M&S Pentesting Report

Chapter 1: Reconnaissance

After a network scan, we were able to discover 3 network devices. One running FreeBSD, one Microsoft Windows and one Linux. We also found a variety of running services.

- 192.168.1.14 - Running FreeBSD, ports 53 (DNS), 80 (webserver), 443 (webserver over https), 5666 (Nagios) open.
- 192.168.1.100 - Windows Server 2016, ports 135 (Microsoft RPC), 139 (NetBIOS), 445 (Microsoft Domain Services), 2179 (Extension to RDP), 3389 (RDP), 5357 (Web services for devices).
- 192.168.1.112 - Running Linux, ports 22 (SSH), 80 (web server), and 443 (web server over HTTPS)

After further investigation, we found the following on the aforementioned machines.

- 192.168.1.14 - Couldn't find any exploits on this machine. We did, however, find what appears to be an attempt to mask the service running on port 5666. Unfortunately, the only public service that runs on said port, is Nagios. So... mission failed?
- 192.168.1.100 - Initial scan was a failure, since the host seemed to block ping scans. This is good for security. In addition, I expected to find exploits for the services running on ports 139 and 135, but they both seem to be updated.
- 192.168.1.112 - This seems to be the Nagios Server. It also seems to not have been updated... ever. We found over 100 exploits, after running a Nmap scan. I believe some portion of these to be false positives, since Nmap isn’t perfect. Nmap also identified some potential CSRF vulnerabilities, but I believe these to be part of the false positives, since they were found on the Nagios Dashboard, running on the server. Recommended action: Update the system immediately and see the scan file provided.

Overall, I’d say that the system is in pretty good shape. A simple apt-get update and upgrade will take care of the issues on the last machine. One thing that we couldn’t find was where the actual application lived, so we could only assume that it wasn’t online, at the time of performing the network scans.

Chapter 2: Social engineering

From the social engineering front, one thing that I would do is to try and give “malicious advice”. More than one group has reached out to us for advice. And while that is very flattering, one thing that we have noticed is that every group has taken our advice, at face value. And that is a security hole.

As the scenario above is somewhat specific to our group, here is another one. Watch out for suspicious looking emails. For example, we noticed that our target group had Nagios and Pfsense installed on their network. Now, that by itself is quite normal, but with just the knowledge that they exist, an attacker can create fake phishing emails. For example, “Would you like a 3-month free trial of Nagios Premium?” And the email would contain a malicious link.

Chapter 3: Tools and testing

All of the reconnaissance and exploit detection we did, was done via Nmap, running on Kali Linux connected to the target group’s network via OpenVPN.