Homework Unit 09

Mission 1

Check (MX) records for “starwars.com” using the following command

* nslookup -type=MX starwars.com

Results of the nslookup command: “SW nslookup”

The mail servers configured for “starwars.com” are as follows:

* alt1.aspx.l.google.com
* alt2.aspmx.l.google.com
* aspmx.l.google.com
* aspmx2.googlemail.com
* aspmx3.googlemail.com

The resistance can not receive emails because neither the new primary mail server nor secondary are configured in the DNS record.

How to fix the issue

* starwars.com mail exchanger = 1 asltx.l.google.com.
* starwars.com mail exchanger = 5 asltx.2.google.com.

Mission 2

Determine the SPF record for “theforce.net”, and run the following command:

* nslookup -type=TXT theforce.net

Results of the nslookup command: “F nslookup”

The text record containing the SPF record is as follows:

* theforce.net text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"

The above SPF record indicates authorized emails coming from “theforce.net” should only come from the following IP addresses:

* 104.156.250.80
* 45.63.15.159
* 45.63.4.215

A corrected SPF record for theforce.net should read as follows when returned from the above nslookup command:

* theforce.net text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:45.23.176.21"

Mission 3

determine how a correct “CNAME” record should look using nslookup, run one of the following commands

* nslookup www.theforce.net
* nslookup -type=CNAME www.theforce.net

Results of the above nslookup command: CNAME nslookup

The relevant portion of the result of the command is:

* www.theforce.net canonical name = theforce.net.

Current DNS records for resistance.theforce.net, run the following command:

* nslookup resistance.theforce.net

Results of the above nslookup command: resistance nslookup

To ensure “resistance.theforce.net” redirects to “theforce.net,” a proper DNS CNAME record should return:

* resistance.theforce.net canonical name = theforce.net.

Mission 4

To confirm the DNS records for “princessleia.site,” run the following commands:

* nslookup princessleia.site = checks the IP address
* nslookup -type=NS princessleia.site = nameservers are being used

Results of the above nslookup commands: princess nslookup

“princessleia.site” is currently these nameservers to provide DNS information on the site:

* nameserver = ns25.domaincontrol.com.
* nameserver = ns26.domaincontrol.com.

The provided DNS server at “ns2.galaxybackup.com” is not in the above record.

You would want to have “nslookup -type=NS princessleia.site” command return:

* princessleia.site nameserver = ns2.galaxybackup.com.

Mission 5

The shortest path to go from Batuu to Jedha, while avoiding Planet N, is as follows:

* Batuu -> D -> C -> G -> O -> R -> Q -> T -> V -> Jedha

total of 23 hops, and does not include Planet N.

Mission 6

To determine the wireless key used to decrypt traffic for the “Darkside.pcap” file, run the following command:

* aircrack-ng Darkside.pcap -w /usr/share/wordlists/rockyou.txt

Results of the above command: darkside

Running aircrack-ng returned the password dictionary, which can be used to decrypt the wireless traffic.

Decrypted ARP traffic yields the following results:

* “ARP” requests originate from the IP address “172.16.0.101,” and come from a NIC with the mac address 00:13:ce:55:98:ef.
* An “ARP” reply indicating which computer is using the IP address “172.16.0.1” suggests that a machine is using an IP address with the mac address “00:0f:66:e3:e4:01.”

The following mac address / IP pairs can be found on the linksys network used by the Dark Side:

* 00:13:ce:55:98:ef => 172.16.0.101
* 00:0f:66:e3:e4:01 => 172.16.0.1

Mission 7

Run the following command to view the TXT DNS record for the record used in Mission 4 “princessleia.site”

* nslookup -type=TXT princessleia.site

Results of the above nslookup command: princess TXT nslookup

The hidden message in the TXT record indicates we should run the following command to receive our reward:

* telnet towel.blinkenlights.nl

Result of the command: star wars