Linux Threat Detection with Attack Range

By Rod Soto

Teoderick Contreras

WHOAMI

Rod Soto

Over 15 years of experience in information technology and security. He has spoken at ISSA, ISC2, OWASP, DEFCON, RSA Conference,Hackmiami, DerbyCon, Splunk .conf, Black Hat,BSides, Underground Economy and also been featured in Rolling Stone Magazine, Pentest Magazine, Univision, BBC, Forbes, VICE, Fox News and CNN. Co-founder of Hackmiami, Pacific Hackers Meetups and Conferences. Co-founder of Pacific Hackers Association.

Erick Contreras - GCFA | GASF

Over 14 years of experience in Cyber Security focus on malware reverse engineering, digital forensics and blue team. Present in ,Splunk .conf, BOTATTACK, TrendMicro SHIFT++ events and CERT-Verbund conference.

Linux Threat Detection with Attack Range

Agenda

1. Linux Introduction
2. Attack Range
3. Linux Common Attack Techniques
4. Demo attacks and Detections
5. Q&A

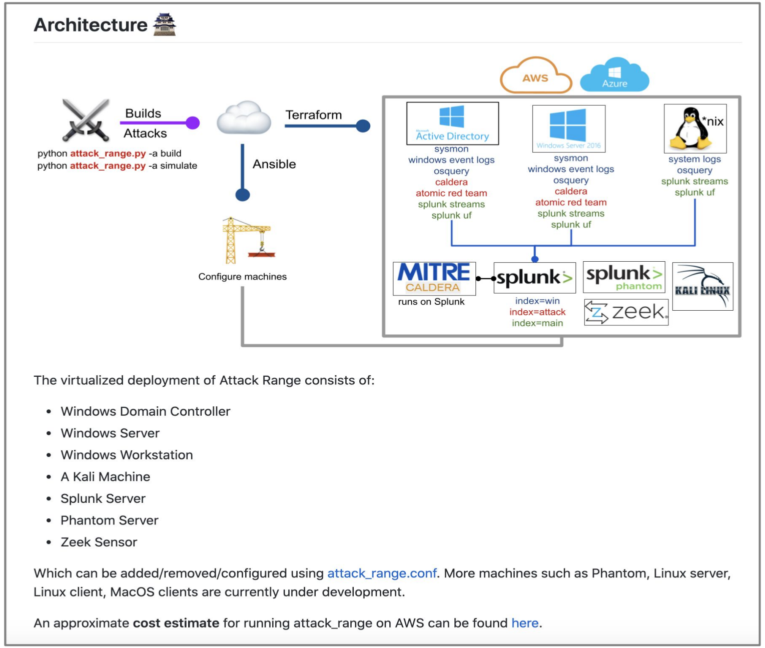
Linux Introduction

- Created by **Linus Torvalds** in the early 1990s
- The operating system of EVERYTHING (lightbulbs, cloud, desktops, phones, cars, drones, etc…)
- Linux Operating System is a flexible, open and customizable operating system available for every user.
- Security has been the priority factor of linux OS. In general Linux is more secure than many other operating systems, however is still hackable.

Linux Introduction

- User is walled off from other user (SoD)
- Password and user id are required for each of user to use linux
- User environment has a low privileges, which makes it harder for threat actor
- Native exploit protections (ASLR, PIE, RELRO,DEP,NX)
- No open ports by default, Password Hashing
- MAC (SELinux, AppArmor, SMACK)

SPLUNK - Attack Range



Architecture 🏯

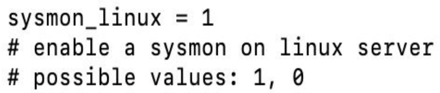
The virtualized deployment of Attack Range consists of:

- Windows Domain Controller
- Windows Server
- Windows Workstation
- A Kali Machine
- Splunk Server
- Phantom Server
- Zeek Sensor

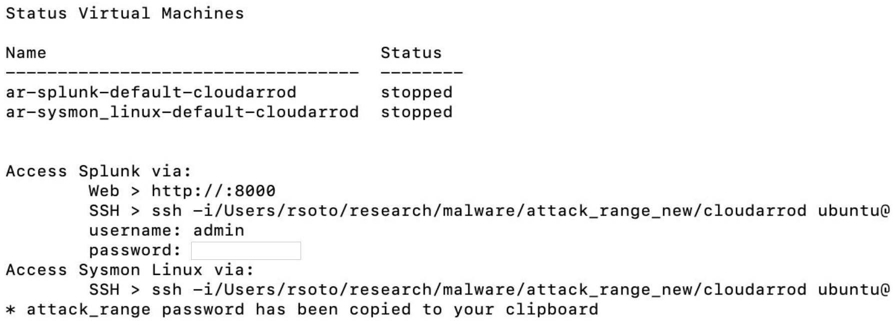
Which can be added/removed/configured using attack_range.conf. More machines such as Phantom, Linux server, Linux client, MacOS clients are currently under development.

An approximate **cost estimate** for running attack_range on AWS can be found here.

You can now build an Attack Range with a Linux Host with preconfigured sysmon policy to ingest Linux events
https://github.com/splunk/attack_range

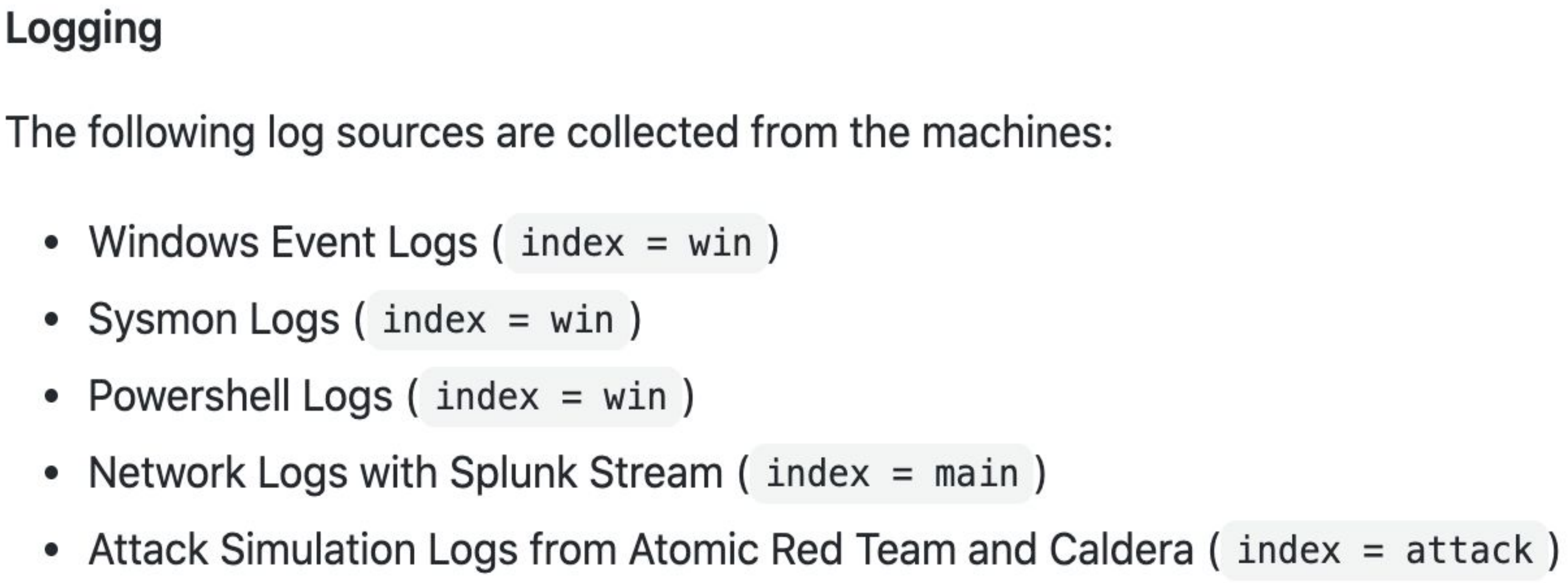


```
sysmon_linux = 1
# enable a sysmon on linux server
# possible values: 1, 0
```



```
Status Virtual Machines

Name                                  Status
----------------------------------   --------
ar-splunk-default-cloudarrod          stopped
ar-sysmon_linux-default-cloudarrod    stopped


Access Splunk via:
        Web > http://:8000
        SSH > ssh -i/Users/rsoto/research/malware/attack_range_new/cloudarrod ubuntu@
        username: admin
        password:
Access Sysmon Linux via:
        SSH > ssh -i/Users/rsoto/research/malware/attack_range_new/cloudarrod ubuntu@
* attack_range password has been copied to your clipboard
```

SPLUNK - Attack Range



Logging

The following log sources are collected from the machines:

- Windows Event Logs (`index = win`)
- Sysmon Logs (`index = win`)
- Powershell Logs (`index = win`)
- Network Logs with Splunk Stream (`index = main`)
- Attack Simulation Logs from Atomic Red Team and Caldera (`index = attack`)

Now with LINUX!

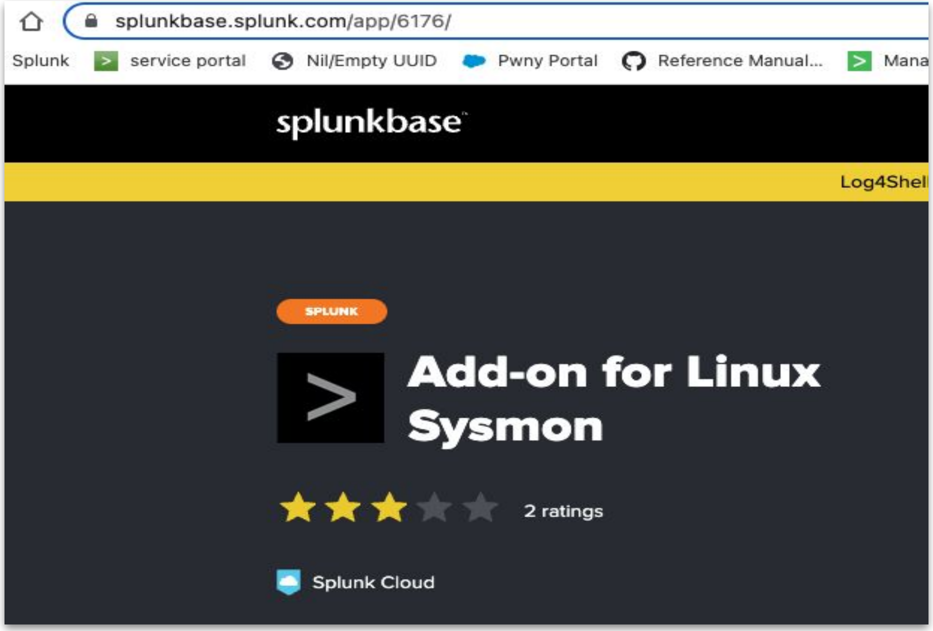
The new Sysmon for Linux add-on by Cedric HIEN, available for download at Splunkbase (splunkbase.splunk.com) allows us to ingest data and investigate attacks on Linux hosts.

We are now able to have visibility into events that may reveal malicious activity.

Index = unix

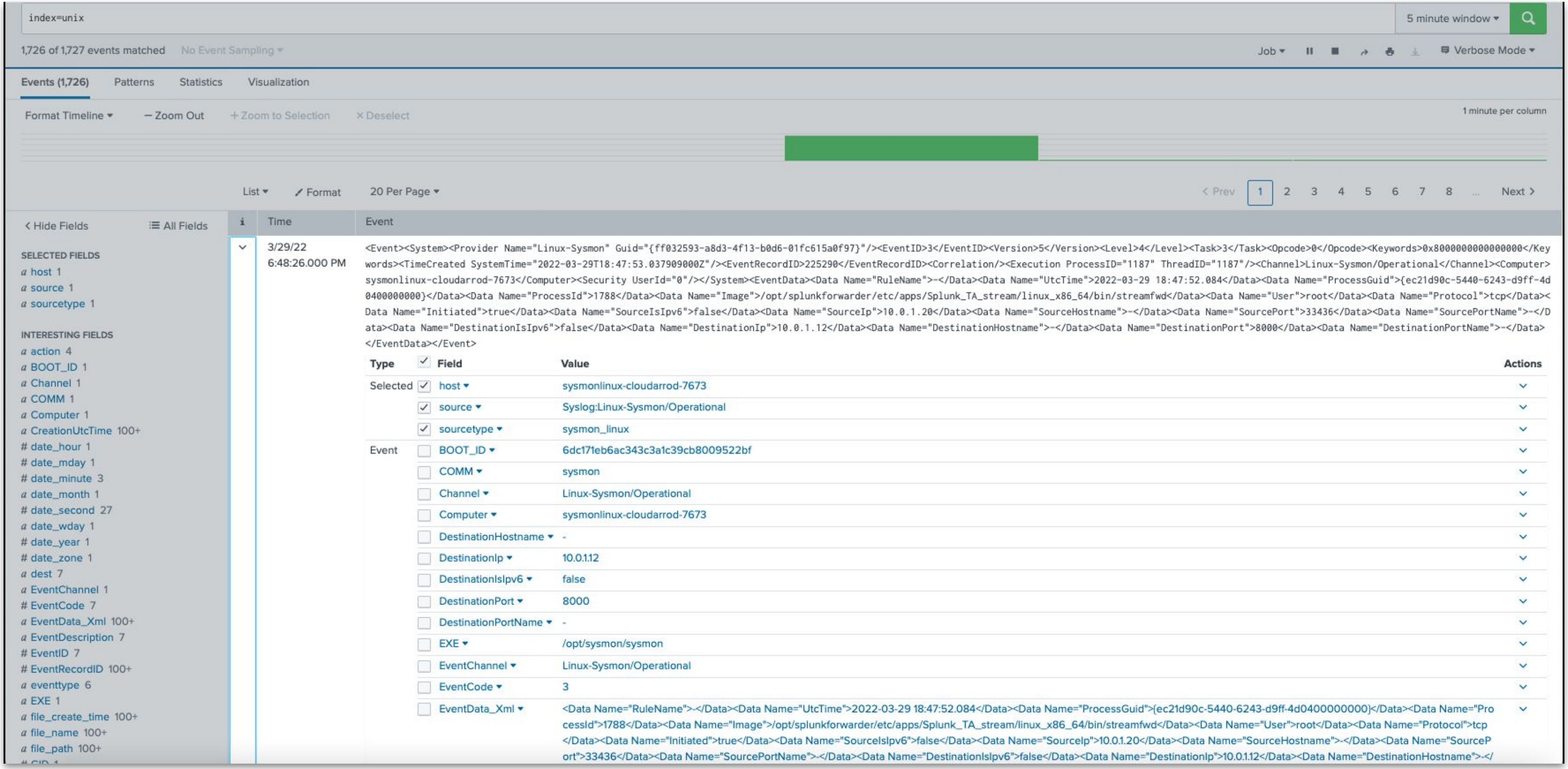
For the purpose of this presentation we will look at some Mitre Techniques and Linux post exploitation tools such as:

- **Credential Access \ Dumping**
- **Persistence and privilege escalation**
- **LinPEAS, AutoSUID, LinEnum**
- **Execution**


splunkbase.splunk.com/app/6176/

Add-on for Linux Sysmon

Index = unix



```
index=unix
```

SELECTED FIELDS

a host	1
a source	1
a sourcetype	1

INTERESTING FIELDS

a action	4
a BOOT_ID	1
a Channel	1
a COMM	1
a Computer	1
a CreationUtcTime	100+
# date_hour	1
# date_mday	1
# date_minute	3
a date_month	1
# date_second	27
a date_wday	1
# date_year	1
# date_zone	1
a dest	7
a EventChannel	1
# EventCode	7
a EventData_Xml	100+
a EventDescription	7
# EventID	7
# EventRecordID	100+
a eventtype	6
a EXE	1
a file_create_time	100+
a file_name	100+
a file_path	100+

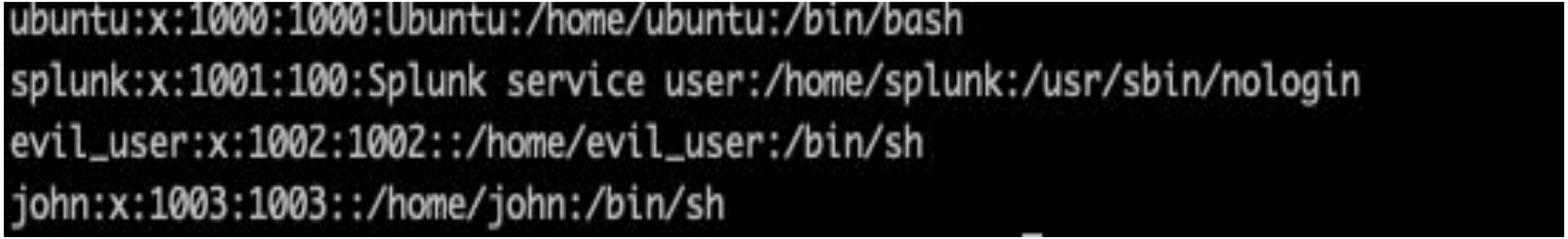
i	Time	Event
⌄	3/29/22 6:48:26.000 PM	

```
<Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}"/><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Key
words><TimeCreated SystemTime="2022-03-29T18:47:53.037909000Z"/><EventRecordID>225290</EventRecordID><Correlation/><Execution ProcessID="1187" ThreadID="1187"/><Channel>Linux-Sysmon/Operational</Channel><Computer>
sysmonlinux-cloudarrod-7673</Computer><Security UserId="0"/></System><EventData><Data Name="RuleName">-</Data><Data Name="UtcTime">2022-03-29 18:47:52.084</Data><Data Name="ProcessGuid">{ec21d90c-5440-6243-d9ff-4d
0400000000}</Data><Data Name="ProcessId">1788</Data><Data Name="Image">/opt/splunkforwarder/etc/apps/Splunk_TA_stream/linux_x86_64/bin/streamfwd</Data><Data Name="User">root</Data><Data Name="Protocol">tcp</Data><
Data Name="Initiated">true</Data><Data Name="SourceIsIpv6">false</Data><Data Name="SourceIp">10.0.1.20</Data><Data Name="SourceHostname">-</Data><Data Name="SourcePort">33436</Data><Data Name="SourcePortName">-</D
ata><Data Name="DestinationIsIpv6">false</Data><Data Name="DestinationIp">10.0.1.12</Data><Data Name="DestinationHostname">-</Data><Data Name="DestinationPort">8000</Data><Data Name="DestinationPortName">-</Data>
</EventData></Event>
```

Type	☑ Field	Value	Actions
Selected	☑ host ▾	sysmonlinux-cloudarrod-7673	⌄
	☑ source ▾	Syslog:Linux-Sysmon/Operational	⌄
	☑ sourcetype ▾	sysmon_linux	⌄
Event	□ BOOT_ID ▾	6dc171eb6ac343c3a1c39cb8009522bf	⌄
	□ COMM ▾	sysmon	⌄
	□ Channel ▾	Linux-Sysmon/Operational	⌄
	□ Computer ▾	sysmonlinux-cloudarrod-7673	⌄
	□ DestinationHostname ▾	-	⌄
	□ DestinationIp ▾	10.0.1.12	⌄
	□ DestinationIsIpv6 ▾	false	⌄
	□ DestinationPort ▾	8000	⌄
	□ DestinationPortName ▾	-	⌄
	□ EXE ▾	/opt/sysmon/sysmon	⌄
	□ EventChannel ▾	Linux-Sysmon/Operational	⌄
	□ EventCode ▾	3	⌄
	□ EventData_Xml ▾	<Data Name="RuleName">-</Data><Data Name="UtcTime">2022-03-29 18:47:52.084</Data><Data Name="ProcessGuid">{ec21d90c-5440-6243-d9ff-4d0400000000}</Data><Data Name="ProcessId">1788</Data><Data Name="Image">/opt/splunkforwarder/etc/apps/Splunk_TA_stream/linux_x86_64/bin/streamfwd</Data><Data Name="User">root</Data><Data Name="Protocol">tcp</Data><Data Name="Initiated">true</Data><Data Name="SourceIsIpv6">false</Data><Data Name="SourceIp">10.0.1.20</Data><Data Name="SourceHostname">-</Data><Data Name="SourcePort">33436</Data><Data Name="SourcePortName">-</Data><Data Name="DestinationIsIpv6">false</Data><Data Name="DestinationIp">10.0.1.12</Data><Data Name="DestinationHostname">-</	⌄

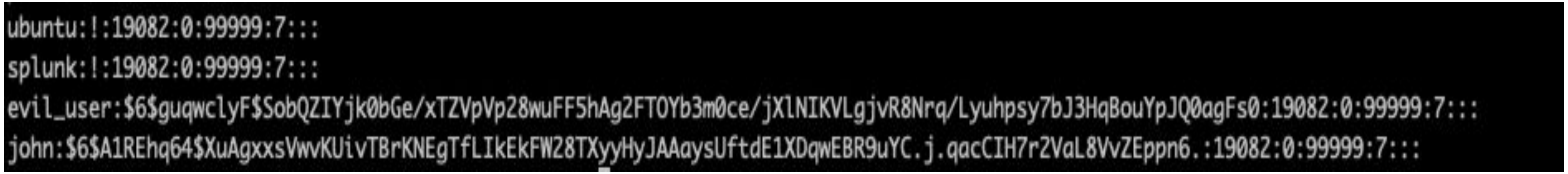
Linux Common Attack Techniques

Cat /etc/passwd



```
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
splunk:x:1001:100:Splunk service user:/home/splunk:/usr/sbin/nologin
evil_user:x:1002:1002::/home/evil_user:/bin/sh
john:x:1003:1003::/home/john:/bin/sh
```

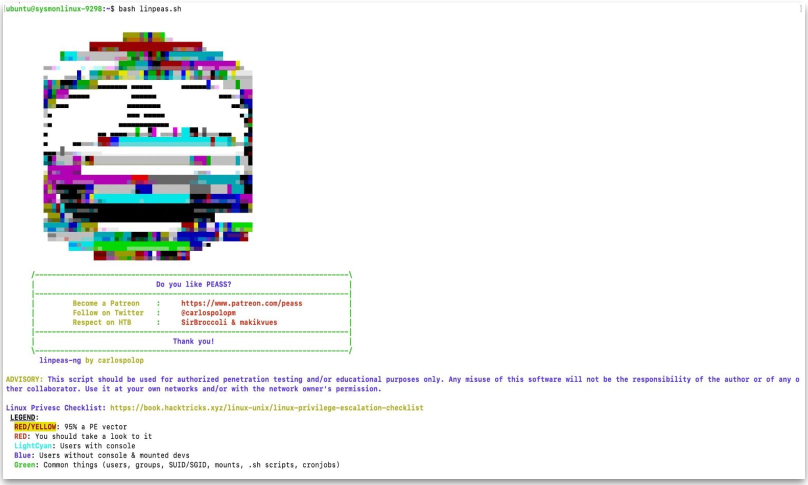
Cat /etc/shadow



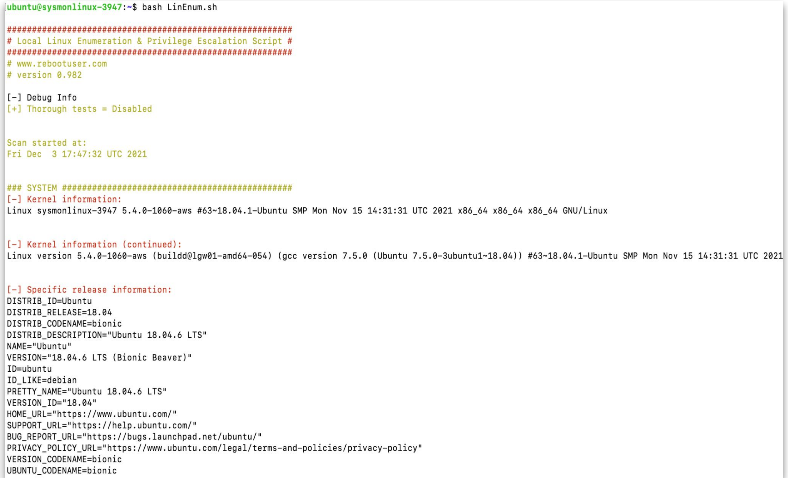
```
ubuntu:!:19082:0:99999:7:::
splunk:!:19082:0:99999:7:::
evil_user:$6$guqwclyF$SobQZIYjk0bGe/xTZVpVp28wuFF5hAg2FTOYb3m0ce/jXlNIKVLgjvR8Nrq/Lyuhpsy7bJ3HqBouYpJQ0agFs0:19082:0:99999:7:::
john:$6$A1REhq64$XuAgxxsVwvKUivTBrKNEgTfLIkEkFW28TXyyHyJAAaysUftdE1XDqwEBR9uYC.j.qacCIH7r2VaL8VvZEppn6.:19082:0:99999:7:::
```

Linux Common Attack Techniques

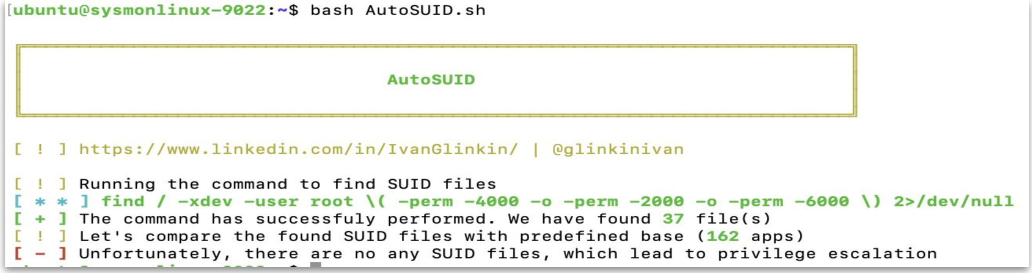
LinePeas, AutoSuid, LinEnum Tools



```
ubuntu@sysmonlinux-9298:~$ bash linpeas.sh

      /---------------------------------------------------------------------------\
      |                             Do you like PEASS?                            |
      |---------------------------------------------------------------------------|
      |         Become a Patreon    :     https://www.patreon.com/peass           |
      |         Follow on Twitter   :     @carlospolopm                           |
      |         Respect on HTB      :     SirBroccoli & makikvues                 |
      |---------------------------------------------------------------------------|
      |                                 Thank you!                                |
      \---------------------------------------------------------------------------/
        linpeas-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any o
ther collaborator. Use it at your own networks and/or with the network owner's permission.

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
```

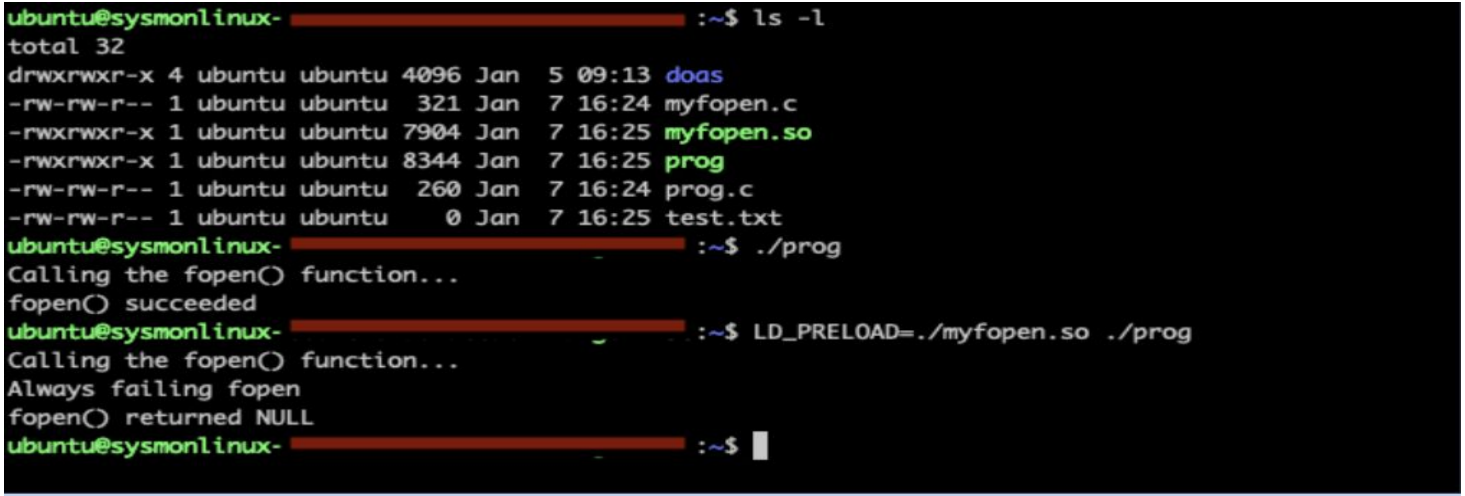


```
ubuntu@sysmonlinux-3947:~$ bash LinEnum.sh

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled


Scan started at:
Fri Dec  3 17:47:32 UTC 2021


### SYSTEM ##############################################
[-] Kernel information:
Linux sysmonlinux-3947 5.4.0-1060-aws #63~18.04.1-Ubuntu SMP Mon Nov 15 14:31:31 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux


[-] Kernel information (continued):
Linux version 5.4.0-1060-aws (buildd@lgw01-amd64-054) (gcc version 7.5.0 (Ubuntu 7.5.0-3ubuntu1~18.04)) #63~18.04.1-Ubuntu SMP Mon Nov 15 14:31:31 UTC 2021


[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu 18.04.6 LTS"
NAME="Ubuntu"
VERSION="18.04.6 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.6 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
```

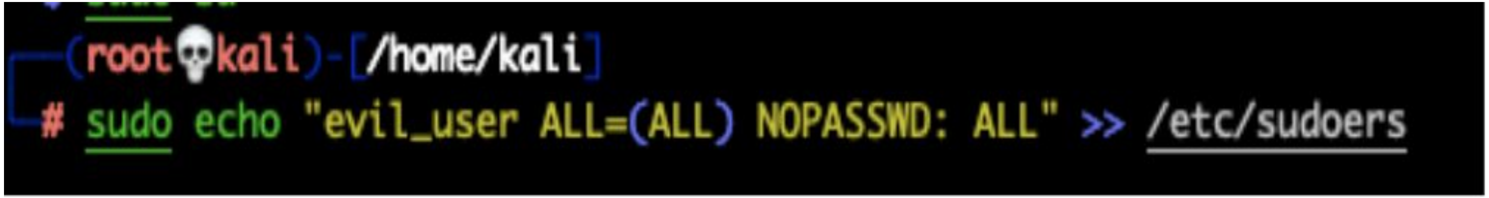


```
ubuntu@sysmonlinux-9022:~$ bash AutoSUID.sh

                              AutoSUID

[ ! ] https://www.linkedin.com/in/IvanGlinkin/ | @glinkinivan

[ ! ] Running the command to find SUID files
[ * * ] find / -xdev -user root \( -perm -4000 -o -perm -2000 -o -perm -6000 \) 2>/dev/null
[ + ] The command has successfuly performed. We have found 37 file(s)
[ ! ] Let's compare the found SUID files with predefined base (162 apps)
[ - ] Unfortunately, there are no any SUID files, which lead to privilege escalation
```

Linux Common Attack Techniques - Persistence



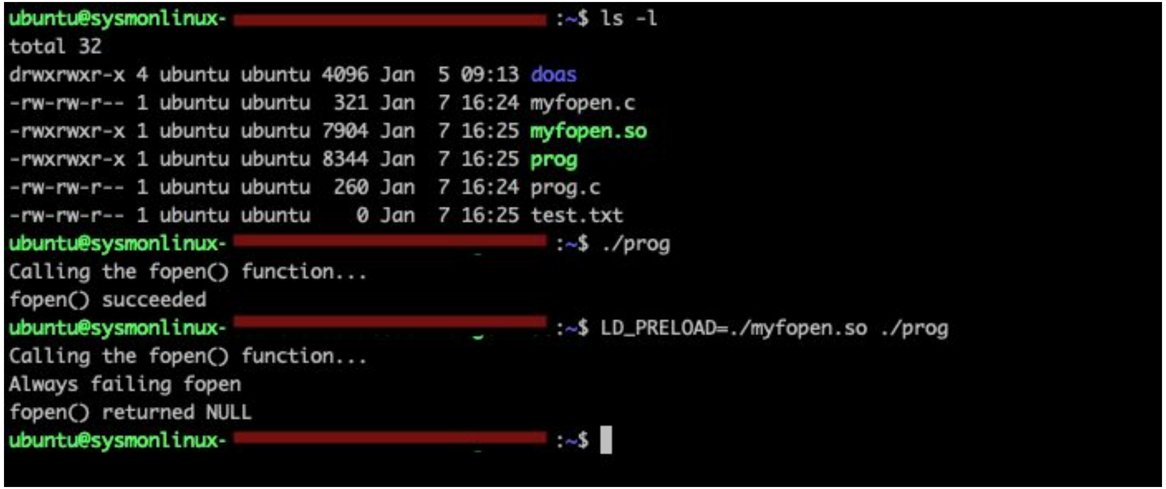
```
ubuntu@sysmonlinux-[redacted]:~$ ls -l
total 32
drwxrwxr-x 4 ubuntu ubuntu 4096 Jan  5 09:13 doas
-rw-rw-r-- 1 ubuntu ubuntu  321 Jan  7 16:24 myfopen.c
-rwxrwxr-x 1 ubuntu ubuntu 7904 Jan  7 16:25 myfopen.so
-rwxrwxr-x 1 ubuntu ubuntu 8344 Jan  7 16:25 prog
-rw-rw-r-- 1 ubuntu ubuntu  260 Jan  7 16:24 prog.c
-rw-rw-r-- 1 ubuntu ubuntu    0 Jan  7 16:25 test.txt
ubuntu@sysmonlinux-[redacted]:~$ ./prog
Calling the fopen() function...
fopen() succeeded
ubuntu@sysmonlinux-[redacted]:~$ LD_PRELOAD=./myfopen.so ./prog
Calling the fopen() function...
Always failing fopen
fopen() returned NULL
ubuntu@sysmonlinux-[redacted]:~$ 
```



```
┌──(root💀kali)-[/home/kali]
└─# sudo echo "evil_user ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers
```

Demo attacks and Detections

Hijacking module execution



```
ubuntu@sysmonlinux-[redacted]:~$ ls -l
total 32
drwxrwxr-x 4 ubuntu ubuntu 4096 Jan  5 09:13 doas
-rw-rw-r-- 1 ubuntu ubuntu  321 Jan  7 16:24 myfopen.c
-rwxrwxr-x 1 ubuntu ubuntu 7904 Jan  7 16:25 myfopen.so
-rwxrwxr-x 1 ubuntu ubuntu 8344 Jan  7 16:25 prog
-rw-rw-r-- 1 ubuntu ubuntu  260 Jan  7 16:24 prog.c
-rw-rw-r-- 1 ubuntu ubuntu    0 Jan  7 16:25 test.txt
ubuntu@sysmonlinux-[redacted]:~$ ./prog
Calling the fopen() function...
fopen() succeeded
ubuntu@sysmonlinux-[redacted]:~$ LD_PRELOAD=./myfopen.so ./prog
Calling the fopen() function...
Always failing fopen
fopen() returned NULL
ubuntu@sysmonlinux-[redacted]:~$
```

Resources

https://Research.splunk.com

https://github.com/splunk/attack_range

https://github.com/splunk/security_content

https://www.splunk.com/en_us/blog/security/approaching-linux-post-exploitation-with-splunk-attack-range.html

Q&A