642-542

Cisco

Cisco SAFE Implementation

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your 642-542 exam in first attempt and also get high scores to acquire Cisco certification.

If you use OfficialCerts 642-542 Certification questions and answers, you will experience actual 642-542 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Cisco exam prep covers over 95% of the questions and answers that may be appeared in your 642-542 exam. Every point from pass4sure 642-542 PDF, 642-542 review will help you take Cisco 642-542 exam much easier and become Cisco certified.

Here's what you can expect from the OfficialCerts Cisco 642-542 course:

** Up-to-Date Cisco 642-542 questions as experienced in the real exam.*
** 100% correct Cisco 642-542 answers you simply can't find in other 642-542 courses.*
** All of our tests are easy to download. Your file will be saved as a 642-542 PDF.*
** Cisco 642-542 brain dump free content featuring the real 642-542 test questions.*

Cisco 642-542 certification exam is of core importance both in your Professional life and Cisco certification path. With Cisco certification you can get a good job easily in the market and get on your path for success. Professionals who passed Cisco 642-542 exam training are an absolute favorite in the industry. You will pass Cisco 642-542 certification test and career opportunities will be open for you.

http://tripleamarine.com/?cert=exams.asp?examcode=642-542

Question: 1
Threats that come from hackers who are more highly motivated and technically competent are called:

A. Sophisticated
B. Advanced
C. External
D. Structured

Answer: D

Explanation:
Structured threats come from adversaries that are highly motivated and technically competent.

Reference:
Cisco Secure Intrusion Detection System (Ciscopress) Page 9

Question: 2
The worst attacks are the ones that:

A. Are intermittent.
B. Target the applications
C. You can not stop them.
D. Target the executables.
E. Target the databases.f
F. You can not determine the source.

Answer: C

Explanation:
The worst attack is the one that You cannot stop. When performed properly, DDoS is just such an attack.

Question: 3
What type of network requires availability to the Internet and public networks as a major requirement and has several access points to other networks, both public and private?

A. Open
B. Closed
C. Intermediate
D. Balanced

Answer: A

Explanation:
The networks of today are designed with availability to the Internet and public networks, which is a major requirement. Most of today's networks have serverla access points to other networks both public and private; therefore, securing these networks has become fundamentally important.

Reference:
CSI Student guide v2.0 p.2-4

Question: 4
The security team at inc. is working on network security design. What is an example of a trust model?

A. One example is NTFS
B. One example is NTP
C. One example is NFS
D. One example is NOS

Answer: C

Explanation:
One of the key factors to building a successful network security design is to identify and enforce a proper trust model. The proper trust model defines who needs to talk to whom and what kind of traffic needs to be exchanged; all other traffic should be denied. Once the proper trust model has been identified, then the security designer should decide how to enforce the model. As more critical resources are globally available and new forms of network attacks evolve, the network security infrastructure tends to become more sophisticated, and more products are available. Firewalls, routers, LAN switches, intrusion detection systems, AAA servers, and VPNs are some of the technologies and products that can help enforce the model. Of course, each one of these products and technologies plays a particular role within the overall security implementation, and it is essential for the designer to understand how these elements can be deployed. Network File Sharing seems to be the best answer out of all the answers listed. Reference: Securing Networks with Private VLANs and VLAN Access Control Lists

Question: 5
Which type of attack can be mitigated only through encryption?

A. DoS
B. Brute force
C. Man-in-the-middle
D. Trojan horse

Answer: C

Explanation:
1. Man-in-the-middle attacks-Mitigated through encrypted remote traffic

Reference:
Safe White papers; Page 26
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

Question: 6
The security team at inc. is working on understanding attacks that happen in the network. what type of attack is characterized by exploitation of well-known weaknesses, use of ports that are allowed through a firewall, and can never be completely eliminated?

A. Network reconnaissance
B. Man-in-the-middle
C. Trust exploitation
D. Application layer

Answer: D

Explanation:
The primary problem with application layer attacks is that they often use ports that are allowed through a firewall.

Reference:

Safe White papers 68
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

Question: 7
You are the security administrator at and You need to know the attacks types to the network. which two general ip spoofing techniques does a hacker use? (choose two)

A. An IP address within the range of trusted IP addresses.
B. An unknown IP address which cannot be traced.
C. An authorized external IP address that is trusted.
D. An RFC 1918 address.

Answer: A C

Explanation:
IP Spoofing
An IP spoofing attack occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer. A hacker can do this in one of two ways. The hacker uses either an IP address that is within the range of trusted IP addresses for a network or an authorized external IP address that is trusted and to which access is provided to specified resources on a network. IP spoofing attacks are often a launch point for other attacks. The classic example is to launch a denial-of-service (DoS) attack using spoofed source addresses to hide the hacker's identity. Normally, an IP spoofing attack is limited to the injection of malicious data or commands into an existing stream of data that is passed between a client and server application or a peer-to-peer network connection. To enable bidirectional communication, the hacker must change all routing tables to point to the spoofed IP address. Another approach hackers sometimes take is to simply not worry about receiving any response from the applications. If a hacker tries to obtain a sensitive file from a system, application responses are unimportant.
However, if a hacker manages to change the routing tables to point to the spoofed IP address, the hacker can receive all the network packets that are addressed to the spoofed address and reply just as any trusted user can.

Reference:
Safe White papers; Page 65
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

Question: 8
john the security administrator at inc. is working on securing the network with strong passwords. what is the definition of a strong password?

A. The definition of a strong password is at least ten characters long and should contain cryptographic characters.
B. The definition of a strong password is at least eight characters long; contains uppercase letters, lowercase letters, numbers, and should not contain special characters.
C. The definition of a strong password is defined by each company depending on the product being used.
D. The definition of a strong password is at least eight characters long; contains uppercase letters, lowercase letters, numbers, and special characters.

Answer: D

Explanation:
Passwords should be at least eight characters long and contain uppercase letters, lowercase letters, numbers, and special characters (#, %, $, and so forth).

Reference:
Safe White papers; Page 67
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

Question: 9
The two Denial of Service attack methods are: (Choose two)

A. Out of Band data crash
B. SATAN
C. TCP session hijack
D. Resource Overload

Answer: A, D

Explanation:
When involving specific network server applications; such as a Web server or an FTP server, these attacks can focus on acquiring and keeping open all the available connections supported by that server, effectively locking out valid users of the server or service. Some attacks compromise the performance of Your network by flooding the network with undesired-and often useless-network packets and by providing false information about the status of network resources.

Reference:
Safe White papers; Page 66 & 67 SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

Incorrect Answers:
B: SATAN is a testing and reporting tool that collects a variety of information about networked hosts.
C: TCP session hijack is when a hacker takes over a TCP session between two machines.

Question: 10
This program does something undocumented which the programmer intended, but that the user would not approve of if he or she knew about it.

A. What is a Virus.
B. What is a Macro Virus.
C. What is a Trojan Horse.
D. What is a Worm.

Answer: C

Explanation:
A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool. An example of a Trojan horse is a software application that runs a simple game on the user's workstation. While the user is occupied with the game, the Trojan horse mails a copy of itself to every user in the user's address book. Then other users get the game and play it, thus spreading the Trojan horse.

Reference:
Safe White papers; Page 70
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

Question: 11
Choose the true statements regarding IP spoofing attack and DoS attack. (Choose all that apply)

A. IP spoofing attack is a prelude for a DoS attack.
B. DoS attack is a prelude for a IP spoofing attack.
C. IP spoofing attack is generally performed by inserting a string of malicious commands into the data that is passed between a client and a server.
D. A DoS attack is generally performed by inserting a string of malicious command into the data that is passed between a client and a server.

Answer: A, C

Explanation:
IP spoofing attacks are often a launch point for other attacks. The classic example is to launch a denial-of-service (DoS) attack using spoofed source addresses to hide the hacker's identity. Normally, an IP spoofing attack is limited to the injection of malicious data or commands into an existing stream of data that is passed between a client and server application or a peer-to-peer network connection.

Reference:
Safe White papers; Page 65
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

Question: 12
What method helps mitigate the threat of IP spoofing?

A. Access control
B. Logging
C. SNMP polling
D. Layer 2 switching

Answer: A

Explanation:
The most common method for preventing IP spoofing is to properly configure access control. To reduce the effectiveness of IP spoofing, configure access control to deny any traffic from the external network that has a source address that should reside on the internal network.

Reference:
Safe White papers; Page 67
SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks

Question: 13
What is an example of a trust model?

A. NTFS
B. NFS
C. NTP
D. NOS

Answer: B

Explanation:
One of the key factors to building a successful network security design is to identify and enforce a proper trust model. The proper trust model defines who needs to talk to whom and what kind of traffic needs to be exchanged; all other traffic should be denied. Once the proper trust model has been identified, then the security designer should decide how to enforce the model. As more critical resources are globally available and new forms of network attacks evolve, the network

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams we offer;
http://www.officialcerts.com/allexams.asp

To contact our Support;
http://www.officialcerts.com/support.asp

View FAQs
http://www.officialcerts.com/faq.asp

Download All Exams Samples
http://www.officialcerts.com/samples.asp

To purchase Full Version and updated exam;
http://www.officialcerts.com/allexams.asp

Shop now using PayPal

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google