Q3

sudo su

yum -y install epel-release wget jq

curl -O https://copr.fedorainfracloud.org/coprs/jasonish/suricata-stable/repo/epel-7/jasonish-suricata-stable-epel-7.repo

yum -y install suricata

wget https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.tar.gz

tar zxvf emerging.rules.tar.gz

rm /etc/suricata/rules/* -f

mv rules/*.rules /etc/suricata/rules/

rm -f /etc/suricata/suricata.yaml

wget -O /etc/suricata/suricata.yaml http://www.branchnetconsulting.com/wazuh/suricata.yaml

systemctl daemon-reload

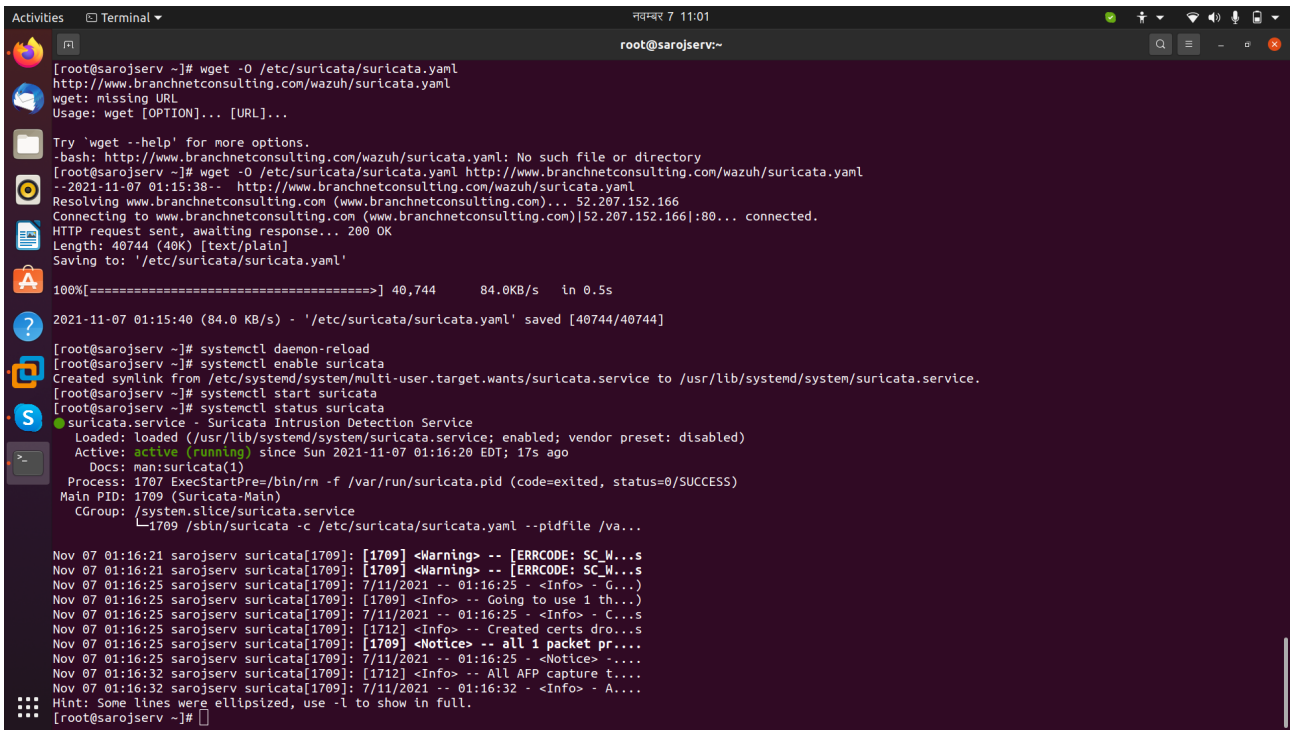
systemctl enable suricata

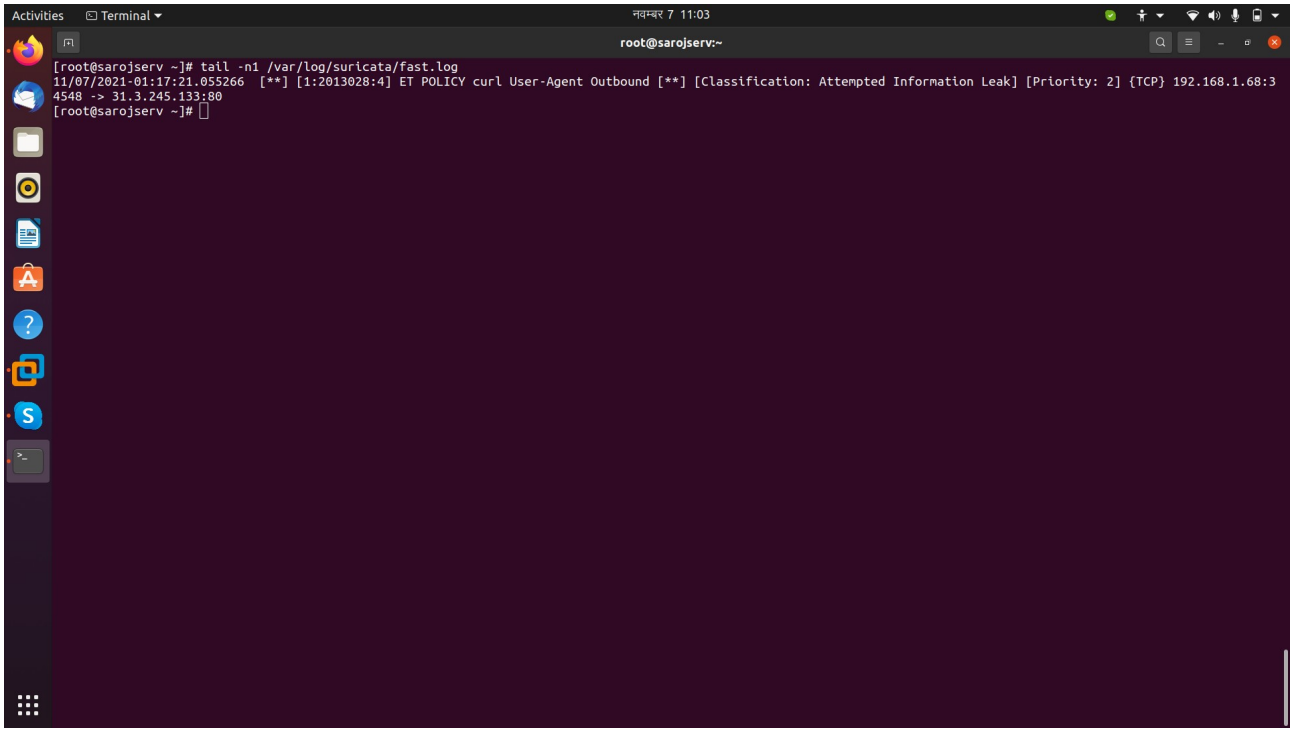
systemctl start suricata

systemctl status suricata

curl http://testmyids.com

tail -n1 /var/log/suricata/fast.log


Activities
Terminal
नवम्बर 7 11:01
root@sarojserv:~
[root@sarojserv ~]# wget -O /etc/suricata/suricata.yaml
http://www.branchnetconsulting.com/wazuh/suricata.yaml
wget: missing URL
Usage: wget [OPTION]... [URL]...
Try `wget --help' for more options.
-bash: http://www.branchnetconsulting.com/wazuh/suricata.yaml: No such file or directory
[root@sarojserv ~]# wget -O /etc/suricata/suricata.yaml http://www.branchnetconsulting.com/wazuh/suricata.yaml
--2021-11-07 01:15:38-- http://www.branchnetconsulting.com/wazuh/suricata.yaml
Resolving www.branchnetconsulting.com (www.branchnetconsulting.com)... 52.207.152.166
Connecting to www.branchnetconsulting.com (www.branchnetconsulting.com)|52.207.152.166|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 40744 (40K) [text/plain]
Saving to: '/etc/suricata/suricata.yaml'
100%[=====================================>] 40,744   84.0KB/s   in 0.5s
2021-11-07 01:15:40 (84.0 KB/s) - '/etc/suricata/suricata.yaml' saved [40744/40744]
[root@sarojserv ~]# systemctl daemon-reload
[root@sarojserv ~]# systemctl enable suricata
Created symlink from /etc/systemd/system/multi-user.target.wants/suricata.service to /usr/lib/systemd/system/suricata.service.
[root@sarojserv ~]# systemctl start suricata
[root@sarojserv ~]# systemctl status suricata
suricata.service - Suricata Intrusion Detection Service
Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; vendor preset: disabled)
Active: active (running) since Sun 2021-11-07 01:16:20 EDT; 17s ago
Docs: man:suricata(1)
Process: 1707 ExecStartPre=/bin/rm -f /var/run/suricata.pid (code=exited, status=0/SUCCESS)
Main PID: 1709 (Suricata-Main)
CGroup: /system.slice/suricata.service
└─1709 /sbin/suricata -c /etc/suricata/suricata.yaml --pidfile /va...
Nov 07 01:16:21 sarojserv suricata[1709]: [1709] <Warning> -- [ERRCODE: SC_W...s
Nov 07 01:16:21 sarojserv suricata[1709]: [1709] <Warning> -- [ERRCODE: SC_W...s
Nov 07 01:16:25 sarojserv suricata[1709]: 7/11/2021 -- 01:16:25 - <Info> - G...)
Nov 07 01:16:25 sarojserv suricata[1709]: [1709] <Info> -- Going to use 1 th...)
Nov 07 01:16:25 sarojserv suricata[1709]: 7/11/2021 -- 01:16:25 - <Info> - C...s
Nov 07 01:16:25 sarojserv suricata[1709]: [1712] <Info> -- Created certs dro...s
Nov 07 01:16:25 sarojserv suricata[1709]: [1709] <Notice> -- all 1 packet pr....
Nov 07 01:16:25 sarojserv suricata[1709]: 7/11/2021 -- 01:16:25 - <Notice> -....
Nov 07 01:16:32 sarojserv suricata[1709]: [1712] <Info> -- All AFP capture t....
Nov 07 01:16:32 sarojserv suricata[1709]: 7/11/2021 -- 01:16:32 - <Info> - A....
Hint: Some lines were ellipsized, use -l to show in full.
[root@sarojserv ~]#


Activities
Terminal
नवम्बर 7 11:03
root@sarojserv:~
[root@sarojserv ~]# tail -n1 /var/log/suricata/fast.log
11/07/2021-01:17:21.055266 [**] [1:2013028:4] ET POLICY curl User-Agent Outbound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.68:3
4548 -> 31.3.245.133:80
[root@sarojserv ~]#