Analysis of an attack (Part 1)

This series will be based on a network vulnerability. What will be introduced in this article is a real attack, starting from exploring to listing, exploiting network services, and ending exploitation strategies for sending notifications. All of these steps will be observed at the packet level, and then explained in detail.

This series will be based on a network vulnerability.What will be introduced in this article is a real attack, starting from exploring to listing, exploiting network services, and ending exploitation strategies for sending notifications.All of these steps will be observed at the packet level, and then explained in detail. Being able to observe and understand an attack at the packet level is extremely important for both system administrators (sys admin) and network security personnel. Outputs of firewalls, Intrusion Detection Systems (IDS) and other security devices will always be used to view actual network traffic. If you don't understand what you're seeing at the packet level, then all the network security technologies you have will become meaningless.

The tools used for simulating a network attack are:

1. Nmap
2. IPEye
3. Tcpdump
4. Metasploit Framework
5. Netcat
6. SolarWinds TFTP Server
7. Tftp client
8. FU Rootkit

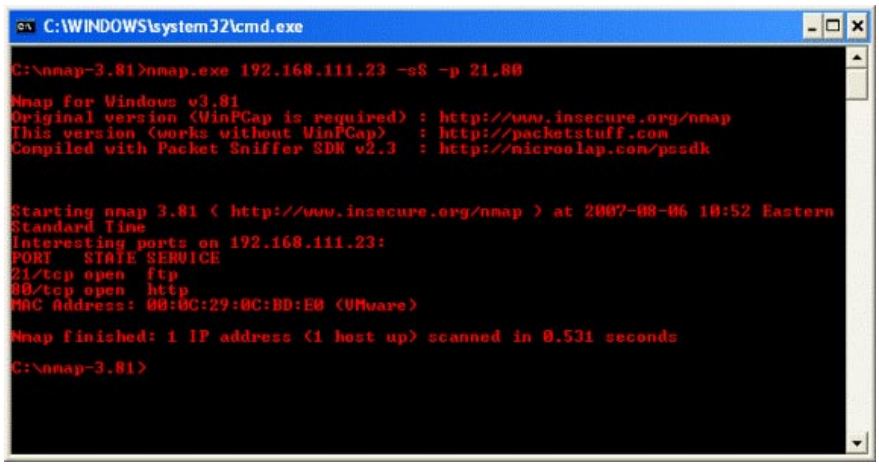
Setup step

There are many scans on the Internet today, not to mention worm actions and other forms of malware such as viruses. All of them will be just like harmless noise with well-protected computer networks. What we should consider is a person who is deliberately targeting a computer network. This article will acknowledge that the attacker has attacked his victim and done previous studies such as finding the IP address and the victim's network addresses. The attacker may have also tried to exploit information such as email addresses related to that network. This type of information is very important in case an attacker has found but has no way to access the network after performing scans, enumeration, and spoofing. The email addresses he has collected will be very useful in setting up a client attack by trying and inviting users to a malicious website via a link in the email. These types of attacks will be introduced in the following articles.

How to perform

We should observe the actions of a hacker when he does a scan, and list the victim's network. The first tool that

hackers use is Nmap. Although Nmap has quite a few IDS symbols, it is still quite a useful tool and is used a lot.



We can see through the syntax used by hackers in the small screen shown above, hackers have chosen port 21 and 80 because he has some exploits that can be used through the Metasploit Framework. Not only that but also both system and protocol services that he understands quite well. It is quite clear that he is using a SYN scan, which is the most commonly used port scan. It is also due to the fact that when a service using TCP listening on a port receives a SYN packet, it sends back a SYN / ACK packet (reply). The SYN / ACK package indicates that a service is indeed listening and waiting for a connection. However, the same problem is not the same as UDP, it is based on services like DNS (DNS also uses TCP but it almost uses UDP for most of its sessions).

The syntax listed below is the output that Nmap collects from the packets it sent, but more precisely from the packets it receives as a result of the SYN scan it has performed. We can see that it looks like both FTP and HTTP services are provided. We don't really care about the MAC address so we'll ignore that. Tools like Nmap don't often have errors, so it's often good to verify your information at the packet level to ensure accuracy. Not only that, but it also allows you to observe both return packets, from the victim network, to obtain the architecture, service, and host information from there.

Look up data packets

There are a number of programs offered today that will explore packages and find the necessary information like operating system type, architecture information, such as x86 or SPARC and many more. It is not enough, but it is also important when we are learning about allowing a program to do the job for us. With that in mind, let's take a look at the Nmap packet trace and find out some information about the victim network.

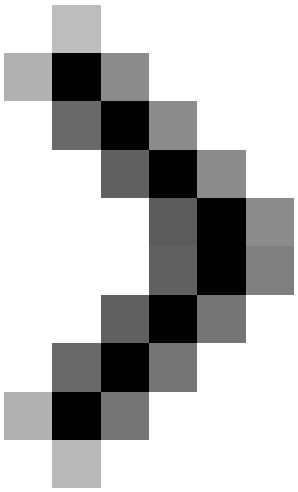
10: 52: 59.062500 IP (tos 0x0, ttl 43, id 8853, offset 0, flags [none], proto: ICMP (1), length: 28) 192.168.111.17> 192.168.111.23: ***ICMP echo request seq 38214*** *, length 8*
0x0000: 4500 001c 2295 0000 2b01 0dd3 c0a8 6f11 E . ". + . o.
0x0010: c0a8 6f17 0800 315a 315f 9546 .o . 1Z1_.F
10: 52: 59.078125 IP (tos 0x0, ***ttl 128*** *, id 396, offset 0, flags [none], proto: ICMP (1), length: 28) 192.168.111.23> 192.168.111.17:* ***ICMP echo reply seq 38214*** *, length 8*
0x0000: 4500 001c 018c 0000 8001 d9db c0a8 6f17 E ... o.
0x0010: c0a8 6f11 0000 395a 315f 9546 0000 0000 .o . 9Z1_.F .
0x0020: 0000 0000 0000 0000 0000 0000 0000 ...

Shown in the above two packets is the open series from Nmap. What it does is send an ICMP echo request to the victim network. You will see that it is not equipped at a certain port, because ICMP does not use ports, but is managed by the ICMP error message set built into the TCP / IP protocol stack. This ICMP package is also labeled with a unique number, in this case 38214 to help the TCP / IP stack be able to check the return traffic, and link it to the previously sent ICMP packet. The packet just above is a response from a victim network, in the form of an ICMP echo reply. Also consider the string number 38214. So the hacker knows that there is a computer or a network behind that IP address.

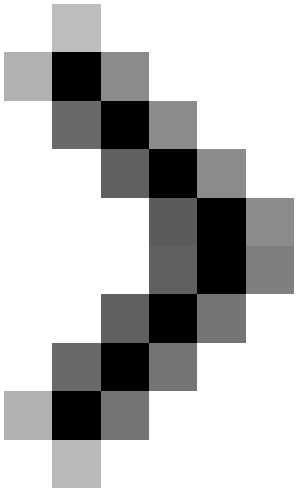
This open ICMP packet sequence is why Nmap has an IDS symbol for it. ICMP host discovery options can be disabled in Nmap if desired. What kind of information can be gathered through the results of the ICMP echo response packet from the victim network? In fact, there is not much information that helps us understand the network. However, it is still possible to use preliminary moves in places related to the operating system. The time to reside in a field and the value next to it is highlighted in the above package. The value 128 shows a fact that this computer can be a computer running Windows operating system. While the ttl value does not respond exactly to what is related to the operating system, it will be based on the next packages that we will consider.

Conclude

In this first part, we looked at a scan for a network in an attack for two specific ports using Nmap. At this point, the attacker was certain that a computer or a computer network resided at that IP address. In Part 2 of this series, we will continue the study of this package's traces, and find out the remaining pieces of information.



Analysis of an attack (Part 2)



Analysis of an attack (Part 3)

Don Parker