Sidney Robinson

Homework Week 9 – Networking-Fundamentals-II

DNA Records;

A = What is a DNS A record? The ‘A’ stands for ‘address’ and this is the most fundamental type of DNS record: it indicates the IP address of a given domain. For example, if you pull the DNS records of cloudflare.com, the A record currently returns an IP address of: 104.17.210.9. A records only hold IPv4 addresses.

PTR = The Domain Name System, or DNS, correlates domain names with IP addresses. A DNS pointer record (PTR for short) provides the domain name associated with an IP address. A DNS PTR record is exactly the opposite of the 'A' record, which provides the IP address associated with a domain name. DNS PTR records are used in reverse DNS lookups.

MX = MX stands for “mail exchanger”. An MX record is a type of DNS record, so any understanding of MX records has to begin with an understanding of the fundamentals of the Domain Name System (DNS). The most important role of DNS for the majority of us is translating names into IP addresses so that network communications can occur.

NS = What is a DNS NS record? NS stands for 'nameserver,' and the nameserver record indicates which DNS server is authoritative for that domain (i.e. which server contains the actual DNS records). Basically, NS records tell the Internet where to go to find out a domain's IP address.

SOA = The DNS 'start of authority' (SOA) record stores important information about a domain or zone such as the email address of the administrator, when the domain was last updated, and how long the server should wait between refreshes. All DNS zones need an SOA record in order to conform to IETF standards.

SRV = The DNS "service" (SRV) record specifies a host and port for specific services such as voice over IP (VoIP), instant messaging, and so on. Most other DNS records only specify a server or an IP address, but SRV records include a port at that IP address as well.

TXT = A TXT record (short for text record) is a type of resource record in the Domain name system (DNS) used to provide the ability to associate arbitrary text with a host or other name, such as human readable information about a server, network, data center, or other accounting information.

MISSION 1:

-Determine and document the mail servers for starwars.com using NSLOOKUP;

sysadmin@UbuntuDesktop:~$ nslookup -type=mx starwars.com

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

starwars.com mail exchanger = 1 aspmx.l.google.com.

starwars.com mail exchanger = 10 aspmx3.googlemail.com.

starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.

starwars.com mail exchanger = 5 alt1.aspx.l.google.com.

starwars.com mail exchanger = 10 aspmx2.googlemail.com.

Authoritative answers can be found from:

-Explain why the Resistance isn't receiving any emails;

http://asltx.1.google.com/ and http://asltx.2.google.com/ domains mail exchange servers are not setup

-Document what a corrected DNS record should be;

starwars.com mail exchanger = 5 asltx.1.google.com.

starwars.com mail exchanger = 5 asltx.2.google.com.

MISSION 2:

-Determine and document the SPF for theforce.net using NSLOOKUP;

sysadmin@UbuntuDesktop:~$ nslookup -type=txt theforce.net

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

theforce.net text = "google-site-verification=XTU\_We07Cux-6WCSOItl0c\_WS29hzo92jPE341ckbOQ"

theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcffhFL\_Qaf8Lc9tMRkZZSuig0d6w"

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"

Authoritative answers can be found from:

-Explain why the Force's emails are going to spam.

theforce.net mail server to 45.23.176.21 is not in the SPF

-Document what a corrected DNS record should be.

Add theforce.net mx server 45.23.176.21 to the spf:

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 ip4:45.23.176.21"

MISSION 3:

-Document how a CNAME should look by viewing the CNAME of www.theforce.net using NSLOOKUP.

nslookup -type=all www.theforce.net

resistance.theforce.net canonical name = www.theforce.net.

-Explain why the sub page of resistance.theforce.net isn't redirecting to www.theforce.net.

Need to create a CNAME for it.

-Document what a corrected DNS record should be.

resistance.theforce.net canonical name = www.theforce.net.

MISSION 4:

-Confirm the DNS records for princessleia.site.

nslookup -type=ns princessleia.site

princessleia.site nameserver = ns25.domaincontrol.com.

princessleia.site nameserver = ns26.domaincontrol.com.

-Document how you would fix the DNS record to prevent this issue from happening again.

princessleia.site nameserver = ns2.galaxybackup.com

MISSION 5:

D,C,E,F,J,I,L,Q,T,V

MISSION 6:

-Figure out the Dark Side's secret wireless key by using Aircrack-ng.

dictionary

-Use the Dark Side's key to decrypt the wireless traffic in Wireshark.

dictionary:linksys

-Once you have decrypted the traffic, figure out the following Dark Side information:

Host IP Addresses and MAC Addresses by looking at the decrypted ARP traffic.

Document these IP and MAC Addresses, as the resistance will use these IP addresses to launch a retaliatory attack.

MAC Addresses, as the resistance will use these IP addresses to launch a retaliatory Attack

Frame 315: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)

IEEE 802.11 Data, Flags: .p....F.

Logical-Link Control

Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: Cisco-Li\_e3:e4:01 (00:0f:66:e3:e4:01)

Sender IP address: 172.16.0.1

Target MAC address: IntelCor\_55:98:ef (00:13:ce:55:98:ef)

Target IP address: 172.16.0.101

MISSION 7:

sysadmin@UbuntuDesktop:/usr/share/wordlists$ nslookup -type=txt princessleia.site

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

princessleia.site text = "Run the following in a command line: telnet towel.blinkenlights.nl or as a backup access in a browser: www.asciimation.co.nz"

Authoritative answers can be found from:

