Katya Bespartochna
Systems Design and Analysis
December 15th, 2020

CyberWar After Action Report

The red team did not have a very detailed strategy for attacking the blue team. Our basic strategy was to scan the network using nmap and grep. Once something unusual showed up in the command line, the team can try some social engineering directed at that file. One of the most valuable pieces of information was the time and date of the file. It is highly unlikely that the blue team could have manipulated the time in that file.

Timing and extent of the event

There were only days out of the week which the cyberwar took place. It was not much of a cyberwar since the blue had successfully hidden their file in a way that would that the red team a long time to figure out. Here is what happened during the two days:

December 8th: test out various network addresses

I'm struggling to get into the network. The hostname 10.4.20.0/24 did not exist. Then I tried logging into VNC to get to the raspberry pi. The good thing was that the VNC viewer did not exist like PuTTY when the network address.

Types 'nmap'. I'm not sure how I got here but I typed in a bunch of commands and they are not responding, not even with a command that does not have an available message.
What does it mean when the command terminal is blank when one of the addresses is entered?
My guess is that the host is down.

```
10.4.20.5 → connection refused
10.4.20. → command not recognized <hpiLO>
```

December 10th,

It might be possible that the file is on the https://penguin.cairn.edu/ server.

How do we find the directories in the https://penguin.cairn.edu/ server?
It looks like the blue is blocking passwords that use keyboard authentication. I can tell because the only server that works, 10.4.20.7 says "`keyboard-interactive authentication, Password: Access denied`"

Possible solution: use `SSH Config Reset`
Another solution: uncheck "`keyboard interactive auth`".

Much of the solutions tells the user what to use but doesn't show where and there might be no networks that let the user.

The blue team had succeeded in protecting their file using OpenSSH servers. This authentication originally allows six retries before locking out a user and not letting them in for a certain amount of time. The keyboard-interactive authentication feature allows as many retries as the users want(eConstantin). If this feature was enabled and the blue was not looking out for attacks, there could have been thousands of passwords retrieved from the red team and that could be the start of the red team planning an attack.

personal reflections

The entire cyber way simulation was very confusing. In the beginning, our team needed to figure out how to get into each network available for the cyberwar. Many of the networks did not work and depending on which user was logging in, it did not allow authentication to work to a certain extent. There might have been a lack of miscommunication between the team. One teammate did not show up and another teammate was behind in discovering how far the entire went. If a group of students was to do another cyberwar, it would to do few cyberwars in the middle of the semester and have everyone present to see in real-time what is going on.

---

eConstantin, Lucian. "Bug Exposes OpenSSH Servers to Brute-Force Password Guessing Attacks." CIO (13284045), July 2015, p. 1. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=bsu&AN=109023606&site=eds-live.

stimations of the recovery cost of the intrusion, any legal ramifications