

Lab 11 – C2s and Firewalls

Firewall Settings

Firewall / Rules / Floating

Floating
WAN
LAN

Rules (Drag to Change Order)

	States	Interfaces	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>												

Firewall / Rules / WAN

Floating
WAN
LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 3 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0 / 2 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

Firewall / Rules / LAN

Floating
WAN
LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	9 / 134 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	29 / 387 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

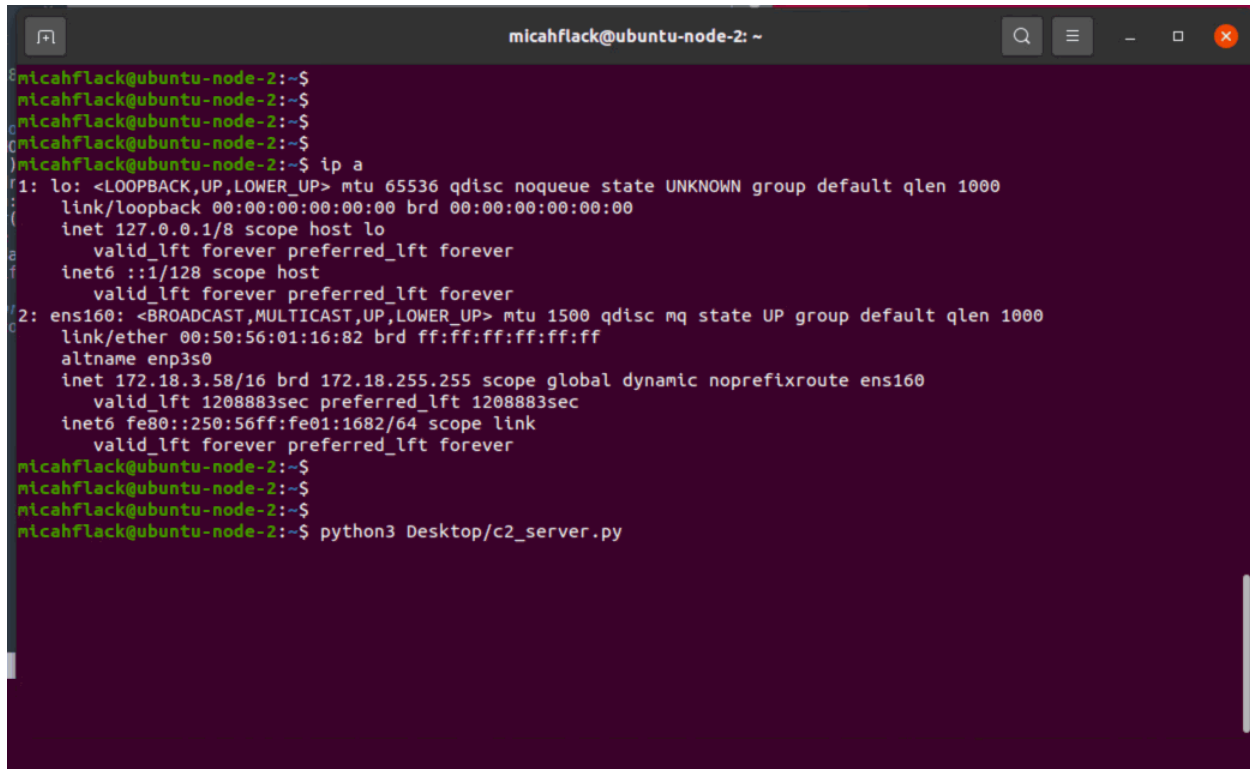
Interfaces

	WAN	↑	autoselect	172.18.5.248
	LAN	↑	autoselect	10.0.0.1

WAN --> vCloud_Internet ; something/24

LAN --> Internal ; 10.0.0.0/24

C2 File Uploading .GIF

A terminal window titled 'micahflack@ubuntu-node-2: ~' with a dark purple background. The terminal shows the user running 'ip a' to display network interface details for 'lo' and 'ens160'. The output for 'lo' shows it's a loopback interface with IP 127.0.0.1. The output for 'ens160' shows it's an ethernet interface with IP 172.18.3.58. After displaying the IP addresses, the user runs 'python3 Desktop/c2_server.py'.

```
micahflack@ubuntu-node-2:~$  
micahflack@ubuntu-node-2:~$  
micahflack@ubuntu-node-2:~$  
micahflack@ubuntu-node-2:~$  
micahflack@ubuntu-node-2:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000  
    link/ether 00:50:56:01:16:82 brd ff:ff:ff:ff:ff:ff  
    altname enp3s0  
    inet 172.18.3.58/16 brd 172.18.255.255 scope global dynamic noprefixroute ens160  
        valid_lft 1208883sec preferred_lft 1208883sec  
    inet6 fe80::250:56ff:fe01:1682/64 scope link  
        valid_lft forever preferred_lft forever  
micahflack@ubuntu-node-2:~$  
micahflack@ubuntu-node-2:~$  
micahflack@ubuntu-node-2:~$  
micahflack@ubuntu-node-2:~$ python3 Desktop/c2_server.py
```

Might be hard to tell because of how much data was sent and the screen was forced to scroll, but the compromised client sent an http response with a “data” json object containing the contents of /etc/passwd to the server.

Pretty basic `_(\`)/`

Read the scripts for a better understanding.

Scripts:

- + c2_server.py

- + c2_client.py