Nicholas Marshall

Dr. Nelbert St. Clair

ITEC 4341 – Network Forensics/Inc Resp

October 31, 2018

NAT Lab 1 – Portscan

Management Summary

In the capture file I was tasked with digging through it appears that someone is attempting to map our network infrastructure. The user(s) are doing this through several different methods using nmap and a ping. He first used nmap to map the 192.168.30.0/24 network and the 192.168.31.0/24 network as well to find every system on our networks. The ping method will act like a sonar detection system like bats use to discover where our systems are sitting on the network. The method this malicious user used worked as he was able to detect several of our systems including where our email sits on the network along with being able to communicate our 2 hosts. The user was also able to log into one of our accounts to gain access one of the servers.

Technical Section

1. What tool generated this traffic? – PING generated the Echo requests and replies but, also there were signs of NMAP being used on the SMTP server and an attempt at ARP ping scans.
2. How many hosts responded to the scan? – The 2 hosts on 192.168.30.1 and 192.168.31.1 both replied to the scan.
3. What is the target subnet in CIDR notation? -  It appears that 192.168.31.0/24 is a target subnet with some activity going on in the 192.168.30.0/24.
4. What's an IP address that had VNC running? – 192.168.30.65
5. What IP address had a mail server running? – 192.168.31.94