Incident Report

Alvin Johns
Group Two
Enterprise Defense

March 13, 2024

”$You're$”

Contents

1 Preparation

1.1 SIEM Installation:

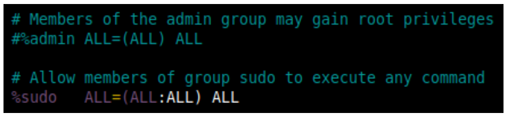
Team installed a Wazuh Manager on host 192.168.1.21. Wazuh Agents were installed on the Domain Controller (192.168.1.20), Windows 10 Workstation (192.168.1.23), and Ubuntu Server (192.168.1.22).

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
Scripts loaded and ran on Saturday, March 9, 2024: scripts run

Proceeded through the CIS Ubuntu Linux 22.04 LTS Benchmarks to harden the server on Saturday March 9, 2024. Completed up to procedure 3.3.9 *NetworkParameters*.
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
```

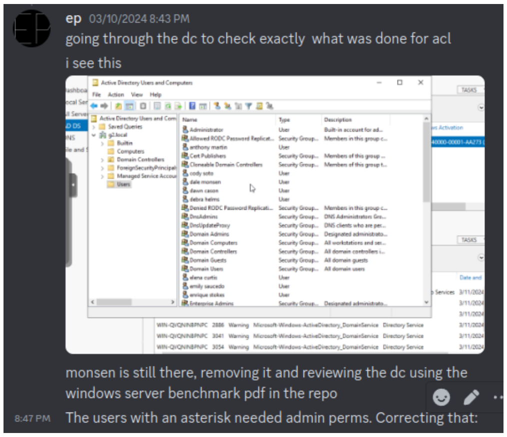
Sample screenshot.
Not taken at time of change.

On the DC, discovered several users that either were not on the user list, or were on the user list who were not supposed to have 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.



ep 03/10/2024 8:43 PM
going through the dc to check exactly what was done for acl
i see this

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RODC Password Replicat...	Security Group...	Members in this group c...
anthony martin	User	
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
cody soto	User	
dale monsen	User	
dawn cason	User	
debra helms	User	
Denied RODC Password Replicati...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
elena curtis	User	
emily saucedo	User	
enrique stokes	User	
Enterprise Admins	Security Group...	Designated administrato...

```
WIN-QVQNINBPNPC  2886  Warning  Microsoft-Windows-ActiveDirectory_DomainService  Directory Service  3/11/2024
WIN-QVQNINBPNPC  3041  Warning  Microsoft-Windows-ActiveDirectory_DomainService  Directory Service  3/11/2024
WIN-QVQNINBPNPC  3054  Warning  Microsoft-Windows-ActiveDirectory_DomainService  Directory Service  3/11/2024
```

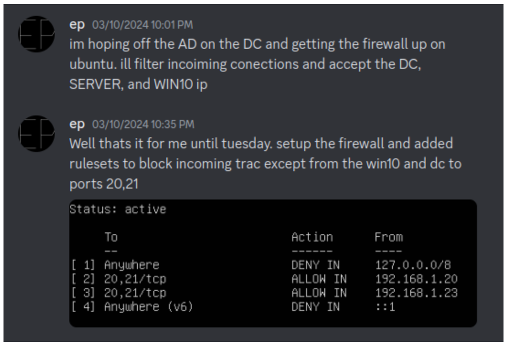
monsen is still there, removing it and reviewing the dc using the windows server benchmark pdf in the repo

8:47 PM The users with an asterisk needed admin perms. Correcting that:

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.



ep 03/10/2024 10:01 PM
im hoping off the AD on the DC and getting the firewall up on ubuntu. ill filter incoiming conections and accept the DC, SERVER, and WIN10 ip

ep 03/10/2024 10:35 PM
Well thats it for me until tuesday. setup the firewall and added rulesets to block incoming trac except from the win10 and dc to ports 20,21

```
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] Anywhere                   DENY IN     127.0.0.0/8
[ 2] 20,21/tcp                  ALLOW IN    192.168.1.20
[ 3] 20,21/tcp                  ALLOW IN    192.168.1.23
[ 4] Anywhere (v6)              DENY IN     ::1
```

1.3 Vulnerability Management:

1.4 List of System Changes:

2 Incident Overview

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.
/etc/ufw/applications.d modified, causing ufw control to be lost. intruder disabled sshd, mysql, and potentially other services.

3 Identification

4 Containment

5 Eradication

6 Recovery

7 Lessons Learned