Intrusion Detection Level Analysis of Nmap and Queso

by Toby Miller

last updated Wednesday, August 30, 2000

1.1 INTRODUCTION

The purpose of this paper is to help Intrusion detection analysts and firewall administrators identify NI This paper will provide bit level analysis in detecting NMAP and QUESO scans. This type of analysis who are performing firewall administration and need to understand more details relating to these scar perform.

1.2 BACKGROUND

A port scanner is a tool used by both system administrators and attacker(s) to identify vulnerabilities i Port scanners identify vulnerabilities by sending normal and abnormal packets to computer ports and to determine what port(s) are 'open'. From this data, a system administrator, or an attacker, can deter be patched or what holes can be exploited.

There are several different types of port scanners. There are free port scanners such as NMAP and C scanners allow for a lot of flexibility in scanning for vulnerabilities. There are commercial scanners ava your company requires a licensed product. A comparison of commercial scanners vs. free scanners is this paper.

1.3 NMAP AND QUESO 1.3.1 NMAP

NMAP is a freely distributed port scanner developed and maintained by Fyodor (www.insecure.org). N variety of operating systems such as Linux, FreeBSD, Open BSD, Solaris and even NT (thanks to eE probably the most popular freely available scanner on the Internet. Because of its ease of use, it can from a novice to an expert. Since NMAP is so easy to use and is ported to almost every available ope one question: how do we (IDS & Firewall community) detect NMAP?

Detecting NMAP is not an easy task to do. NMAP has many switches available for a person to use - c and its option's are beyond the scope of this paper. For the purpose of explanation, the following swit of the selected switches will be described in detail later):

```
-sS  This switch performs a SYN scan.
-sX  This switch performs XMAS scan.
-sF  This switch performs a Fin scan.
-O This switch performs Operating System detection.
```

Figure 1 (below) shows the -sS scan along with a couple of common signatures associated with NMA

```
12:19:04.981033 attacker.com > victim.com: icmp: echo request (ttl 40, id 28524)
                        4500 001c 6f6c 0000 2801 2573 xxxx xxxx
                        xxxx xxxx 0800 e152 16ad 0000
12:19:04.981207 victim.com > attacker.com: icmp: echo reply (ttl 255, id 0)
                        4500 001c 0000 0000 ff01 bdde xxxx xxxx
                        xxxx xxxx 0000 e952 16ad 0000
12:19:04.981574 attacker.com.58397 > victim.com.www: . ack 0 win 3072 (ttl 54,
id 47895)
                        4500 0028 bb17 0000 3606 cbb6 xxxx xxxx
                        xxxx xxxx e41d 0050 5720 0003 0000 0000
```

```
                        5010 0c00 6a41 0000
12:19:04.981687 victim.com.www > attacker.com.58397: R 0:0(0) win 0 (ttl 255, id
                        4500 0028 0001 0000 ff06 bdcc xxxx xxxx
                        xxxx xxxx 0050 e41d 0000 0000 0000 0000
                        5004 0000 cd70 0000
12:19:05.065741 attacker.com.58377 > victim.com.1531: S 1899041970:1899041970(0)
id 22525)
                        4500 0028 57fd 0000 3606 2ed1 xxxx xxxx
                        xxxx xxxx e409 05fb 7131 14b2 0000 0000
                        5002 0c00 35f8 0000
12:19:05.065924 victim.com.1531 > attacker.com.58377: R 0:0(0) ack 1899041971 wi
                        4500 0028 0002 0000 ff06 bdcb xxxx xxxx
                        xxxx xxxx 05fb e409 0000 0000 7131 14b3
                        5014 0000 41e5 0000
12:19:05.066228 attacker.com.58377 > victim.com.522: S 1899041970:1899041970(0)
id 45591)
                        4500 0028 b217 0000 3606 d4b6 xxxx xxxx
                        xxxx xxxx e409 020a 7131 14b2 0000 0000
                        5002 0c00 39e9 0000
The two RST were cut for space reasons.
```

Figure 1: NMAP -sS scan

First, let's look at some of the common NMAP signatures. Figure 1 shows that NMAP sends out one- (highlighted in red). This is done to ensure the victim is up and running. The second signature in this packet that that set the 32 -bit Acknowledgement field to 0. (Figure 1 - in red) This ACK field should a in an ACK packet.

Why is this done? The reason for setting the ACK field to 0 is simple: "stealth". Why would NMAP sen anyway? RFC 793 can shed some light on this question and help you understand why certain packet mapping. RFC 793 pp. 64 covers how TCP responds to specific packets; these responses are based These states are CLOSED and LISTEN. RFC 793 states that when a port is in the closed state, the f

- Any incoming segment containing a RST is discarded.
- Any incoming segment NOT containing a RST (i.e. SYN, FIN, and ACK) will cause a RST to be

For a port in the LISTEN state, the following rules apply:

- Any incoming segment containing a RST will be ignored (dropped), and
- Any incoming segment containing an ACK will cause a RST to be sent in response.
- If the SYN bit is set:
  - If the incoming segment is not allowed then a RST is sent in response.
  - If the incoming segment is allowed then a SYN|ACK is sent in response (part 2 of the thr

Knowing this, we can conclude that the two ACK packets are sent to verify that the computer to be sc running.

Another common signature of NMAP are the high source ports. Normally, NMAP's source ports are ab can be changed with the -p switch). The thought process behind setting the port so high is that some programs will not flag these scans because of this. That thought process still holds true today in some high source ports alert an IDS analyst or firewall administrator that they are being scanned.

The first switch we will look at is the -sS switch (Figure 1). The -sS switch sends a SYN(s) to a port(s response. The response should be either a SYN | ACK if the port is open or a RST | ACK if the port i considered a "half-scan", the theory behind a "half -scan" is NMAP will send SYN's to a computer, if t then a rest is sent back notifying NMAP that the port is closed. If NMAP sends a SYN to an open port with a SYN | ACK. Once NMAP detects the SYN | ACK it automatically replies back with a RST. This

connection and in some cases, a computer will not log this attempt. This also lets NMAP know what p ports are closed.

The -sX switch does performs a Xmas tree scan (Figure 2). Because of the odd TCP flags (FIN, PSH scan, some firewalls (poorly configured) will allow these packets to pass through. Figure 2 indicates tl sends out two echo request and ACK packets to ensure that the target is in fact up and running.

What is so strange about FIN, PSH and URG all set at the same time? To answer that question lets ta flag does:

- FIN : "The sending machine is finished sending data."[1] *I'm through!*
- PSH : "Set when the receiver should pass this data to the applications as soon as possible."[2] *H data!*
- URG: "The urgent pointer is valid."[3] "Allows one end to tell the other end that "urgent data" of s place in the normal stream of data."[4] *Speaks for itself.*

```
12:07:47.251547 attacker.com > victim.com: icmp: echo request (ttl 52, id 57064)
                        4500 001c dee8 0000 3401 a9f6 xxxx xxxx
                        xxxx xxxx 0800 98d3 5f2c 0000
12:07:47.251720 victim.com > attacker.com: icmp: echo reply (ttl 255, id 2136)
                        4500 001c 0858 0000 ff01 b586 xxxx xxxx
                        xxxx xxxx 0000 a0d3 5f2c 0000
12:07:47.252111 attacker.com.40335 > attacker.com.www: . ack 0 win 2048 (ttl 53,
                        4500 0028 04e6 0000 3506 82e8 xxxx xxxx
                        xxxx xxxx 9d8f 0050 1b98 0003 0000 0000
                        5010 0800 f057 0000
12:07:47.252225 victim.com.www > attacker.com.40335: R 0:0(0) win 0 (ttl 255, id
                        4500 0028 0859 0000 ff06 b574 xxxx xxxx
                        7f00 0001 0050 9d8f 0000 0000 0000 0000
                        5004 0000 13ff 0000
12:07:47.336218 attacker.com.40315 > victim.com.824: FP 0:0(0) win 2048 urg 0 (t
43059)
                        4500 0028 a833 0000 3506 df9a xxxx xxxx
                        xxxx xxxx 9d7b 0338 0000 0000 0000 0000
                        5029 0800 0906 0000
12:07:47.336392 victim.com.824 > attacker.com.40315: R 0:0(0) ack 0 win 0 (ttl 2
2138)
                        4500 0028 085a 0000 ff06 b573 xxxx xxxx
                        xxxx xxxx 0338 9d7b 0000 0000 0000 0000
                        5014 0000 111b 0000
```

Figure 2: NMAP XMAS scan

In short what the FIN, PSH, URG combination tells the computer is to begin tearing down the connect and then there is "urgent" data to be passed on the normal stream of data. In my experience, this doe you're trying to map a network). Another signature of NMAP is when it uses the Xmas tree scan also - it is always set to 0 (blue in Figure 2).

Finally, we are going to look at the -sF switch along with the -O switch. The -sF scans computers with switch does Operating System fingerprinting. If you get a chance before you compile NMAP take a loo file. It's impressive, the collection of OS fingerprints Fyodor has collected really amazes me. Figure 3 -O option also being used.

```
11:00:09.360631 attacker.com.49044 > victim.com.219: F 0:0(0) win 4096 (ttl 59,

11:00:09.361056 attacker.com.49044 > victim.com.48: F 0:0(0) win 4096 (ttl 59, i

11:00:12.820777 attacker.com.49051 > victim.com.sunrpc: S 561959278:561959278(0)
<wscale 10,nop,mss 265,timestamp 1061109567 0,eol> (ttl 59, id 11173)

11:00:12.821526 victim.com.sunrpc > attacker.com.49051: S 2988831197:2988831197(
561959279 win 16165 <mss 265,nop,nop,timestamp 2872982 1061109567,nop,wscale 0>
(DF) (ttl 64, id 3059)

11:00:12.821923 attacker.com.49052 > victim.com.sunrpc: . win 4096 <wscale 10,no
265,timestamp 1061109567 0,eol> (ttl 59, id 25812)

11:00:12.822090 attacker.com.49053 > victim.com.sunrpc: SFP 561959278:561959278(
win 4096 urg 0 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol> (ttl 59, id 10

11:00:12.822519 attacker.com.49054 > victim.com.sunrpc: . ack 0 win 4096 <wscale
10,nop,mss 265,timestamp 1061109567 0,eol> (ttl 59, id 36725)

11:00:12.822795 attacker.com.49055 > victim.com.34459: S 561959278:561959278(0)
<wscale 10,nop,mss 265,timestamp 1061109567 0,eol> (ttl 59, id 36400)

11:00:12.823071 attacker.com.49056 > victim.com.34459: . ack 0 win 4096 <wscale
10,nop,mss 265,timestamp 1061109567 0,eol> (ttl 59, id 46890)
                        4500 003c b72a 0000 3b06 ca8f xxxx xxxx
                        xxxx xxxx bfa0 869b 217e d16e 0000 0000
                        a010 1000 81fb 0000 0303 0a01 0204 0109
                        080a 3f3f 3f3f 0000 0000 0000

11:00:12.823347 attacker.com.49057 > victim.com.34459: FP 561959278:561959278(0)
urg 0 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol> (ttl 59, id 733)
                        4500 003c 02dd 0000 3b06 7edd xxxx xxxx
                        xxxx xxxx bfa1 869b 217e d16e 0000 0000
                        a029 1000 81e1 0000 0303 0a01 0204 0109
                        080a 3f3f 3f3f 0000 0000 0000

11:00:12.823642 atttacker.com.49044 > victim.com.34459: udp 300 (ttl 57, id 6079
                        4500 0148 ed77 0000 3911 952b xxxx xxxx
                        xxxx xxxx bf94 869b 0134 40db 6060 6060
                        6060 6060 6060 6060 6060 6060 6060 6060
                        6060 6060 6060 6060 6060 6060 6060 6060

11:00:12.823746 victim.com > attacker.com: icmp: victim.com udp port 34459 unrea
(ttl 255, id 3067)
                        45c0 0164 0bfb 0000 ff01 afdb xxxx xxxx
                        xxxx xxxx 0303 fc44 0000 0000 4500 0148
                        ed77 0000 3911 952b 7f00 0001 7f00 0001
                        bf94 869b 0134 40db 6060 6060 6060 6060
```

Figure 3: NMAP -sF -O scan

The theory behind NMAP's -sF scan is quite simple and we covered it at the beginning of this paper. I TCP and what state the port(s) are in (CLOSED or LISTENING). Here is a real quick summary:

1. If the port(s) are in closed and a FIN is sent a reset is sent in response.
2. In this case, if a FIN is sent and the port(s) are open then TCP drops the FIN and does not sen

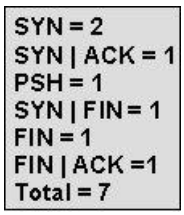
This method may get past a **few** Intrusion Detection System's and Firewalls because there are a few for a FIN | ACK combination not just a FIN.

NMAP's -O function identifies a probbable Operating System to the user. As you can see in Figure 3 N of packets which include FIN | PUSH | URG, SIN | FIN | PSH, SYN packets and a few UDP packets. most of the UDP packets have been 300 bytes.

1.3.2 QUESO

Although QUESO is not as popular or robust as NMAP, it still provides great signatures to look at and written by savage@apostols.org. It is available at any of your local neighborhood port scanning webs free.

QUESO usually sends out seven (7) packets at a time. If you read the documentation.txt (file that com states that QUESO sends out seven (7) packets at a time. QUESO send out the following packets:



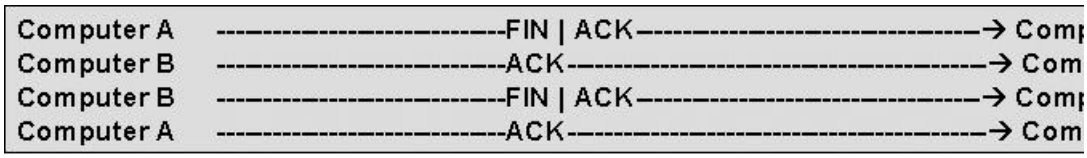
QUESO allows a user to spoof his/her address and to choose what port he/she wants to scan. QUES source ports (4000 -65000). Figure 4 shows us what a scan by QUESO looks like:

```
17:24:43.328743 attacker.com.19909 > victim.com.sunrpc: S 1567977113:1567977113(
(ttl 255, id 51246)
                        4500 0028 c82e 0000 ff06 6095 xxxx xxxx
                        xxxx xxxx 4dc5 006f 5d75 6e99 0000 0000
                        5002 1234 f05f 0000
17:24:43.352137 attacker.com.19910 > victim.com.sunrpc: S 1567977113:1567977113(
4660 (ttl 255, id 51247)
                        4500 0028 c82f 0000 ff06 6094 xxxx xxxx
                        xxxx xxxx 4dc6 006f 5d75 6e99 0000 0000
                        5012 1234 f04e 0000
17:24:43.370082 attacker.com.19911 > victim.com.sunrpc: F 1567977113:1567977113(
(ttl 255, id 51248)
                        4500 0028 c830 0000 ff06 6093 xxxx xxxx
                        xxxx xxxx 4dc7 006f 5d75 6e99 0000 0000
                        5001 1234 f05e 0000
17:24:43.390301 attacker.com.19912 > victim.com.sunrpc: F 1567977113:1567977113(
4660 (ttl 255, id 51249)
                        4500 0028 c831 0000 ff06 6092 xxxx xxxx
                        xxxx xxxx 4dc8 006f 5d75 6e99 0000 0000
                        5011 1234 f04d 0000
17:24:43.410079 attacker.com.19913 > victim.com.sunrpc: SF 1567977113:1567977113
(ttl 255, id 51250)
                        4500 0028 c832 0000 ff06 6091 xxxx xxxx
                        xxxx xxxx 4dc9 006f 5d75 6e99 0000 0000
                        5003 1234 f05a 0000
17:24:43.430076 attacker.com.19914 > victim.com.sunrpc: P win 4660 (ttl 255, id
                        4500 0028 c833 0000 ff06 6090 xxxx xxxx
                        xxxx xxxx 4dca 006f 5d75 6e99 0000 0000
                        5008 1234 f054 0000
17:24:43.450082 attacker.com.19915 > victim.com.sunrpc: S 1567977113:1567977113(
(ttl 255, id 51252)
                        4500 0028 c834 0000 ff06 608f xxxx xxxx
```

```
4500 0028 c834 0000 ff06 6081 xxxx xxxx
xxxx xxxx 4dcb 006f 5d75 6e99 0000 0000
50c2 1234 ef99 0000
```

Figure 4: QUESO scan

Looking at the scan (Figure 4), we see all seven (7) packets are there. What we need the hex dumps that do not stand out. The first signature that we see is one (1) lonely FIN packet. What makes these there is no connection (why would you send a FIN to a terminate a connection that never was made.) contain an ACK. Although, TCP uses a three - way handshake to make a connection, it uses a four - disconnect. The process of connection termination goes like this:



Still looking at the scan, we see a PSH flag set, this should raise some eyebrows as well because in T be accompanied by an ACK (as long as a connection has been made).

We see that QUESO sets the SYN | FIN flags which tell the receiving computer to OPEN and CLOSE once.

n/a	n/a	urg	ack	psh	rst	svn	fin
8	4	2	1	8	4	2	1

Figure 5: 13th byte in the TCP Header

The most interesting signature that QUESO sends is one (1) SYN packet that sets the reserved bits (Figure 5 shows what byte 13 in the TCP header looks like. The last two bits on the left (labeled n/a) a not be set. This is easy to identify, if you see c2 set in the 13th byte of the TCP header, you know tha malicious intentions for your network.

1.4 CONCLUSION

In conclusion, this paper was written to help administrators understand some detailed information abo With this level of understanding, IDS analyst(s) and firewall administrators will be able to identify thes respond accordingly. Any questions or comments can be addressed at infowar@erols.com.

1. W. Richard Stevens, TCP/IP Illustrated, Volume 1, Addison-Wesley, Massachusetts, 1994, pp. 227
2. W. Richard Stevens, TCP/IP Illustrated, Volume 1, Addison-Wesley, Massachusetts, 1994, pp. 227
3. W. Richard Stevens, TCP/IP Illustrated, Volume 1, Addison-Wesley, Massachusetts, 1994, pp. 227
4. W. Richard Stevens, TCP/IP Illustrated, Volume 1, Addison-Wesley, Massachusetts, 1994, pp. 292

Toby Miller currently works at SYTEX Inc. based out of Pennsylvania. Toby holds a B.S in Computer Information Systems . Toby is a GIAC Microsoft Certified Professional. In his seven years in the computer field he has worked in many area such as Firewalls, Unix administration mainframe work.