|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | **KITRI 모의해킹 28기** | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | **작성:신세은** | | |  | |
|  | **Scanning** | | | | | | |  |
|  | | **-arp scan-** | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| **1. 개요(공격개념/원리/취약점/공격 시 예상피해 등)** |
|  |
| **ARP Scan** |
| * **Arp 프로토콜을 이용해서 네트워크 대역의 정보를 확인한다**   **예를 들어, 같은 네트워크 대역에서 ARP Request를 보내면 살아있는 host는 ARP Reply로 응답하게 되고 공격자는 타깃 PC의 존재 유무를 알 수 있게 된다.**   * **ICMP는 보안 문제상 막을 수 있지만 ARP는 막아버리면 통신이 안되기 때문에 막아 놓을 수 없다** * **ARP 프로토콜의 한계는 라우터를 넘지 않기 때문에(2계층 프로토콜이기 때문에) 같은 네트워크의 정보만 알 수 있다.** |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| **2. 공격과정** |
| **실습환경**  **공격호스트(Kali linux): 1.1.1.10/25**  **타겟 호스트(CentOS7): 1.1.1.12/25** |
| 1. **Arp-scan 툴 설치** |
| * **arp-sacn 설치** * **# apt-get install arp-sacn** |
| 1. **arp -Scan** |

* **# arp-scan ① –I etho0 ② –l**
  1. **Interface or –I: 네트워크 인터페이스 사용**
  2. **localnet or –l: 네트워크 인터페이스 설정에서 주소를 생성**

****

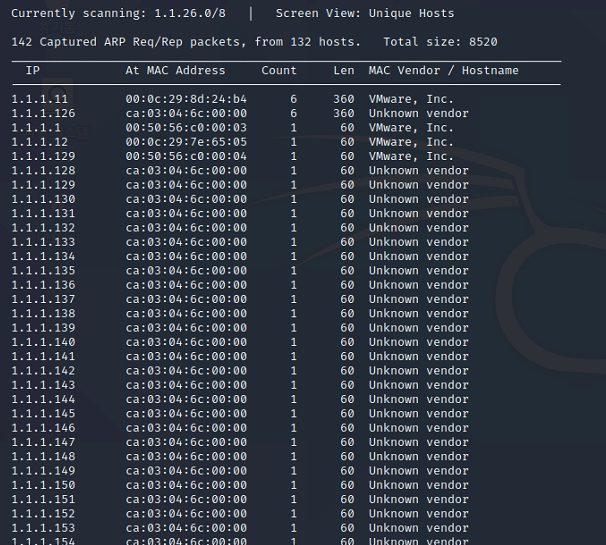
|  |
| --- |
| 1. **netdiscover 툴 설치** |

* **# apt-get install netdiscover**

****

|  |
| --- |
| 1. **Netdiscover- Scan** |

* **네트워크 대역대 확인**
* **# netdiscover –r 1.1.1.10/8**

****