Understanding Nmap by using hping

Lotus Eater Follow
Jul 8, 2018 · 4 min read

Nmap: the Network Mapper - Free Security Scanner

Nmap Free Security Scanner, Port Scanner, & Network Exploration Tool. Download open source software for Linux, Windows...

nmap.org

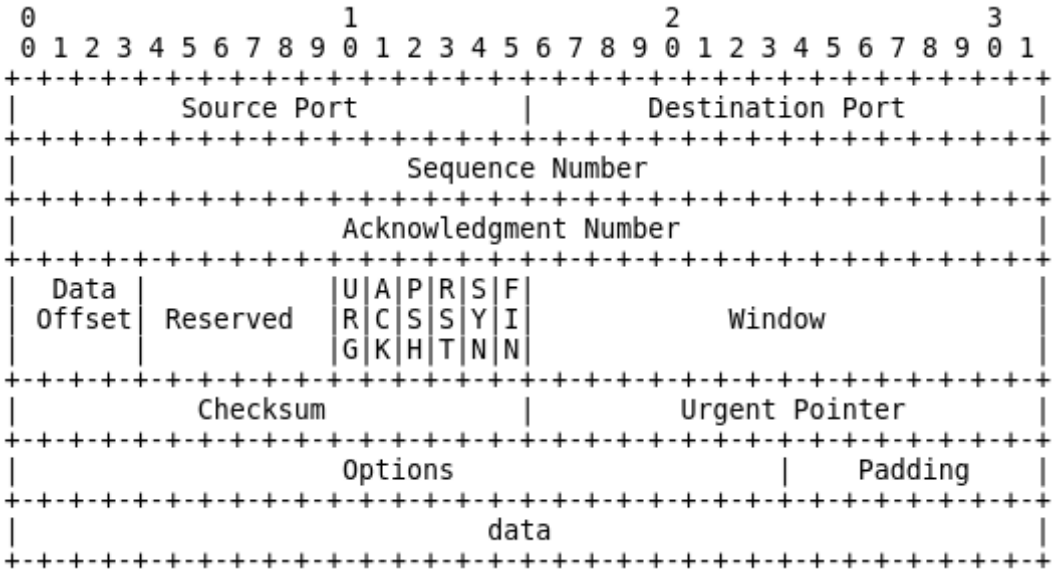
Nmap is essential in any pentester's toolkit. A versatile open-source utility that takes full advantage of scan automation. To fully understand this tool we will dive into packet crafting tool **hping**, another great tool that allows us to set specific control flags.

. . .

Make sure you also have a packet sniffer open so you can visualize the the layers of the OSI. Wireshark is another great utility used for packet analysis.

Transmission Control Protocol Breakdown

Each TCP packet has a section in it's memory buffer where Control Bits such as URG | ACK | PSH | RST | SYN | FIN can be set.



Model of TCP Packet https://tools.ietf.org/html/rfc793#section-3.1

The beauty in hping resides in it's full control of which of these packets can be set in the request.

First, let's find which hosts are alive :

```
hping : hping -S <address block>
Nmap : nmap -sS <address block>
fping : fping -a -g <address block>
```

hping

-S : Sets the SYN flag getting passed onto the packet

nmap

-sS : SYN flag scan

-sn: ICMP ECHO scan

. . .

It’s important to know how networks respond against probes. In the modern network configurations we see today ICMP Echo ping requests are usually blocked or filtered. The great thing about SYN request is that it partly completes the three-way-handshake. Let’s look at an example.

Sending ICMP Echo requests to host that blocks them

Sending SYN Packets to host on a port

As you can see ICMP Echo request is not a reliable way to determine if a certain ports are alive. In the Hping replies you can see that the flags that are set in the return are set to **SA (SYN and ACK)**. To minimize the noise on this network we don't send an **ACK** back to complete the handshake.

Nmap can also automate this for us too.

```
nmap -sS <ip address>
```

Wireshark capture for nmap syn request

In this case, Nmap sprays the ip address sending SYN packets to see if any SYN ACK request respond back. It's similar to how hping gets a reply for

SYN-ACK. Nmap packages up this information it receives and gives us a table of which ports are open due to the SA packets.

Nmap table

But what happens in the case that the firewall has a configuration that detects malicious SYN packets? If the goal is avoiding detection, spraying the host for certain ports is going to make a lot of noise. We want to minimize the amount of noise we make towards detection systems.

Let's take a step back and think about the scope of how advanced these detection systems are in world today. If you are at all familiar with conferences likeDefCon or BlackHat, all the detection systems you are

trying to avoid are of the thousands of third party software vendors at these events. By no means these tactics are silver bullets for avoidance but it should be the bare minimum.

SOC Analysts be like

NULL Scan and XMAS Scan

So let's take it one level deeper. Introducing the XMAS (Christmas scan).

```
hping -F -P -U <ip address> -c <number of packets>
```

In this particular request the flags that are set are : **FIN** | **PSH** | **URG**. Let's use this against a port we know that is open from our previous scans to see how it works.

Hping with flags set for Xmas for port 445

We get no response back which means the packet was discarded and the port was open.

If it sends us back a RST flag then we know that is port is closed. The Null scan is a lot similar to the Xmas scan but the it has no flags set at all. The response procedure is going to be the same.

> Open : No response | Closed : RST response

Nmap Implementation :

```
-sX (Xmas scan)
-sN (Null scan)
```

This loophole dates back to the TCP RFC, it explains that if a packet does not contain a RST, it results in a RST sent back as a response. When a packet is sent without a SYN | RST | ACK flag, they are discarded.

These loopholes not only provide a pivotal scanning mechanism for open ports but also exemplify why it is important to understand how these

protocols work in essence. As Pentesters, you learn how to use them, but it is important to understand how to modify and exploit these lower level modules of TCP/IP to cater for your testing environment.

Networking Cybersecurity

WRITTEN BY

Lotus Eater

Web Security Professional | Developer | Hacking the WWW

Follow

Write the first response

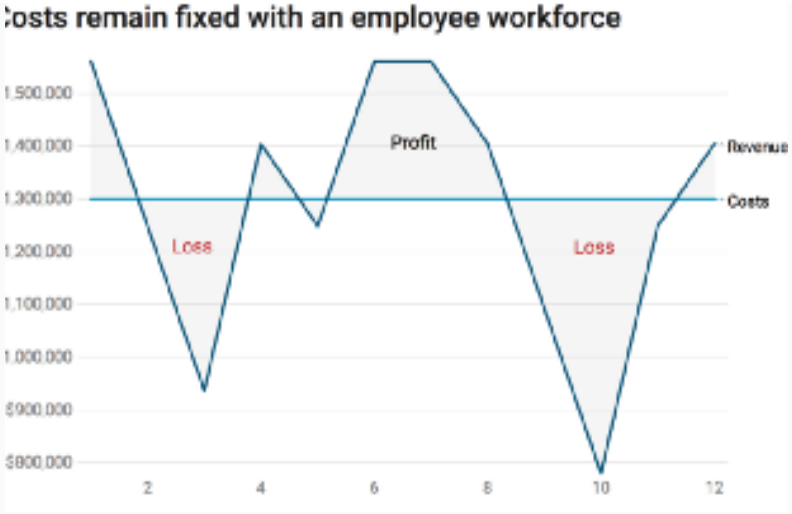
More From Medium

Related reads

CFO Series: The 3 Mistakes That Crushed Zirtual Overnight

Teampay
Aug 2, 2018 · 8 min read

94



Related reads

How to Hire the Right People for your Startup

Alison Lee
Nov 19, 2018 · 7 min read

110

Related reads

Captain Alien's guide to Super-Massive Data Structures

Eric Botcher
Apr 29 · 8 min read ★

50