

Forum:[Hack Forums](#)

Thread: [Automate Nmap Scans](#)

IMMORTALITY - November 29, 2023, 7:11 pm

This tutorial assumes that you have a basic understanding of Python and Nmap. You should be familiar with the following concepts:

Python programming syntax

Nmap command-line options

Networking concepts such as IP addresses, ports, and protocols

Installing Python-Nmap

Python-Nmap is a Python module that provides a Python API for Nmap. To install Python-Nmap, you can use the following command:

Code `pip install python-nmap` Scanning a Network

The most basic Nmap scan is a ping scan, which simply checks whether a host is alive or not. To perform a ping scan with Python-Nmap, you can use the following code:

This code will scan all hosts in the subnet 192.168.1.0/24 and print the hostname and status of each host:

Code `import nmap`

```
nm = nmap.PortScanner()
scan_results = nm.scan('192.168.1.0/24')
```

```
for host in scan_results['all_hosts']:
    print(host['hostname'], host['status'])
```

Scanning for Open Ports:

To scan for open ports on a host, you can use the following code:

Code `import nmap`

```
nm = nmap.PortScanner()
scan_results = nm.scan('192.168.1.100', arguments='-sS -T8')
```

```
for host in scan_results['all_hosts']:
    for port in scan_results['all_hosts'][host]['ports']:
        print(host['hostname'], port['port'], port['state'], port['service'])
```

This code will scan host 192.168.1.100 for open ports using a SYN scan (-sS depending on your distro) and adds timeout of eight seconds (-T4). It will then print the hostname, port number, port state, and service name for each open port.

Using Nmap Scripting Engine (NSE) Scripts

(NSE) is a powerful tool that allows you to write scripts to extend the functionality of Nmap. You can

use NSE scripts to perform a variety of tasks, such as vulnerability scanning, version detection, and OS identification.

To use an NSE script with Python-Nmap, you can use the following code:

Code import nmap

```
nm = nmap.PortScanner()  
scan_results = nm.scan('192.168.1.100', arguments='--script=http-vuln')
```

```
for host in scan_results['all_hosts']:  
    for script in scan_results['all_hosts'][host]['scripts']:  
        print(host['hostname'], script['id'], script['name'], script['output'])
```

This code will scan host 192.168.1.100 using the NSE script http-vuln. It will then print the hostname, script ID, script name, and script output for each script that was executed.

Replace as you see fit to automate the regular tasks that you would typically use nmap for when testing websites for SQL injection and/or any other type of security flaw that it can aid in penetrating. This is for educational purposes only to be used on your own virtual box and I do not condone any illicit port scanning without prior permission from the device user.

blgtsc - February 8, 2024, 9:17 pm

i neded this tutorial thx