Network Administration HW5

B04705003 資工三 林子雋

1 Reference

1.1 DHCP

1. How to force Windows 7 to ask for a “fresh” IP address from DHCP server?

2. How to Set Up DHCP Reservations (and Never Check an IP Address Again)

3. https://www.wikiwand.com/en/Dynamic_Host_Configuration_Protocol#/DHCP_discovery

4. http://www.zytrax.com/books/dns/ch15/#answer

1.2 DNS

1. Advantages of Distributed DNS Infrastructure Architecture

2. DNS Caching and How It Makes Your Internet Better

3. (a) http://techgenix.com/understanding-dns-protocol-part3/
   (b) DNS Message Header and Question Section Format
   (c) DNS-primer.pdf

4. What is the largest Safe UDP Packet Size on the Internet

5. (a) Top 10 DNS attacks likely to infiltrate your network
   (b) What is Distributed Reflection Denial of Service?
   (c) 小心網域名稱伺服器快取毒害 (DNS cache poisoning) 攻擊
   (d) https://www.wikiwand.com/en/DNS_spoofing
   (e) https://ithelp.ithome.com.tw/articles/10193791
   (f) https://www.plixer.com/blog/network-security-forensics/what-is-dns-tunneling/
   (g) https://tw.saowen.com/a/8409cb82c0446bcb99b0df8a180975fc9dc2374706c36d0f9af63a2e
   (h) https://www.infoworld.com/article/3027195/security/protect-yourself-against-dns
   html

2 Problem

2.1 DHCP

1. DHCP Reservation: If the system administrator set your MAC address to the reservation pool, you will definitely always get same ip address even you try to renew a ip address.

2. DHCP Client request last-known ip address: A dhcp client may reqeust its last-known ip address. If the dhcp server is an authoritative server, it may grant that request.

2.2 DNS

(a) Because if DNS servers are distributed, users can query to the nearest DNS server and get faster replies. From the viewpoint of maintainer of DNS servers, distributed system can balance load of huge DNS queries traffic and prevent point of failure. Here are three disadvantages if a single server handles all queries.

  (1) Tremendous traffic in single server

  (2) Point of failure: if this single DNS server is crashed, then if will affect all the Internet users.

  (3) Potential high delay at some places: users far from that single DNS server have longer response time.

(b) **What is DNS cache**: A DNS cache is a temporary database maintained by a computer's operating system that contains DNS records of all the recent visits, attempted visits to websites and other domains.
Why is it helpful: Even if there are many public DNS servers in the world, caching can speed up the process of domain name resolution and reduce load of DNS servers.
How it works: Before a computer issues its DNS query to the outside network, operating system will intercept it and first look up the DNS query in its local DNS cache. If resolution process in local does not succeed, operating system will issue the DNS query to the outside network.

(c) IP address of www.csie.ntu.edu.tw is **140.112.30.26**. Details are shown below:

  (a) ID: 0000

  (b) Flags: 8100

  (c) QDCOUNT: 0001 (One question follows)

  (d) ANCOUNT: 0001(One answer follows)

  (e) NSCOUNT: 0003(Three records follow)

  (f) ARCOUNT: 0003(Three additional records follow)

(g) Question data:

i. 03: String of length 3 follows
ii. 777777: String is www
iii. 04: String of length 4 follows
iv. 63736965: String is csie
v. 03: String of length 3 follows
vi. 6e7475: String of ntu
vii. 03: String of length 3 follows
viii. 656475: String of edu
ix. 02: String of length 2 follows
x. 7477: String of tw
xi. 00: End of this name
xii. 0001: Query type is A
xiii. 0001: Query class is IN

(h) Answer section:

i. c: Name is a pointer
ii. 00c: Pointer is to the name at offset 0x00c
iii. 0001: Answer is a Type A query
iv. 0001: Answer is class IN
v. 00 00 01 00: Time to live
vi. 00 04: Address is 4 bytes long
vii. 8c 70 1e 1a: IP address is 140.112.30.26

(i) (Omit authority and additional section)

(d) **How to decompress**: As details above, we can find out ”0xc” in authority section and the following three hex number are the offset of names. For example, for ”csman2” in authority section, the offset from the begining of this packet is ”0x010”, which is ”04 63 73 69 (csie), 03 6e 74 75(ntu), 03 65 64 75(edu), 02 74 77(tw)”, and then you can decompress ”0xc010” after ”csman” hex numbers. Finally, you can concatenate ”csman” with ”csie ntu edu tw” and get the full domain name.
What may happen?: Because DNS uses UDP by default, it do not guarantee packets will reach desired place. If a DNS server does not compress large response, it will have bigger packet size and have higher probability of being fragmented or data loss in link layer. Also, a 512-byte UDP payload is considered a safe size, so the compression of larger response can reduce the chance of packet loss.

(e) (a) Distributed Reflection DoS attack:
How they occur?: The attacker would send a DNS query with spoofed source IP, with the intention of a larger response being delivered to the host who actually resides at that spoofed source IP.
How to prevent: Filtering out DNS traffic as far upstream as possible. For example, build a firewall and set rules on it.

(b) Cache Poisoning:
How they occur?: If a DNS server doesn't verify DNS responses it gets, it may end up caching the incorrect records and serving them to other users or downstream DNS servers.
How to prevent?: Ignore unauthoritative responses and reponses that are not directly relevant to the query. Nowadays, DNS servers can use DNSSEC for safer DNS communication.

(c) DNS tunneling:
How they occur?: One can encode the data in DNS queries and reponses so that one can bypass captive portals or firewalls but can still communicate with each other.
How to prevent?: Set up a firewall to check if someone are attempt at data exfiltration. Also, a firewall can check if there are abnormal pattern in the queries section.