|  |  |
| --- | --- |
| **Ex. No. 3** | **NMAP** |
| **Date of Exercise** | 29/08/23 |

**Aim:**

The objective of this experiment is to:

• Perform a system and network scan

• Enumerate user accounts

• Execute remote penetration

• Gather information about local network computers

**Description:**

NMAP is an essential tool in any hacker's arsenal. Originally written by Gordon Lyon aka Fydor, it's used to locate hosts and services and create a map of the network. NMAP has always been an incredibly powerful tool, but with its newest release, which dropped mid-November of last year, they've really out done themselves.

NMAP version 7 comes equipped with a ton of new scripts you can use to do everything from DoSing targets to exploiting them (with written permission, of course). The scripts cover the following categories

Auth: Use to test whether you can bypass authentication mechanism

Broadcast: Use to find other hosts on the network and automatically add them to scanning que.

Brute: Use for brute password guessing.

Discovery: Use to discover more about the network.

Dos: Use to test whether a target is vulnerable to DoS.

Exploit: Use to actively exploit a vulnerability.

Fuzzer: Use to test how server responds to unexpected or randomized fields in packets and determine other potential vulnerabilities.

Intrusive: Use to perform more intense scans that pose a much higher risk of being detected by admins.

Malware: Use to test target for presence of malware.

Safe: Use to perform general network security scan that's less likely to alarm remote

Administrators.

Vuln: Use to find vulnerabilities on the target.

**Output:**

Run NMAP

When scanning devices to determine which ports are open, there are various basic scanning options:

-sS –Performs a “stealth” TCP scan (that does not fully complete the “TCP three-way

handshake,” and closes the connection once the service responds).

-sT –Performs a full TCP scan (a full connection is established with open TCP ports).

-sU –Performs a UDP scan (as UDP is a connectionless protocol, these scans can take

significantly longer than TCP scans).

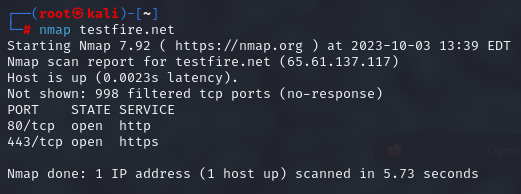
-p – Tells Nmap which ports to scan (e.g., –p1-65535 will specify every port).

There is an entire category of scripts dedicated to finding vulnerabilities on a target. Invoking the following command will run all of the scripts against your target.

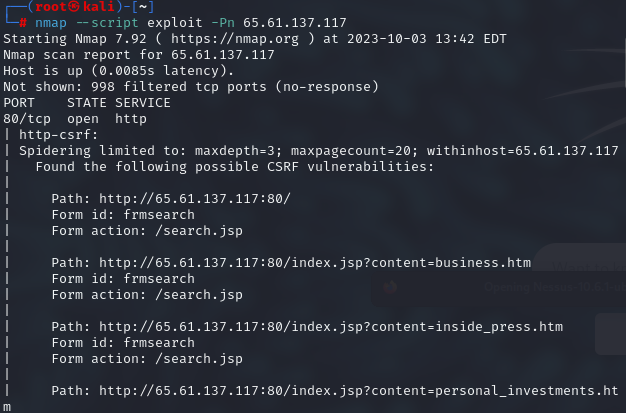
nmap -Pn --script vuln <target.com or ip> <enter>

Use NMAP to Actively Exploit Detected Vulnerabilities

As mentioned, you can also use NMAP's exploit script category to have NMAP actively exploit detected vulnerabilities by issuing the following command:



nmap --script exploit -Pn <target.com or ip> <enter>



**Use NMAP to Brute Force Passwords**

Nmap contains scripts for brute forcing dozens of protocols, including http-brute, oracle-brute, snmp- brute, etc. Use the following command to perform brute force attacks to guess authentication credentials of a remote server.

nmap --script brute -Pn <target.com or ip> <enter>



**Use NMAP to Test if Target Is Vulnerable to Dos**

Use the following command to check whether the target is vulnerable to DoS:

nmap --script dos -Pn <target.com or ip> <enter>

This will tell you whether the target is vulnerable without actually launching a dos attack.

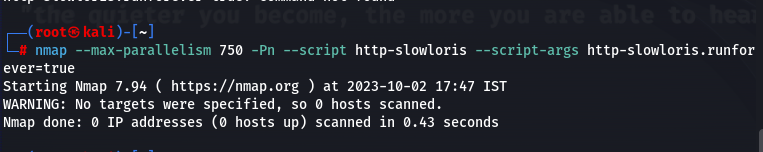
A computer screen with white text

Description automatically generated100

Use the following command to perform an active DoS attack against a target for an indefinite period of time:

nmap --max-parallelism 750 -Pn --script http-slowloris --script-args http-

slowloris.runforever=true



A screen shot of a computer

Description automatically generated

**Result:**

The objective of scanning network, remote penetration and gathering information about local network computers is successfully accomplished using NMAP tool in Kali Linus.