UNITED​ ​ STATES​ ​ MILITARY​ ​ ACADEMY

INCIDENT RESPONSE REPORT

CY 450

SECTION​ ​ I1

LTC JUSTIN SHAFER

BY

CADET​ ​ KENDYL T. MCFARLAND​ ​ ’21, ​ ​ CO​ ​ G1

CADET​ ​ GREYSON M. OLEP​ ​ ’21, ​ ​ CO​ ​ E1

CADET​ ​ TAYLOR R. SCHORLEMMER ​ ’21, ​ ​ CO​ ​ F2

CADET​ ​ BENJAMIN M. SIEGEL​ ​ ’21, ​ ​ CO​ ​ E1

CADET​ ​ JOSEPH N. ZUCCARELLI​ ​ ’21, ​ ​ CO​ ​ F1

WEST​ ​ POINT, ​ ​ NEW​ ​ YORK

11 MAY 2021

\_\_\_\_​ ​ OUR​ ​ DOCUMENTATION​ ​ IDENTIFIES​ ​ ALL​ ​ SOURCES​ ​ USED​ ​ AND​ ​ ASSISTANCE RECEIVED​ ​ IN​ ​ COMPLETING​ ​ THIS​ ​ ASSIGNMENT.

KM;GO;TS;BS;JZ\_\_\_\_​ WE​ DID​ ​ NOT​ ​ USE​ ​ ANY​ ​ SOURCES​ ​ OR​ ​ ASSISTANCE​ ​ REQUIRING​ ​ DOCUMENTATION IN​ ​ COMPLETING​ ​ THIS​ ​ ASSIGNMENT.

Shape, arrow

Description automatically generated



SIGNATURE: ​ ​ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



**Executive Summary.**

For the culmination of the capstone exercise, our group experienced a cybersecurity breach and attempted to not only keep the adversary out of the network in real time, but also mitigate any fall-out consequences. At the start of the incident response exercise, we had already created a functioning network that provided full availability and some security measures. After creating this minimally functioning network, we decided to take snapshots of each VM—the client, internal DNS, external DNS, and web server—so that we could revert to the functioning state should a devastating attack occur.

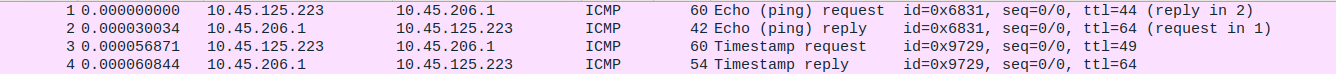
Along with taking snapshots, we also assigned each team member a single VM to monitor during the incident. The individual team members primarily examined log files and network activity through Wireshark. Due to this monitoring, our group quickly realized when an attack occurred. Once we noticed suspicious activity in the network, we took measures such as blocking nefarious IP addresses on the router and deleting new users on the VMs.

Although our monitoring plan was somewhat effective, the attacker still successfully penetrated the network. After the attack occurred, we examined old log files and Wireshark captures and learned from our mistakes. This reflection encouraged us to revert back to the old snapshots to restore the minimally functioning network, but it also taught us to enact more thorough security measures such as restricting SSH access to the internal network in order to create a more robust network moving forward.

**Monitoring Plan.**

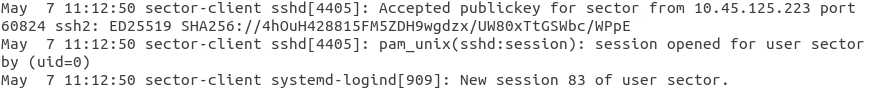
Initial plans to monitor the network led our group to the conclusion that we should assign a team member to each virtual machine because there was one virtual machine for each individual. This led to the following assignments for the virtual machines: Web Server – Joseph Zuccarelli, Client – Iggy Siegel, Router – Taylor Schorlemmer, External DNS – Kendyl McFarland, and Internal DNS – Greyson Olep. On each VM we used Wireshark to actively monitor activity within our network. Wireshark allowed us to capture the packet files in real time during the incident and monitor any suspicious activity. Each team member saved Wireshark incident capture files following the conclusion of the exercise, which we then used to conduct post incident analysis. Specifically, we filtered these capture files by the IP address that we identified for the attacker (10.45.25.223 & 10.45.25.222). Using this filter, we were able to effectively trace the attacker’s actions within our network. We also examined log files on each VM during the incident. The log files were also used to conduct post incident analysis; however, this was not nearly as efficient and effective as filtering the Wireshark incident capture files.

**Incident Narrative.**

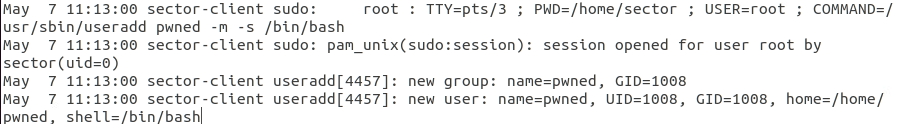
The attacker started by surveying our network using pings and port probing on hosts.



The attacker then used SSH to log into the sector account on the client VM.



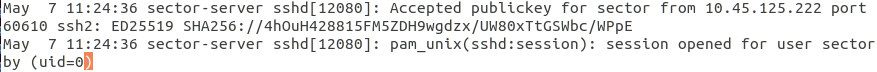
The attacker then created a new user called ‘pwned’ with elevated privileges.



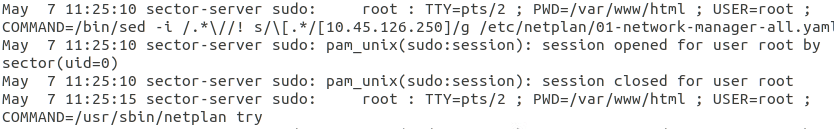
Finally, the attacker changed the sector user’s background on the Client VM.



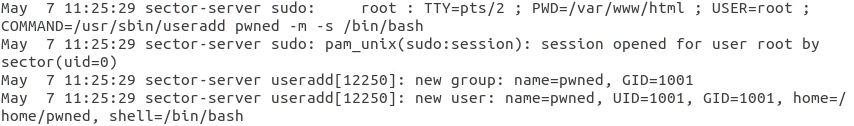
The attacker then attempted to SSH into the Web VM from the Client VM, yet this failed. Afterwards, the attacker used SSH to connect to the VM from a new IP address.



The attacker then modified the DNS server IP address on the Web VM.



Finally, the attacker created another ‘pwned’ user on the Web VM.



**During Incident Actions.**

During the incident response exercise, we successfully identified that an unknown IP address was carrying out malicious actions within our network. This IP address was identified as 10.45.25.223. Along with the IP address identified, an unknown user was discovered on the network.

To counteract the unknown IP address trying to gain access to our network, we went on to the router and blocked all traffic from the unknown IP address. We did this because the IP address was from an unknown source and potentially disrupting our network. This momentarily prevented the attacker from gaining access to the network and was thus effective at eliminating attacks from this source. However, the attacker then switched to the IP address 10.45.25.222. In order to deal with the pwned user on the VM, we simply removed the user from the network, as they were not authorized to be on the network. Similar to the security implementation earlier in the project, we decided that the best course of action to secure our network was to remove the suspicious user. This action was effective in that the user was removed from the network immediately and no longer had access to the network.

**Recovery Plan.**

After reviewing the incident and analyzing our response, we decided that in order to protect our network from future attacks we must give less access to unknown sources. When viewing this from a tradeoff analysis lens, this would indicate that we are sacrificing availability for security, but the security of the network is of higher importance after vulnerabilities have been exposed.

In response to the incident, we would first revert to the captures of the virtual machines before the incident. We would then make the access control lists stricter and disable SSH from IP addresses outside of our network. While the design specifications of this network initially indicated to enable all SSH into the network, this incident showed that allowing SSH from all sources is a vulnerability. To prevent future attacks like this in the future, the first step is to prevent similar attacks from happening, which can be prevented by disabling SSH from all sources into the network.