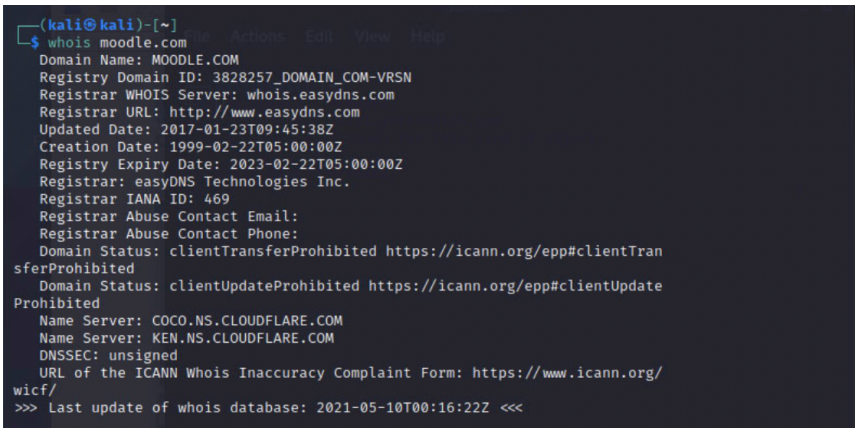
CS 231: Penetration Testing

Rebecca Fox and Yemi Shin

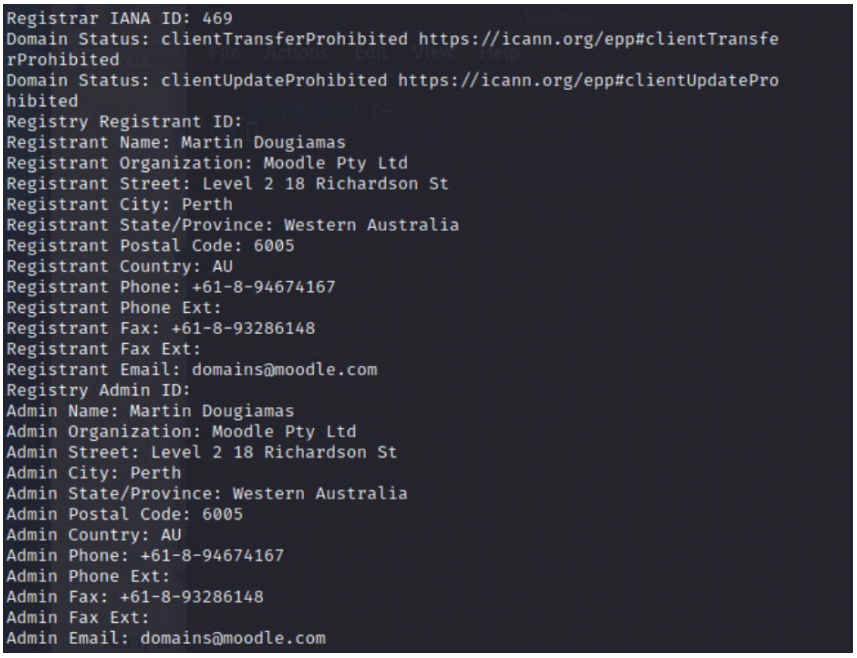
1. Passive Information Gathering

Domain: moodle.com

a. Pick a domain you're interested in, and execute: whois [domain-name]



```
┌──(kali㉿kali)-[~]
└─$ whois moodle.com
   Domain Name: MOODLE.COM
   Registry Domain ID: 3828257_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.easydns.com
   Registrar URL: http://www.easydns.com
   Updated Date: 2017-01-23T09:45:38Z
   Creation Date: 1999-02-22T05:00:00Z
   Registry Expiry Date: 2023-02-22T05:00:00Z
   Registrar: easyDNS Technologies Inc.
   Registrar IANA ID: 469
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTran
sferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdate
Prohibited
   Name Server: COCO.NS.CLOUDFLARE.COM
   Name Server: KEN.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/
wicf/
>>> Last update of whois database: 2021-05-10T00:16:22Z <<<
```



```
Registrar IANA ID: 469
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransfe
rProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdatePro
hibited
Registry Registrant ID:
Registrant Name: Martin Dougiamas
Registrant Organization: Moodle Pty Ltd
Registrant Street: Level 2 18 Richardson St
Registrant City: Perth
Registrant State/Province: Western Australia
Registrant Postal Code: 6005
Registrant Country: AU
Registrant Phone: +61-8-94674167
Registrant Phone Ext:
Registrant Fax: +61-8-93286148
Registrant Fax Ext:
Registrant Email: domains@moodle.com
Registry Admin ID:
Admin Name: Martin Dougiamas
Admin Organization: Moodle Pty Ltd
Admin Street: Level 2 18 Richardson St
Admin City: Perth
Admin State/Province: Western Australia
Admin Postal Code: 6005
Admin Country: AU
Admin Phone: +61-8-94674167
Admin Phone Ext:
Admin Fax: +61-8-93286148
Admin Fax Ext:
Admin Email: domains@moodle.com
```

```
Tech Organization: Moodle Pty Ltd
Tech Street: Level 2 18 Richardson St
Tech City: Perth
Tech State/Province: Western Australia
Tech Postal Code: 6005
Tech Country: AU
Tech Phone: +61-8-94674167
Tech Phone Ext:
Tech Fax: +61-8-93286148
Tech Fax Ext:
Tech Email: sysadmin@moodle.com
Name Server: ken.ns.cloudflare.com
Name Server: coco.ns.cloudflare.com
DNSSEC: unsigned
Registrar Abuse Contact Email: abuse@easydns.com
Registrar Abuse Contact Phone: +1.4165358672
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic
.net/
>>> Last update of WHOIS database: 2021-05-10T00:16:46Z <<<

"For more information on Whois status codes, please visit https://icann.org
/epp"

This domain is being managed via EASYDNS

The DNS Hosting specialists since 1998

DNS Hosting / Dynamic DNS / Failover DNS / DNS Anycast
```

b. Do the same thing, but this time with nslookup [domain-name]

```
Server:         137.22.198.41
Address:        137.22.198.41#53

Non-authoritative answer:
Name:   moodle.com
Address: 104.21.5.204
Name:   moodle.com
Address: 172.67.133.211
```

c. You can also try getting more info with: nslookup -query=any [domain-name]

d. Repeat the whois and nslookup commands, but use the IP address you discovered in the previous steps instead of a domain name. Do you get any new information, or is it the same as what you got from the domain names?

```
NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2017-02-17
Comment:        All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse
Ref:            https://rdap.arin.net/registry/ip/104.16.0.0


OrgName:        Cloudflare, Inc.
OrgId:          CLOUD14
Address:        101 Townsend Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2010-07-09
```

- Using the IP address gives different information, including a different address and no information about the registrant or admin.

```
Server:         137.22.198.41
Address:        137.22.198.41#53

** server can't find 205.4.21.104.in-addr.arpa: NXDOMAIN
```

QUESTIONS:

a. The domain we explored was moodle.com.
b. The IP address was 104.21.5.204 and 172.67.133.211 (Why are there two IPs?).
c. The domain's registration expires 02-22-2023.
d. We found information about the registrar/admin of moodle, including his name, address, phone number, and email address.

2. Host detection

QUESTIONS:

Local Network:

a. The IP addresses we found were 10.0.2.1, 10.0.2.2, 10.0.2.4, and 10.0.2.15
b. What entities do those IP addresses represent?
    i. We ran the command 'sudo nmap -O -v [ip-address]' to derive these results.
    - This command seemed to complete a sweeping analysis of kali
    - ARP Ping scans, DNS scans, as well as SYN Stealth Scans, which was interesting.
    - These IP addresses represent the hosts that are currently active.
    - Some of the hosts that were active were:
    - **10.0.2.1**
        - Some of the ports that were running on this host were:

        - 53/tcp open domain
    - Some “aggressive OS guesses for what this entity might be are:
        - Grandstream GXP1105 VoIP phone (98%), Garmin Virb Elite action camera (94%), 2N Helios IP VoIP doorbell (93%), NodeMCU firmware (lwIP stack) (92%), Philips Hue Bridge (lwIP stack v1.4.0) (92%), Ocean Signal E101V emergency beacon (FreeRTOS/lwIP) (91%), Espressif esp8266 firmware (lwIP stack) (91%), lwIP 1.4.0 lightweight TCP/IP stack (91%), Rigol DSG3060 signal generator (91%), Sony PlayStation 2 game console (91%)
- **10.0.2.2**
    - Some of the ports that were running on this host were:
        - 22/tcp   filtered ssh
        - 88/tcp   open   kerberos-sec
        - 1947/tcp open   sentinelsrm
        - 5900/tcp filtered vnc
    - Some “aggressive OS guesses for what this entity might be are:
        - Grandstream GXP1105 VoIP phone (92%), Garmin Virb Elite action camera (90%), 2N Helios IP VoIP doorbell (89%), FireBrick FB2700 firewall (87%), Cognex DataMan 200 ID reader (lwIP TCP/IP stack) (86%), Enlogic PDU (FreeRTOS/lwIP) (86%), HP LaserJet 2200dtn printer (85%), HP LaserJet 4MV or 4000TN printer (85%), HP LaserJet 4Si or LaserJet 4 Plus printer (85%), lwIP 1.4.0 lightweight TCP/IP stack (85%)

c. For each possible candidate IP address it was searching in the local network, what steps did nmap take? (You can answer this question by examining the Wireshark captured packets. If you want to make it easier to read the relevant packets, try doing "nmap -sn [just-one-ip-address]" instead of the /24 thing.)
    - Tested with a single IP address: 10.0.2.1
    - nmap (a client, kind of like browser that sends network queries on kali) sends a special type of TCP [SYN] packet to 10.0.2.1 (“Hey host do you exist” message)
    - 10.0.2.1 sends back an [RST, ACK] packet back, thus revealing its active status.
    - After this special handshake has been established, only for those that respond nmap uses reverse DNS resolution protocol to query the host name of the IP address (which I think is what is indicated in the query response under the header “Authoritative nameservers” -> mname: prisoner.iana.org)

Math/CS Network:

a. The IP addresses that were found were:
    i. 137.22.4.5 (elegit.mathcs.carleton.edu)
    ii. 137.22.4.17 (perlman.mathcs.carleton.edu)

iii. 137.22.4.19 (ada.mathcs.carleton.edu)
iv. 137.22.4.20
v. 137.22.4.22
vi. 137.22.4.175 (awb1.mathcs.carleton.edu)

b. These IP addresses represent the currently active Carleton network hosts
    i. Some of the hosts for which we ran OS scan yielded the following results:
        1. Reasonably, OS scans for the Math/CS network took a much longer time.
        2. **137.22.4.19** (ada.mathcs.carleton.edu)
            a. There were two ports running on ada host.
                i. 22/tcp open ssh
                ii. 1718/tcp filtered h323gatedisc
        3. 137.22.4.20
            a. There were three ports running on this host.
                i. 80/tcp
                ii. 443/tcp
                iii. 22/tcp
    ii. To each candidate IP address, nmap sends a TCP [SYN] packet to try to solicit a response. For the IP addresses that send back a reply, nmap initiates a reverse DNS resolution to obtain the name of the IP address, if one exists. There were also sometimes ARP broadcasts that were captured by Wireshark, but it was indeterminable whether it was a result of an ARP Ping scan done by nmap, or a miscellaneous communication that happened to cross at that time.

3. Port Scanning

QUESTIONS:

a. The following image contains all open ports on Metasploitable.

```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

b. What database server(s) is/are available on Metasploitable?
   i. MySQL (port 3306)
   ii. PostgreSQL (port 5432)

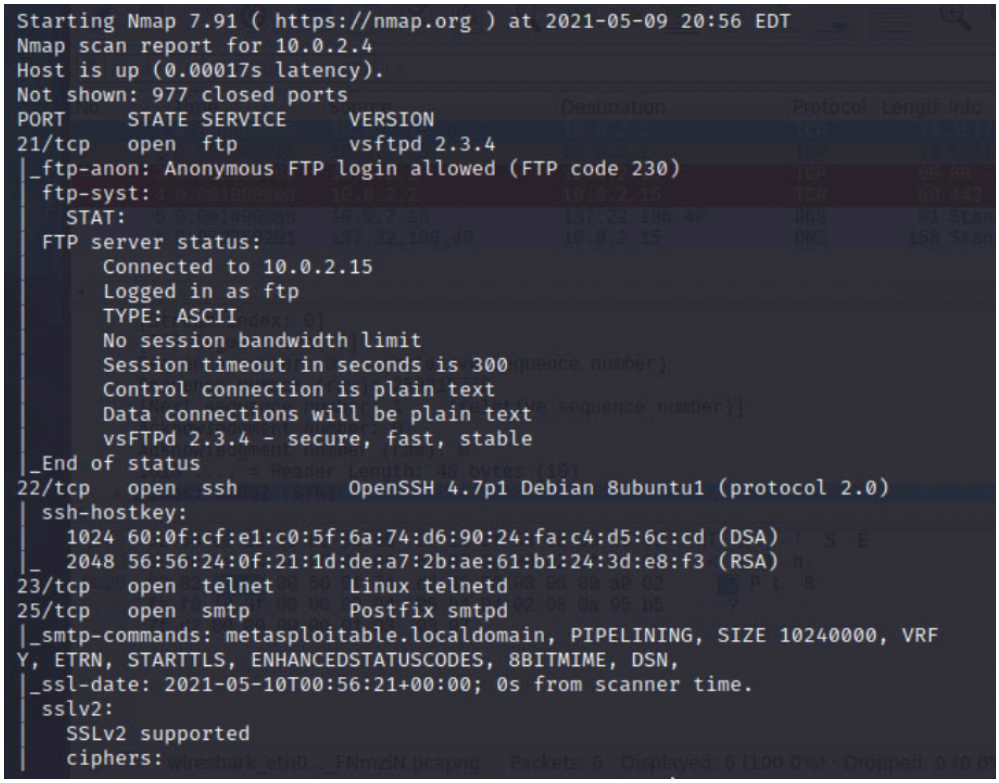
```
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: ConnectWithDatabase, Support41Auth, SupportsTransact
ions, SwitchToSSLAfterHandshake, LongColumnFlag, SupportsCompression, Speak
s41ProtocolNew
|   Status: Autocommit
|_  Salt: #"}tNhAM<&ElpnWHE^+Z
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2021-05-10T23:28:16+00:00; +1s from scanner time.
```

c. The value of the RSA SSH host key is used to help the client know that they are connected to the correct host.

```
56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
```

d. Port 111 has **Rpcbind**. Rpcbind is a server that converts RPC program numbers into universal addresses. RPC, or Remote Procedure Call is when a computer program causes a procedure to execute in a different address space. When an RPC service is started, it tells rpcbind the address at which it is listening, and the RPC program numbers it is prepared to serve. When a client wishes to make an RPC call to a given program number, it first contacts rpcbind on the server machine to determine the address where RPC requests should be sent.

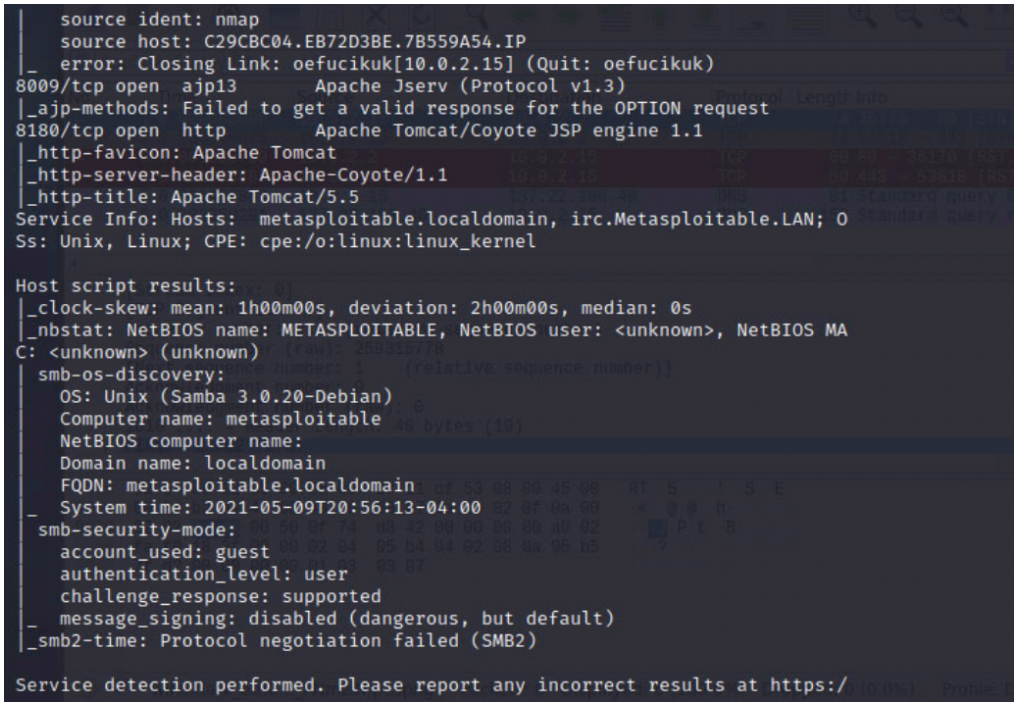
Full nmap -A results for Metasploitable:



```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-09 20:56 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00017s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRF
Y, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2021-05-10T00:56:21+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
```

```
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      46579/tcp   mountd
|   100005  1,2,3      54910/udp   mountd
|   100021  1,3,4      38013/udp   nlockmgr
|   100021  1,3,4      39885/tcp   nlockmgr
|   100024  1          45143/tcp   status
|_  100024  1          48211/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
```

```
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SwitchToSSLAfterHandshake, SupportsTr
ansactions, SupportsCompression, LongColumnFlag, Speaks41ProtocolNew, Conne
ctWithDatabase
|   Status: Autocommit
|_  Salt: zLIk`|rGIw=goy305[J?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2021-05-10T00:56:21+00:00; 0s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
```



4. Further Questions

1. In part 1, when we are analyzing the results of the whois command, what are *'domain statuses'*? Ex. clientUpdate prohibited.
2. When we do ifconfig, what are *eth0, lo, and mtu* exactly and why are they named this way?
3. When we were doing nmap experiments, we sometimes saw ARP protocol happening, which was a broadcast that went something like 'Who has [ip-address]? Tell [ip-address].' What is going on?
4. In the same context as question 3, what are DHCP? Dynamic Host Configuration Protocol? Is this part of the nmap process?
    a. Some router requesting for a specific IP address (wireless)
5. During the nmap experiments, live hosts sent back not just [ACK] packet but also an [RST] packet, and the entire packet was somehow colored red on Wireshark. What is RST and why is the packet colored red? Is that indicative of some security breach?