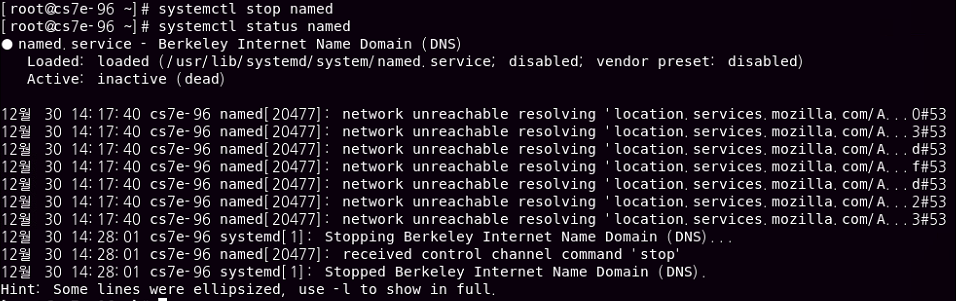
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | **KITRI 모의해킹 28기** | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | **작성:신세은** | | |  | |
|  | **Scanning** | | | | | | |  |
|  | | **-UDP Open Scan-** | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| **1. 개요(공격개념/원리/취약점/공격 시 예상피해 등)** |
|  |
| 1. **UDP Open Scan 이란?** |
| **피해자**  **공격자**  **피해자**  **공격자**  UDP 패킷  UDP 패킷  ICMP Unreachable  응답X  **Port close**  **Port Open**   * **UDP 프로토콜은 TCP와 다르게 핸드쉐이킹 과정이 존재하지 않고, 따라서 일반적으로는 포트가 열려 있다고 하더라도 서버에서 아무런 응답을 하지 않을 수도 있다.**   **하지만, 많은 시스템에서는 보낸 패킷에 대한 응답이 없을 때 ICMP unreachable 메시지를 보낸다.**   * **많은 UDP 스캐너는 이 메시지를 탐지하는 방향으로 동작하며 이 방식은 ICMP 메시지를 보내지 않는 경우 닫혀 있는 포트를 열려 있다고 판단하는 경우가 존재한다.** * **다른 방식으로는 각 포트에 따라서 그에 대응하는 프로토콜 패킷을 전송하는 방식이다.**   **예를 들어, DNS 서버는 53번 포트에서 동작하며, UDP 스캐너는 해당 포트에 DNS 정보 요청 패킷을 보낸 후 응답을 받는 방식이다.**  **이러한 방식은 잘 알려진 포트와 대응 프로토콜에 대해서만 사용할 수 있다는 한계가 있지만, ICMP 메시지가 없는 경우 활용 할 수 있다.** |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| **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 named**    **[공격자PC]**  **# nmap ① –sU ② –p 53 ③ 1.1.1.12**   1. **-sU: UDP 포트 스캔** 2. **-p 53: 포트번호, 도메인 네임 시스템 DNS, 호스트/ 도메인명과 IP 주소 사이의 대화를 위한 보안이 안 된 시스템** 3. **Target IP**     **CentOs(1.1.1.12)의 53번 포트를 스캔**  **# wireshark 실행 후, Filter: ip.addr == 1.1.1.12**     * **포트가 열려있을 경우, UDP 패킷 전송 후, 응답 없음** |
| 1. **Port Close** |

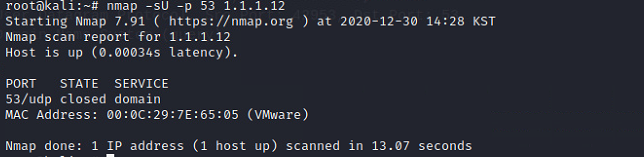
**[타겟PC]**

**# systemctl stop named**

****

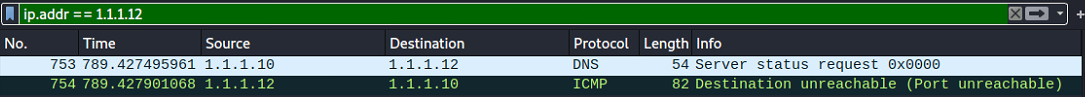
**[공격자PC]**

**# nmap –sU –p 53 1.1.1.12**

****

**CentOs(1.1.1.12) 의 53번 포트를 스캔**

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

****

* **포트가 닫혀있을 경우, UDP 패킷 전송 후, ICMP Destination Unreachable 회신**

**(데몬이 아닌 운영체제가 ICMP Unreachable 회신을 함)**