|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | **KITRI 모의해킹 28기** | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | **작성: 신세은** | | |  | |
|  | **Soofing** | | | | | | |  |
|  | | **-DNS Spoofing-** | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| **1. 개요(공격개념/원리/취약점/공격 시 예상피해 등)** |
|  |
| 1. **DNS Spoofing 이란** |
| * **특정 사용자를 ARP Spoofing 을 통한 MITM 상태에서 DNS Query 를 가로채서 자신이 원하는 DNS Response를 사용자에게 전송하여 자신이 원하는 사이트로 유도하는 공격이다.** * **DNS Server 가 DNS Response를 전송해도 먼저 도착한 공격자의 DNS Response 만을 사용자는 수용하고 뒤늦게 도착한 DNS Server 의 DNS Response는 무시하고 폐기한다.** |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| **2. 공격과정 (필요시 가정이나 예상 시나리오 포함)** |
| **실습환경**  **실습 툴: ettercap**  **공격자PC(KALI LINUX): 192.168.0.101**  **타겟PC(CENTOS7): 192.168.0.102**   |  | | --- | | 1. **etter.dns 파일 수정** |  * **# vi /etc/Ettercap/etter.dns**      * **네이버 관련 된 주소를 공격자의 IP 로 수정** |
| 1. **Ettercap 툴 실행** |
| * **# ettercap –G**      * **[Kali linux] – [프로그램] – [sniffing & Spoofing] –[ettercap]**      * **실행화면** |
| 1. **Sniffing & Spoofing** |

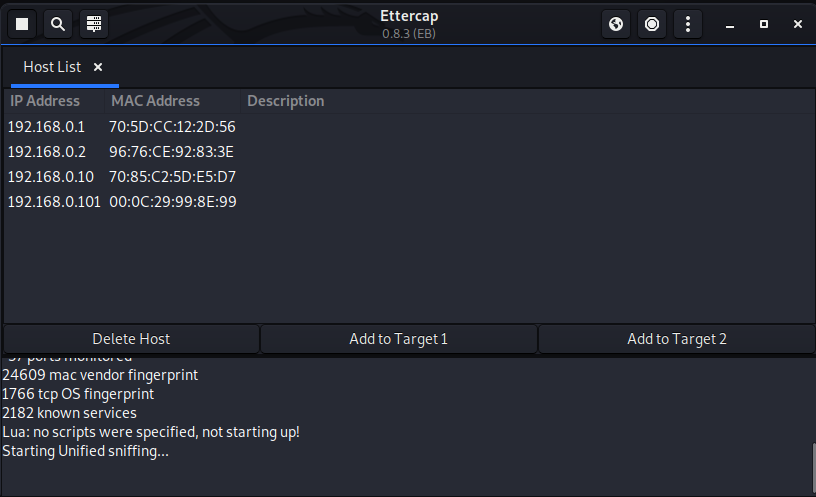
* **Spoofing을 하기 위해선 패킷을 감시하고, DNS 질의를 먼저 반환해야 하기 때문에 공격대상의 ARP 테이블을 조작(ARP Spoofing)하여 패킷 감시 후, DNS Spoofing 진행**

1. **LAN 구간 호스트 스캔**

* **[Host]-[Scan for hosts]-[Host list]**

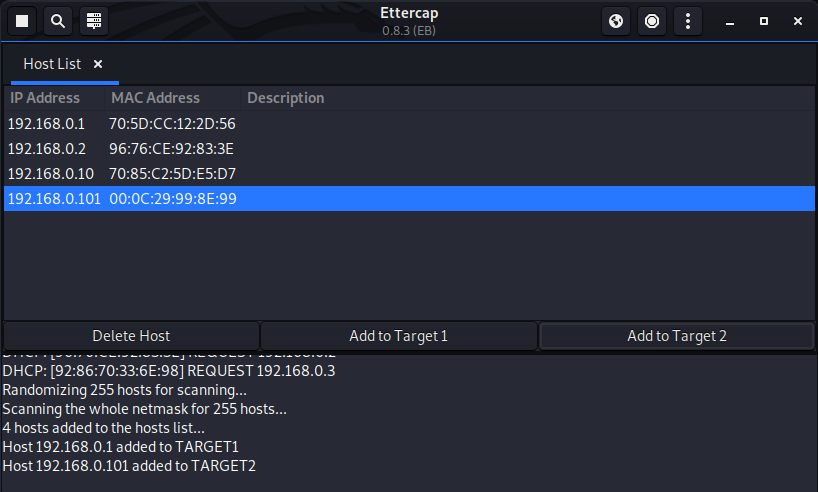
****

**-Host 목록**

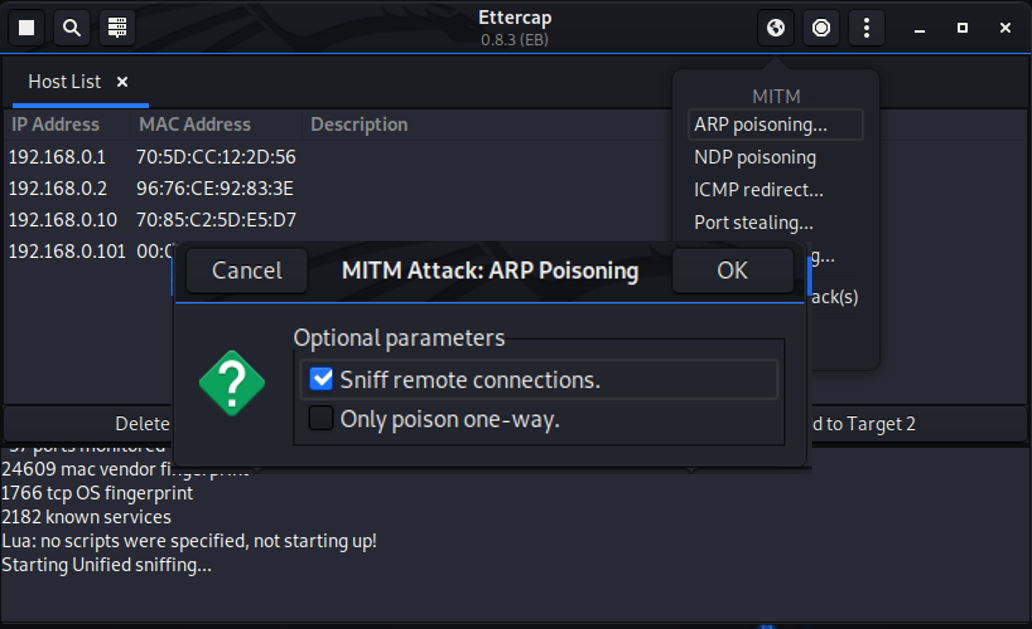
****

1. **타겟 설정**

* **Add to Target 1: Gate way**
* **Add to Target 2: 타겟 IP**

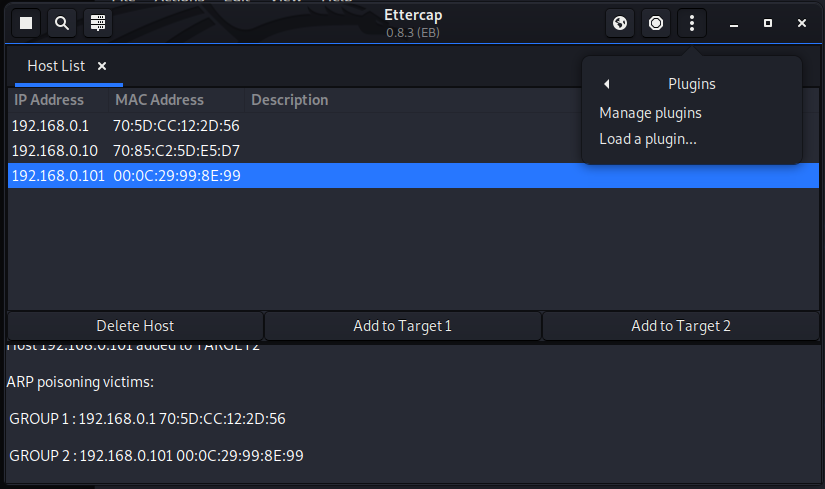
****

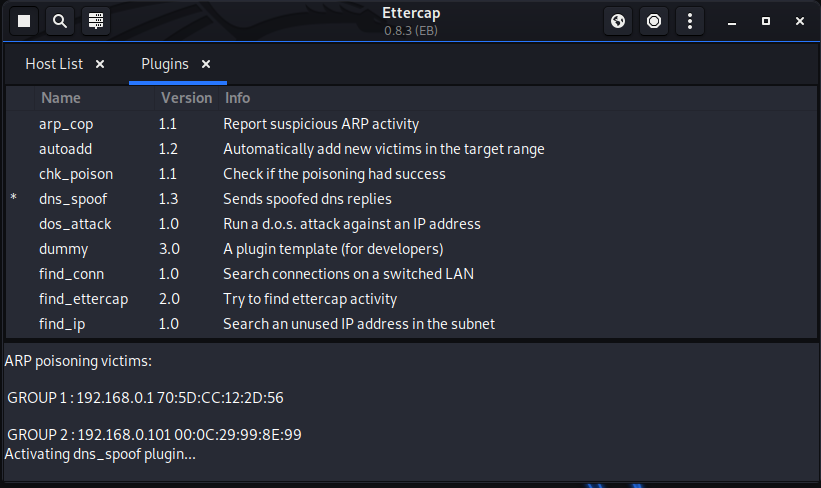
1. **[MITM] – [ARP poisoning …] –[ Sniff remote connection]-[ok]**

****

1. **플러그인 설정**

**[Plugins] – [Manage the plugins] – [dsn\_spoof]**

****

****

|  |
| --- |
|  |
| **3. 공격 결과** |
| 1. **ping 응답** |
| * **클라이언트에서** [**www.naver.com**](http://www.naver.com) **으로 ping 을 보내보면 공격자 IP 로 응답하는 것을 확인** * **ping www.naver.com** |
| 1. **클라이언트에서 웹 사이트 접속 시도** |
| * **Microsoft Edge 에서 네이버 접속 결과, 공격자의 웹페이지로 이동하는 것을 확인** |
|  |

|  |
| --- |
| **4. 보안진단 및 대책** |
|  |
| 1. **hosts 파일을 사용** |
| * **사이트에 접속하면 도메인 이름에 대한 IP 주소가 캐시에 저장되었다가 다시 접속했을 때 DNS Query를 보내지 않고 캐시에서 읽어드린 다음 hosts파일을 통해서도 도메인 이름에 대한 IP 주소를 해석**   **즉, 중요 사이트의 IP 주소를 확인하여 적어 두면, hosts에 있는 사이트에 대해서는 DNS Spoofing 공격에 대한 대응이 가능**   * **파일경로: C:\Windows\System32\drivers\etc** * **네이버 주소 추가** |

|  |
| --- |
| **5. 보안대책 적용시 공격결과 (최종 매뉴얼에 포함)** |
| 1. **ping 응답 확인** |
| * **다시 한 번 DNS spoofing 공격을 하여도 ping 을 보내보면 네이버 주소로 응답것을 확인** |