The HoneyNet Project
Scan Of The Month – Scan 27

23rd April 2003

Shomiron Das Gupta
shomiron@lycos.co.uk

1.0 Scope

This month's challenge is a Windows challenge suitable for both beginning and intermediate analysts. If you rate your skill level as beginning, you can submit answers to only the beginning questions. If you rate your skill level as intermediate, you can submit answers to both the beginning and intermediate questions. In either case, your objective is to analyze the aftermath of an attack on a Windows 2000 honeypot, captured by members of the Azusa Pacific University Honeynet Project. Remember, the purpose of the challenge is to learn.

2.0 Questions

Beginning Questions

2.1 What is IRC?

IRC (Internet Relay Chat) is a service that enables communication between people across the globe. This service requires central servers running the IRC service. The clients use IRC client applications to access the service and communicate with all the other members who are using the service.

IRC (Internet Relay Chat) provides a way of communicating in real time with people from all over the world. It consists of various separate networks (or "nets") of IRC servers, machines that allow users to connect to IRC. The largest nets are EFnet (the original IRC net, often having more than 32,000 people at once), Undernet, IRCnet, DALnet, and NewNet.

http://www.irchelp.org

2.2 What message is sent by an IRC client when it asks to join an IRC network?

Following is a sample conversation of an IRC server and a client the type in blue is what the client sends to the IRC network.

```
NOTICE AUTH :*** Looking up your hostname…
NOTICE AUTH :*** Checking Ident
NOTICE AUTH :*** No Idnet response

NICK eohisou
USER eohisou localhost localhost :eohisou
```

2.3 What is a botnet?

To explain a botnet we first need to understand a bot. A bot is an IRC client running on a client machine. This is a Trojan installed in the form of an IRC client on the infected machine. Once this infected machine connects to the Internet the installed bot connects to a predefined IRC server and then a predefined IRC channel. In a distributed scenario there are many such infected machines on the Internet, which connect to a central IRC server and a central IRC channel. The attacker can then control all the connected bots through the IRC channel. This can then be used to launch several different kinds of attacks like a DOS or a DDOS. This network of bots connected to a central server and channel is called a botnet.

http://zine.dal.net/previousissues/issue22/botnet.php

2.4 What are botnets commonly used for?

Botnets are commonly used to launch DOS attacks, DDOS attacks, Spam attacks, flood attacks etc. The method of infection and attack is explained in the section above.

2.5 What TCP ports does IRC generally use?

IRC generally uses the following ports
6667 / tcp

2.6 What is a binary log file and how is one created?

A binary log file is used to capture network traffic into a single file. A binary log stores captured network traffic in pcap format. It can be created using tools like Tcpdump, snort, ethereal etc.

Following example shows the usage of Tcpdump to create a binary file.

```
# tcpdump –w binary.log –s 1514
```

Note:
The –s switch is used to change the default snapshot length from 68 bytes to 1514 bytes
The –w switch is used to write the captured data into a file named ‘binary.log’

2.7 What IRC servers did the honeypot, which has the IP address 172.16.134.191, communicate with?

Following are the IRC servers, the honeypot 172.16.134.191 tried to connect.

```
   209.126.161.29
   66.33.65.58
   63.241.174.144
   217.199.175.10
   209.126.161.29
   209.196.44.172
```

tcpdump –r sotm27 host 172.16.134.191 and port 6667 and tcp[13] = 0x02

2.8 During the observation period, how many distinct hosts accessed the botnet associated with the server having IP address 209.196.44.172?

During the observation period one host accessed the botnet at IP address 209.196.44.172. Following is the IP address that accessed the botnet.

```
172.16.134.191
```

2.9 Assuming that each botnet host has a 56 kbps network link, what is the aggregate bandwidth of the botnet?

The aggregate bandwidth of the botnet is 56 kbps as only one host is accessing the botnet i.e. 209.196.44.172

Intermediate Questions

2.10 What IP source addresses were used in attacking the honeypot?

Following are the IP source addresses that were used in attacking the honeypot.

```
68.37.54.69
12.252.61.161
206.149.148.192
218.4.87.137
66.81.131.17
61.177.56.98
200.74.26.73
61.132.88.90
24.167.221.106
67.201.75.38
61.8.1.64
61.132.88.90
68.84.210.227
66.233.4.225
200.50.124.2
12.253.142.87
12.83.147.97
61.150.72.7
218.92.13.142
61.134.45.19
61.132.88.90
61.132.88.50
218.4.99.237
216.229.73.11
61.150.72.7
168.243.103.205
216.192.145.21
61.185.29.9
4.33.244.44
24.74.199.104
81.57.217.208
61.185.212.166
213.170.56.83
218.4.48.74
61.150.72.7
212.162.165.18
200.135.228.10
213.122.77.74
61.185.242.190
218.244.66.32
61.150.120.72
```

```
68.45.123.130
61.203.104.148
61.177.62.66
217.35.65.9
219.145.211.3
61.134.45.19
218.4.99.237
205.180.159.35
61.150.120.72
61.185.215.42
67.81.161.166
61.150.72.7
212.122.20.74
218.4.65.115
219.145.211.132
61.111.101.78
129.116.182.239
```

Used snort to obtain the results

2.11 What vulnerabilities did attackers attempt to exploit?

Following are the vulnerabilities the attackers attempted to exploit.

```
Windows File Share Attacks
Web IIS Attack
MS-SQL Worm propagation
SCAN SOCKS Proxy
```

Used snort and manual analysis to obtain the results

2.12 Which attacks were successful?

Following attacks were successful.

```
Windows File Share Attacks
```

Used manual analysis to obtain the results.

General Questions

2.13 What did you learn about analysis as a result of studying this scan?

By analyzing this scan one understands the concept of a botnet. This further leads us into higher grounds i.e. DOS attacks. It was a wonderful scan for us beginners to find our feet in intrusion analysis.

2.14 How do you anticipate being able to apply your new knowledge and skills?

Our new knowledge and skills can be applied in the real world for analyzing real attacks on our networks. It will give us a tremendous start in intrusion analysis of worms and for that matter real attack.

2.15 How can we improve the SotM challenge? What would you like to see added? What would you like to see done differently?

The SotM challenge has been an excellent way of learning for us. One is able to analyze and review their analysis through this forum. This forum needs to continue the way it is without changing a thing. I guess the only request would be to have at least one such binary log analysis challenges per month.

3.0 Initial Inspection

The initial inspection was conducting by downloading the challenge from the website and then verifying the integrity of the file by generating an md5sum. Following were the commands used to perform the same.

```
# md5sum sotm27.gz
b4bfc10fa8346d89058a2e9507cfd9b9 sotm27.gz
```

Following was the md5sum obtained from the website.

MD5 (sotm27.gz) = b4bfc10fa8346d89058a2e9507cfd9b9

The comparison of both the checksum outputs turned out to be positive. Hence the test was successful and we could proceed further with our analysis.