WEB HONEYPOT

Lets Build Web Honeypot In Ubuntu,
To setup a Simple web honeypot we need two things,
requirements
1)web server
2)Intrusion Detection Tool

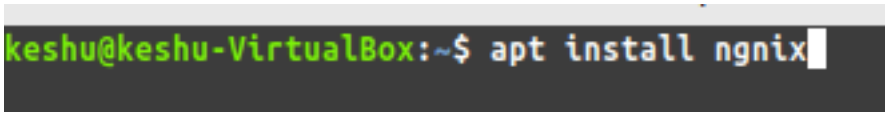
web server:
To setup a Simple web honeypot you we need a web server (example: Apache or Nginx),
But in this Article im going to use Nginx Server.

Intrusion Detection System:
we need intrusion detetion system because it provides real-time network traffic analysis and data packet logging,
and also helps us to identify suspicious network activity by analyzing and monitoring traffic, and give indicators of compromise.
there are many intrusion detection system just like SNORT, SURICATA, OSSEC etc

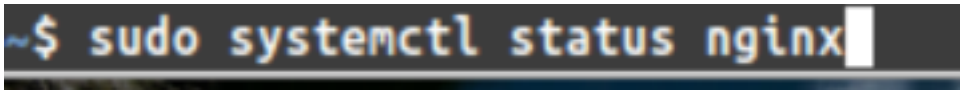
But im going to use snort

step1

Install Nginx Server In you Virtual Box
installation command given below



let check it is installed or not,
type this below command



you get this output

```
keshu@keshu-VirtualBox:~$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2023-04-21 17:22:27 IST; 2h 31min ago
       Docs: man:nginx(8)
    Process: 4052 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, s>
    Process: 4053 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/S>
   Main PID: 4142 (nginx)
      Tasks: 2 (limit: 2215)
     Memory: 3.2M
        CPU: 39ms
     CGroup: /system.slice/nginx.service
             ├─4142 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             └─4145 "nginx: worker process" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" >

Apr 21 17:22:27 keshu-VirtualBox systemd[1]: Starting A high performance web server and a reverse pro>
Apr 21 17:22:27 keshu-VirtualBox systemd[1]: Started A high performance web server and a reverse prox>
lines 1-16/16 (END)
```

In above figure you can this Nginx server is Running.

Setp2

in ubuntu we have a pre installed firewall(ufw) which block all incoming traffic,
first we have to allow firewall, after that it allows us to access our web server from outside,

type this below command
sudo ufw app list
output look this below picture

```
keshu@keshu-VirtualBox:~$ sudo ufw app list
[sudo] password for keshu:
Available applications:
  CUPS
  Nginx Full
  Nginx HTTP
  Nginx HTTPS
  OpenSSH
keshu@keshu-VirtualBox:~$
```

Lets give permission to Ngnix HTTP
used below command to give permission

```
$ sudo ufw allow 'Nginx HTTP'
```

if your command is correct than your output look this below figure

```
keshu@keshu-VirtualBox:~$ sudo ufw allow 'Nginx HTTP'
Rule updated
Rule updated (v6)
keshu@keshu-VirtualBox:~$
```

now you can access your web server from any machine
types this in your browser
http://(machine ip on which your Nginx server is running)
for example http://192.168.2.9 → it is only example , instead of this ip you use your ip of machine,

if you want to know your ip address in ubuntu machine type this bellow command and you get it,
you can use any one of them
ifconfig → it is a command used to find ip address
ip a -→ it is a command used to find ip address

output of your we server look this below figure

Step3
in step1 or step2 we set up our web server , now install your detection tool(snort).
 i already writed a article on how to install snort on ubuntu machine so im giving you that article link
 go and follow all step to instsall snort successfully.
   click on link button → LINK

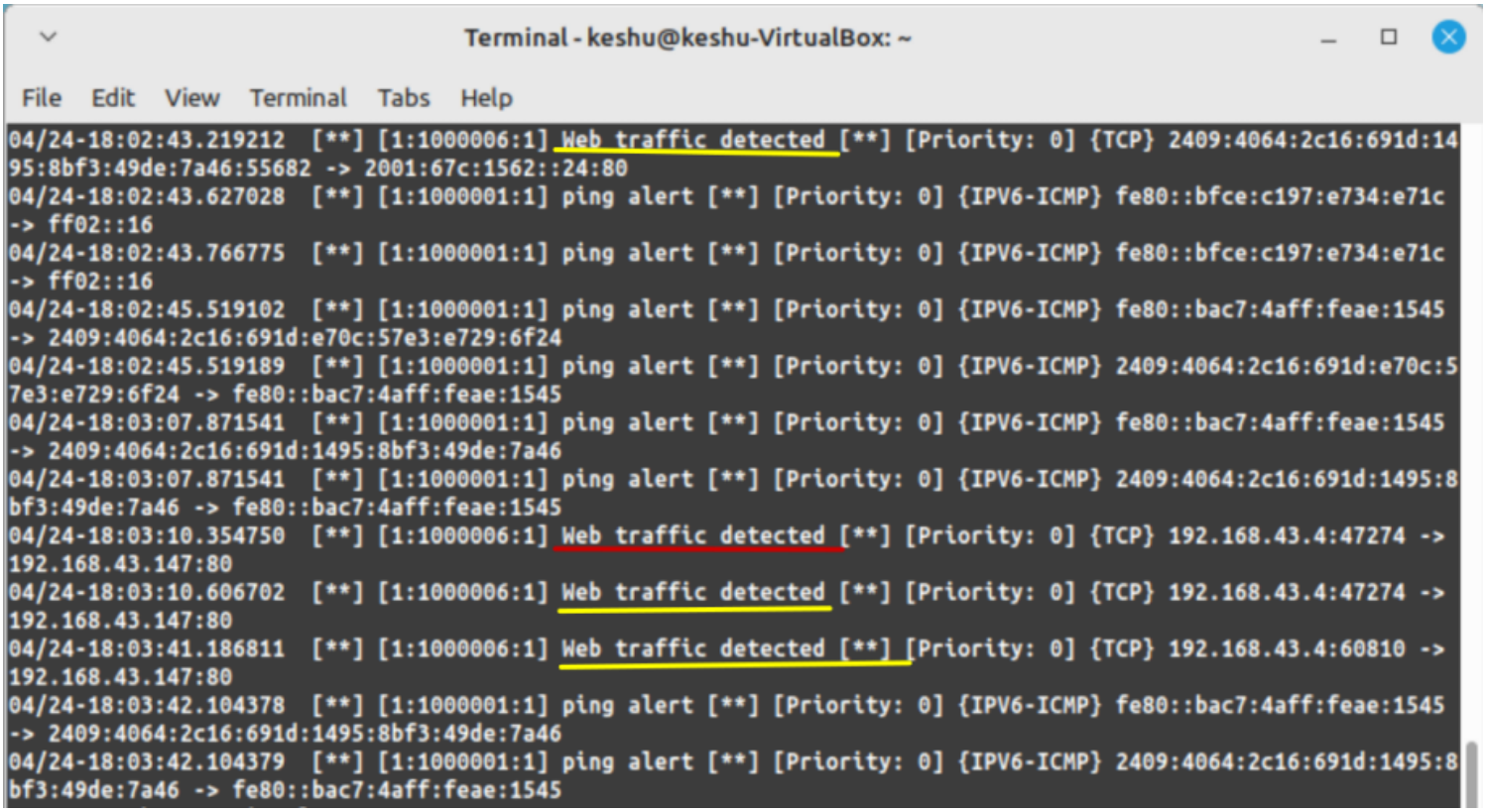
now our lab installed successfully,
lets use pre writed snort rules for capturing web traffic, and save for further analysis.
In snort installation process i writed custom rules for SSH,FTP,PING but in web honeypot we dont need custom rules
we already have it, snort have large amount of pre installed rules, lets use them,

if you follow my snort installation process, than you know how to run snort
command is give below, use this commmand to run snort.

```
$ sudo snort -q -i enp0s3 -A console -c /etc/snort/snort.conf
```

enp0s3 → it is my interface ,please use your interface, use (ifconfig or ip a) command to check your interface id name
lets run it ,after running, now visit our website which we set up earlier, and keep watching your terminal, whenever anyone visit our web site then we will get alert,

Example output is given below,



Whenever we use snort default/pre writen rules , snort capture lots of traffic,
that's why we mostely used custom rules for particular task.
you can see in above figure lots of traffic captured , i highlited web traffic alerts.

To set-up a advance web honeypot, you need to learn about custom rule writing and set up a vulnerable machine to test
your rules is working or not and it will help you in bulding advance web honeypot.