P.O.D

by: c3c / c3c.fr

Brief

- Professional Offensive Operations is a long name in the cyber security world.

Little Bobby Tables is nothing into hacking, but we are very happy to welcome a cousin of the pro-hacker family, Little Bobby Tables Enterprise Edition.

P.O.D. is designed to put your skills in practice in a realistic internal network and corresponds to a pentest on the certification level of OSCP. Many vulnerabilities are spread across various services, misconfigurations, weak passwords and technologies.

The goal is to compromise the domain hard, escalate privileges and ultimately compromise the domain controller while avoiding some flags along the way.

Scanning

We are interested in highlight the available TCP and UDP ports.

```
root@kali:~# nmap -sV -sC -p- -vvv -oN nmap/pod.tcp 10.10.10.240
```

We then can change to exploitation the moment we have, nmap -sV -sC -p- -T4 -vvv -oN

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-17 01:47 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 01:47
Completed NSE at 01:47, 0.00s elapsed
Initiating NSE at 01:47
Completed NSE at 01:47, 0.00s elapsed
Initiating NSE at 01:47
Completed NSE at 01:47, 0.00s elapsed
Initiating Ping Scan at 01:47
Scanning 10.10.10.240 [4 ports]
Completed Ping Scan at 01:47, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:47
Completed Parallel DNS resolution of 1 host. at 01:47, 0.13s elapsed
DNS resolution of 1 IPs took 0.13s. Mode: Sequential.
Nmap scan report for 10.10.10.240
Hostname resolution disabled
Initiating Connect Scan at 01:47
Scanning 10.10.10.240 [65535 ports]
Discovered open port 135/tcp on 10.10.10.240
Discovered open port 445/tcp on 10.10.10.240
Discovered open port 1433/tcp on 10.10.10.240
Discovered open port 5985/tcp on 10.10.10.240
Discovered open port 49152/tcp on 10.10.10.240
Discovered open port 49153/tcp on 10.10.10.240
Discovered open port 49154/tcp on 10.10.10.240
Discovered open port 49155/tcp on 10.10.10.240
Discovered open port 49156/tcp on 10.10.10.240
Discovered open port 49157/tcp on 10.10.10.240
Connect Scan Ignoring error 101 (Network unreachable) for 10.10.10.240:47001
```