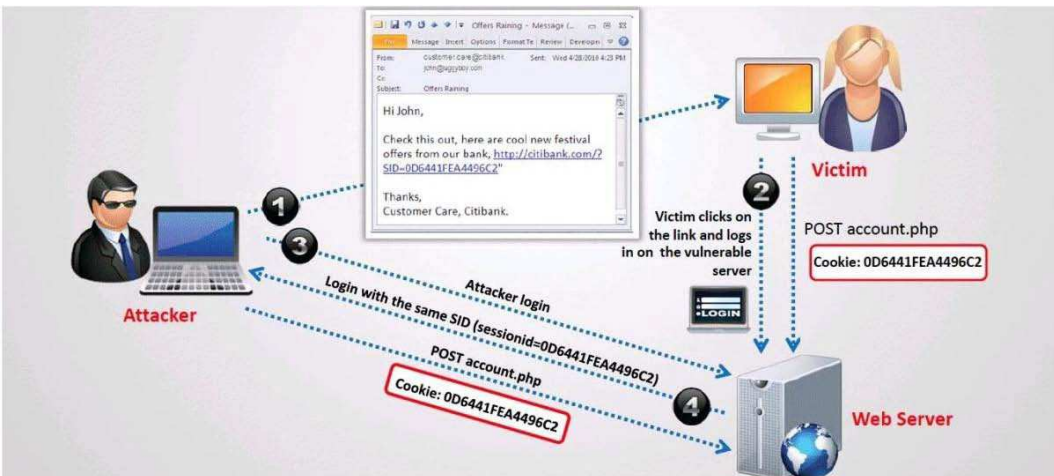
A. Cross-site scripting Attack

B. SQL Injection Attack

C. Token sniffing Attack

D. Session Fixation Attack

Answer: D

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

One Year Free Update

Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee

To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.