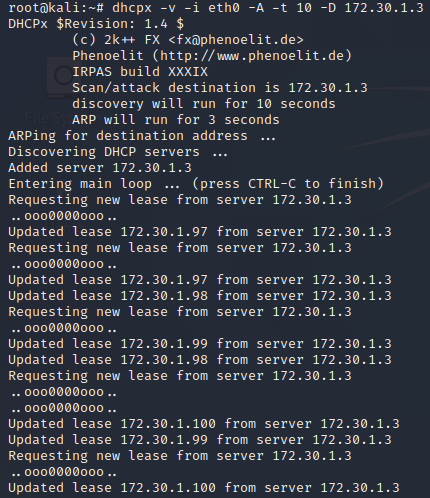
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:고준혁 | | |  | |
|  | DHCP SPOOFING | | | | | | |  |
|  | | dhcpx를 이용한 공격 | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요 |
| \*DHCP SPOOFING?  DHCP는 네트워크 상에 동적으로 IP 정보를 할당하여 사용자에게 편의를 제공하기 위한 프로토콜로 서버로부터 IP, netmask, gateway, dns 정보를 자동으로 할당받는 서비스이다.  DHCP는 UDP로 동작하기 때문에 인증이 불가능하다. 즉, UDP 자체가 비신뢰성/비연결지향성 프로토콜이기 때문에 인증된 DHCP인지 판별이 불가능하다.  DHCP SPOOFING은 DHCP 프로토콜이 인증이 불가능한 취약점을 이용하여 DHCP 프로토콜이 제공하는 정보를 변조해 공격자가 자신이 DHCP 서버인 것처럼 거짓 정보를 클라이언트에게 제공하는 공격이다.  **▶ 정상적인 DHCP 프로토콜의 동작 과정** |
| DHCP의 패킷은 DISCOVER - OFFER - REQUEST - ACK 의 순서로 동작한다.  ① PC는 네트워크에 접속하면 먼저 DHCP DISCOVER 패킷을 전송한다. 해당 패킷은 네트워크 상에 존재하는 DHCP 서버를 찾는 역할을 한다.  ② DHCP DISCOVER 패킷을 받은 DHCP 서버는 DHCP OFFER 패킷을 DISCOVER 패킷을 보낸 PC 에 전달한다.  ③ DHCP OFFER 패킷은 Windows 환경을 제외한 나머지 환경은 Unicast 로 동작하며, Windows 환경의 DHCP 서버는 Broadcast 로 동작한다.  ④ DHCP OFFER 패킷을 받은 PC 는 DHCP REQUEST 패킷을 Broadcast하며, 해당 패킷을 받은 DHCP 서버는 ACK 패킷을 보내게 된다. |
|  |
|  |
|  |
|  |

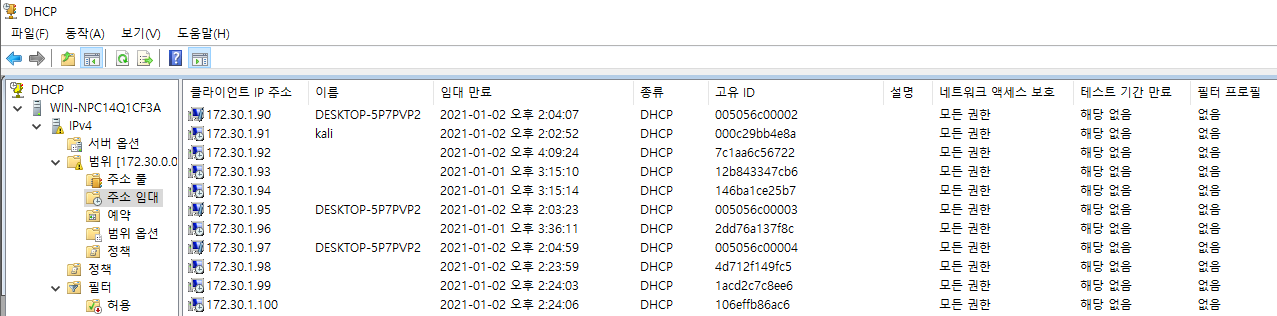
|  |
| --- |
|  |
| 2. 공격과정 |
| |  |  | | --- | --- | | **실습 환경** | **OS** | | **공격자 시스템** | **Kali Linux** | | **피해자 시스템** | **Server - Windows Server 2016** | | **Client - CentOS7** |   시나리오 : CentOS7(client)이 Win2016(DHCP)에게 DHCP 정보를 받아야 하지만 Kali에게서 받게 됨. |
| (Win2016)  **서버 관리자 ---🡪 역할 추가 ---🡪 DHCP 역할 설치**  **DHCP IP Pool : 172.30.1.90 ~ 172.30.1.100**  **NetMask : 255.255.0.0**  **DNS server : 8.8.8.8**    <DHCP 서버가 정상적으로 작동 중>    ipconfig /all 명령을 통해 게이트웨이 주소 확인.  (Kali)  dhcpx를 이용하여 DHCP IP에 대한 자원 고갈을 시도한다.  **#dhcpx -v -I eth0 -A -t 10 -D 172.30.1.254**  **(\*dhcpx 패키지가 없어서 작동 안 할 시 #apt-get install irpas로 패키지 설치)** |



<DHCP 서버로부터 IP를 받고 있다>

(Win2016)

DHCP IP 임대 현황을 확인하면 대역을 모두 소진하였다.



▶ MAC address인 고유 ID를 보면 이상하게 되어 있음.

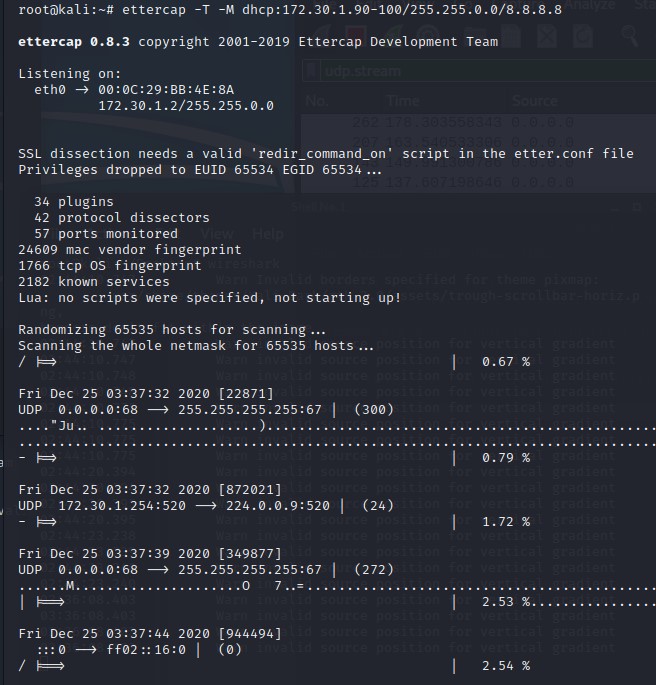
(Kali)

Ettercap을 이용하여 타겟 PC에서 DHCP IP를 재할당한다

#ettercap ①-T ②-M ③dhcp:172.30.1.90-100/255.255.0.0/④8.8.8.8

1. -T : Terminal(CLI) 모드로 진행
2. -M : Man in the Middile(MITM) 중간자 공격 진행
3. -dhcp:172.30.1.90-100 : 90번부터 100번까지의 DHCP IP Pool과 서브넷마스크 확인
4. 8.8.8.8 : DNS 서버 IP 주소

\*게이트웨이가 없는 이유는 본인 IP가 게이트웨이.



▶ 타겟 PC에서 DHCP IP를 재할당

|  |
| --- |
|  |
| 3. 공격 결과 |
|  |
| (CentOS7)  ▶ **클라이언트의 IP가 kali의 IP로 되어있으며 IP, DNS에 대해 kali로부터 받은 것을 확인할 수 있다.** |

|  |
| --- |
|  |
| 4. 보안진단 및 대책 |
| **DHCP Snooping**  \*DHCP Snooping  DHCP 서버를 보호하기 위해 사용하는 기능으로, DHCP Spoofing을 방어하기 위해 스위치가 DHCP 메시지의 내부까지 확인하는 기능이다  DHCP Snooping은 Trusted Port와 Untrusted Port로 구분한다.  ▶ Trusted Port – DHCP 서버 or DHCP Relay Agent가 접속된 포트  ▶ Untrusted Port – DHCP 클라이언트가 접속된 포트 |
| 신뢰하는 포트와 신뢰하지 못하는 포트를 나누게 되는데 비신뢰성 포트에서 DHCP 서버, DHCP Relay Agent가 보내는 메시지는 가짜로 판단해서 무조건 차단하게 된다.(가짜 DHCP 서버 역할 방지)  또한 DHCP 클라이언트가 보내는 메시지를 검사하게 되는데, Ethernet 프레임의 src MAC 주소 = DHCP 메시지의 클라이언트 MAC 주소를 확인한 후 같으면 정상, 다르면 공격 메시지로 판단해 차단하게 된다.  **스위치 설정 방법** |
| *Switch#conf t Switch(config)#ip dhcp snooping Switch(config)#ip dhcp snooping vlan [vlan id] Switch(config)#interface range gigabitEthernet 0/1 ~ 10   Switch(config)#ip dhcp snooping limit rate [num] Switch(config)#interface gigabitEthernet 0/24 Switch(config)#ip dhcp snooping trust*  - ip dhcp snooping    : dhcp snooping 기능 활성화.  - ip dhcp snooping vlan [vlan id]    : dhcp snooping 기능을 사용할 Vlan을 정해준다. 기본적으로 모든 인터페이스는 신뢰할 수 없는 인터페이스가 된다.  - interface range gigabitEthernet 0/1 ~ 10 - ip dhcp snooping limit rate [num]    : 신뢰하지 않는 인터페이스에 들어가서 초당 dhcp 패킷 수를 조정한다. 혹시 내부에서 dos 공격이 있을 경우 차단하기위한     옵션이다. - interface gigabitEthernet 0/24  - ip dhcp snooping trust    : 사용하는 dhcp 서버가 연결되어 있는 인터페이스가 있다면 신뢰 인터페이스로 변경해 준다.  **DHCP Snooping 상태 확인**    *Swtich#sh ip dhcp snooping* |
|  |

|  |
| --- |
|  |
| 5. 보안대책 적용시 공격결과 (최종 매뉴얼에 포함) |
|  |
|  |
|  |
|  |
|  |
|  |