Linux Logging for SOC

TryHackMe

Informações do documento	
Referência	CTF de estudo – Gabriel Garritano de Mendonça Villela
N° Revisão	1
Data de publicação	30/09/2025
Link	https://tryhackme.com/room/linuxloggingforsoc

Redação	Gabriel Garritano	Estudante
Revisão	Nome do revisor	Orientador
Aprovação	Nome do aprovador	Diretor

Histórico de revisões		
N°	**Entregas**	**Descrição**
0	DD/MM/AAAA	Produção
1	DD/MM/AAAA	Revisão
2	DD/MM/AAAA	Aprovação

Informações do CTF	
Nível de Dificuldade	Easy
Tipo de acesso	Gratuito
Conceitos envolvidos	WebHacking
Plataforma	TryHackMe
Área	Blue Team

Contextualização

Linux has long been a leader in servers and embedded systems, and now its use is even more widespread with the growth of cloud adoption. As a SOC analyst, you are now very likely to investigate Linux alerts and incidents, either from traditional on-premises servers or from cloud-native containerized workloads. In this room, you will explore the most common Linux logs sent to SIEM and learn how to view them directly on-host.

Conceitos utilizados

- Explore authentication, runtime, and system logs on Linux
- Learn the commands and pitfalls when working with logs
- Uncover how tools like auditd monitor and report the events
- Practice every learned log source in the attached VM

Desenvolvimento

Working With Text Logs

A primeira tarefa do CTF envolve a extração de informações a partir da consulta do log do sistema. É necessário a exploração da /var/log para identificar as seguintes informações: Nome de um servidor e mensagem deixada pelo usuário Yama. Para isso, utilizam-se os comandos less e grep. Os comandos utilizados estão visíveis no print.

Respostas:

ntp.ubuntu.com

Becoming mindful.

```
ubuntu@thm-vm:~$ less /var/log/syslog | grep server
2025-08-13T13:41:48.185573+00:00 thm-vm systemd[1]: Listening on ssh.socket - OpenBSD Secure Shell server socket.
2025-08-13T13:42:17.819639+00:00 thm-vm systemd-timesyncd[275]: Contacted time server 185.125.190.58:123 (ntp.ubuntu.com).
2025-08-13T13:44:21.248447+00:00 thm-vm systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
2025-08-13T13:44:21.337390+00:00 thm-vm systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
2025-08-13T13:57:19.919423+00:00 thm-vm systemd[1]: Listening on ssh.socket - OpenBSD Secure Shell server socket.
2025-08-13T13:57:49.388678+00:00 thm-vm systemd-timesyncd[268]: Contacted time server 185.125.190.58:123 (ntp.ubuntu.com).
2025-08-13T13:59:39.116136+00:00 thm-vm systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
2025-08-13T13:59:39.164709+00:00 thm-vm systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
2025-08-28T14:02:07.694115+00:00 thm-vm systemd-timesyncd[282]: Contacted time server 185.125.190.58:123 (ntp.ubuntu.com).
2025-08-28T14:02:07.701729+00:00 thm-vm systemd[1]: Listening on ssh.socket - OpenBSD Secure Shell server socket.
2025-08-28T14:02:07.702490+00:00 thm-vm systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
2025-08-28T14:02:07.745248+00:00 thm-vm systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
2025-09-09T13:45:41.665964+00:00 thm-vm systemd-timesyncd[266]: Contacted time server 185.125.190.58:123 (ntp.ubuntu.com).
2025-09-09T13:45:41.666994+00:00 thm-vm systemd[1]: Listening on ssh.socket - OpenBSD Secure Shell server socket.
2025-09-09T13:45:41.816961+00:00 thm-vm systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
2025-09-09T13:45:42.071277+00:00 thm-vm systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
2025-09-30T19:16:37.058928+00:00 thm-vm systemd[1]: Listening on ssh.socket - OpenBSD Secure Shell server socket.
2025-09-30T19:16:37.122594+00:00 thm-vm systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
2025-09-30T19:16:37.276379+00:00 thm-vm systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
ubuntu@thm-vm:~$
```

```
ubuntu@thm-vm:~$ less /var/log/syslog | grep Yama
2025-08-13T13:41:48.176653+00:00 thm-vm kernel: Yama: becoming mindful.
2025-08-13T13:57:19.908956+00:00 thm-vm kernel: Yama: becoming mindful.
2025-08-28T14:02:07.691523+00:00 thm-vm kernel: Yama: becoming mindful.
2025-09-09T13:45:41.659300+00:00 thm-vm kernel: Yama: becoming mindful.
2025-09-30T19:16:37.056146+00:00 thm-vm kernel: Yama: becoming mindful.
```

Authentication Logs

Para a seguinte etapa é necessário explorar os registros de identificação. do sistema. O payload a ser criado utiliza-se dos mesmos conceitos dos anteriores. Felizmente, a sala do TryHackMe oferece informações necessárias para os argumentos adicionais a serem buscados, junto de explicações de como cada tipo de autentication log funciona no Linux. É necessário encontrar qual usuário tentou conectar-se repetidas vezes via protocolo SSH e falhou e qual usuário foi adicionado ao servidor. Para isso, utilizou-se os comandos abaixo:

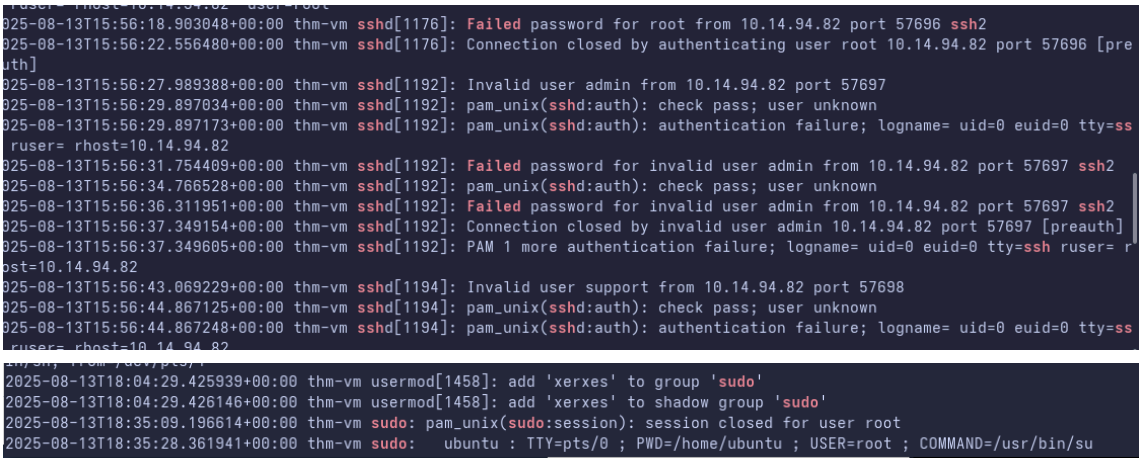
less /var/log/auth.log | grep -E ‘ssh|Failed’

less /var/log/auth.log | grep -E ‘useradd|sudo

Respostas:

10.14.94.82

xerxes



Common Linux Logs

Esta etapa ensina conceitos essenciais sobre funcionamento e exploração de logs genéricos do sistema, aplicações e como visualizar o histórico do bash de outros usuários. É necessário encontrar a versão do programa unzip funcionando no sistema e a mensagem escondida no histórico de um dos usuários. Para a primeira tarefa bastou seguir o mesmo protocolo de comando utilizado nas etapas anteriores, apenas alterando o parâmetro buscado pelo grep para ‘unzip’. A segunda demandou buscar qual usuário havia deixado a mensagem, Primeiro foi realizada busca nos usuários ubuntu (aquele que estamos conectados) e no xerxes, em nenhum deles foi encontrado nada. Como o usuário que estamos utilizando possuí privilégio de administrador, foi possível buscar o histórico dentro do usuário root. Utilizando o comando less /home/root/.bash_history encontrou-se o segredo.

Respostas:

6.0-28ubuntu4.1 T

HM{note_to_remember}

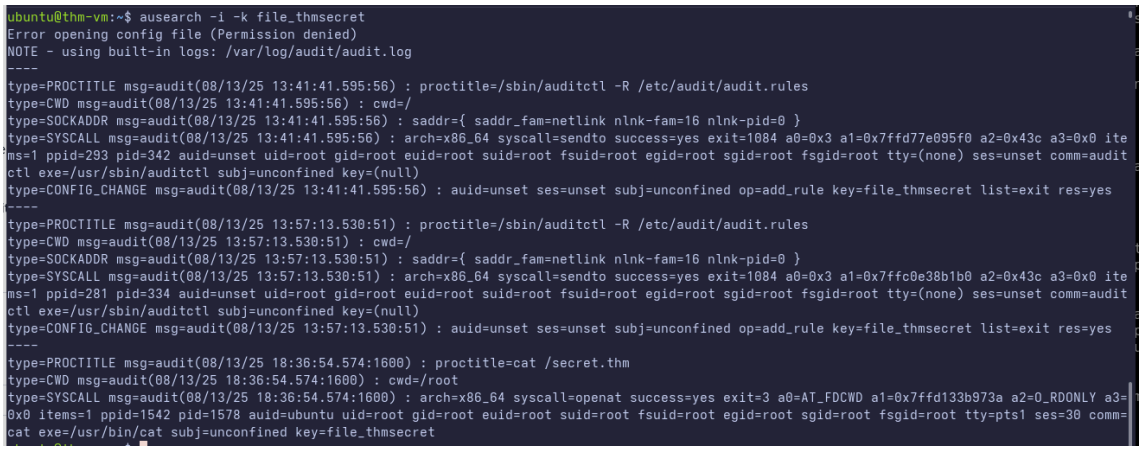
```
ubuntu@thm-vm:~$ less /var/log/dpkg.log | grep 'unzip'
2025-08-12 16:41:24 install unzip:amd64 <none> 6.0-28ubuntu4.1
2025-08-12 16:41:24 status half-installed unzip:amd64 6.0-28ubuntu4.1
2025-08-12 16:41:25 status unpacked unzip:amd64 6.0-28ubuntu4.1
2025-08-12 16:41:25 configure unzip:amd64 6.0-28ubuntu4.1 <none>
2025-08-12 16:41:25 status unpacked unzip:amd64 6.0-28ubuntu4.1
2025-08-12 16:41:25 status half-configured unzip:amd64 6.0-28ubuntu4.1
2025-08-12 16:41:25 status installed unzip:amd64 6.0-28ubuntu4.1
```

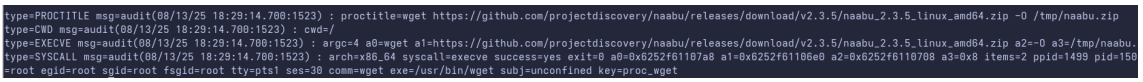
```
nano /etc/ssh/sshd_config
exit
ll -h /var/log
echo "THM{note_to_remember}" >> notes.txt
apt install auditd
cd /etc/audit/
ls
cd rules.d/
nano audit.rules
ll `which python3`
systemctl restart auditd
systemctl status auditd
nano audit.rules
cd /etc/logrotate.d
ls
rm *
exit
```

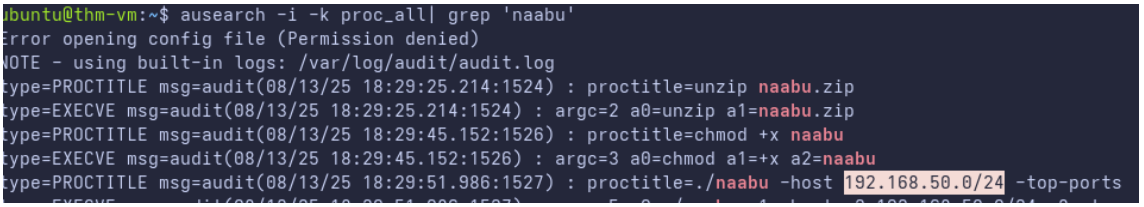
Using Auditd

Para a última etapa da sala é necessário explorar os registros de Audit, um programa de monitoramento comumente utilizado por times de SOC. A sala ensina como utilizar o comando ausearch e a maneira no qual os logs são registrados. Para montar o payload, basta combinar as informações requeridas com a lógica de busca com grep utilizada nas etapas anteriores.

Respostas:
08/13/25 18:36:54
naabu_2.3.5_linux_amd64.zip
192.168.50.0/24







Conclusão

O desafio aborda diversos tipos de registros diferentes comuns no dia a dia de um agente de segurança SOC. O CTF simula a exploração realizada por funcionários de blue team na manutenção e segurança de um servidor. Os conceitos aprendidos apesar de possuírem payloads relativamente simples na execução são essenciais para o monitoramento da segurança de um servidor.