Red Team vs Blue Team CTF

The cybersecurity field has 750,000 open job positions in the United States, with 60,000 in Virginia (Cyberseek, 2023). In addition, hands-on work is a requirement if students want to be competitive in the industry. As a result, the ODU Cyber Security Student Association (CS2A) proposes a Red Team/Blue Team CTF to give students experience with both hardware and software they may encounter in the workplace. CS2A will create a network for a fictitious business with security flaws. Participants can either be on the team that attacks or defends the network. The defending team will get points for keeping services up, while the attacking team will get points for taking services offline.

Purpose

The Bureau of Labor Statistics projects about 377,500 openings yearly in the Computer and Information Technology Operations occupation group (Computer and Information Technology Occupations, n.d.). With the growing amount of technology that encompasses everyone's daily lives, more people are needed in cybersecurity. Additionally, increasing the number of professionals is not enough; it is also imperative that these professionals are trained and knowledgeable about the industry. As a result, hands-on work is a requirement to ensure systems are protected. This project aims to give students experience with the hardware and software they may encounter in the workplace.

The Project

The Cyber Security Student Association (CS2A) will be hosting a Red Team/Blue Team CTF (capture the flag) (referred to as the CTF). The CTF infrastructure will emulate the network of a local business, PENG Corp. As PENG Corp's business expanded, they added more cybersecurity infrastructure. However, they did not have a security operations center (SOC), and their security infrastructure had holes. The Blue Team participants are part of PENG Corp's SOC.

As PENG Corp's business continues to expand, they get more clients. As a result, the 0xe10cr4hc APT (advanced persistent threat) group wants to exfiltrate data on high-value customers PENG Corp does business with. The 0xe10cr4hc APT group is the Red Team in the competition.

Hardware & Software

The CTF infrastructure will consist of three desktop computers, three switches, and the personal computers of competitors. The first device in the network is a main firewall to route traffic between the infrastructure and the Internet. This firewall will filter all traffic except

destination ports 80 (HTTP) and 443 (HTTPs) to ensure devices in the network are not accessing unknown services.

In addition, the infrastructure has a DNS server to manage DNS queries for the network. The firewall blocks all outbound DNS queries from devices except the DNS server. This results in devices on the network using the infrastructure DNS server to access domains on the Internet. The infrastructure team can block domains using direct strings or regular expressions.

Connected to this filter firewall is a switch that emulates the Internet. The Red Team connects their computers to this switch to access the Internet and the Blue Team network. Therefore, anything connected to this switch is on a “virtual Internet.”

The Blue Team network consists of two more firewalls with two more switches. There is a single connection from the Blue Team firewalls to the switch emulating the Internet. However, the Blue Team firewall is configured insecurely. This incorrect configuration allows the Red Team to access and attack services from the emulated Internet. On the other hand, the configuration mandates that the Blue Team patches the security holes.

The aforementioned hardware and software have been tested and are functioning. CS2A does not need additional hardware to add services to the CTF infrastructure. However, CS2A needs access points or USB/USB-C to ethernet adapters for students whose devices cannot access the infrastructure through an ethernet cable.

If CS2A is not permitted to connect the infrastructure to the Internet, then students have to use an ethernet cable to connect to the infrastructure. They will use Wi-Fi to connect to the Internet.

Teams

The competition will consist of two teams: the Red Team and the Blue Team. Each team will have up to ten students. The Red Team will attack the Blue Team’s network, while the Blue Team will defend their network and services from the Red Team.

The teams will be in different rooms to coordinate, plan, and execute actions without the other team knowing about their plans. For example, if the Red Team discovers a vulnerability, the Blue Team should not hear the Red Team talking about it because the two teams are in the same room. The same goes for the other way around. If the Blue Team configures a honey pot to distract the Red Team, the Red Team should not discover this by listening to the Blue Team’s conversation from across the room.

Points

Points are given according to the number of services the Blue Team keeps online every minute. The Blue Team will start with zero points and all services online. The Red Team starts with a set amount of points and loses them for each online service every minute. Each service will have a different point value according to its importance to PENG Corp's business.

In addition to getting points from the availability of services, participants can get points from finding flags on the network. This is similar to a jeopardy-style CTF. There will be protections to ensure the Blue Team does not prohibit the Red Team from getting a flag and vice versa. Both teams will lose points if a flag is not available. These additional flags also make it easier for the participants with less knowledge to contribute to the points for their team.

Conclusion

The Cyber Security Student Association wants to create a Red Team/Blue Team Capture the Flag event for its members. The purpose of the CTF is to give students valuable hands-on experience with hardware and software they may encounter in their careers. The CS2A has most of the hardware needed to build the infrastructure for the CTF. However, USB/USB-C to ethernet adapters and access points may be required for students who do not have an ethernet port on their device. The CTF will have two teams: a Blue Team and a Red Team. The Blue Team emulates the security operations center of a fictitious business PENG Corp. The Red Team is an APT group trying to exfiltrate data from PENG Corp. The network is initially configured insecurely, and the Blue Team has to secure it, while the Red Team has to exploit the vulnerabilities.

References

Cyberseek. (2023). Cybersecurity supply and demand heat map. Cyberseek. Retrieved December 16, 2022, from https://www.cyberseek.org/heatmap.html

Computer and information technology occupations: Occupational outlook handbook: : u. S. Bureau of Labor Statistics. (n.d.). U.S. BUREAU OF LABOR STATISTICS. Retrieved March 23, 2024, from https://www.bls.gov/ooh/computer-and-information-technology/home.htm