

L337 H4XX0R QUIZ!!!

Are you über l33t? Answer all the following questions, and check your answers at the end.

0x000 - You just noticed a hacker sending an email to an address you know does not exist. Why is he doing this?

- {0} To determine who is the holder of the root account.
- {1} To determine if the email server is vulnerable to any form of relay attack.
- {2} To test the network's IDS systems.
- {3} To get a response from the mailer daemon which will reveal server information.

0x001 - What is the range for dynamic random ports?

- {0} 102449151
- {1} 2048
- {2} 4915265535
- {3} 1024

0x002 - What does the following command achieve?

```
telnet <IP address> 80  
HEAD /HTTP/1.0  
<Return>  
<Return>
```

- {0} Returns the homepage for the specified address.
- {1} Opens a back door Telnet session to the specified address.
- {2} Returns the banner of the specified address.
- {3} Allows the hacker to determine if the server has an open SQL database.

0x003 - You would like to perform a port scan that will allow you to determine if a stateless firewall is being used. Which of the following would be your best option?

- {0} XMAS scan
- {1} Idle scan
- {2} Stealth scan
- {3} ACK scan

0x004 - You have become concerned that someone could attempt to poison your DNS cache. What setting determines how long cache poisoning would last?

- {0} A
- {1} CNAME
- {2} SOA
- {3} MX

0x005 - Which of the following Trojans uses port 6666?

- {0} Subseven
- {1} NetBus
- {2} Back Orifice
- {3} Beast

0x006 - Which of the following best describes a wrapper?

- {0} Wrappers are used as tunneling programs.
- {1} Wrappers are used to cause a Trojan to self execute when previewed within email.
- {2} Wrappers are used as backdoors to allow unauthenticated access.
- {3} Wrappers are used to package covert programs with overt programs.

0x007 - The Loki trojan uses which of the following by default?

- {0} ICMP
- {1} UDP 69
- {2} TCP 80
- {3} IGRP

0x008 - You become concerned one of your workstations has become infected with a malicious program. Which of the following netstat switches would be the best to use?

- {0} -an
- {1} -r
- {2} -p
- {3} -s

0x009 - You have just completed a scan of your servers, and you found port 12345 open. Which of the following programs uses that port by default?

- {0} Donald Dick
- {1} Back Orifice
- {2} Subseven
- {3} NetBus

5K1ZL5 4ND L1FE 5&C710N

Check off all that applies:

- [] Qx00A - Ever changed the value of 4?
- [] Qx00B - ... unintentionally?
- [] Qx00C - ... in FORTRAN?
- [] Qx00D - Have you complained when a "feature" you "use" got fixed?
- [] Qx00E - Have you named a computer?
- [] Qx00F - Do you know how many days old you are?
- [] Qx010 - ... how many minutes?
- [] Qx011 - ... how many seconds?
- [] Qx012 - Do you know what ASCII stands for?
- [] Qx013 - ... EBCDIC?
- [] Qx014 - Can you read and write ASCII in Hex?
- [] Qx015 - ... Octal?
- [] Qx016 - ... Binary?
- [] Qx017 - Can you convert from EBCDIC to ASCII and vice versa?
- [] Qx018 - Do you know what characters are the same in both ASCII and EBCDIC?
- [] Qx019 - Do you know maxint on your system?
- [] Qx01A - Can you name powers of two up to 2^{16} ?
- [] Qx01B - ... 2^{32} ?
- [] Qx01C - ... 2^{64} ?
- [] Qx01D - Can you successfully mount /dev/sda4?
- [] Qx01E - ... /dev/sda8?
- [] Qx01F - Have you optimized an idle loop?
- [] Qx021 - Have you optimized a bubble sort?
- [] Qx022 - Have you ever talked to a modem?
- [] Qx023 - ... did it answer?
- [] Qx024 - Can you whistle 300 baud?
- [] Qx025 - Can you play music on a line printer?
- [] Qx026 - Have you written an unkillable daemon?
- [] Qx027 - ... did you kill it?
- [] Qx028 - Do you know the RS-232C pinout?
- [] Qx029 - Do you own a copy of the Hacker's Dictionary?
- [] Qx02A - ... did you contribute to it?
- [] Qx02B - Do you own a copy of the Anarchist's Cookbook?
- [] Qx02C - Do you use more than 1 terabyte of storage?
- [] Qx02D - ... 1 petabyte?
- [] Qx02E - Do you know what IBM part number 7320154 is?
- [] Qx02F - Can you program in BASIC?
- [] Qx030 - ... do you admit it?
- [] Qx031 - Can you program in LISP?
- [] Qx032 - ... do you deny it?
- [] Qx033 - Does your touch tone phone have 16 DTMF buttons on it?
- [] Qx034 - Have you ever built a black box?
- [] Qx035 - Do you know what follows "09 f9 11 02"?
- [] Qx036 - ... "45 5F E1 04"?
- [] Qx037 - ... Did you discover either of them?
- [] Qx038 - Have you memorized the UUCP map for your country?
- [] Qx039 - Can you name all the top-level nameservers and their addresses?
- [] Qx03A - Do you know RFC-822 by heart?
- [] Qx03B - ... Can you recite all the errors in it?
- [] Qx03C - Do you know the max packet lifetime?
- [] Qx03D - Have you ever paged or swapped off a tape drive?
- [] Qx03E - ... off a card reader/punch?
- [] Qx03F - ... off a teletype?
- [] Qx040 - ... off a networked disk?
- [] Qx041 - Do other people have difficulty using your customized environment?
- [] Qx042 - Do you dream in any programming languages?
- [] Qx043 - Do you use "foobar" in daily conversation?
- [] Qx044 - Can you read a machine dump?
- [] Qx045 - Did you ever write a program that ran correctly the first time?

41N5W&R5

0x000 - {3} Sending a bogus email is one way to find out more about internal servers, gather additional IP addresses, and learn how they treat mail.

0x001 - {2} Dynamic random ports range from 4915265535. Most established well-known applications range from 01023. Answers {0}, {1}, and {3} are incorrect because well-known ports range from 01023, registered ports range from 102449151, and dynamic ports range from 4915265535.

0x002 - {2} This command is used for banner grabbing. Banner grabbing helps identify the service and version of the web server running.

0x003 - {3} An ACK scan would be the best choice to determine if stateless inspection is being used. If there is an ACL in place, the ACK would be allowed to pass. Answer {1} is incorrect because an XMAS scan is not used to bypass stateless inspection. It uses an abnormal flag setting. Answer {1} is incorrect, as an idle scan requires a third idle device and is used because it is considered stealthy. Answer {2} is incorrect, as a stealth scan simply performs the first two steps of the three-step handshake.

0x004 - {2} The TTL is the value that would determine how long cache poisoning would last. It is typically found in the SOA record. Answer {0} is incorrect, as the A record maps a hostname to its IP address. Answer {1} is incorrect because the CNAME is an alias. Answer {4} is incorrect because the MX record maps to mail exchange servers.

0x005 - {3} Beast uses port 6666 and is considered unique because it uses injection technology.

0x006 - {3} Wrappers are used to package covert programs with overt programs. They act as a type of file joiner program or installation packager program.

0x007 - {0} Loki is a Trojan that opens and can be used as a backdoor to a victim's computer by using ICMP.

0x008 - {0} Netstat -an would be the proper syntax. The -a displays all connections and listening ports. The -n displays addresses and port numbers in numerical form.

0x009 - {3} NetBus uses port 12345 by default.

R&5U<75

Multiply your score on the first section by 5, and add it to your score on the second section. This is your total score. If you scored 95 or more (counting from 1), you are über 133t. Congratulations. If you scored 75-94, you are a hacker. Hacker. Not H4xx0r. You probably won't get laughed at on hacker IRC channels. If you scored 50-74, you're a n00b hacker. Keep trying. If you scored 25-54, you're a script kiddie. We all hate you. Go away. If you scored below 25, you are Michelle Madigan (look it up, n00b!).