Incident Report

Alvin Johns
Group Two
Enterprise Defense

March 14, 2024

"$You're$"

Contents

SIEM installation and configuration (describe the systems your team put in place to detect non-allowed activities) System Hardening (what you did to make the systems less vulnerable to attack, including the tools used if any, and why you needed to perform that task) Vulnerability Management (describe your process for detecting known vulnerabilities in the system, the vulnerabilities found, and how you mitigated them) List of changes made to each system (this may exceed your page limit, which is ok)

1 Preparation

1.1 SIEM Installation:

Team installed a Wazuh Manager on host 192.168.1.21. Wazuh Agents were installed on the Domain Controller (192.168.1.20), Windows 10 Workstation (192.168.1.23), and Ubuntu Server (192.168.1.22).

1.2 System Hardening:

Full detail of steps taken are listed under the *closed* and *open* issues.
Open issues (*Bug/Unhandled*): open issues
Closed issues: closed issues
Proceeded through the CIS Ubuntu Linux 22.04 LTS Benchmarks to harden the server on Saturday March 9, 2024. Loaded and ran the following scripts up to procedure 3.3.9 *NetworkParameters*.
Scripts loaded and ran on Saturday, March 9, 2024: scripts run

Sunday evening, conducted a user audit of the Ubuntu Server and Active Directory.

Starting with the ubuntu server, located the users with DEV permissions: Adams, Soto, Jones. Removed those user's access to admin and sudo privilege elevation by commenting out the %admin ALL=(ALL) ALL line in the */etc/sudoers* file.

```
# Members of the admin group may gain root privileges
#%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

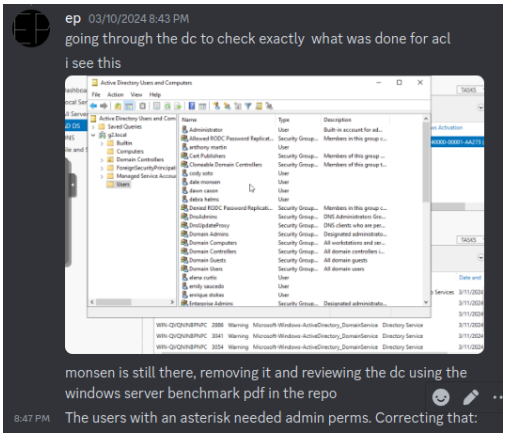
Sample screenshot.
Not taken at time of change.

On the DC, discovered several users that either were not on the authorized user list, or were on the authorized user list who had unauthorized admin access.

Removed Monsen, Garza, Lewis, Armstrong, Mixon, Beeson.

In all cases, Remote Desktop Control was enabled. Disabled that feature for all users, including admins.

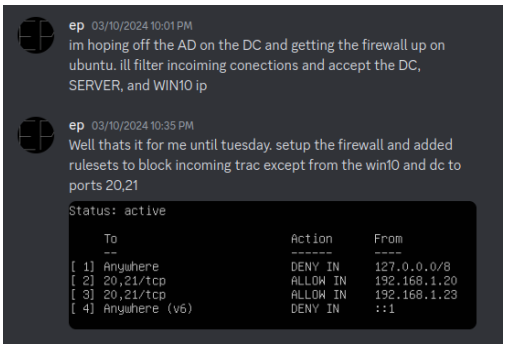
Completed audit of AD User List at 9:50pm.



Enabled firewall and ruleset on the Ubuntu Server at 10:30p.

Incoming TCP traffic allowed to port 20,21 from the domain controller and windows workstation.

Denied incoming loopback traffic to reduce network noise.



2 Incident Overview

Day 1:

Tuesday, March 12, 2024 between 02-02:35p, an unknown entity gained access to the user account on the Ubuntu Server (192.168.1.22) from IP address 192.168.1.161. The initial attempts to boot the user from the server failed. Attempts to create a firewall rule to block the intruder's IP address failed. Lost access to critical system services including ssh and mysql. If recovery is still an option, an audit should be conducted to determine the extent of the attack.

Observations while server access was still available:

- /etc/ufw/applications.d modified, causing ufw control to be lost.
- was able to kick user on pts/4 from server
- removed root ssh host key from /etc/ssh/*key*
- Intruder disabled sshd, mysql, and potentially other services.

Performed on audit of AD users:

Admins:
CODY SOTO
DEBRAH HELMS
DOMAIN ADMIN
RNTERPRISE ADMIN
KENNETH JAMES
ROSA ADAMS
RUTH JONES
TOBY ATKINSON

Users:
ADMINISTRATOR
ANTHONY MARTIN
CODY SOTO
DAWN CASON
DEBRAH HELMS
EMILY SAUCEDO
ENRIQUE STOKES
JANET PAGAN
JOSEPH FLORIAN
JOSEPH LEE
KENNETH JAMES
KERBEROS
KIRTSTIN SUMMERFIELD
ROSA ADAMS
RUTH JONES
STUDENT
TOBY ATKINSON

3 Lessons Learned

Removing root access via modifying the sshd config file would have increased the security of the system. I opted not the remove or alter root or user profile ssh access given that we were told not to remove or change passwords and maintain access to the VMs. In hindsight, I should have done what I would have done and restrict access to a set of users and change ssh keys. This was the mistake that led to the system hijacking. During the system hardening steps, spending more time auditing the firewall to secure the perimeter network would have been better. Trying to be thorough within the timeframe came at the cost of the data lost in the first attack scenario.