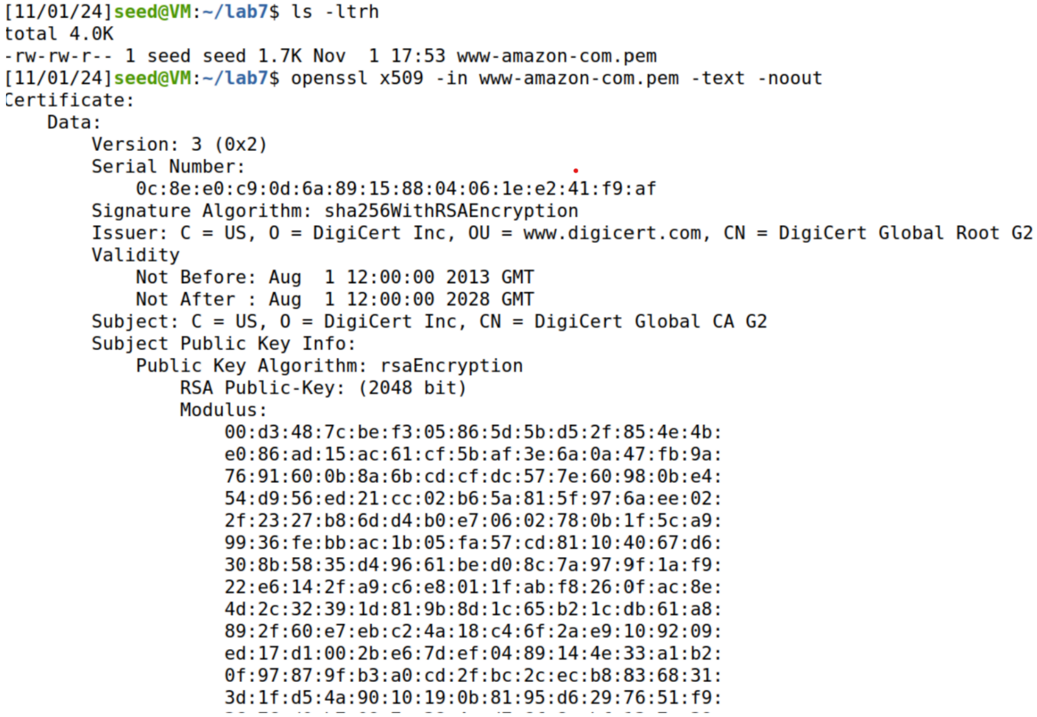
1. The Comodo breach occurred in March 2011 when a hacker compromised the verification process of Comodo, a popular certificate authority, in Southern Europe where they had the company send out nine certificates to seven different domains. Out of those seven domains one was addons.mozilla.org, a key domain for the firefox browser.

2. The DigiNotar breach occurred from June to July 2011 when an attacker gained access to a top certificate authority's, DigiNotar, private key. The attacker was able to issue approximately 531 rogue certificates through intercepting network traffic intended for Google’s subdomains in an apparent MITM (man in the middle) attack.

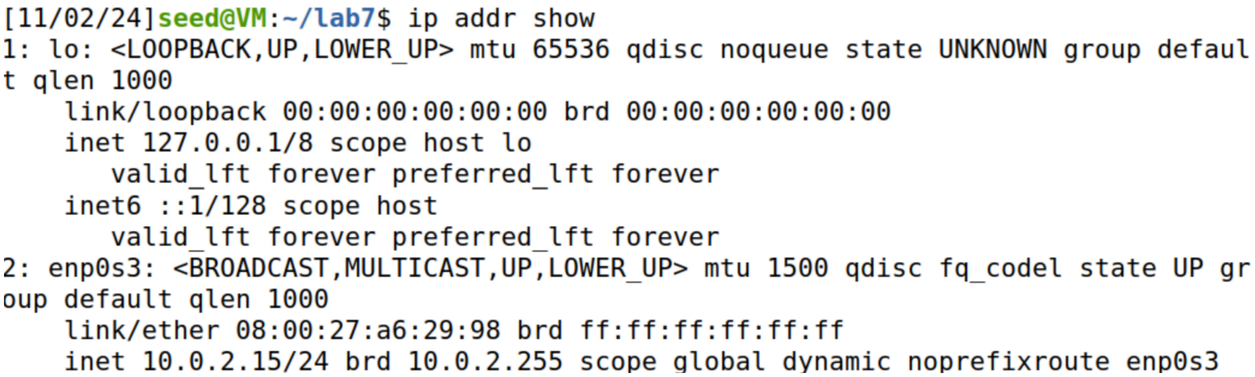
3. The SHAttered attack, also known as a SHA-1 collision, occurs when a hacker uses a hash collision to create two different files that have the same hash value. Because many systems use hashes to verify a file’s authenticity, this type of attack does pose a potential threat when a system accepts, verifies, and signs a file that may end up having a different output or result than originally intended. This can have disastrous results depending on the type of file and what data is intended to be pulled from it.

4.

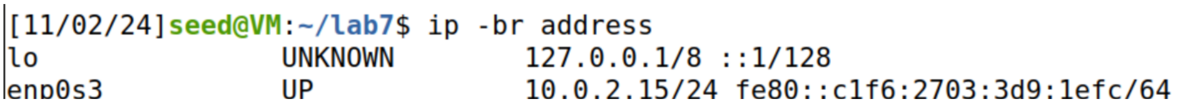


```
[11/01/24]seed@VM:~/lab7$ ls -ltrh
total 4.0K
-rw-rw-r-- 1 seed seed 1.7K Nov  1 17:53 www-amazon-com.pem
[11/01/24]seed@VM:~/lab7$ openssl x509 -in www-amazon-com.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:8e:e0:c9:0d:6a:89:15:88:04:06:1e:e2:41:f9:af
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
        Validity
            Not Before: Aug  1 12:00:00 2013 GMT
            Not After : Aug  1 12:00:00 2028 GMT
        Subject: C = US, O = DigiCert Inc, CN = DigiCert Global CA G2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d3:48:7c:be:f3:05:86:5d:5b:d5:2f:85:4e:4b:
                    e0:86:ad:15:ac:61:cf:5b:af:3e:6a:0a:47:fb:9a:
                    76:91:60:0b:8a:6b:cd:cf:dc:57:7e:60:98:0b:e4:
                    54:d9:56:ed:21:cc:02:b6:5a:81:5f:97:6a:ee:02:
                    2f:23:27:b8:6d:d4:b0:e7:06:02:78:0b:1f:5c:a9:
                    99:36:fe:bb:ac:1b:05:fa:57:cd:81:10:40:67:d6:
                    30:8b:58:35:d4:96:61:be:d0:8c:7a:97:9f:1a:f9:
                    22:e6:14:2f:a9:c6:e8:01:1f:ab:f8:26:0f:ac:8e:
                    4d:2c:32:39:1d:81:9b:8d:1c:65:b2:1c:db:61:a8:
                    89:2f:60:e7:eb:c2:4a:18:c4:6f:2a:e9:10:92:09:
                    ed:17:d1:00:2b:e6:7d:ef:04:89:14:4e:33:a1:b2:
                    0f:97:87:9f:b3:a0:cd:2f:bc:2c:ec:b8:83:68:31:
                    3d:1f:d5:4a:90:10:19:0b:81:95:d6:29:76:51:f9:
```

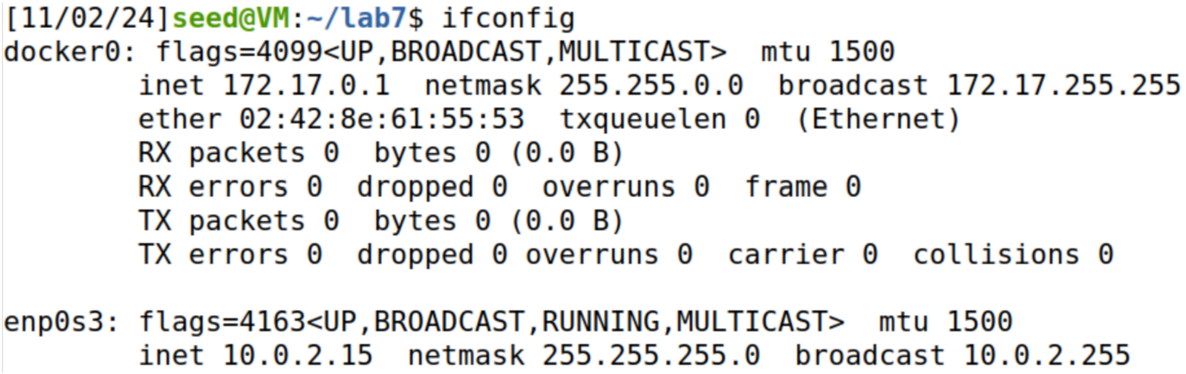
5.



```
[11/02/24]seed@VM:~/lab7$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:a6:29:98 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
```

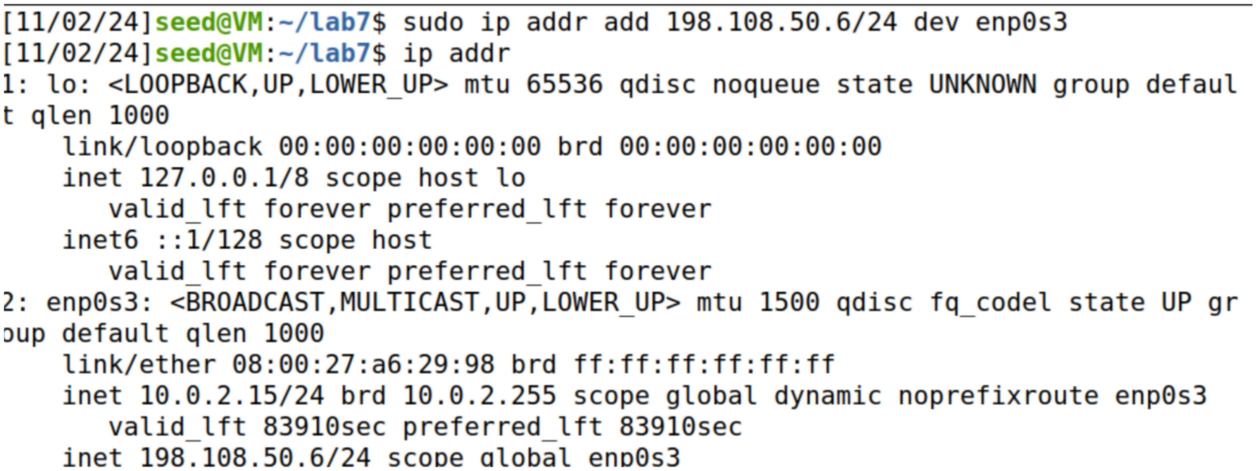


```
[11/02/24]seed@VM:~/lab7$ ip -br address
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             10.0.2.15/24 fe80::c1f6:2703:3d9:1efc/64
```



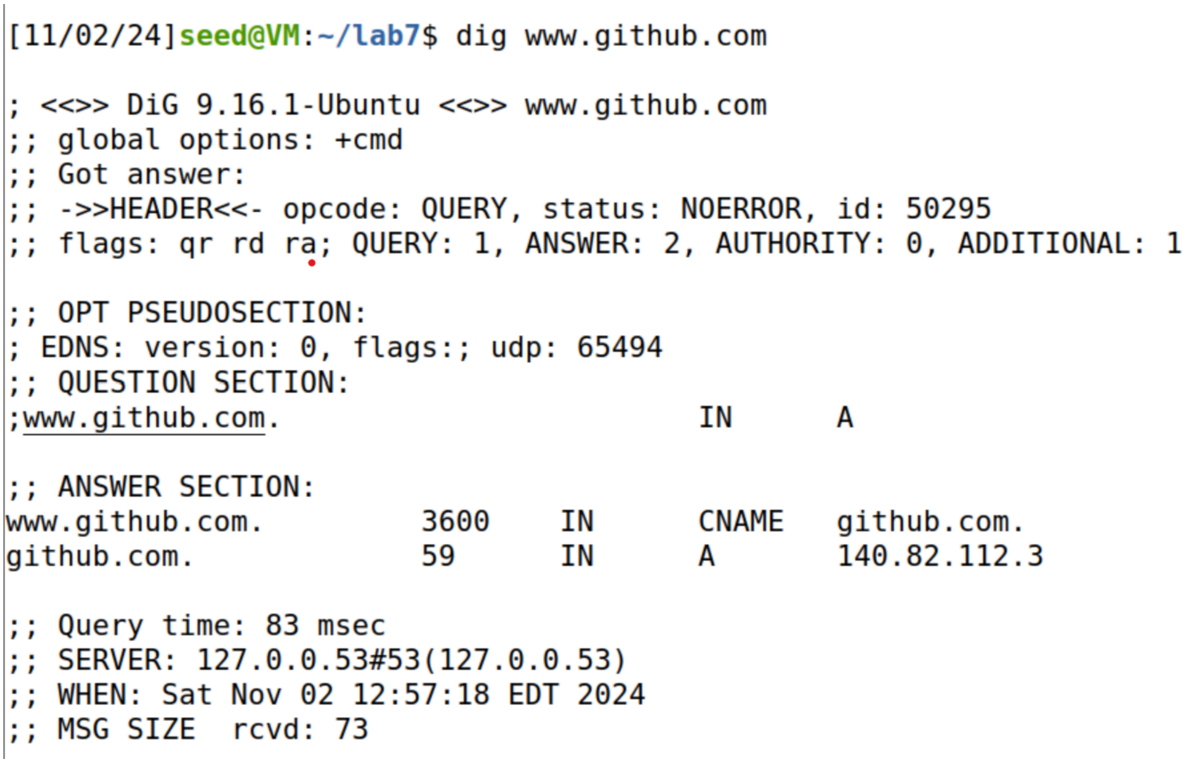
```
[11/02/24]seed@VM:~/lab7$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:8e:61:55:53  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
```

6.



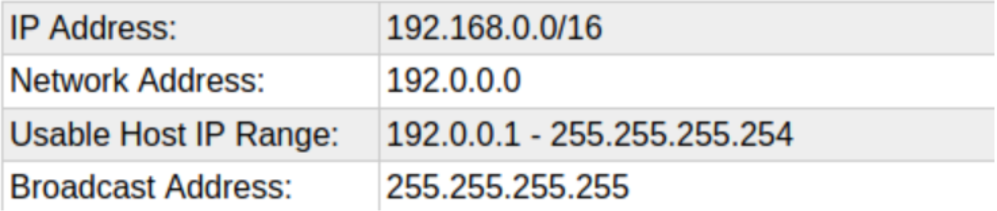
```
[11/02/24]seed@VM:~/lab7$ sudo ip addr add 198.108.50.6/24 dev enp0s3
[11/02/24]seed@VM:~/lab7$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:a6:29:98 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 83910sec preferred_lft 83910sec
    inet 198.108.50.6/24 scope global enp0s3
```

7.



```
[11/02/24]seed@VM:~/lab7$ dig www.github.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.github.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50295
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.github.com.                        IN      A

;; ANSWER SECTION:
www.github.com.         3600    IN      CNAME   github.com.
github.com.             59      IN      A       140.82.112.3

;; Query time: 83 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Nov 02 12:57:18 EDT 2024
;; MSG SIZE  rcvd: 73
```

8.



IP Address:	192.168.0.0/16
Network Address:	192.0.0.0
Usable Host IP Range:	192.0.0.1 - 255.255.255.254
Broadcast Address:	255.255.255.255