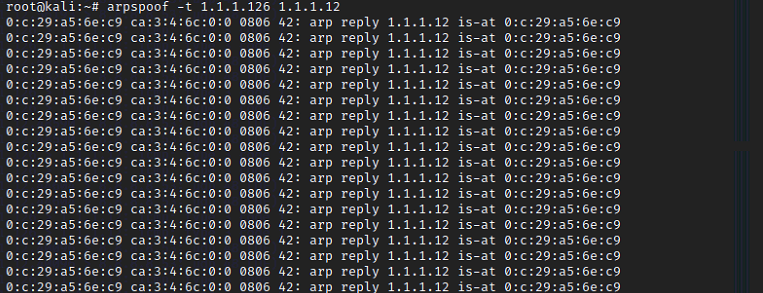
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:신세은 | | |  | |
|  | **Spoofing** | | | | | | |  |
|  | | **-ARP Spoofing-** | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
| 1. **ARP Spoofing 이란?** |
| * **근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법입니다.**   **즉, 자신의 MAC 주소를 다른 컴퓨터의 MAC 주소인 것처럼 속이는 공격입니다.**   * **ARP Cache 정보를 임의로 바꾼다 하여 ‘ARP Cache Poisoning 공격이라고도 합니다.** |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 2. 공격과정 |
| **실습 환경**  **공격 호스트(kali linux): 1.1.1.10 /25**  **타겟 호스트(centos7): 1.1.1.12 /25**  **게이트웨이(라우터): 1.1.1.126** |
| 1. **공격자 PC 에서 arpsoof 프로그램(툴)을 이용해 공격** |
| * **# arpsoof ① [ -i interface] ② [ -t target] ③ host**  1. **-i: 사용할 인터페이스를 지정** 2. **-t: 타깃이 될 대상의 IP 주소** 3. **host: 속일 IP 주소**  * **# arpsoof –i eth0 –t 1.1.1.12 1.1.1.126**      * **타겟 호스트 (1.1.1.12) 에게 게이트웨이(1.1.1.126)의 MAC 주소를 공격자의 MAC 주소라고 계속해서 응답을 보내게 됩니다.** * **정상적인 경우에는 게이트웨이 MAC 응답을 주겠지만 arpsoof 툴을 사용하면 ARP 응답을 속여서 보낼 수 있습니다.** |
| 1. **게이트웨이에도 arpsoof 수행** |

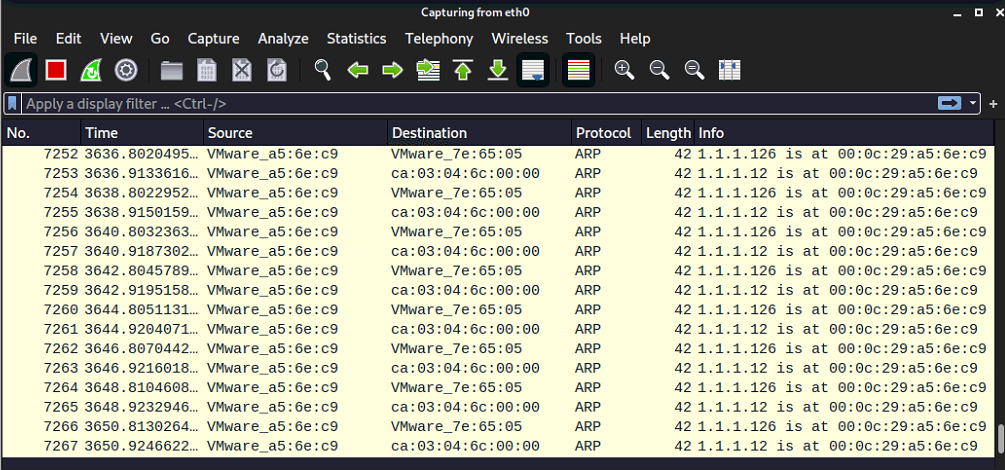
* **arpsoof –t 게이트웨이 피해자IP**
* **# arpsoof –t 1.1.1.126 1.1.1.12**

****

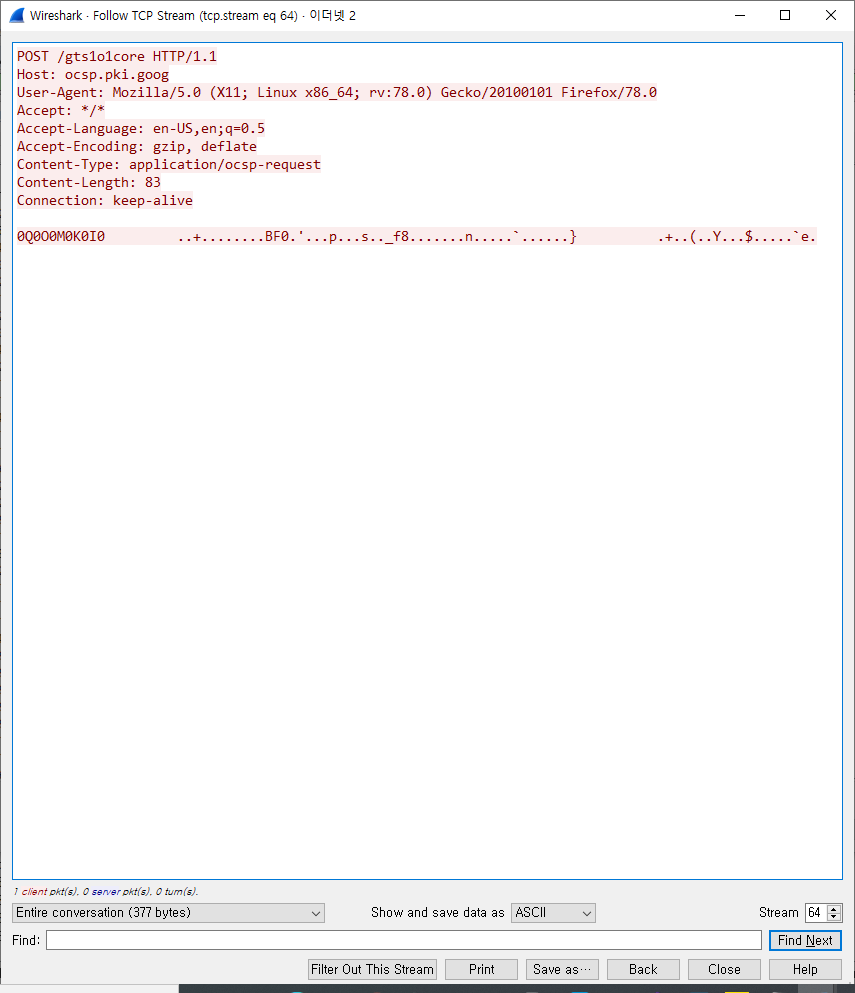
* **게이트웨이 또한 피해자IP 의 MAC 주소가 공격자PC의 주소인 것처럼 계속해서 응답을 보낸다.**

|  |
| --- |
| 1. **TCP dump 수행** |

* **공격자 PC 에서의 wireshak를 통해 패킷분석을 해보면 가짜 mac 주소를 타겟 호스트에게 보내고 있는 것을 확인할 수 있습니다. 즉, 성공적으로 공격이 시행되고 있는 것을 확인할 수 있습니다.**

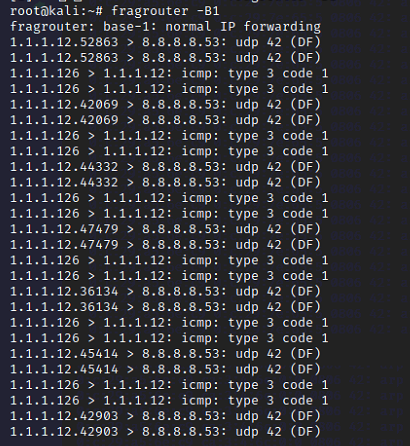
****

* **타겟 호스트에서의 firefox에 접속한 기록 또한 볼 수 있습니다.**



|  |
| --- |
| 1. **Fragrouter** |

* **Fragrouter 명령으로 가로챈 네트워크 패킷을 라우팅 해줍니다.**

****

|  |
| --- |
| 1. **TCP dump 수행** |

* **TCPdump를 이용하여 희생자PC의 패킷을 덤프 뜰 수도 있습니다.**
* **# tcpdump src 1.1.1.12 and port 80**

****

|  |  |  |
| --- | --- | --- |
| 3. 공격 결과 | | |
|  | | |
| 1. **MAC 주소 확인** | | |
| * **ARP Table 확인** * **# arp –a**     **처음 MAC 주소**    **공격 후 MAC 주소**   * **공격을 수행 후 타겟 호스트의 게이트웨이 MAC주소가 공격자의 MAC 주소로 바뀐 것을 확인할 수 있습니다.** | | |
| 1. **패킷 확인** | | |
| * **타겟 호스트 에서의 wireshak를 통해 패킷분석을 해보면 공격자가 가짜 mac 주소를 계속해서 보낸다는것을 확인할 수 있습니다.** * **Wiresha를 통해서도 게이트웨이 MAC 주소가 바뀐 것을 확인할 수 있습니다.** | | |
|  | | |
|  | | |
|  | | |
| 4. 보안진단 및 대책 | |
|  | |
| 1. **타겟 PC의 ARP Cache Table 에서 gatway에 해당하는 MAC 주소를 정적으로 바꿔줍니다.** | |
| * **# arp –s [ip 주소] [MAC 주소]** * **# arp –s 1.1.1.126 ca:03:04:6c:00:00**      * **arp –a 로 확인 결과 설정해준 값으로 바뀐 것을 볼 수 있습니다.** | |
|  |
| 5. 보안대책 적용시 공격결과 |
|  |
| 1. **확인** |
| * **패킷은 계속 해서 날라오지만 arp –a 로 확인 결과 MAC 주소가 바뀌지 않는 것을 확인할 수 있습니다.**      * **# arp –a 로 MAC 주소 확인** |