Penetration Testing

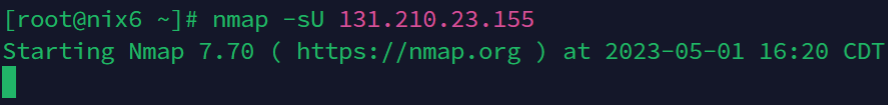
Text

Description automatically generated

Text

Description automatically generated

1. The first image shows a general scan with no firewall configured. The second image shows the general scan with the firewall configured and shows that there is one host up on the network with the IP address provided. Nmap detected two ports on the host: port 22/tcp for SSH and port 80/tcp for HTTP. Nmap also detected 998 filtered ports which were blocked by the firewall. The scan also was able to detect that the host is running on a VMware virtual machine. The scan with no firewall configured detected a closed port 9090/tcp (zeus-admin).



Text

Description automatically generated

1. This was a UDP scan done on my IP Address. The first image shows a scan done to my machine with no firewall configured. For some reason the scan kept freezing. The second image shows a scan done with a firewall configured. The firewall scan showed that all 1000 ports were filtered. This was because of the firewall configuration. The firewall is configured to use TCP versus UDP since TCP is more secure.

Text

Description automatically generated

Text

Description automatically generated

1. This next scan determines the version of all services that are currently running on my machine. The first image shows the scan done with no firewall configured. The second image shows the scan with the firewall configured. Both show ports 22 and 80 for SSH and http respectively. The first scan, however, shows port 9090/tcp zeus-admin.

Text

Description automatically generated

Text

Description automatically generated

1. This scan runs scripts on all open ports to determine vulnerabilities. The first image was with not firewall configured and the second was with a firewall configured. This scan revealed SSH host keys used by the server. The scan with no firewall also showed port 9090 for zeus-admin.

Text

Description automatically generated

Text

Description automatically generated

1. This scan traces the route that packets take from the source to the target system. The first image is with no firewall configured and the second image is with a firewall configured. Just as the previous scans, the only difference is port 9090/tcp zeus-admin. But they both show that there was only 1 hop which means that the target host is directly reachable from the scanning host without going through any intermediary routers. The RTT (Round Trip Time) was .22 ms meaning the target host is located close to the scanning host providing minimal network latency.