|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:문관필 | | |  | |
|  | **Scanning** | | | | | | |  |
|  | | **-XMAS Scan-** | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

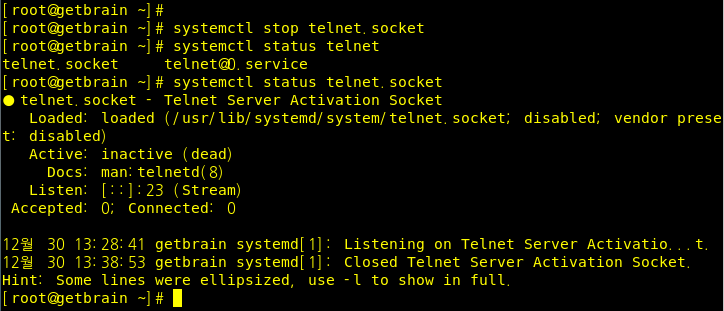
|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
| 1. **X-MAS Scan이란?** |
| **<Port Close>**  **<Port Open>**  피해자  공격자  공격자  피해자  **X-mas**  **X-mas**  **RST**  **응답 없음**   * **TCP 플래그 값을 모두 설정하거나 일부 값을 설정하여 패킷을 보내 스캔** * **여기서 일부 값이란 SYN+FIN 과 같은 말도 안되는 패킷** * **응답이 없으면 Open으로 간주, RST 패킷이 돌아오면 Closed로 간주** * **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** | 192.168.0.102/24 | | 타겟 호스트 | **CentOS 7** | 192.168.0.101/24 | |
| 1. **Port Open** |
| **[타겟PC]**  **# systemctl start telnet.socket**  **# systemctl status telnet.socket**    **[공격자PC]**  **# nmap ① –sX ② –p 23 ③ 192.168.0.101**   1. **-sX : 패킷을 크리스마스 트리처럼 비추는 FIN, PSH 및 URG 플래그를 설정** 2. **-p: 포트번호** 3. **Target IP**     **CentOS(192.168.0.101)의 23번 포트를 스캔**  **# wireshark 실행 후, Filter: ip.addr == 192.168.0.101**     * **포트가 열려 있을 경우, 아무 응답이 없음** |
| 1. **Port Close** |

**[타겟PC]**

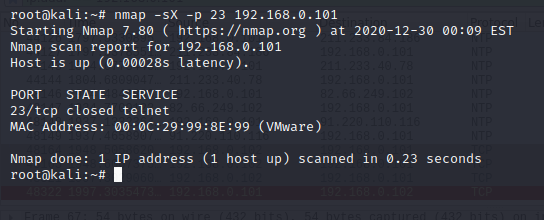
**# systemctl stop telnet.socket**

**# systemctl status telnet.socket**



**[공격자PC]**

**# nmap –sN –p 23 192.168.0.101**

****

**CentOS(192.168.0.101) 의 23번 포트를 스캔**

**# wireshark 실행 후, Filter: ip.addr == 192.168.0.101**

****

* **포트가 닫혀 있을 경우, RST/ACK 패킷 회신**