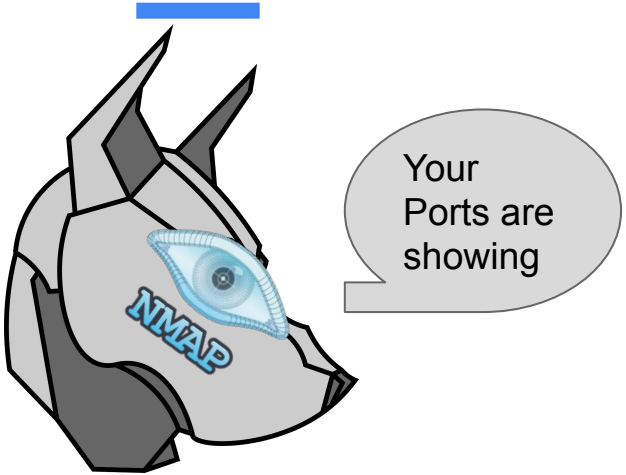
Cyber Defense Organization

Spring 2020 - NMAP



WORD OF THE WEEK: PORT KNOCKING

What is Port Knocking

- A way to keep a port closed unless specific condition is met
- Knock on a sequence of ports in order to open the correct port
- Defense against Nmap
- Cool article: https://www.the-art-of-web.com/system/port-knocking-knockd/

What is NMAP???

- Short for network mapper
- Used for network discovery, network assessment
- Some call it a port scanner but it can do WAY more than just that!
- Nmap can also work on Mac and Windows but we will be using Kali today

History of NMAP

- Originally released as a Linux-only port scanner in 1997
- Created by Gordon Lyon
- Originally written in C++ but changed to Python layer for Windows compatibility
- Unlike other older tools NMAP has been under constant development since release

In Simple Terms What Can It do?

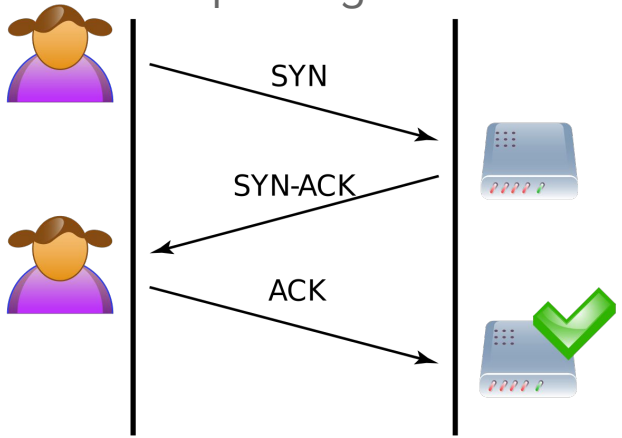
- Tells you what ports are open on a given server/Website.
- What services are running on these ports.
- What version of the service is running.
- The operating system of the target.
- Even the MAC address of the target.
- What type of packet filtering firewalls are being used.
- Powerful scripting usability to even automate all of this!

NMAP vs ZENMAP

- NMAP is command line
- ZENMAP is GUI based

Privileged vs Unprivileged users

- Root = Raw SYN stealth scanning
- Unprivileged = TCP connect scan (full connect scan)
- This means that as a privileged user you only have to complete a SYN,SYN-ACK in order to see the open ports
- An unprivileged user is required to complete all three steps in order to scan
- The benefit of only doing two is being less likely to show up in logs of the person you are scanning and speed.



Basic Commands

- Nmap *target*

```
kali@kali:~$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-04 17:01 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (1.2s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 106.74 seconds
```

Target specification

- Multiple targets
- Website names
- CIDR notation (/24)

```
root@kali:/home/kali# nmap 192.168.1.1-3
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-04 22:48 UTC
Nmap scan report for 192.168.1.1
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap scan report for 192.168.1.2
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.1.2 are filtered

Nmap scan report for 192.168.1.3
Host is up (1.0s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
16113/tcp open  unknown

Nmap done: 3 IP addresses (3 hosts up) scanned in 55.87 seconds
root@kali:/home/kali#
```

Command variations

- -O = OS detection
- -sS = stealth scan
- -vv = shows the scanning process live
- -D = send scans from a spoofed ip
- -iL = scan the targets listed in a file
- -oN = put the output in a file

Let's play!

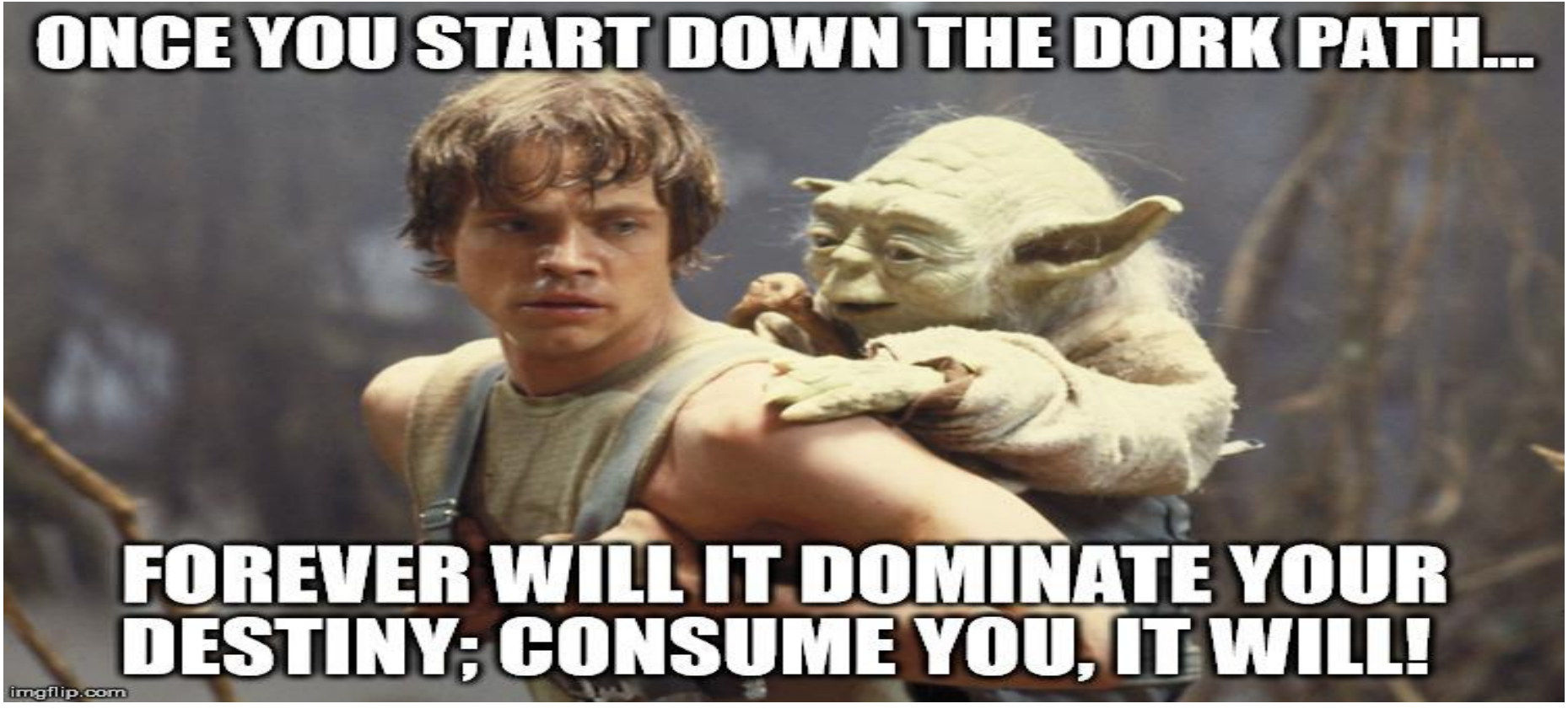
https://tinyurl.com/nmapcdolab

Below is also a great cheat sheet for commands!

https://www.stationx.net/nmap-cheat-sheet/

Or just type nmap -h for a manual

Next Week: Google Dorking



Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!