Penetration Test Ex04

Esteban Calvo

2023-09-18

Contents

1 Attack Narrative

1.1 Finding my IPs

To begin the assignment, I began by running the ipconfig command and found

```
    ipconfig
        eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.24.0.10  netmask 255.255.255.0  broadcast 172.24.0.255
        inet6 fe80::1f2:7280:6ad8:30f3  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:87:86:8f  txqueuelen 1000  (Ethernet)
        RX packets 1786  bytes 167709 (163.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1908  bytes 174253 (170.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 84  bytes 4240 (4.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 84  bytes 4240 (4.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1.2 Plunder traceroute

When running the traceroute command on plunder.pr0b3.com, there were a total of 35 pings sent several of them dying in the process as the TTL was exceeded. During the traceroute, there were 2 different sources and 1 destination. Traceroute sends out as many pings as needed until either the destination is reached or the max TTL is exceeded. In our case, traceroute stopped pinging once the destination was reached and therefore did not send them all.

```
    sudo traceroute -I plunder.pr0b3.com
traceroute to plunder.pr0b3.com (45.79.141.233), 30 hops max, 60 byte packets
 1  outerouter (172.24.0.1)  0.245 ms  0.226 ms  0.221 ms
 2  202.150.115.1 (202.150.115.1)  0.853 ms  0.848 ms *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * plunder.pr0b3.com (45.79.141.233)  1.587 ms  1.405 ms
```

1.3 Arts Tailor traceroute

For the traceroute to ns.artstailor.com, there were more packets sent with several runs of traceroute averaging out to around 40 packets sent. To get to ns.artstailor.com, there were only two hops: One to the outerrouter and one to ns.artstailor.com.

```
    sudo traceroute -I ns.artstailor.com
traceroute to ns.artstailor.com (172.70.184.133), 30 hops max, 60 byte packets
 1  outerouter (172.24.0.1)  0.229 ms  0.210 ms  0.204 ms
 2  ns.artstailor.com (172.70.184.133)  0.548 ms  0.543 ms  0.538 ms
```

1.4 Missing ICMP ECHO

For the most part, the host would respond with the appropriate echo response. However, if the host does not respond with the appropriate echo response, it is possible that there are some firewall issues at play blocking the pings from being executed in the appropriate time. To circumvent this issue, it is possible to use the -T flag which sends TCP packets.

1.5 key

The key for this assignment was broken up into a response and a request packet and when put together yielded the key

$$KEY006 - LHQ0LWLBEE1FnwPr9clv5A$$