Discovering Live Hosts and Open Ports

Dale Meredith

MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

“Give me a ping, Vasili. One ping only please.”

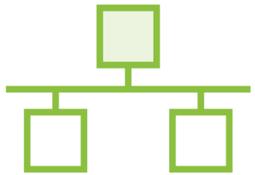
The Hunt for Red October

Demo

Angry IP Scanner

Your New Best Friend: Nmap

Your New Best Friend Nmap



-p <port range> = scan a specific port

-r = scan ports consecutively

--top-ports <a number> = scans the top # of ports

Your New Best Friend Nmap

-6 = IPv6

-iL <input filename> = scans the hosts listed in a file

-R = Try to resolve DNS names using reverse DNS lookup

Your New Best Friend Nmap

-O = Try to resolve the operating system of the target(s)

-A = enable OS detection, service versions, script scanning and traceroute

--script = <scriptname> = use an NSE script

Your New Best Friend Nmap

-sC = Scan using all the default scripts

-v = Increase verbosity of the output (-vv, -vvv)

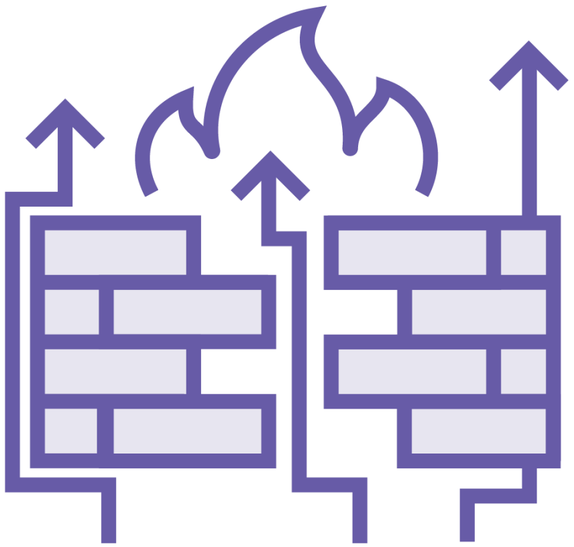
-oN / -oX / -oS / -oG / -oA <filename> save the output in various formats

Demo

Hping3

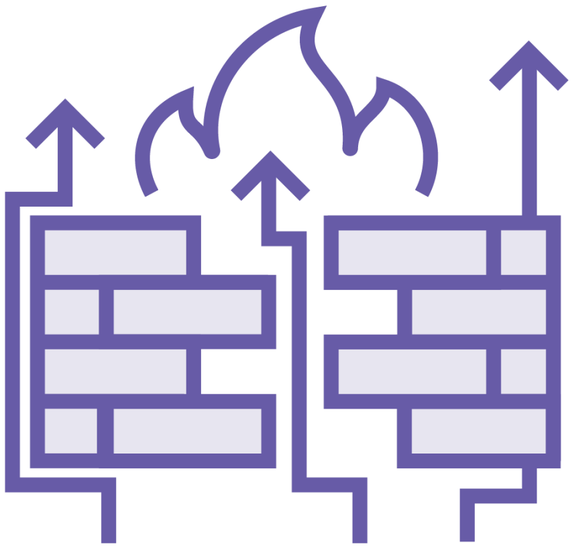
What is Firewalking?

What is Firewalking?



Determines whether or not a particular packet can pass from the attacker's system to the target via a packet-filtering device

What is Firewalking?



Identifies the firewall's access control list (ACL)

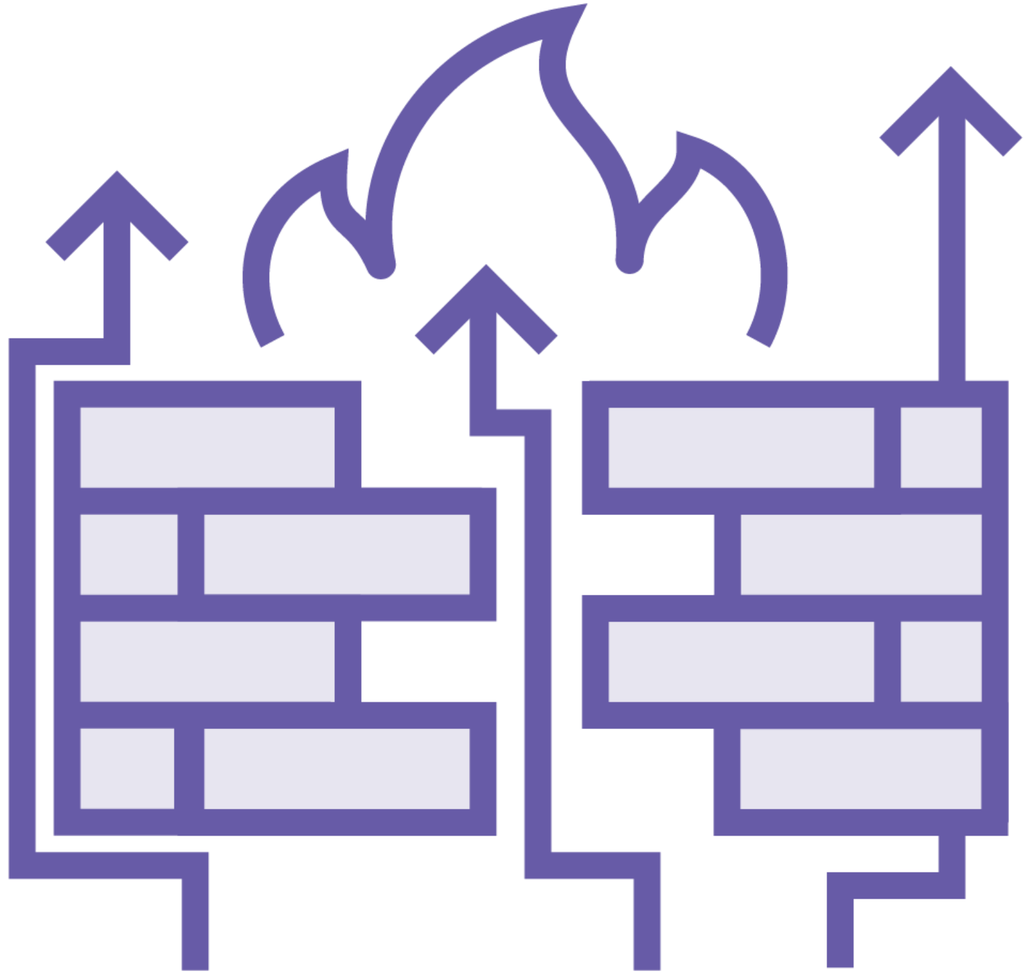
Traceroute

A traceroute provides a map of how data on the internet travels from your computer to its destination.

Utilizes a TTL (time-to-live).

TTL exceeded in transit

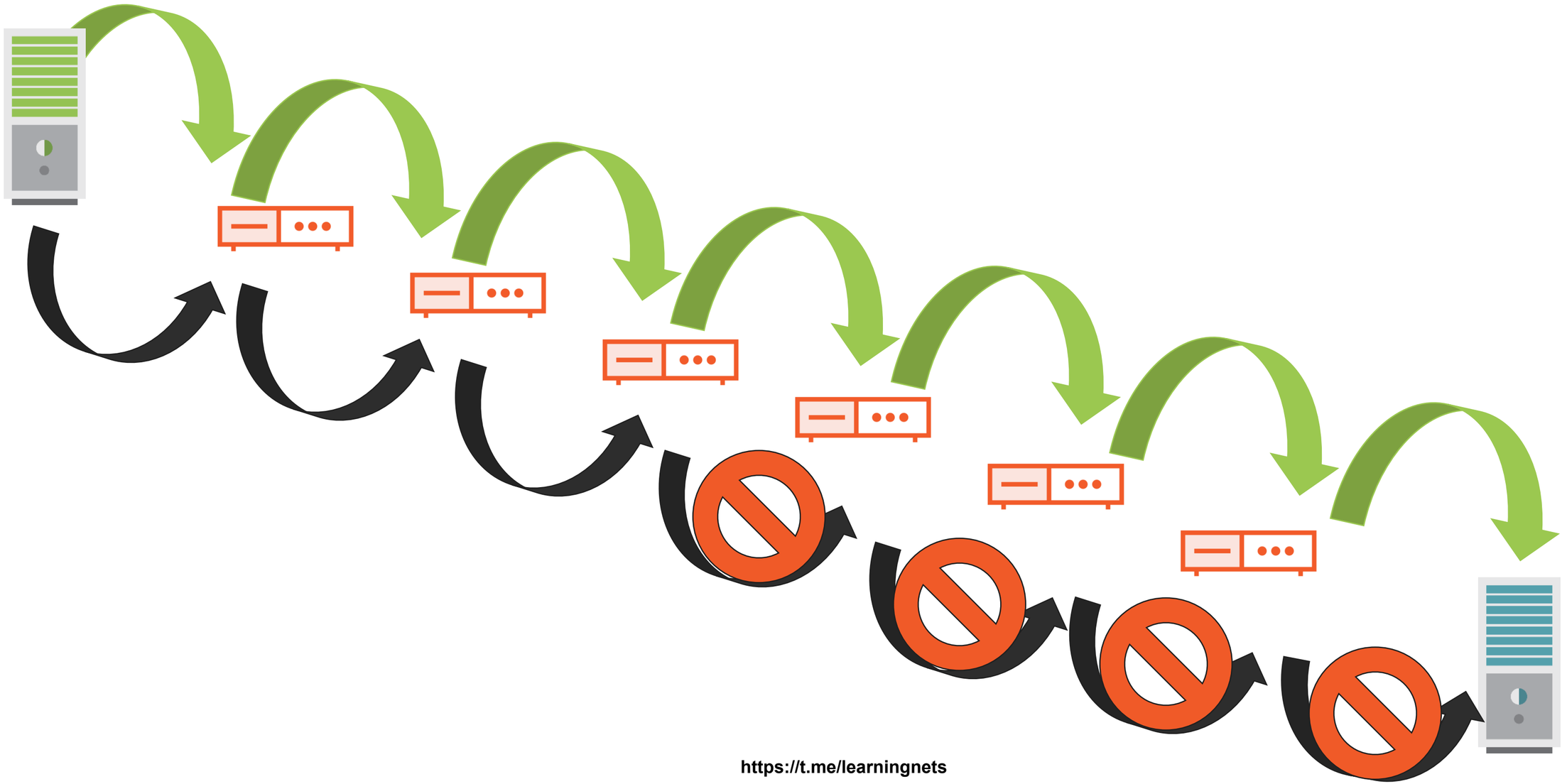
https://www.fortinet.com/resources/cyberglossary/traceroutes



Forwarded if the port is open

Dropped if the port is closed

Never Give Up



Examining a Firewalk

Standard Traceroute

```
traceroute 192.168.0.10

traceroute to 192.168.0.10(192.168.0.10), 30 hops max, 40 byte packets

1 192.168.0.1 (192.168.0.1) 0.540 ms 0.394 ms 0.397 ms

2 192.168.0.2 (192.168.0.2) 2.455 ms 2.479 ms 2.512 ms

3 192.168.0.3 (192.168.0.3) 4.812 ms 4.780 ms 4.747 ms

4 * * *

5 * * *
```

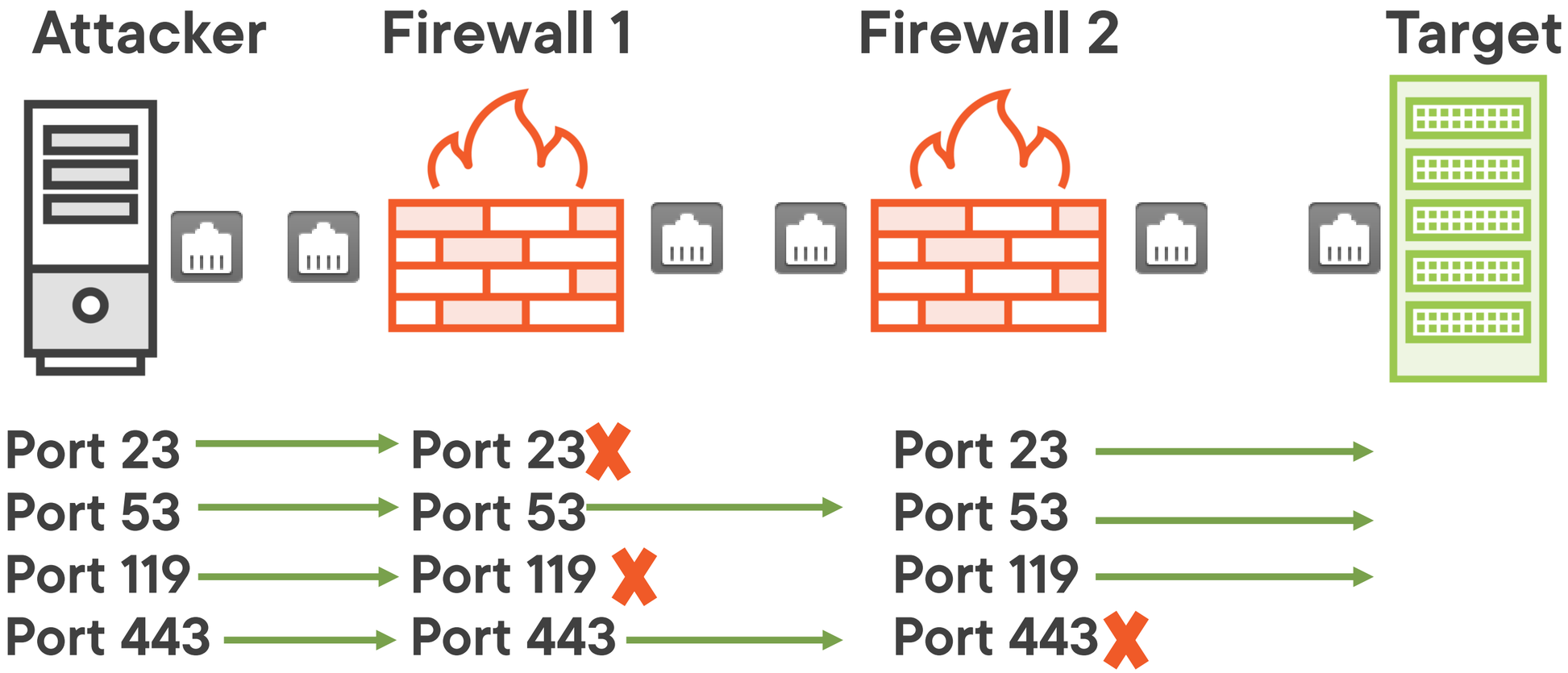
Standard Traceroute (Add a Port)

```
traceroute -p53 192.168.0.10

traceroute to 192.168.0.10(192.168.0.10), 30 hops max, 40 byte packets

1 192.168.0.1 (192.168.0.1) 0.540 ms 0.394 ms 0.397 ms

2 192.168.0.2 (192.168.0.2) 2.455 ms 2.479 ms 2.512 ms

3 192.168.0.3 (192.168.0.3) 4.812 ms 4.780 ms 4.747 ms

4 192.168.0.4 (192.168.0.4) 5.342 ms 5.304   ms 5.283 ms

5 * * *
```

Firewalk

```
firewalk -s20-100 -i eth0 -n -pTCP 192.168.0.254 192.168.0.10

Scanning Phase:
port 52: *no response*
port 53: A! open (port not listen) [192.168.0.1]
port 54: *no response*
```

Thus, You Can Firewalk Beyond



Learning Check

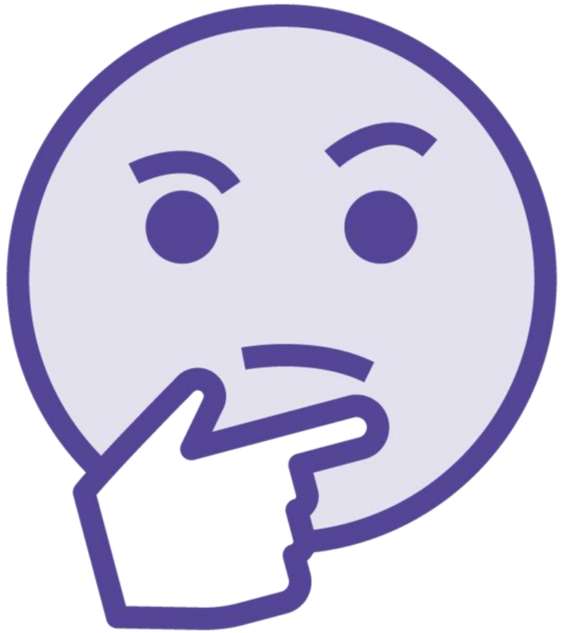
Learning Check

-p

AngryIP Scanner

-O

Firewalking



Next Up:

Utilizing Banner Grabbing and OS Fingerprinting