Contents

1 Network Administration

1.1 More on SYN Cookies

(a) Each SYN

1.2 DDoS Mitigation

(a) As solving puzzle takes time, it can prevent a large amount of connection at the same time, therefore mitigate ddos attack.

(b) Answer: NASA{5H4256_Puzz1e_9ro0f_0f_Wor1c}

```
21:17:28 X james@James-NB ~
$ nc linux10.csie.org 15001
Wanna access the service? Pass my challenge first!
Give me an X (<= 20 Bytes) such that sha256(X) ends with 019d00: 11111111111111750f98
Challenge Completed. Here is the flag.
NASA{5H4256_Puzz1e_9ro0f_0f_Wor1c}
```

1.3 SSL Stripping

(a) Pre: Two VMWare Machines: A. Kali Linux, B. Ubuntu 18.04(IP:192.168.226.144)
Follow the steps in the tutorial video:

(i) ifconfig to get the info of interfaces.

(ii) echo 1 > /proc/sys/net/ipv4/ip_forward

(iii) iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 8080

(iv) route -n

(v) nmap -sS -O 192.168.226.254/24

(vi) arpspoof -i eth0 -t 192.168.226.144 -r 192.168.226.254

(vii) (in a new terminal) sslstrip -l 8080

(in Ubuntu) type 0rz.tw/4p2Sz and we enter the website with http. Open another new tab and type council.csie.ntu.edu.tw/cscamp/2018/wp-login.php and still we use http. Only when we https header will we use https to visit the website. Submit the username and password, then in kali» cat sslstrip.log we find info about what we just type.

(b) » curl -I https://www.facebook.com we can see 'strict-transport-security: max-age=15552000; preload'; try curl another website: twitter and we can see below images.

```
17:22:14 james@James-NB ~
$ curl -I https://facebook.com
HTTP/2 301
location: https://www.facebook.com/
strict-transport-security: max-age=15552000; preload
content-type: text/html; charset="utf-8"
x-fb-debug: Ax6ZPQQHjRTADpS3nIYHjecC7mcxAaztW8wy2/2fVxipT/DPOPzyt/QwpRfbcc5Sa7/wldQAjWszObYYEGrxFQ==
content-length: 0
date: Sat, 11 May 2019 09:22:17 GMT
```

```
17:26:08 james@James-NB ~
$ curl -I https://twitter.com | grep strict
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0  275k    0     0    0     0      0      0 --:--:--  0:00:01 --:--:--     0
strict-transport-security: max-age=631138519
```

(c) The number of max-age means a period of time that the browser will automatically turn any insecure links referencing the web application into secure links. (That is, to modify the http into https before accessing the server.) In previous examples, 15552000 means exactly 180 days, and 631138519 means...7304 years. (Twitter is so optimistic that they believe it will survive until then?)

(d) Set max-age to 0 will remove the HSTS policy. However, malicious website owners might exploit HSTS to track users. For example, when a user visit one website of the owner, the page might include several links to other other domains that the owner control, and use HSTS policy to inform user to visit them respecively with https or http. If there are 5 links in this one page, then the possible combination of HSTS policy is up to $2^5 = 32$ kinds (every link has one bit: use HSTS or not) By this way, the owner of the website can distinguish amongst $2^{30} = 1$ billion user if one page contains 30 links (a resonable amount). Therefore, browsers run into a dilemma between the SECURITY and PRIVACY.

References

[1] Use curl to obtain info of header

[2] en-WIKI HSTS

[3] Anatomy of a browser dilemma – how HSTS 'supercookies' make you choose between privacy or security

[4] The Double-Edged Sword of HSTS Persistence and Privacy

[5] HTTP Strict Transport Security : Five common mistakes and how to fix them

1.4 Security on Cisco Switch

(a) Steps:

(i) Set up two PC and connect them to one switch (2960)

(ii) Set up port in switch: ena / conf t / interface fastethernet 0/1(0/2) / switchport mode access

(iii) Set up DHCP ip in respective two PCs.

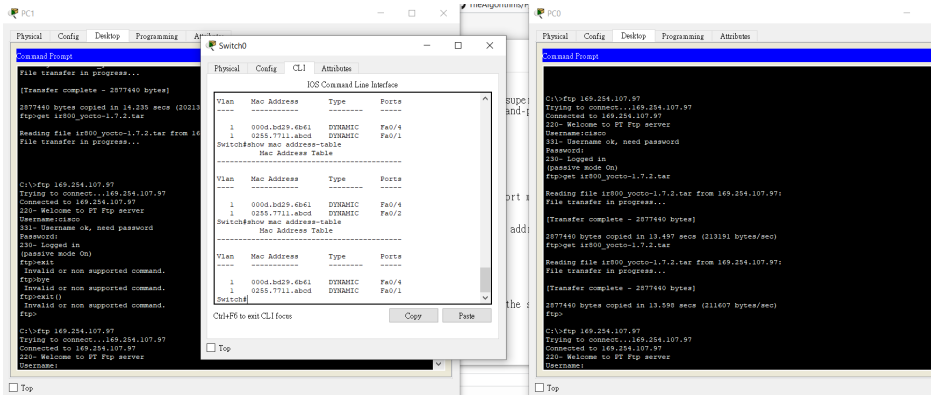
(iv) In cmd of two PCs, try to ping the other PC and it worked.

(v) Set up mac addresses of two PCs to 0255.7711.ABCD in Config tab->Interface->MAC address.

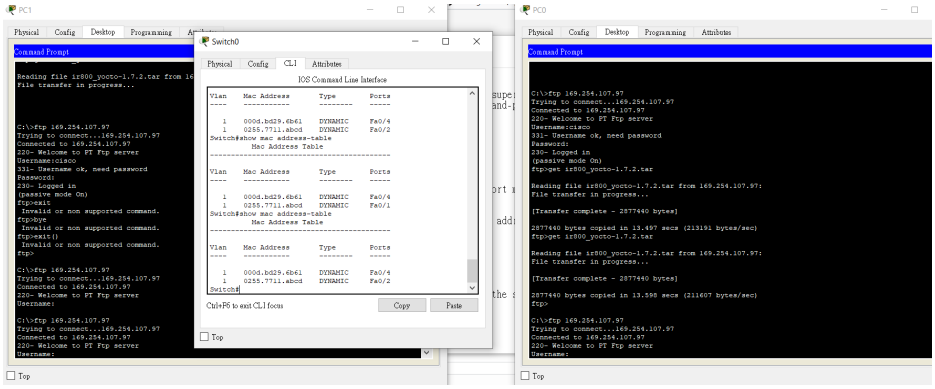
(vi) Set up a FTP server and set its ip to dhcp as Internet.

(vii) In respective cmd of two pcs, connect the server via ftp.

(viii) In switch, show mac address-table, we can see the mac address is mapping to one port of two pcs. For example, the below image shows that the port connecting to switch is fa0/1.



However, if we reconnect ftp server with pc1(connected to switch via fa 0/2), then in switch we can see the mac-address table is updated with fa0/2, shown as below.



(ix) Conclusion: If there're two devices with same mac address, their ip will be same(if using dhcp), and they can't access to the internet simultaneously.

(b) Steps:

(i) In switch: conf t/ int fastEthernet 0/1(0/2) / switchport port-security Suppose the mac addresses of two pc are different, use one to ping the other, and the switch records mac addresses of two pc respectively. We can find it in switch terminal.

(ii) Then, try to assign mac address of pc0 to its counterpart, then ping again. The switch will show that FastEthernet0/2 is down due to mac spoofing.

(c) Steps:

(i) Set up two servers, one pc, and one switch. Connect three end devices to the switch.

(ii) Set up both two servers.

- In Service tab->DHCP, check Service 'On'; Start IP Address set to 192.168.1.2(192.168.2.2), subnet mask to 255.255.255.0 and save.
- In Config tab->FastEthernet0, set IP Configuration to Static, and IP Address set to 192.168.1.1(192.168.2.1). Subnet Mask set to 255.255.255.0.

(iii) Set up the PC: in Desktop tab->IP Configuration, check DHCP and we get a ip from a DHCP server: 192.168.2.2.
Assume we only want to get dhcp offer from FastEthernet 0/1 (192.168.1.2/24):

(iv) In switch: ena / conf t / ip dhcp snooping / interface fastEthernet 0/1 / ip dhcp snooping trust

(v) Then in the PC, reset IP configuration to DHCP, we will get a ip from fastEthernet 0/1 DHCP server. If we turn off DHCP service in that server, then reset the IP configuration of the PC, we will get a message that DHCP failed.

References

[1] NASA2019-lab4

[2] Port-Security

[3] Packet Tracer - Simple DHCP Server

[4] DHCP Snooping Setting Examples

2 System Administration

2.1 There's nothing there but root

(a) Find Something:
'ls /etc -al | grep nasa' and we find a file named ".shadow.swp" which is the only file in /etc/ that is belong to user nasa instead of root. Therefore, we have permission to read and write this specific file. Also, it is the vim swap file of .shadow, the file stored passwords of all users, including root.

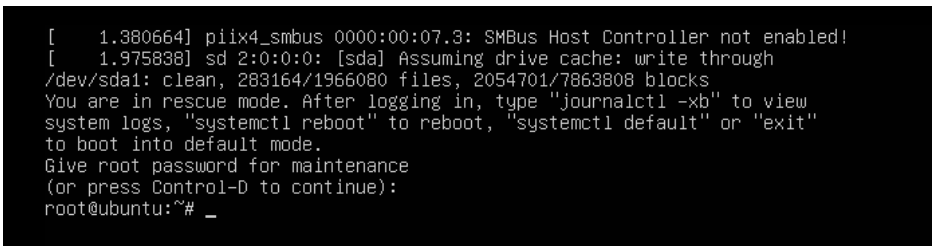
(b) Strange File:

(1) The passwords of users are stored in the "shadow" file that is only writable to root. To allow a normal user to change its password directly, we then introduce the "SUID". If a file has SUID, and it's execuable to others, then when a normal user executes "passwd", it will have the permission as the owner of the file, in this case, the root.

(2)
- /usr/bin/find
  We can use it to get the content of directories that we're not allowed to enter, such as /root/ example command: find /root/
- /usr/bin/fish
  type whoami in fish shell, and it will print 'root'. It means that we can do anything that root is able to do.

(c) Root password:
Find '6vY5HyXFk$J8MBl...' in /etc/shadow, then 'john –wordlist=/usr/share/wordlists/rockyou.txt password' and we find that the password is 'kamisama'.

(d) Single login:



References

[1] File Manager

[2] Cracking everything with John the Ripper

[3] Linux Grub Change root password

2.2 Try another hash

1. Download hashcat
2. .\hashcat64.exe -a 3 -m 0 ”729708903e584f17e018f5b0a97c4dd7”

Answer: 98b14842

2.3 SHA1 of PDFs

1. git clone `https://github.com/nneonneo/sha1collider`
2. python collide.py sha1-1.pdf sha1-2.pdf –progressive