Ferhat Elmas
Przemyslaw Pietrzkiewicz
Javier Martín De Valmaseda Castro

Lab-3 Network Discovery

(Less) Easy Reversing

When we disassembled simple2 file, we noticed a memfrob function. We looked it up on google and discovered it to be simple pseudo-crypto tool that xor given memory with number 42. It means the strings were obfuscated simply by xoring with 42. Therefore, we had two options to get the password:
1) We could set a breakpoint in strcmp function where actual and given password are compared. When the program is stopped there, we can look at memory addresses that eax and edx registers point to (since eax register points to actual password and other points to the string that we entered). Then we read the ascii codes of characters (this was correct codes since we saw memfrob has been called on this string before). We got the password: **toomanysecrets** after entering this we accessed the key :**rosebud**
2) Other option was not to bother assembly and registers and just apply memfrob on whole file and get the strings as in the first version of simple.

Network Discovery

Scan

The option being discussed force Nmap not to do port scan after finding if host is up; so it just prints out the available hosts that responded the scan. Therefore, it is usually known as ping scan. Its main functionality is to easily count available machines on a network. -sP (skip port scan) option sends an ICMP echo request, TCP SYN to port 443, TCP ACK to port 80, and an ICMP timestamp request by default. If the host is active, we will get an RST flag in reply of TCP sent.

ping sends ICMP echo_request and if the host is active and nonblocked, it responds with ICMP echo_reply.

When we run -sP scan, we see simply that there are five hosts that are up, namely

- 10.10.0.1
- 10.10.0.2
- 10.10.0.3
- 10.10.0.4
- 10.10.0.5

When we try to ping each host by hand, we see that all hosts other than 10.10.0.2 respond to ICMP echo_request. However, 10.10.0.2 didn't respond. When we entered the container and checked iptables, we saw that ICMP packets are blocked.

- vzctl enter 1000
- iptables -S

    - -A INPUT -p icmp -m icmp --icmp-type 8 -j DROP

Nmap still worked, because its packets weren't filtered out by this rule.

After we run default scan

- nmap 10.10.0.0/24

we see that host 10.10.0.3 has two test services working (port 7 echo, port 13 daytime). They are potential security holes so to filter corresponding packets we can:

- vzctl enter 1001
- iptables -t filter -INPUT -p tcp -i eth0 --dport 7 -j DROP (for echo)
- iptables -t filter -INPUT -p tcp -i eth0 --dport 13 -j DROP (for daytime)

These rules works for all tcp flags so we don't see this weird thing about mysql 3306 here. In mysql filter rule,

- -A INPUT -s 10.10.0.1/32 -p tcp -m tcp --dport 3306 --tcp-flags FIN,SYN,RST,ACK SYN -j DROP

As we can see from this rule only TCP SYN is filtered so when we do TCP SYN scan we see mysql is filtered but when we do TCP ACK scan, we see that mysql is unfiltered.
For echo and daytime, after adding above rules we see them as filtered in two scan since these rules filtered all tcp connections on ports 7 and 13.

Tu sum up, there are three options:

- Filtering packets according to their flags as in the example of mysql.
    - It doesn't work for some flags while it works for others. (SYN vs ACK)
- Filtering packets according to the protocol
    - That is what we did above
- Completely disabling the service.
    - Modern linux distributions switched into xinetd from inetd and we see configuration files under /etc/xinetd.d and each configuration file contains a line to quickly disable them
        - # This is for quick on or off of the service
        - disable = yes

Tarpits

The concept is quite simple tarpit. The connections come in, but not get out. IPtables achieves this by allowing the ports to use tarpit to accept any incoming TCP connection. When the transfer of data begins to occur, the size of the TCP window is set to zero, so no data can be transferred within the session. The connection then remains open, and any request by the remote to close the session is ignored. This means that the attacker must wait for time out of the connection to be disconnected. This kind of behavior is bad for automated scanning tools (such as worms) because they rely on a rapid response potential victims. Default nmap scan isn't affected because the TCP SYN scan never actually creates a TCP session, so isn't logged by the destination host's applications.