Michael Esposito

Network Defense 2

HW 4 - Intrusion Script

The network I am attempting to infiltrate seems like a pretty standard corporate network. It has an externally facing router that creates a DMZ. Inside the DMZ are the email servers, DNS servers, and public websites. Behind the DMZ is another router that protects the internal network. On this network lies the workstation of regular users, admins and executives. This local network also contains the company intranet, financial exchange, public wireless and some other devices. My plan for infiltrating the network is below.

1. Initial Inject

My initial foothold into the organization would be through a broad spearphishing campaign. My goal is to obtain the login credentials of a low-level user. Not an admin or an executive because they are well-trained in spotting phishing attempts. Just a regular employee at the company. I would say that there was a malicious login on the Office 365 account and they need to login to my portal and update their credentials. Once one of these users submit credentials, I would intercept the credentials.

With these credentials, I would login to the corporate VPN and perform passive network reconnaissance. I will try to glean as much information as I can, and I am especially interested in the employee lists contained in the intranet portal. This list contains a full directory of employees at the company, their departments, and their titles. With this information, I note the high-level IT staff who might have privileged credentials, as well as executives whose workstations may contain valuable company information.

1. Command and Control Mechanism

I am not focused on creating a complex, distributed network where my victims machine will look for updates. That would be too noisy. Instead, I will host an innocuous looking website on a public-facing server that I control. This website will contain information for a local business, therefore any traffic to it will not appear suspicious. I will encrypt any traffic going to and from this server so it cannot be filtered by the company’s firewalls.

1. Recon

To perform recon on the host that I received credentials for, I would login to the account during a time of the day that would not draw attention. The user should not be at their workstation, which leaves before work, at lunch, and just after the user leaves as valid times to login. Once logged in, I would observe the various applications and services running on the host and network. I would check first to see if any of the services running are old and missing patches. If so, that would be a potential way to achieve privilege escalation. If the machine is vulnerable, I could escalate privileges, steal hashed credentials, or create a backdoor in for later entry.

I don’t want to do a port scan on the company network, that would create a lot of suspicious network activity and probably set off whatever antivirus software protects the company devices. Instead, I would perform a passive network capture to try and determine what other devices are running on the LAN. Maybe some of them may be vulnerable, too. If the company is running a windows network, I would be able to identify the IP address for the domain controller, the Intranet server, other Windows hosts, any printers and scanners. This information helps give me an overview of the company LAN before I attempt propagating through the network.

1. Network Propagation

As mentioned before, the recon I perform on the initial host provides information helpful when preparing to propagate through the network. While a network capture helps to identify other hosts on the network, it also makes it possible to see if there are any other vulnerable applications running on the network as well. Perhaps the Intranet server is serving web pages with an insecure version of Apache or Microsoft IIS? Maybe the printers are outdated and insecure, and I can capture whatever information is sent to be printed? The AD server might be blasting out packets that indicate it is an older version with a public exploit. Any of these are potential possibilities.

I may also have local administrator access to the initial foothold host if a vulnerable application allows me to escalate privileges. I could then install a keylogger, intentionally break something on the victim computer and wait for the employee to call IT for assistance. IT would then need to login with the necessary credentials, and I could intercept them and try to propagate through the network with these additional credentials.

1. Exfiltration Methods

As mentioned before, I could have an additional service running on my public-facing website. I would encrypt web traffic and have an ability to encrypt and upload files to the website. This way, I could exfiltrate any important data I discover. I would also attempt to use Veil to mask the delivery of my payloads. A lot of antivirus solutions would pick up attempts at me performing a privilege escalation attack on a host. By using Veil, the shellcode is injected into memory in a subtler manner.