Networks Security
Labs 3 & 4

CIT 288

Chaz Davis

BCTC
Spring 2020

February 6, 2020

Lab 3 Questions

Question 1

As an administrator, would you choose to use your router, or your domain controller as your DHCP? No right or wrong answer, but the choice is important when considering your infrastructure.

i) Answer The popular wisdom would appear to say, at least for larger multi router configured networks, windows loves to control things, and routers love to route things. So Domain Controller for DHCP.

As for home-use it gets conflicting. Again, popular convention holds that the domain controller can handle spitting out DHCP requests just fine to non-domain joined machines that request one. If you have just the one subnet then you likely want the domain controller to manage the DHCP but you can certainly allow the router to handle other subnets or segregated access points, etc. so that really just depends.

I've also seen with the new pfsense and grander use of virtualization at home, that people are moving towards using the router with pfsense and collision avoidance.

Question 2

What is wrong with a DHCP without lease time restrictions?

ii) Answer DHCP Lease Time is the amount of time in minutes or seconds a network device can use an IP Address in a network. The IP Address is reserved for that device until the reservation expires. Without it, you would have to manually assign every network device a static IP. At 50% lease time, a device tries to renew their current DHCP lease, so for 8 days, that would be the fourth day, when they secure a renewal that time is now started over with another 8 days. For static devices that works great, but with lots of traffic in and out, that could become very problematic, very quickly.

For example, If you have a coffee bar and you get 400 visitors a day. They stay on average 30 to 60 minutes and you have a DHCP Pool of 200 IP Address (192.168.0.10 – 192.168.0.210 for example). When you leave the DHCP Lease Time on the default 24 hours (1440 minutes) after 200 guest no other guest can use the free wifi network. Because all the 200 IP Addresses are reserved for the first 200 guests.

So in this case you want to lower the DHCP Lease Time to one hour for example. This way the reservation is released soon enough for the other guests: With a lease time one hour, the client will try to renew the lease after 30 minutes. At 35 min it contacts the DHCP server to extend/renew the lease. It's granted so the timers reset, a new lease is acquired for another 60 minutes. In total, the IP Address is reserved for 95 minutes. With 200 addresses available you can have 130 guests per hour on average on your network.

Question 3

Why don't we see WINS servers anymore? Is there still a reason we would have to have one in our network?
iii) Answer
WINS shouldn't be necessary these days, however, people's propensity for hanging on to old and outdated components, programs, and architectures. The reason we don't see them anymore is because of DNS, most domain controllers handle this dynamically now. However, if you still have someone running windows 95, windows 98, or windows ME, and windows server 3.51 - server 4.0 then you would still need WINS.

Question 4

How important is a limited pool of IP's in a given DHCP domain? Why?
iv) Answer
DHCP exist in every network, including telecom internal networks, and enterprise or home networks. DHCP has prolonged the life of IPv4, providing the possibility to serve more users with a limited pool of public IP addresses.

However, DHCP has fundamental importance for the global Internet and for the telecommunication worked based on the internet technologies for providing a plug-and-play approach for access to the internet. Besides the dynamically allocated IP address, the DHCP sets other networking information, of which the most important are the IP addresses of the DNS servers because without access to a DNS server a given host cannot resolve domain names into the IP addresses.

Question 5

Why would DHCP just use UDP? Why not TCP?
v) Answer
The DHCP employs a connectionless service model, using UDP. It is implemented with two UDP port numbers for its operation which are the same as

for the BOOTP protocol. UDP port 67 is the destination port of a server, and port 68 is used by the client.

The reason it uses UDP over TCP has many outlying factors, as well, as one and only one real reason. The outlying factors would be the low overhead of running UDP vs TCP, and second that it is a broadcast connectionless server protocol, as stated above.

But the main, and only true reason is that TCP requires an IP address to connect to it, and if you had an IP address, you wouldn't really be broadcasting a signal to the DHCP requesting an IP address on their network.

Question 6

Why is it a good idea to require a DHCP server to be authorized?
vi) Answer
If a server is authorized, then when it logs on to a system and asks nearby DHCP servers for authorized addresses, it will find its own among the addresses, and can then validate itself and can then begin to lease out addresses.

Question 7

MAC address reservations are a good stopgap for unauthorized access to a DHCP scope, but can you think of a situation in which an attacker with a laptop inside the network could thwart this?
vii) Answer
It seems like it would stop few things, because all you'd have to do is login to your laptop, run a scan to find the addressing scheme and which ones aren't in use, and then spoof your MAC address to one that is in the subnets range, and you would have access.

Question 8

Why would we want to exclude certain IP's from our pool/scope?
viii) Answer
It seems like there are two main reasons.

One would be due to multiple DHCP servers on the same network, you would set all servers up to handle the network, and then exclude the range being handled by another server.

The second, would be for statically assigned addresses. You wouldn't want your static address to be arbitrarily handed out to another computer.

Question 9

Why would it be important to activate the DNS role in a domain controller rather than the router or firewall?

ix) Answer

So that it would have access to active directory, although, again, it seems that this is beginning to be steered away from. Due to being able to break things up. have an external ISP DNS resolution setup outside the firewall. a DNS and DHCP on the internal side for all local ips and connected devices. and something like PFSense on the router to handle a bit of firewall and a bit of DNS.

Question 10

Is there a way to have DNS running on more than one device in the network? How?

x) Answer

As stated above, yes, you can have it on multiple devices, as long as you have one main hub to connect to the outside and one main hub to do internal resolution and put to other servers that control portions of the network.

Lab 4 Questions

Question 11

What is done to configure TELNET server on a device?
xi) Answer
The Telnet protocol enables you to set up TCP/IP connections to a host. Telnet allows a person at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

Question 12

How is SSHD configured on a Linux Backtrack/Kali?
xii) Answer

- If you're only going to use it for a short amount of time:
  - `systemctl start ssh.socket`
  - `systemctl stop ssh.socket`
- If you're wanting to use it for extended periods of time:
  - `dpkg-reconfigure openssh-server`
  - `vim /etc/ssh/sshd_config`
  - `PubkeyAuthentication yes`
  - `PasswordAuhentication no`
  - `systemctl enable ssh.service`
  - `systemctl start ssh.service`

Question 13

List the port numbers for the following: FTP, TELNET, SSH, HTTP, HTTPS, and TFTP.
xiii) Answer

- port 20: FTP
- port 21: FTP
- port 22: SSH
- port 23: TELNET
- port 69: TFTP
- port 80: HTTP
- port 443: HTTPS

Question 14

Should a firewall ever allow ALL outbound traffic to leave the network? Why or why not?
xiv) Answer
No, while open ports with services running aren't inherently bad, all open ports is not a great idea, because without a service running on the port, the port should be closed, otherwise there is no protocol to protect and guard that open port.

Question 15

Why block Ping?
xv) Answer
The Internet Control Message Protocol (ICMP) allows Internet hosts to notify each other of errors and allows diagnostics and troubleshooting for system administrators. Because ICMP can also be used by a potential adversary to perform reconnaissance against a target network, and due to historical denial-of-service bugs in broken implementations of ICMP, some network administrators block all ICMP traffic as a network hardening measure.

Question 16

Why block FTP?
xvi) Answer
You almost certainly want to disable anonymous FTP connections. For one thing Googlebot has a nasty habit of exploring anonymous ftp which could result in the wrong files being exposed. If you do need to allow FTP then can you restrict access to specific ip addresses within your local network or a clients network? If so you should set up a white-list. Most FTP hacking attempts are

automated so rely on guessing both the username and the password. For example, if your domain name is www.example.net the hacking script will try ”example”, ”examplenet”, ”admin@example.net”, ”webmaster@example.net” and so on. Generic usernames including ”admin”, ”www”, ”data” and ”test” are also being tried.

If the script is unable to guess a valid username then it will not be able to try any passwords. You should ensure your FTP usernames are not predictable in any way from the domain name - by appending some random letters or digits for example.

Hackers are also equipped with dictionaries and large databases of exposed username/password combinations from previously exploited servers. So make sure your passwords, not just for FTP, are long and complicated and don’t match common patterns.