|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:김홍규 | | |  | |
|  | **Scanning** | | | | | | |  |
|  | | **-decoy scan-** | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
| 1. **Decoy Scan이란?** |
| **﻿다른 컴퓨터를 스캔할 때 공격자 IP를 숨기길 원한다.**  **﻿명백하게, 모든 패킷은 source address를 포함하고 있어야만 한다. 그렇지 않으면 대상 시스템에서 응답이 어디에 돌아가는지 알 수가 없다.**  **Nmap을 사용하여 IP를 spoofing할 때 -S를 통해 IP 주소를 spoof 할 수 있지만 그 결과로 얻고자 하는 어떠한 응답이나 정보는 spoof된 IP로 돌아 감**  **🡪 정보수집에 있어서 유용하지 않음**  **따라서, 공격자 IP주소를 알아채지 못하게 만들어야 한다.**  **🡪 공격자 IP를 다른 IP들 속에 숨겨서 네트워크나 보안 관리자가 스캔의 주체를 알아채지 못하게 한다**  **Nmap은 decoy IP 주소 사용을 통해 마치 다수의 IP가 타겟을 스캐닝하고 있는 것처럼 보이게 한다.**  **-D switch 사용을 통해 할수 있다** |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) |
| |  | | --- | | 1. **실습환경** |  |  |  |  | | --- | --- | --- | |  | OS | IP | | 공격 호스트 | **Kali Linux** | 1.1.1.201/24 | | 타겟 호스트 | **CentOs7** | 1.1.1.202/24 | |
| 1. **실습** |
| **[타겟PC]**   |  |  |  | | --- | --- | --- | | SERVICE | STATE | PORT | | ssh | **open** | 22/tcp | | http | **closed** | 80/tcp |   **# systemctl start sshd**    **# systemctl stop telnet**    **[공격자PC]**  **# nmap ①-T4 ②-sS ③-p 22, 80 ④1.1.1.202 ⑤-D ⑥10.10.10.1, 10.10.10.2, 10.10.10.3**   1. **-T4 : 속도 옵션(T0~T4), T4 (Aggressive : 가장 빠름), T0 (Paranoid : 가장 느림)** 2. **-sS: TCP half Scan** 3. **-p: 포트번호** 4. **Target IP** 5. **-D : 지정된 여러 decoy들로부터 패킷이 유입되는 걸로 위장함 (-sV 에서 사용할 수 없음)** 6. **decoy IP**     **# wireshark 실행 후, Filter: ip.addr == 1.1.1.202**     * **1.1.1.201 -> 1.1.1.202 SSH(tcp/22) SYN 요청 패킷 전송 외에도**   **연속적으로(대략 0.0001초 단위로 이어져서)**  **10.10.10.1, 10.10.10.2, 10.10.10.3 를 Source로 하는**  10.10.10.1 -> 1.1.1.202 SSH(tcp/22) SYN  10.10.10.2 -> 1.1.1.202 SSH(tcp/22) SYN  10.10.10.3 -> 1.1.1.202 SSH(tcp/22) SYN  **위조된 IP로 스캔이 수행된다**   * **1.1.1.201 -> 1.1.1.202 HTTP(tcp/80) SYN 요청 패킷 전송 외에도**   **연속적으로(대략 0.0001초 단위로 이어져서)**  **10.10.10.1, 10.10.10.2 를 Source로 하는**  10.10.10.1 -> 1.1.1.202 SSH(tcp/22) SYN  10.10.10.2 -> 1.1.1.202 SSH(tcp/22) SYN  10.10.10.3 -> 1.1.1.202 SSH(tcp/22) SYN  **위조된 IP로 스캔이 수행됨을 확인할 수 있다.** |