Lab 3: CEN4048 Due xx/xx/19

Brandon Thompson 5517

October 7, 2019

1 Section 1 Images

2 Section 1 Research Report

2.1 Executive Summary

The websites `x128bit.com`, `iskytap.com` and `cloudparadox.com` are managed by the same people because the registered administrator is the same for all three. An attacker could use this because weaknesses in one could be used in another, `x128bit.com` and `iskytap.com` are less secure than `cloudparadox.com`.

Amazon being a large e-commerce company will be difficult to attack because they put so much effort into defending against it and verifying transactions. That being said because of the number of employees in the company they are more susceptible to social engineering attacks.

2.2 Methodology

The technical research involved the use of the Sam Spade tool to provide domain information from multiple sources about the site in question. The Sam Spade tool can also ping the site. The technical research also utilized the `nslookup` tool from the command prompt. `Nslookup` is used for DNS queries to provide associated IP addresses for a domain. The last tool used in this section is the `tracert` (traceroute) tool. Traceroute gives a list of names and IP addresses of all intermediate systems between the target and caller. This can provide additional attack points or the geographic location of the target system.

2.3 Technical Research Results

2.3.1 `x128bit.com`

The Sam Spade tool provided the email address (`shulbert@securitycentric.net`) and phone number (+1 (925) 292-4309) of the registered administrator.Using the ping tool of Sam Spade provides 10 pings to the IP address `208.91.197.27`. The `nslookup` tool showed that there were no additional IP addresses associated. Traceroute gave 14 intermediary servers between the virtual machine and the target.

2.3.2 iskytap.com

Iskytap.com has the same information as the previous x128bit.com.

2.3.3 cloudparadox.com

Sam Spade tool was unable to ping cloudparadox.com at IP address 50.225.131.227. Nslookup provided no alternative IP addresses, traceroute timed out after jumping the 17^{th} time at 162.151.79.166.

2.4 Public Domain Research Results

The organization that i decided to target is Amazon because they are a large e-commerce site and I use them often. The domain name is amazon.com and they use the same URL for their online sales. They physical address is listed as 410 Terry Avenue North Seattle, Washington 98109-5210, but they are planning to expand to another building soon. There are 10 officers of the company, the CEO being Jeffrey Bezos, with 7 senior vice presidents and 2 vice presidents. Amazon employs over 600,000 people, 15,000 of those are corporate employees in 40 different locations. Amazon also owns more than 40 subsidiaries including audible.com, A9.com, Goodreads, Ring and twitch.com.

2.5 Findings and Conclusions

X128bit.com and iskytap.com could be vulnerable to attackers because we were able to ping the server multiple times and follow a traceroute to the home system. Cloudparadox.com is more secure because it does not allow pings and we could not follow the trace back. Amazon, being such a large company with almost all business going through the internet, probably has a lot of security in place, but the large amount of employees means they are susceptible to social engineering attacks.

2.6 Avenues of Future Research

Additional research into the companies would include how secure the physical building is for social engineering attacks or physical attacks. If i was planning a hack into these companies I would ask questions like how would they defend against _____ or what is the best method to gain access to the system.

3 Section 2 Research Report

3.1 Executive Summary

3.2 Methodology

3.3 Technical Research Results

3.4 Public Domain Research Results

Target organization if Amazon, all info is the same as Section 1 Research Report ??PDR1PDR1 Target organization if Amazon, all info is the same as Section 1 Research Report ??