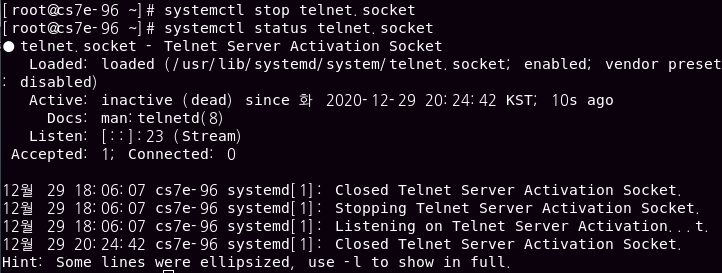
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:신세은 | | |  | |
|  | **Scanning** | | | | | | |  |
|  | | **-Tcp half open scan-** | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
| 1. **TCP Half Open Scan이란?** |
| **피해자**  **공격자**  **피해자**  **공격자**  SYN  SYN  SYN+ACK  RST+ACK  RST  **Port Open**  **Port close**   * **특정 시스템의 포트로 SYN 패킷을 전송해 응답을 기다리는 방법으로,**   **만약, 해당 포트가 접속할 수 있도록 열려 있다면 SYN + ACK 패킷으로 응답하며, 닫힌 상태라면 RST + ACK 패킷으로 응답한다.**   * **TCP SYN 패킷을 이용해 접속을 시도하고 포트가 열려 있는 경우 응답 패킷은 SYN/ACK에 대해 접속을 강제 종료(RST) 해 정상적인 TCP 3-way handshaking 과정을 맺지 않는 스캔 기법이다.** * **스캔하는 대상에 단순히 로그를 남기지 않고, 공격 대상을 속이고 자신의 위치 또한 숨기는 은닉 스캔(Stealth Scan) 기법의 일종이다.** |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) |
| |  | | --- | | 1. **실습환경** |  |  |  |  | | --- | --- | --- | |  | OS | IP | | 공격 호스트 | **Kali Linux** | 1.1.1.10/25 | | 타겟 호스트 | **CentOs7** | 1.1.1.12/25 | |
| 1. **Port Open** |
| **[타겟PC]**  **# systemctl start telnet,socket**    **[공격자PC]**  **# nmap ① –sS ② –p 23 ③ 1.1.1.12**   1. **-sS: 하나의 패킷을 보내어 Syn/Ack 응답을 받으면 그 즉시 RST 패킷을 보내서 접속을 끊어버린다. 즉, 접속이 이루어지지 않은 상태에서 접속을 끊었기 때문에 로그 기록을 남기지 않는다.** 2. **-p: 포트번호** 3. **Target IP**     **CentOs(1.1.1.12) 의 23번 포트를 스캔**  **# wireshark 실행 후, Filter: ip.addr == 1.1.1.12**     * **포트가 열려있을 경우, SYN/ACK 패킷 회신 후 RST 전송** |
| 1. **Port Close** |

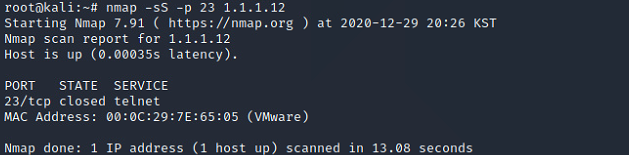
**[타겟PC]**

**# systemctl stop telnet,socket**



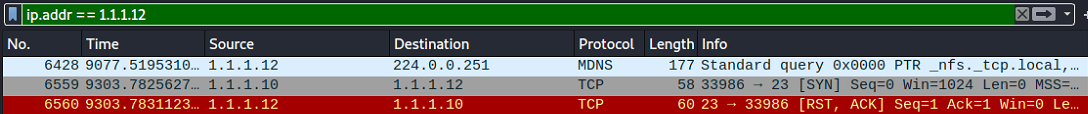
**[공격자PC]**

**# nmap –sS –p 23 1.1.1.12**

****

**CentOs(1.1.1.12) 의 23번 포트를 스캔**

**# wireshark 실행 후, Filter: ip.addr == 1.1.1.12**

****

* **포트가 닫혀있을 경우, RST/ACK 패킷 회신**