**CNIT 47000 Lab 2 Report**

**Group 44**

**09/14/23**

**Ethan Hammond**

**Jordan Sexton**

**David Hjelmeland**

**Geoffrey Vest**

**Ubuntu Machine:**

Evidence recovered off of the Ubuntu machine has been broken up into three categories. The evidence obtained can be categorized as benign evidence showing that nothing has been tampered with, suspicious evidence that shows something may have been modified or accessed with certain parameters, or confirmed evidence proving that something has been wrongfully modified or accessed.

**Benign evidence:**

Benign evidence from the Ubuntu machine was recovered as proof that certain important directories have not been accessed or connection attempts have not been made. All evidence explained can be seen in Figures 1-3 below.

At the time of initial investigation, there were confirmed no SSH users currently connected to the system. Important files like /etc/hosts, /etc/resolv.conf, /etc/passwd, /etc/shadow, and /etc/group were confirmed to not have been modified. This does not rule out unauthorized access, but solely modification.

who -a

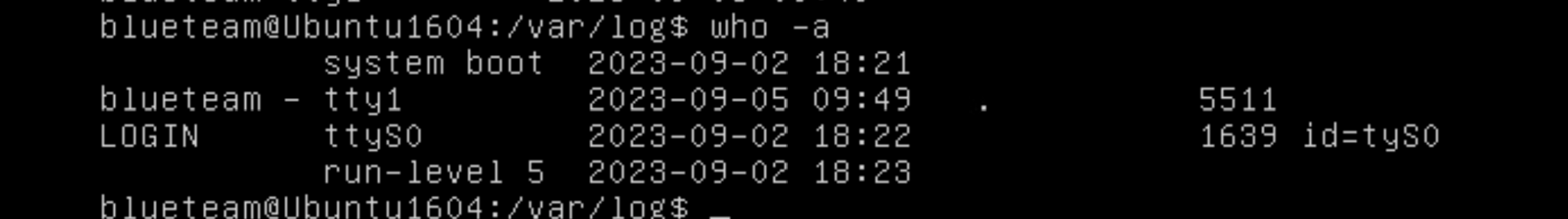


Figure 1: No SSH users currently connected to the system.

cd /etc

ls -alh | grep hosts

ls -alh | grep resolv.conf

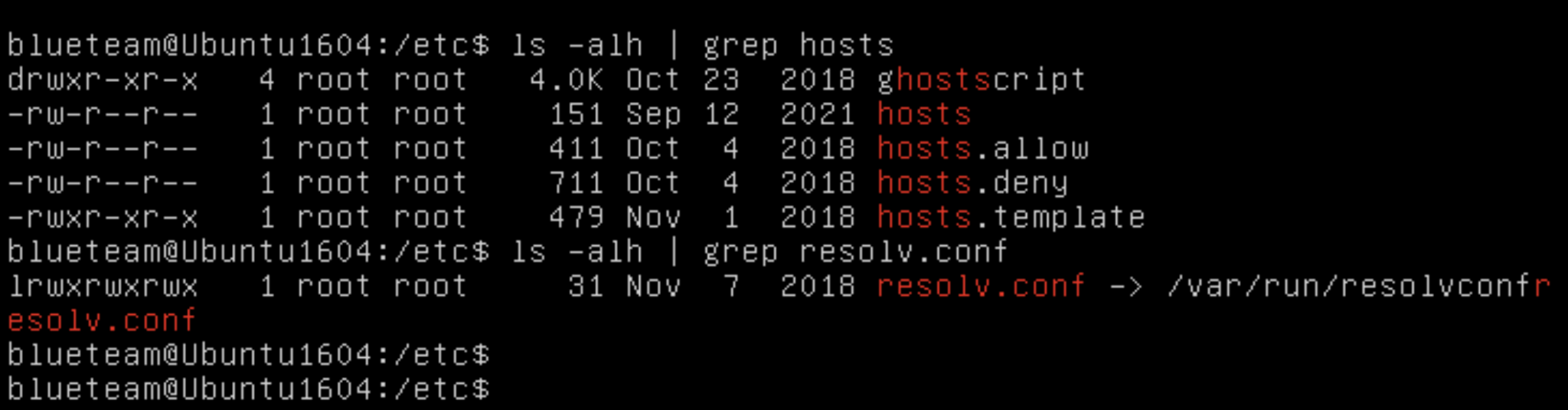


Figure 2: No hosts or DNS files tampered with.

cd /etc

ls -alh | grep passwd

ls -alh | grep gshadow

ls -alh | grep group

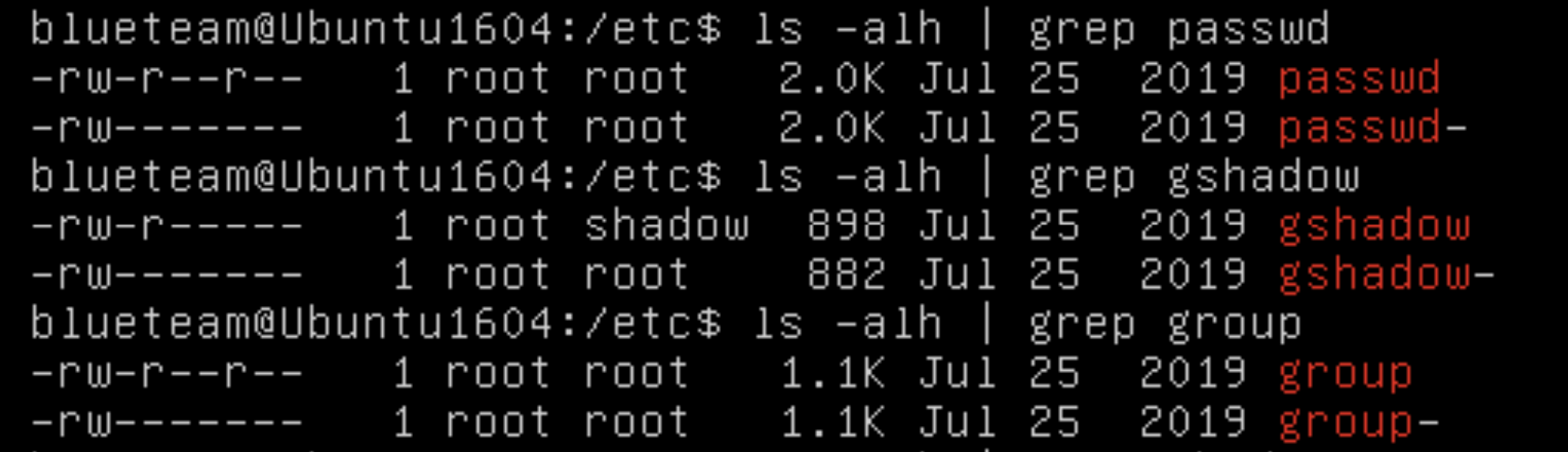


Figure 3: No passwd, gshadow, or group files tampered with in /etc

**Suspicious evidence:**

Suspicious evidence was gathered from the machine outlining acquired evidence that does not prove malicious access, but could be worth further investigation to determine if this was malicious activity or not. This evidence is outlined in Figures 4-9 below.

Evidence that is not confirmed malicious action, but could be considered suspicious includes modification of the /etc/network/interfaces file. As this file contains network interfaces, this could be utilized as a backdoor for a malicious user. Next, a device file ‘f’ was modified or created in /tmp recently that could be worth looking into. WTMP and BTMP log files were accessed to check for login attempts, however, the log files seem to have been erased. Lastly, /var/log/syslog shows a remove command used on the previously stated /tmp/f device file many times. This could be considered suspicious as the file itself was suspicious, let alone someone trying to delete it.

cd /etc  
ls -alh | more

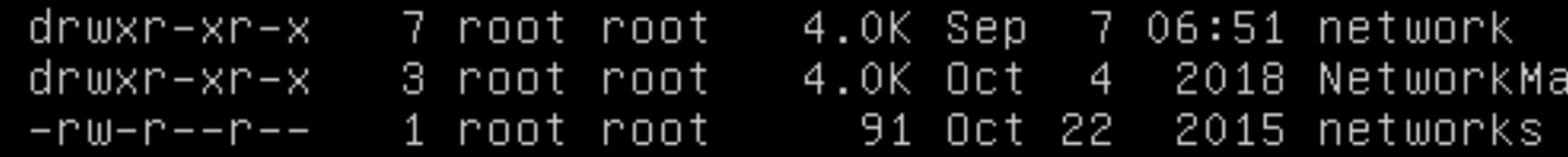


Figure 4: /etc/network directory changed today.

cd /etc/network  
ls -alh | more

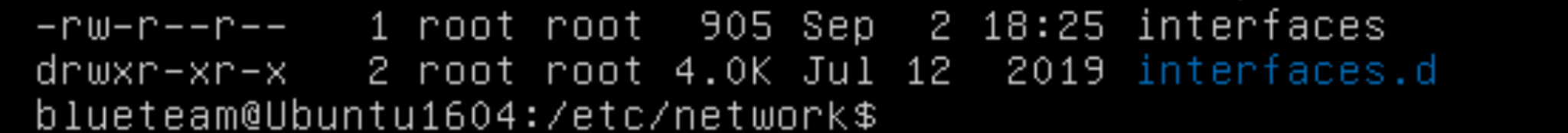


Figure 5: Specifically /etc/network/interfaces file changed

cd /  
ls -alh | more

Figure 6: /tmp directory changed today.

cd /tmp  
ls -alh | more

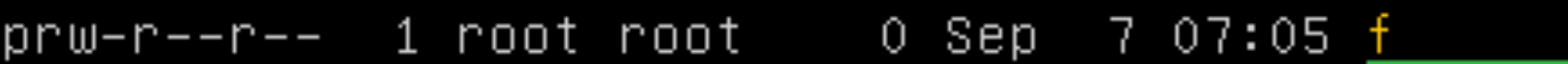


Figure 7: Specifically /tmp/f device file created or changed today.

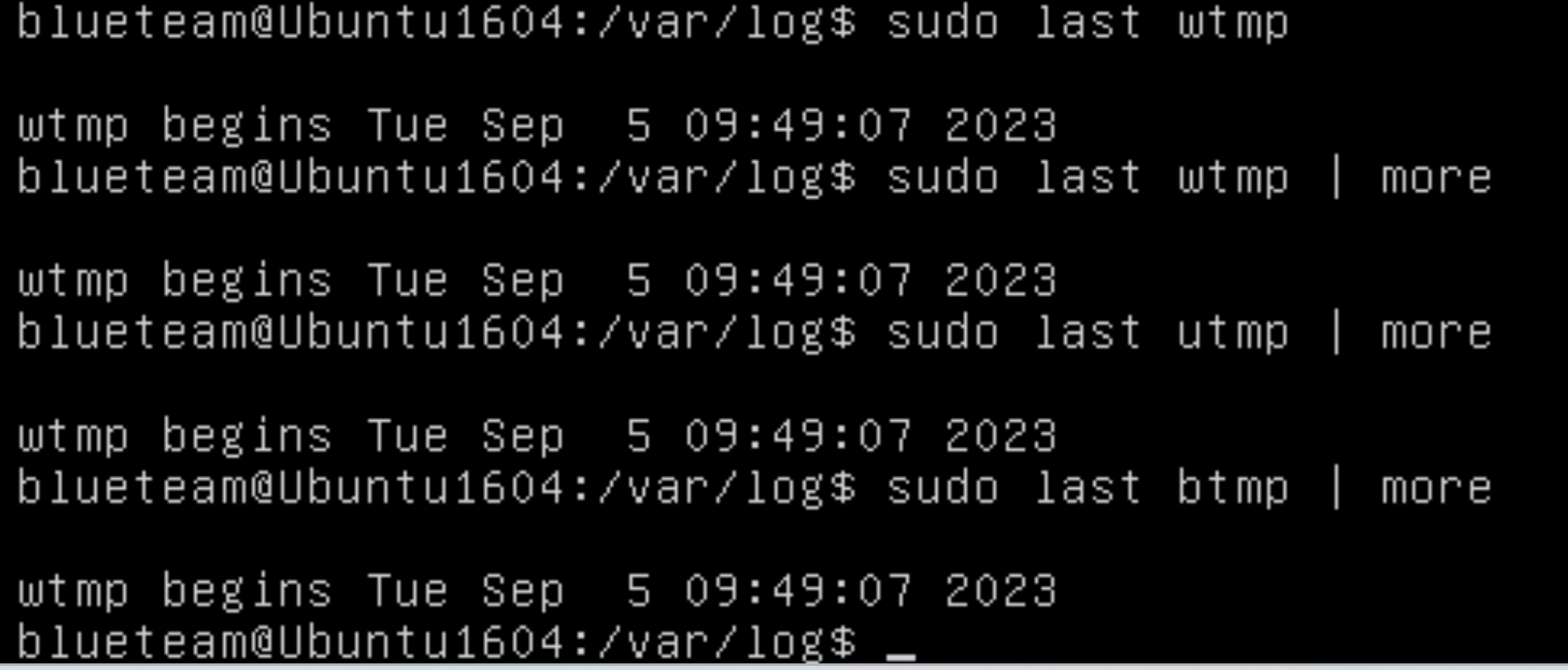


Figure 8: All log files containing login data are empty.

more /var/log/syslog

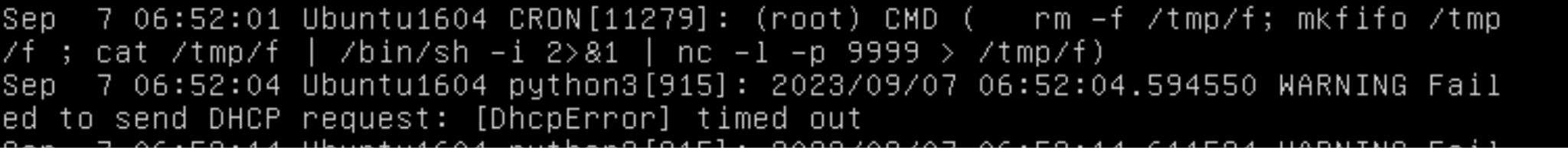


Figure 9: remove command for /tmp/f device file appears several times.

**Confirmed evidence:**

Confirmed evidence that has been gathered is evidence that proves malicious activity in the systems. This could contain modification of important files, unauthorized access of files, copying of file data, or login attempts. This evidence is outlined in Figures 10-15 below.

First, the /etc/shadow file was changed at the time of the attack, which should never be changed unless a user’s password is changed. Second, /var/log/auth.log shows an SSH connection success of root user at the time of the attack. The stat command was used to prove that /etc/passwd, /etc/group, /etc/shadow, and /etc/network/interfaces were all accessed at the time of the attack. /etc/shadow and /etc/network/interfaces were modified as well. At this time, the goal of the attack is unknown, but it is confirmed that sensitive files were accessed and modified.

cd /etc  
ls -alh | more

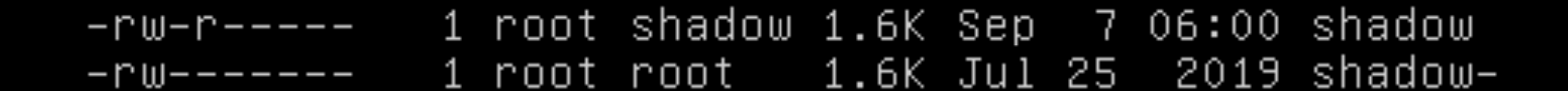


Figure 10: /etc/shadow file changed today.

more /var/log/auth.log

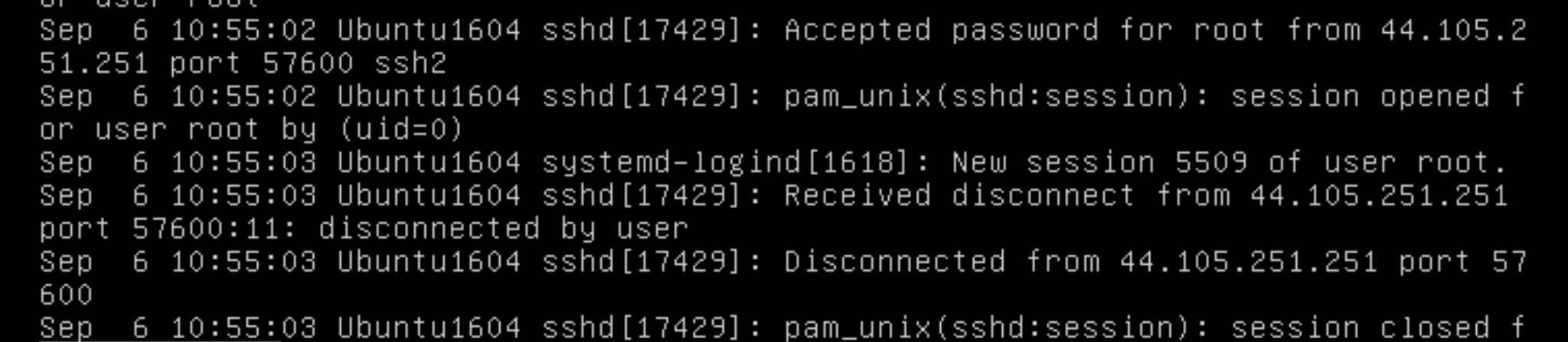


Figure 11: SSH session for root user on Sept 6 at 10:55am.

stat /etc/passwd

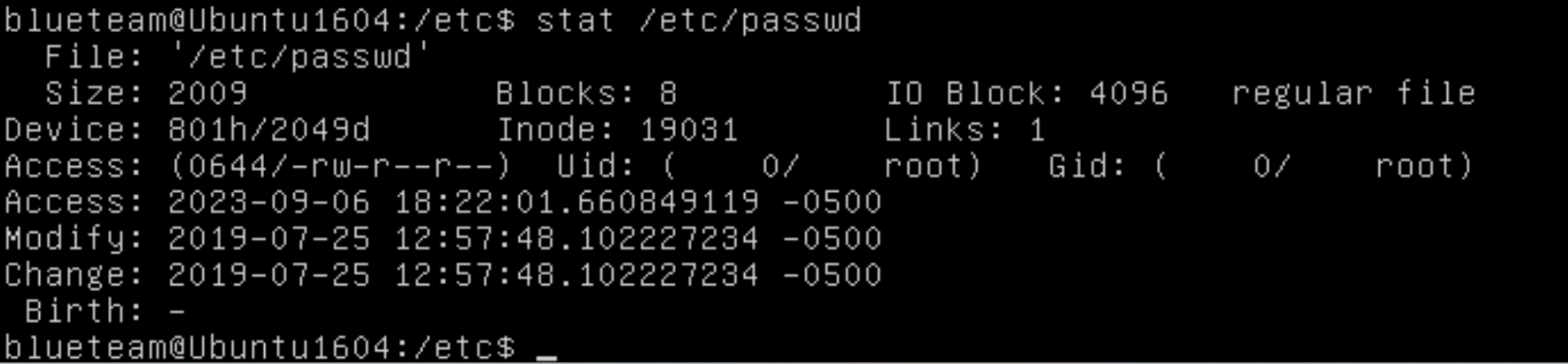


Figure 12: /etc/passwd accessed on Sept 6.

stat /etc/group

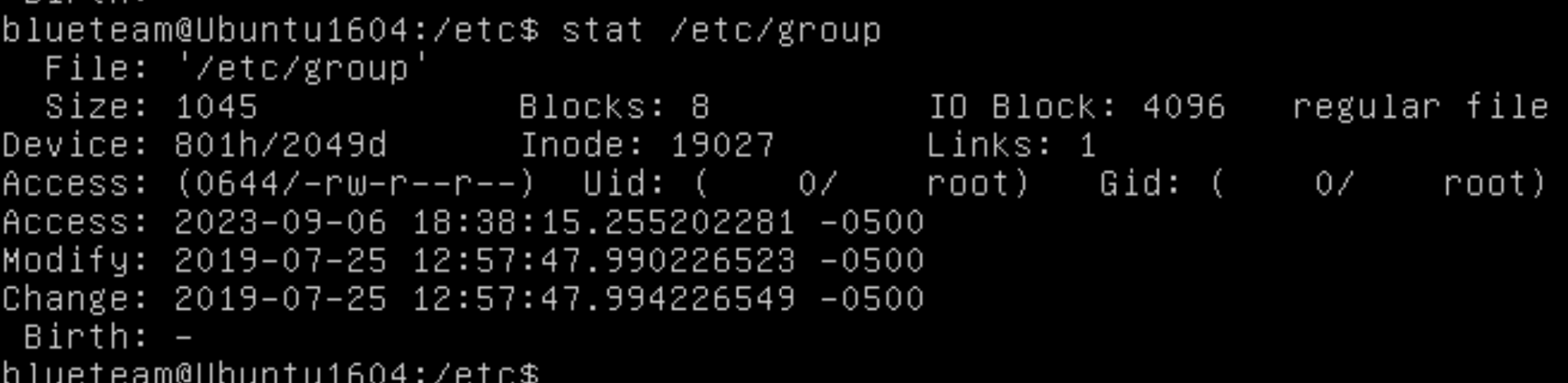


Figure 13: /etc/group accessed on Sept 6.

stat /etc/shadow



Figure 14: Further evidence of tampering/accessing of /etc/shadow

cd /etc/network

stat interfaces

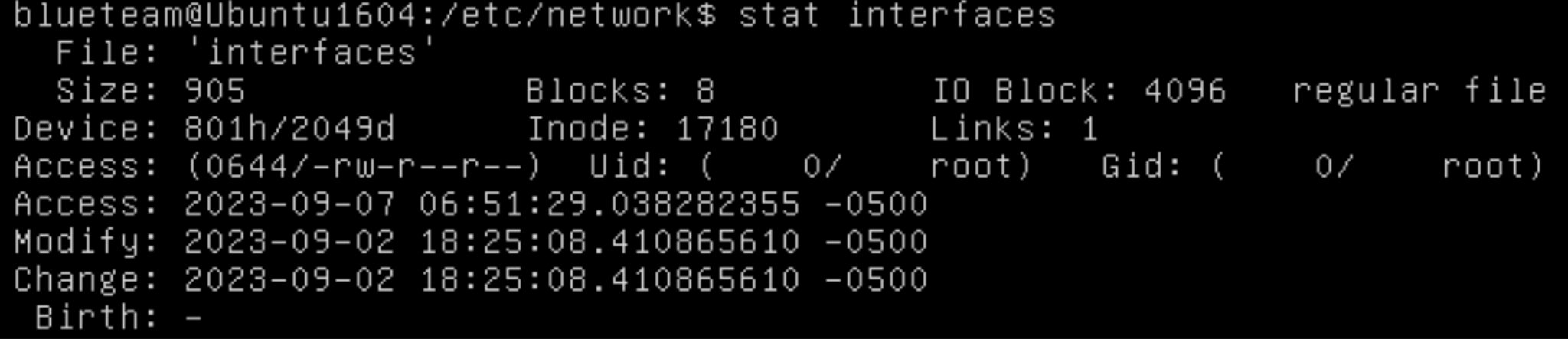


Figure 15: /etc/network/interfaces file accessed recently.

**Debian Machine:**

**Benign evidence:**

Certain important directories have not been accessed or connection attempts have not been made on the Debian machine. The evidence showing this is detailed in this section as benign evidence, and all evidence explained can be seen in Figures 16-26 below.

At the time of initial investigation, there were confirmed no SSH users currently connected to the system. Important files like /etc/hosts, /etc/resolv.conf, /etc/passwd, /etc/shadow, and /etc/group were confirmed to not have been modified. This does not rule out unauthorized access, but solely modification.

who -a

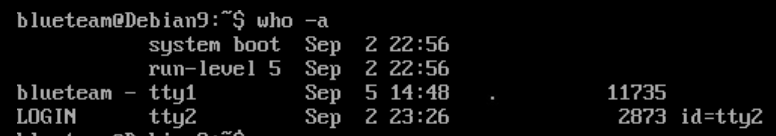


Figure 16: No odd logins

cd /etc

ls -alh | grep hosts

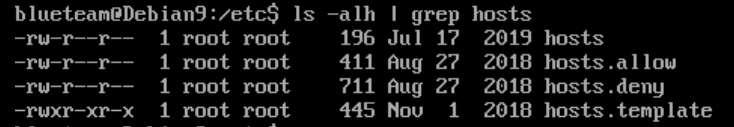


Figure 17: No files altered

ls -alh | grep resolv.conf



Figure 18: resolv.conf altered last week (for last week's lab?)

cd /etc

ls -alh | grep passwd

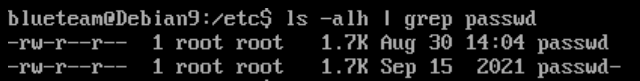


Figure 19: No files altered

ls -alh | grep gshadow

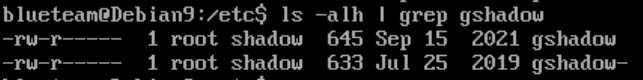


Figure 20: No files altered

ls -alh | grep group

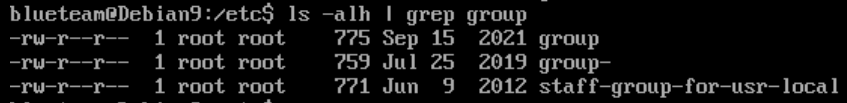


Figure 21: No groups altered

cd /etc  
ls -alh | more

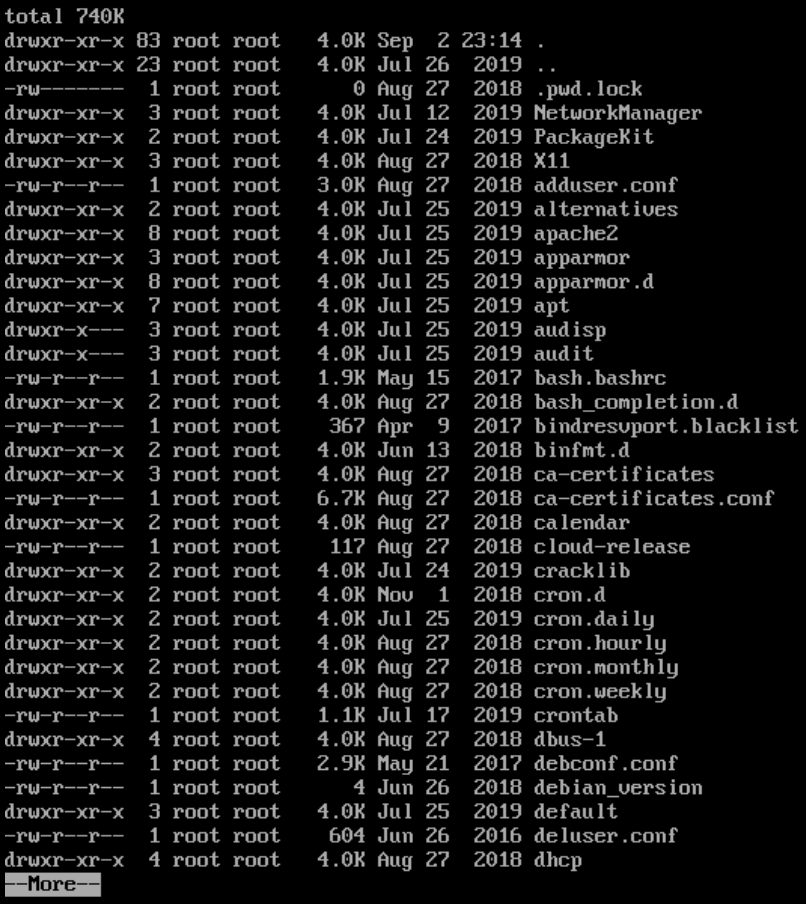


Figure 22: Nothing odd

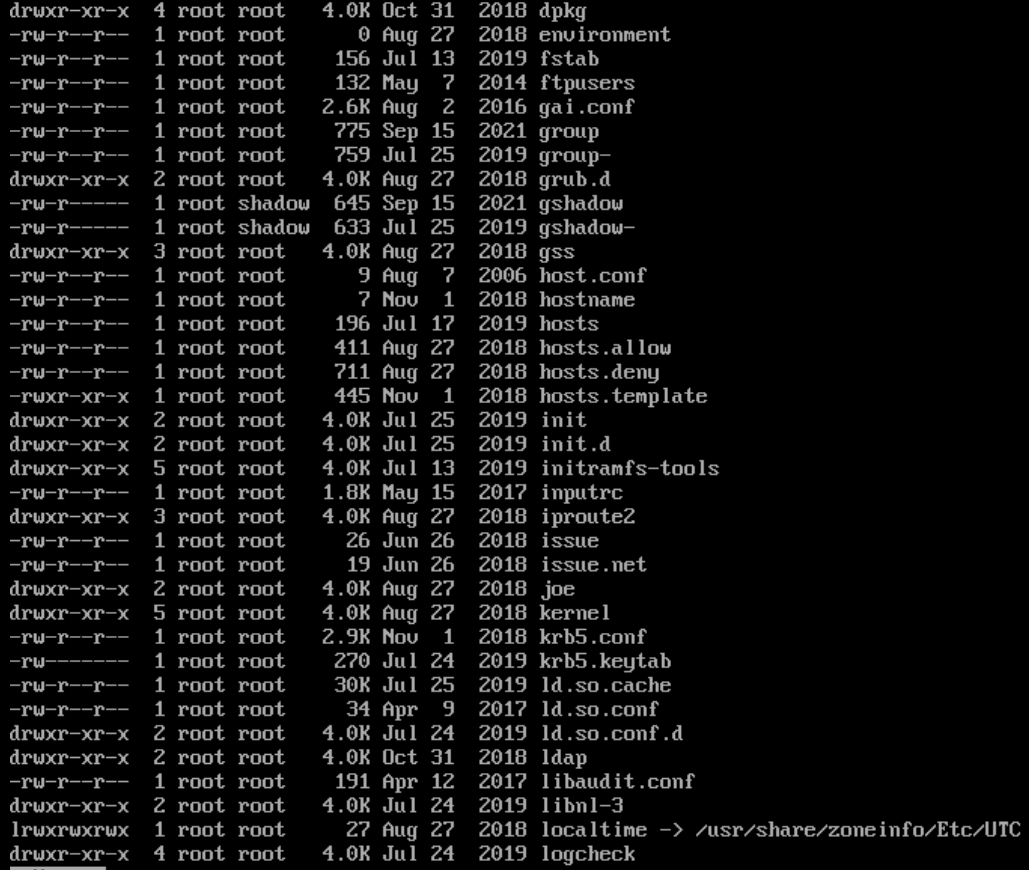


Figure 23: Nothing odd

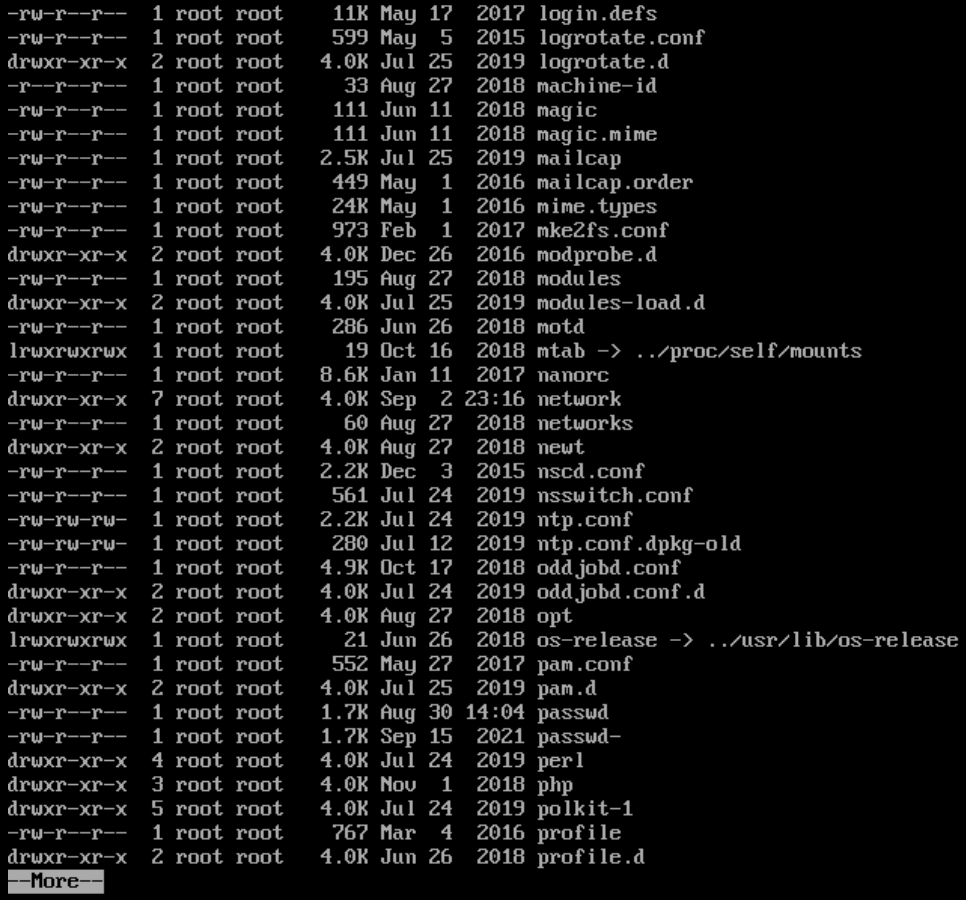


Figure 24: Nothing odd; Aug 30 and Sept 2 (lab setup?)

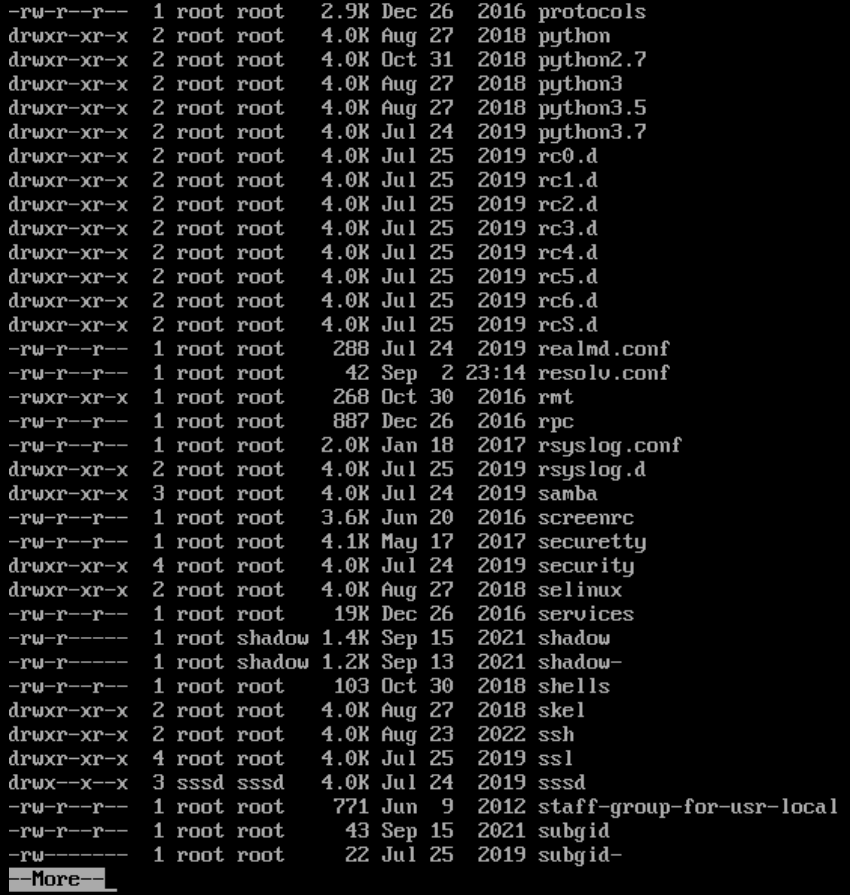


Figure 25: Nothing odd Sept 2 (lab setup?)

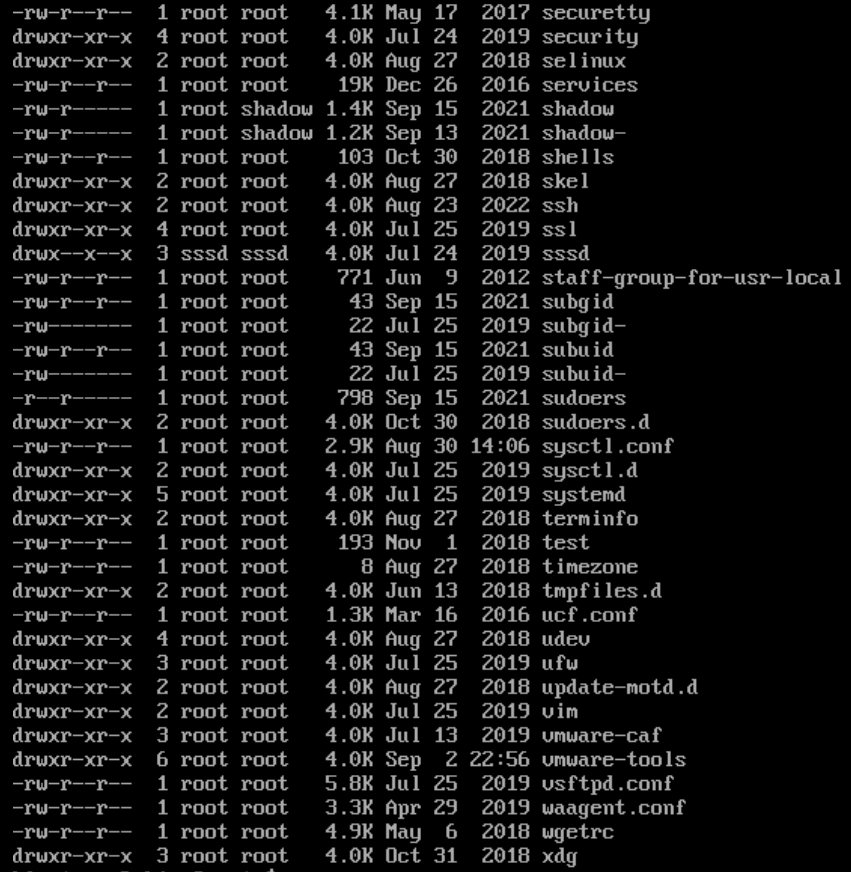


Figure 26: Nothing odd; Aug 30, Sept 2 (lab setup)

**Suspicious Evidence**

Some evidence was gathered and was deemed suspicious; outlining acquired evidence that does not prove malicious access. It could be worth investigating further to determine if this was malicious activity or not. This evidence is outlined in Figures 27-31 below.

Evidence that is not confirmed malicious action, but could be considered suspicious includes the /etc/passwd, etc/group, /etc/shadow, and /etc/networks files being accessed on 9/6/23. Another suspicious piece of evidence is a failed login from an unknown user on 9/5/23.

more /var/log/auth.log

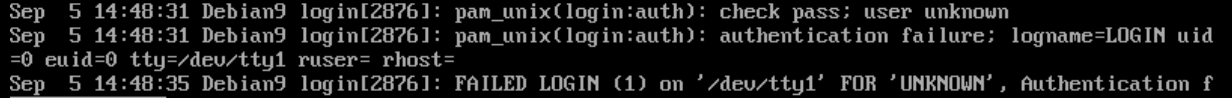


Figure 27: Unknown user attempts login Sept 5 (14:48)

stat /etc/passwd

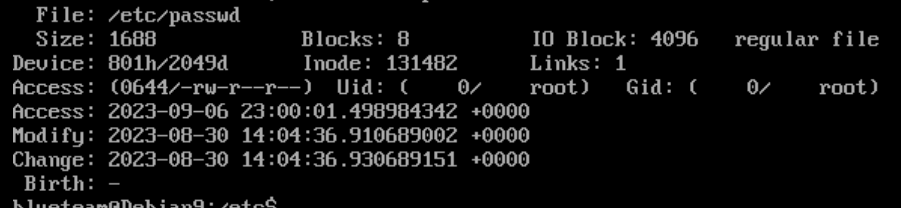


Figure 28: Accessed on Sept 6 (23:00)  
stat /etc/group

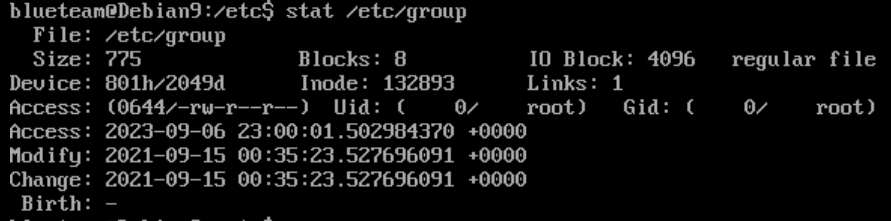


Figure 29: Accessed on Sept 6 (23:00)

stat /etc/shadow

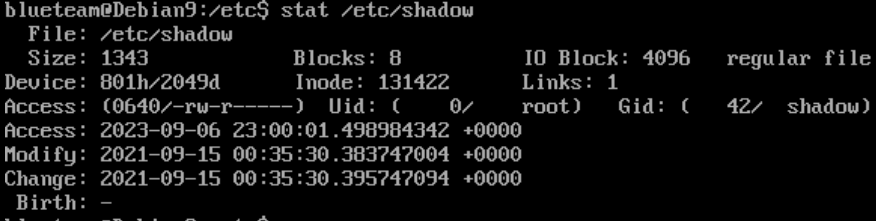


Figure 30: Accessed on Sept 6 (23:00)

cd /etc/network

stat interfaces

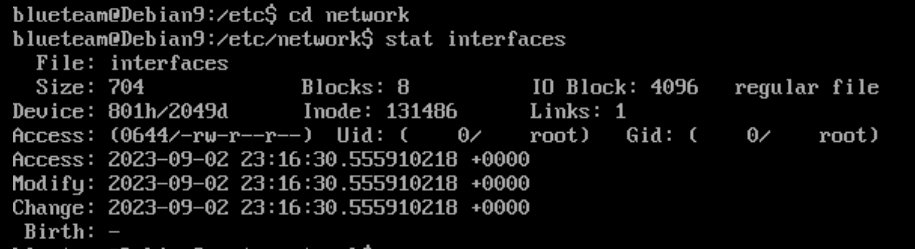


Figure 31: Accessed, modified and changed on Sept 2 (23:16) (Lab setup?)

more /var/log/auth.log

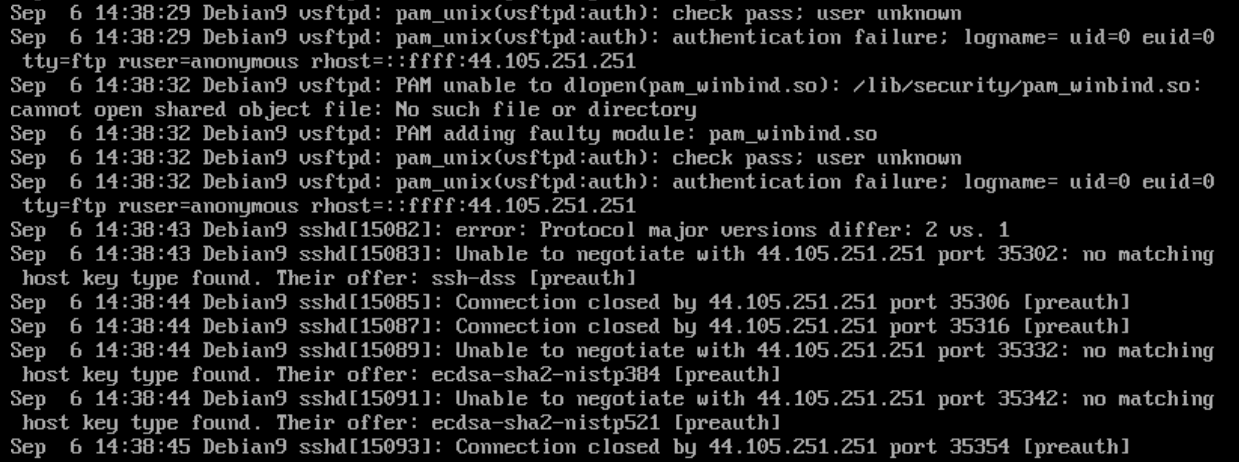


Figure 32: Unknown user attempts login Sept 6 (14:38). SSH connection from 44.105.251.251

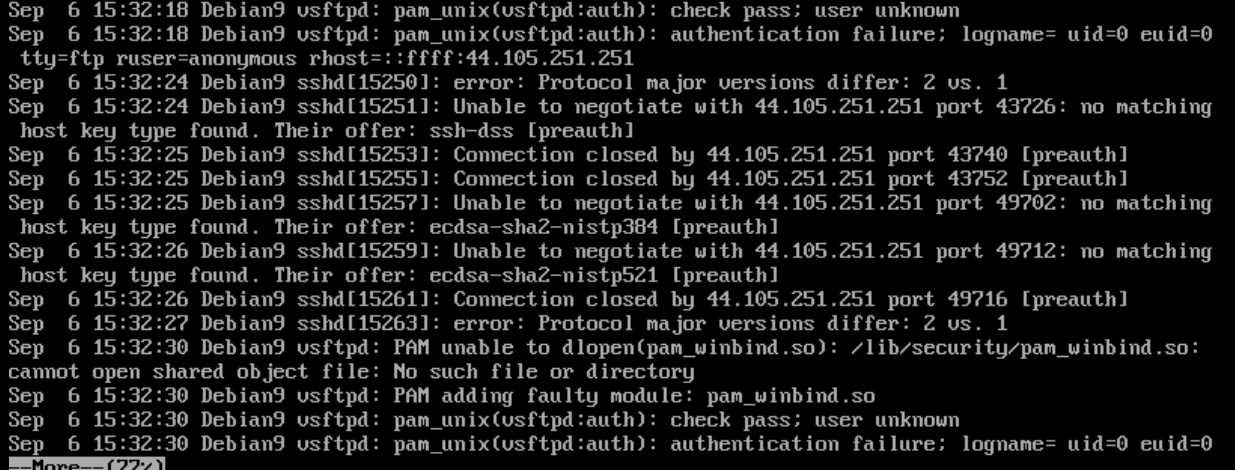


Figure 33: Unknown user attempts login Sept 6 (15:32) SSH connection from 44.105.251.251

**Confirmed evidence:**

Going through the files on the Debian machine, there was no proof of any files being altered, changed or copied. While there is suspicious activity that warrants investigation; the information the suspicious actors attempted to access could not be found.

**Windows Machine:**

Evidence gathered off the Windows Server is categorized into three categories. The current amount of auditing makes it nearly impossible to definitively come to the conclusion that the server was tampered with through unauthorized means. There were enough logs to attempt to tentatively piece together what may have happened but not what was affected in the server.

**Benign Evidence:**

Searches were conducted throughout the file system to detect any modification to any core components of the server or its users. No files were seemingly modified by external actors. Some files containing logs were automatically updated leading to them showing that the folder was modified, but upon further inspection there seems to have been no modification done to them. Similar inspections were carried out to user profiles to detect any unauthorized modification to the user folder. As can be seen in figure 35, no user folders were modified outside of blueteam’s folder. This modification was due to an automated file that is created when a user accesses the machine.

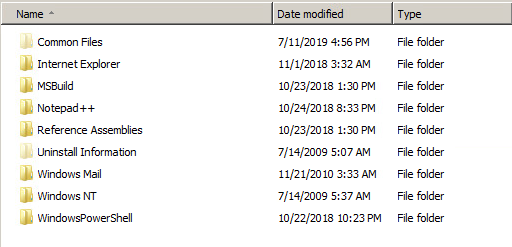


Figure 34: Program Files and Dates Modified

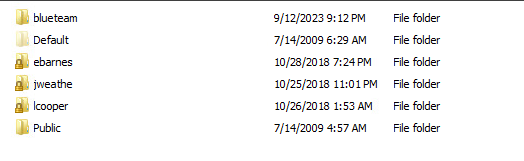


Figure 35: User Folders and Dates Modified

**Conclusive Evidence:**

The only conclusive act that can be definitively stated is that the threat actor gained access to the system. This can be seen through figures 36 and 37. Around the same time that SSL errors started occurring an anonymous user logged in. About 30 seconds after the errors started occurring, the unknown user logged into the system. This is the only conclusive statement that can be said about the Windows server.

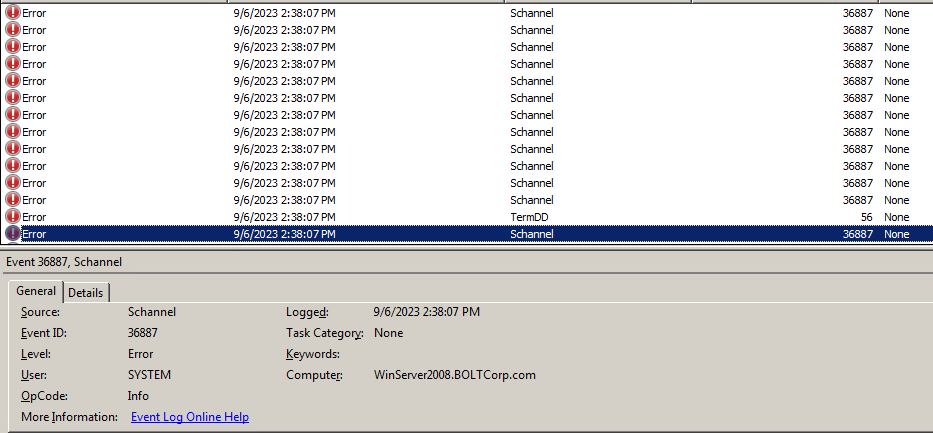


Figure 36: SSL Errors Starting at 2:38:07 PM Computer Time

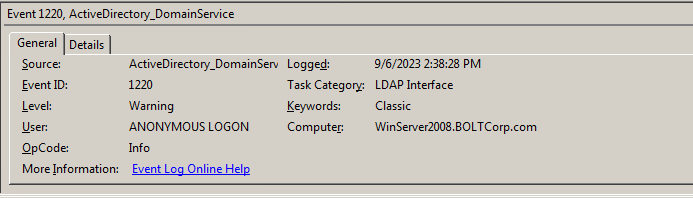


Figure 37: Anonymous Login to Active Directory at 2:38:28 PM, just after the SSL errors started

**Suspicious Artifacts:**

A couple of suspicious logs revealed some information that may reveal information about the attacker. The first log can be seen in figure 38. The server's security disconnected an unknown IP. This is the only log that reveals an IP, making it unusable as definitive evidence. While this could be an employee trying to access the system from a new location, this occurred shortly after the SSL errors started occurring. The second log can be seen in figure 39. This log shows that crypto keys were generated shortly after the SSL errors started. After scrubbing through all of the logs, this is a rare event that doesn’t happen on a daily basis. The timing of this key generation aligning with the SSL errors makes the log very suspicious. It is possible that this is how the attacker gained access to the system, although this is a guess as there is no definitive evidence that states exactly how attackers gained access.



Figure 38: Discovered an unknown IP from Windows system logs

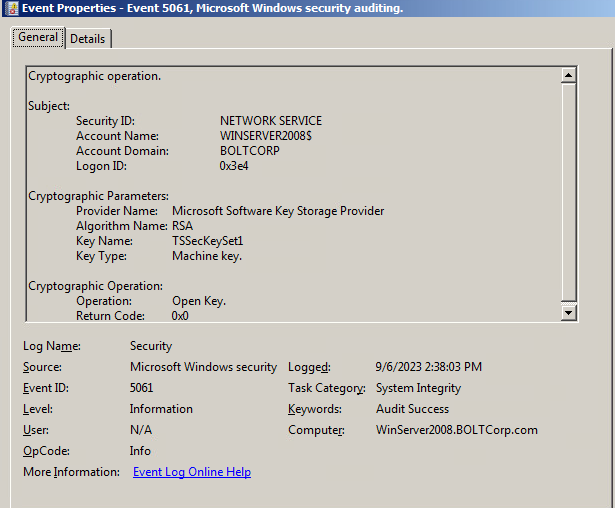


Figure 39: Crypto keys were generated around the time of the SSL errors occurring

**Preventing Future Access for Windows Server:**

The most evident issue present in the Windows server is the lack of auditing for anything that isn’t logging in. Once an attacker gains access to a system there is no easy way for a team to inspect what is changing in the system. Figure 40 shows the system’s current configurations for auditing any changes in the file system. Both object access and privilege use should be fully audited to give realtime information about what is changing in the system.

The other evident issue is the ability for outside IPs to contact the system. The IP seen in figure 38 shouldn’t be able to contact the server as it is outside the network. A firewall should be implemented to protect the server from IPs outside the internal environment. The IP that was seen in figure 38 should also be blacklisted to prevent any additional attempts of an attack from that IP.

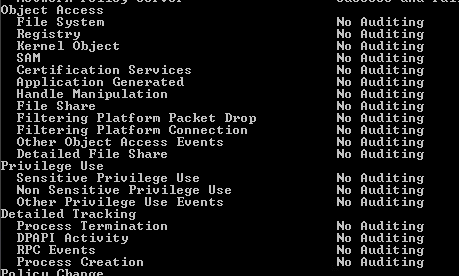


Figure 40: Auditing configuration for Object Access, Privilege Use, and Detailed Tracking

**Recommendations:**

This section lays out what tools and resources could be used to help prevent these attacks in the future from happening. For the ubuntu machine it was discovered that a root user using an OpenSSH connection had accessed a number of files including the shadow file for unknown reasons. A good way in future to mitigate this type of SSH attack is to disable the root user account. As it was used to modify the files the safest option would be to remove it. Also setting up a custom SSH port is advised as well to help. As for software getting a management system, like for example Tripwire, to be able to detect SSH connections and get alerts for changing of files. The debian machine was in a similar situation to the ubuntu machine, however, there were no files changed in this case. There was a failed sign in attempt in this case as well though that changes little in the fact of the attack. Cybersecurity software like Tripwire again would help minimize these actions and give information regarding the attack and allow proper response. Finally, with the windows machine we discovered that there was indeed an attack due to the fact we could tell there was a sign in attempt with the SSL information. As discussed in the bottom of that section there is no auditing put into place within the windows environment and that is the ideal way to be able to investigate and fix the potential risk. A good software with auditing capabilities is ManageEngine which allows you to be able to see all edited files and access with date and time provided. All three of these systems are in deep need of a security software install and more in depth auditing systems.

References

*Linux File Access Monitoring*. Unix & Linux Stack Exchange. (2011, April 28). https://unix.stackexchange.com/questions/12247/linux-file-access-monitoring

*Linux logging basics - The ultimate guide to logging*. Log Analysis | Log Monitoring by Loggly. (2022). https://www.loggly.com/ultimate-guide/linux-logging-basics/

*Managing saved passwords using windows credential manager*. Windows OS Hub. (2021, August 9). https://woshub.com/saved-passwords-windows-credential-manager/

*Monitoring Active Directory for SIGNS OF COMPROMISE*. Microsoft Learn. (2023, February 15). https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise

Pyle, N. (2019, April 4). *Introducing auditing changes in Windows 2008*. techcommunity.microsoft.com. https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/introducing-auditing-changes-in-windows-2008/ba-p/394933

*Where is the log of used commands in linux?*. Unix & Linux Stack Exchange. (2015, October 8). https://unix.stackexchange.com/questions/234731/where-is-the-log-of-used-commands-in-linux