UNIVERSITY OF SCIENCE AND TECHNOLOGY OF HANOI

INTRUSION DETECTION AND PREVENTION SYSTEMS

Report

NVT: Weak Host Key Algorithm(s) (SSH)

Nguyễn Tài Anh – 22BI13028 – Cyber Security

Lecturers: Assoc. Prof. Pham Thanh Giang, Mr. Tran Dai Duong

Hanoi, October 29, 2024

A. Introduction to this vulnerability

I. What is this vuln and type of vulnerability is this?

1. What is this vulnerability?
   - NVT: Weak Host Key Algorithm(s) (SSH)
   - The remote SSH server is configured to allow / support weak host key algorithm(s).
2. Type of vulnerability
   - Server-side vulnerability

II. Outline the technical mechanism of the vulnerability.

1. Key Exchange Vulnerabilities
   - SSH sessions start with a key exchange process to establish a secure communication channel.
   - In weak key exchanges, outdated algorithms like Diffie-Hellman Group1 (1024-bit) are often used, which can be vulnerable to man-in-the-middle (MITM) or logjam attacks, as they rely on short key lengths that can be brute-forced.
   - Attackers can intercept this exchange, potentially deriving the shared session key if the computation requirements are low due to a weak key size.
2. Cipher Vulnerabilities
   - SSH uses symmetric encryption to encrypt data after the key exchange. If weak ciphers (such as 3DES, Blowfish, or AES-128-CBC) are used, an attacker might break the encryption by leveraging known cryptographic weaknesses, such as padding oracle attacks or cipher block chaining (CBC) vulnerabilities.
   - Weak ciphers make the encrypted data more susceptible to cryptographic attacks, like known-plaintext or chosen-ciphertext attacks, which could reveal sensitive information or the entire session's contents.
3. Hashing Algorithm Weaknesses
   - Hash functions are used in SSH for creating digital signatures and integrity checks. However, older algorithms like MD5 and SHA-1 have known vulnerabilities (e.g., susceptibility to collision attacks).
   - If these weak algorithms are used for message authentication (HMAC), attackers could potentially forge or tamper with messages by exploiting hash collisions, which undermine the integrity of the SSH session.
4. Small Key Sizes
   - SSH keys generated with smaller bit sizes, such as RSA-1024 or DSA-1024, are easier to crack with modern computational power.

- If an attacker can break these keys, they could impersonate the server or client, hijack sessions, or decrypt past communications if they have been captured.

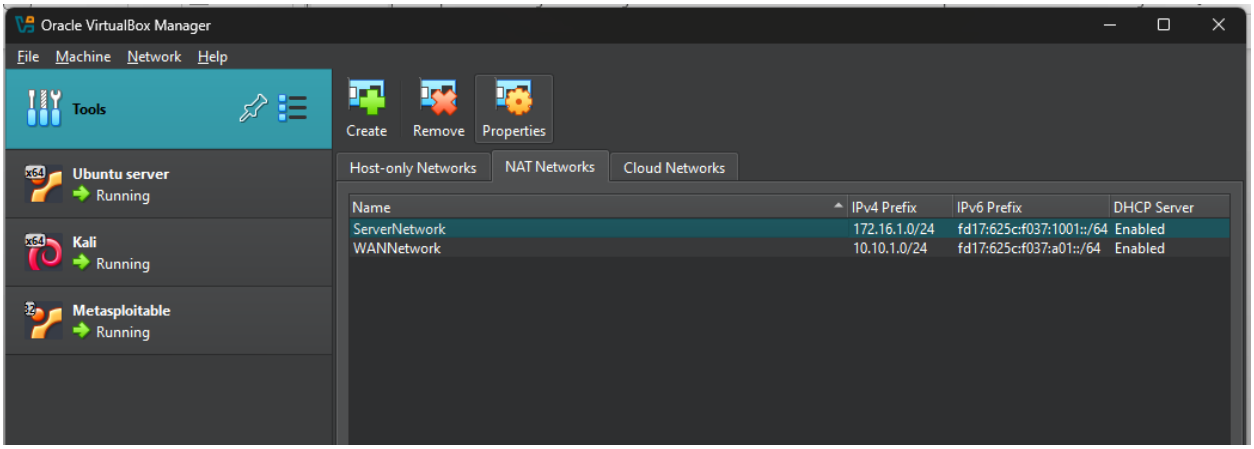
III. Impact and Severity

1. Potential Impact
   - Increased Risk of Man-in-the-Middle (MitM) Attacks.
   - Brute-Force Attacks on SSH Keys
   - Compromised Confidentiality and Integrity of Data
   - Potential Access to the System via Weak Authentication
2. Severity level
   - CVSS: 5.3
   - Quality of Detection (QoD): 80%

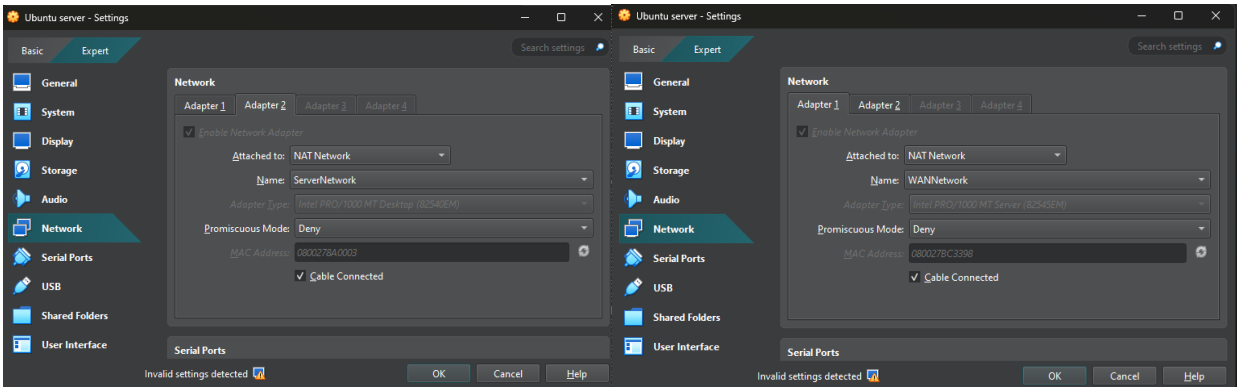
B. Implementation

I. Labwork 1: Creating environment for testing

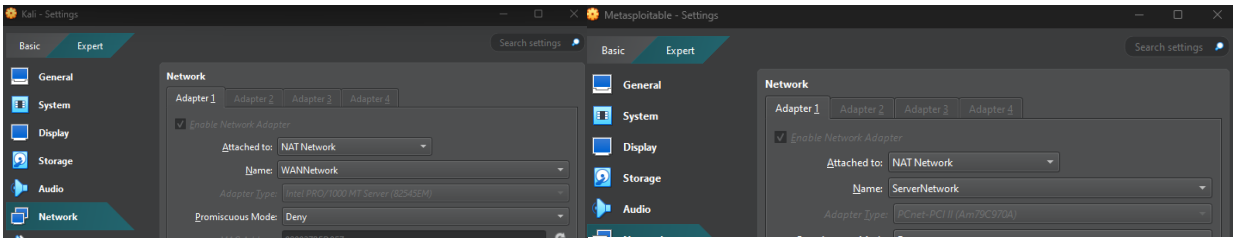
1. Requirement
   - VirtualBox or VMware
   - OVA or ISO file for Kali, Ubuntu server, Metasploitable 2
2. Configure virtual machine network



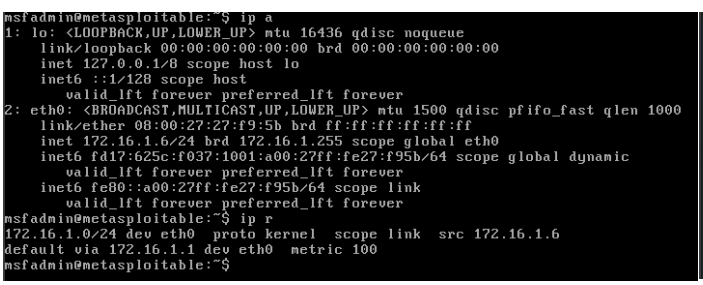
- For Ubuntu server, I will create 2 network adapters, both using NAT Network, one connects to ServerNetwork, the other connect to WANNetwork



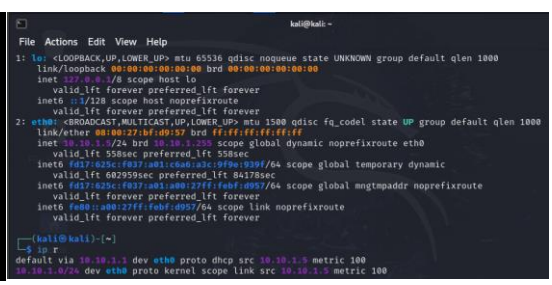
- For Kali, I will connect to WANNetwork and for Metasploitable 2, I will connect to ServerNetwork, both using NAT Network



- After configure network outside in VirtualBox, continue to configure the IPs inside the virtual machine → Result:



```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:27:f9:5b brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.6/24 brd 172.16.1.255 scope global eth0
    inet6 fd17:625c:f037:1001:a00:27ff:fe27:f95b/64 scope global dynamic
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe27:f95b/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ip r
172.16.1.0/24 dev eth0  proto kernel  scope link  src 172.16.1.6
default via 172.16.1.1 dev eth0  metric 100
msfadmin@metasploitable:~$
```

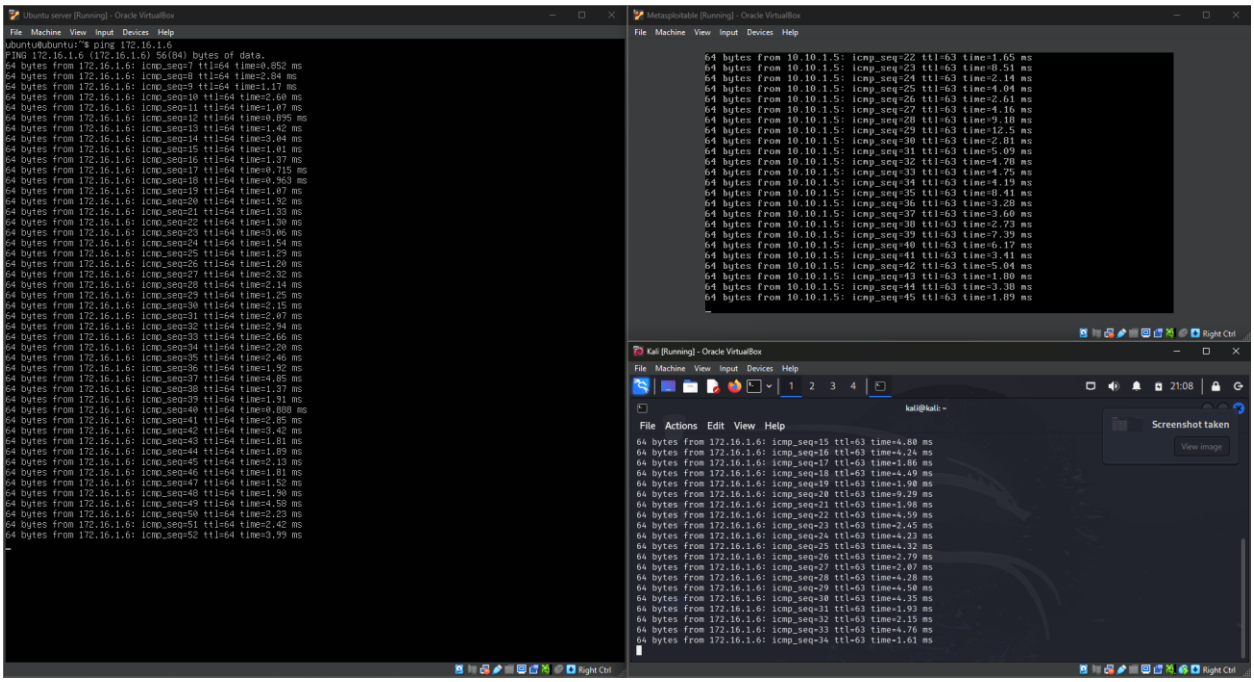


```
kali@kali: ~
File  Actions  Edit  View  Help
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:bf:d9:57 brd ff:ff:ff:ff:ff:ff
    inet 10.10.1.5/24 brd 10.10.1.255 scope global dynamic noprefixroute eth0
       valid_lft 558sec preferred_lft 558sec
    inet6 fd17:625c:f037:a01:c6a6:e3c:9f9e:939f/64 scope global temporary dynamic
       valid_lft 602959sec preferred_lft 84178sec
    inet6 fd17:625c:f037:a01:a00:27ff:febf:d957/64 scope global mngtmpaddr noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:febf:d957/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ip r
default via 10.10.1.1 dev eth0 proto dhcp src 10.10.1.5 metric 100
10.10.1.0/24 dev eth0 proto kernel scope link src 10.10.1.5 metric 100
```

```
ubuntu@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:8a:00:03 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.1/24 brd 172.16.1.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fd17:625c:f037:1001:a00:27ff:fe8a:3/64 scope global mngtmpaddr noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe8a:3/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:bc:33:98 brd ff:ff:ff:ff:ff:ff
    inet 10.10.1.1/24 brd 10.10.1.255 scope global enp0s17
       valid_lft forever preferred_lft forever
    inet6 fd17:625c:f037:a01:a00:27ff:febc:3398/64 scope global mngtmpaddr noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:febc:3398/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$ ip r
10.10.1.0/24 dev enp0s17 proto kernel scope link src 10.10.1.1
172.16.1.0/24 dev enp0s8 proto kernel scope link src 172.16.1.1
```

- Kali: **10.10.1.5**
- Metasploitable 2: **172.16.1.6**
- Ubuntu server: Gateway **10.10.1.1** and **172.16.1.1**

  ➔ Successfully ping these machines together



II. Labwork 2: Security threats and scanning

1. Using nmap (Network Mapper): Scan for ports
   - nmap: Host Discovery

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 172.16.1.*
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 10:50 CDT
Nmap scan report for 172.16.1.1
Host is up (0.00099s latency).
All 1000 scanned ports on 172.16.1.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap scan report for 172.16.1.2
Host is up (0.0035s latency).
All 1000 scanned ports on 172.16.1.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 172.16.1.6
Host is up (0.0043s latency).
Not shown: 977 closed tcp ports (reset)
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

Nmap done: 256 IP addresses (3 hosts up) scanned in 26.46 seconds
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap 172.16.1.6
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 03:38 CDT
Nmap scan report for 172.16.1.6
Host is up (0.014s latency).
Not shown: 977 closed tcp ports (reset)
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

Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds
```

- nmap: Port Scanning
  - SYN packets ***"sudo nmap -sS 172.16.1x"***
  - Full TCP connections ***"sudo nmap -sT 172.1.16.x"***
  - ACK packets ***"sudo nmap -sA 172.16.1.x"***
  - Fin packets ***"sudo nmap -sF 172.16.1.x"***
  - Basic 100 UDP ports ***"sudo nmap -sU 172.16.1.x"***
  - Not scan any port, only host discovery ***"sudo nmap -sn 172.16.1.x"***

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 172.16.1.6
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 10:22 CDT
Nmap scan report for 172.16.1.6
Host is up (0.039s latency).
Not shown: 977 closed tcp ports (reset)
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

Nmap done: 1 IP address (1 host up) scanned in 14.00 seconds
```

- nmap: OS Detection ***"sudo nmap -O 172.16.1.x"***

```
└─$ sudo nmap -O 172.16.1.6
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 03:56 CDT
Nmap scan report for 172.16.1.6
Host is up (0.0049s latency).
Not shown: 977 closed tcp ports (reset)
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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.47 seconds
```

- nmap: Service Detection ***"sudo nmap -sV 172.16.1.x"***

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 172.16.1.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 03:57 CDT
Nmap scan report for 172.16.1.6
Host is up (0.0068s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 195.69 seconds
```

2. Using GVM (Greenbone Vulnerability Management): Scan for threats

- Architecture: Maily consists of the following three components
    - GSA (Greenbone Security Assistants)
    - GVM (Greenbone Vulnerability Management)
    - OpenVAS Scanner

- Installation:
    - Install GVM: ***"sudo apt install gvm"***
    - Setup GVM: ***"sudo gvm-setup"***

```
┌──(kali㉿kali)-[~]
└─$ sudo gvm-setup

[>] Starting PostgreSQL service

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database
[i] User _gvm already exists in PostgreSQL
[i] Database gvmd already exists in PostgreSQL
[i] Role DBA already exists in PostgreSQL

[*] Applying permissions
NOTICE:  role "_gvm" has already been granted membership in role "dba" by role "postgres"
GRANT ROLE
[i] Extension uuid-ossp already exists for gvmd database
[i] Extension pgcrypto already exists for gvmd database
[i] Extension pg-gvm already exists for gvmd database
[>] Migrating database
[>] Checking for GVM admin user
[*] Configure Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
 Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus
/var/lib/notus
```

```
 Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/nasl/
/var/lib/openvas/plugins
rsync: getaddrinfo: feed.community.greenbone.net 873: Temporary failure in name resolution
rsync error: error in socket IO (code 10) at clientserver.c(139) [Receiver=3.3.0]
Releasing lock on /var/lib/openvas/feed-update.lock

Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
 Downloading SCAP data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/scap-data/ to
/var/lib/gvm/scap-data
rsync: getaddrinfo: feed.community.greenbone.net 873: Temporary failure in name resolution
rsync error: error in socket IO (code 10) at clientserver.c(139) [Receiver=3.3.0]

 Downloading CERT-Bund data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/cert-data/
/var/lib/gvm/cert-data
rsync: getaddrinfo: feed.community.greenbone.net 873: Temporary failure in name resolution
rsync error: error in socket IO (code 10) at clientserver.c(139) [Receiver=3.3.0]

 Downloading gvmd data from rsync://feed.community.greenbone.net/community/data-feed/22.04/ to
/var/lib/gvm/data-objects/gvmd/22.04
rsync: getaddrinfo: feed.community.greenbone.net 873: Temporary failure in name resolution
rsync error: error in socket IO (code 10) at clientserver.c(139) [Receiver=3.3.0]

Releasing lock on /var/lib/gvm/feed-update.lock

[*] Checking Default scanner
08b69003-5fc2-4037-a479-93b440211c73  OpenVAS  /run/ospd/ospd.sock  0  OpenVAS Default
[i] No need to alter default scanner

[+] Done
[i] Admin user already exists for GVM
[i] If you have forgotten it, you can change it. See gvmd manpage for more information

[>] You can now run gvm-check-setup to make sure everything is correctly configured
```

- Setup username and password for GVM: ***"sudo -u _gvm --gvmd --user=admin --new-password=letmein"***

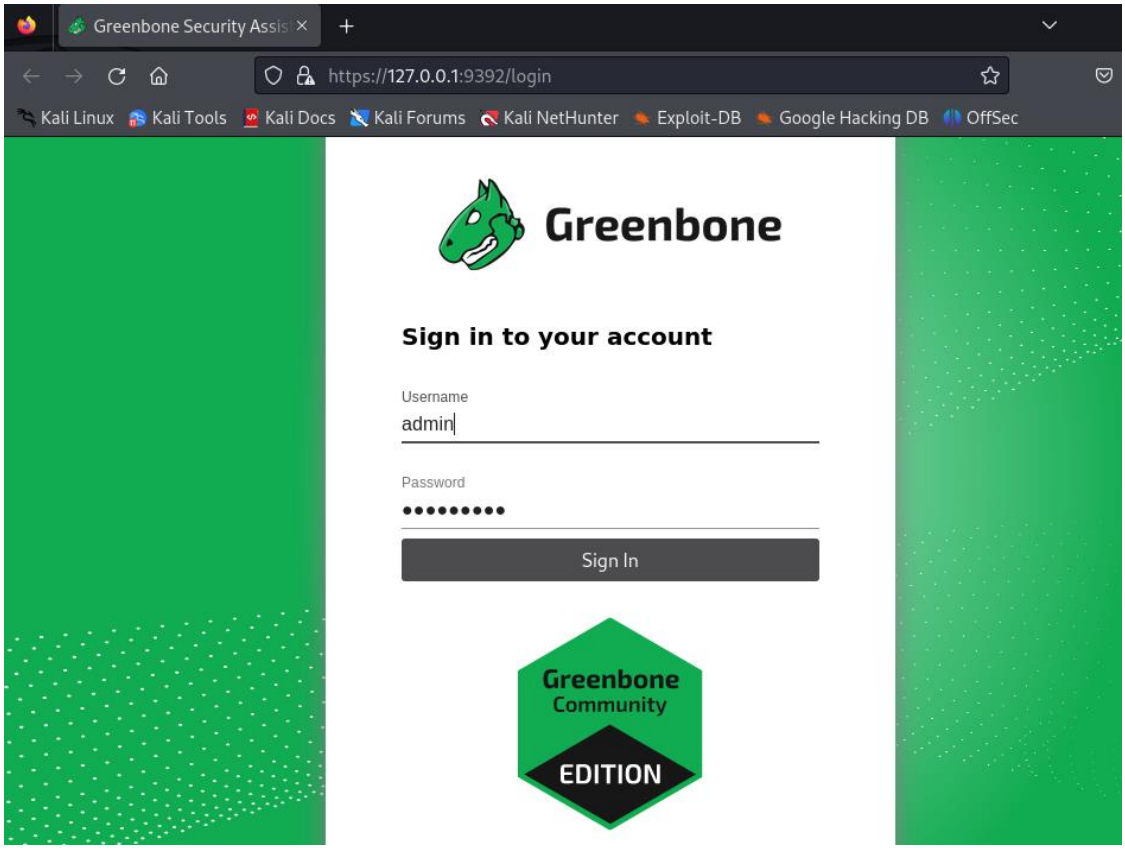
```
┌──(kali㉿kali)-[~]
└─$ sudo -u _gvm gvmd --user=admin --new-password=moonlight

┌──(kali㉿kali)-[~]
```

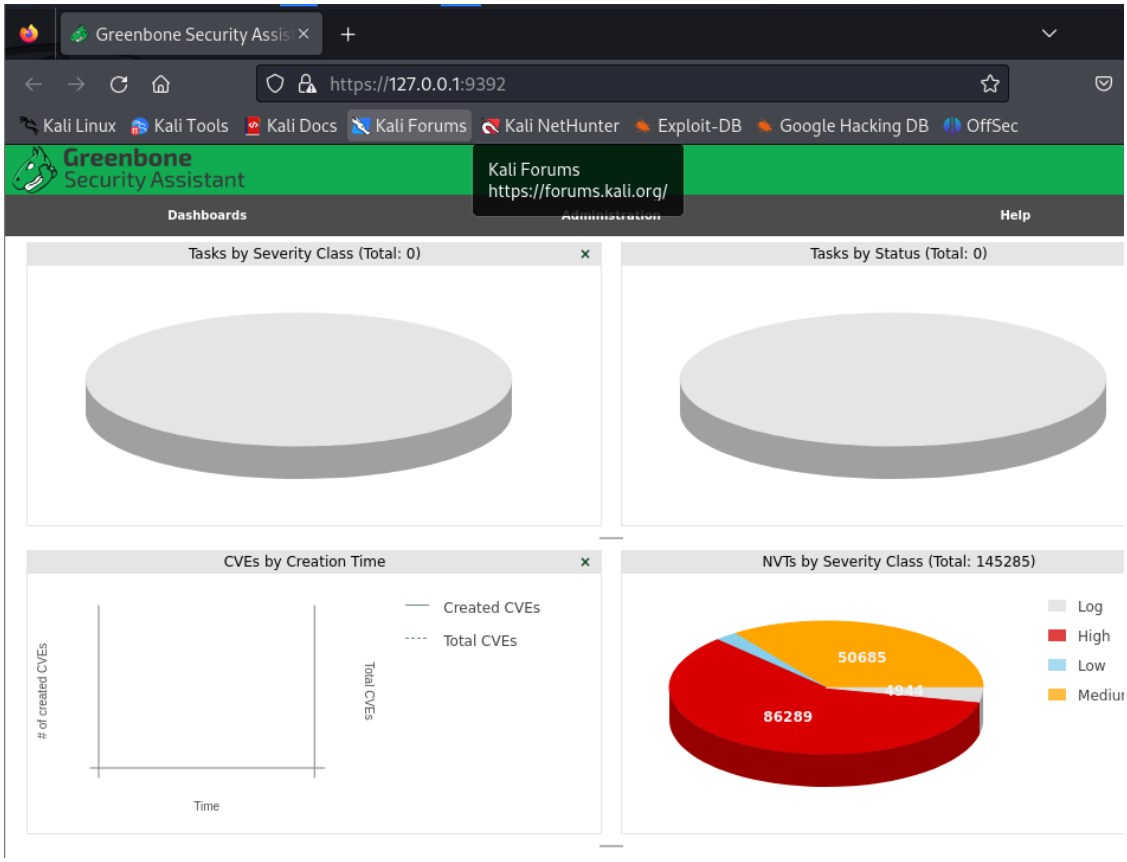
```
Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/nasl/
/var/lib/openvas/plugins
rsync: getaddrinfo: feed.community.greenbone.net 873: Temporary failure in name resolution
rsync error: error in socket IO (code 10) at clientserver.c(139) [Receiver=3.3.0]
Releasing lock on /var/lib/openvas/feed-update.lock

Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
Downloading SCAP data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/scap-data/ to
/var/lib/gvm/scap-data
rsync: getaddrinfo: feed.community.greenbone.net 873: Temporary failure in name resolution
rsync error: error in socket IO (code 10) at clientserver.c(139) [Receiver=3.3.0]

Downloading CERT-Bund data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/cert-data/
/var/lib/gvm/cert-data
rsync: getaddrinfo: feed.community.greenbone.net 873: Temporary failure in name resolution
rsync error: error in socket IO (code 10) at clientserver.c(139) [Receiver=3.3.0]

Downloading gvmd data from rsync://feed.community.greenbone.net/community/data-feed/22.04/ to
/var/lib/gvm/data-objects/gvmd/22.04
rsync: getaddrinfo: feed.community.greenbone.net 873: Temporary failure in name resolution
rsync error: error in socket IO (code 10) at clientserver.c(139) [Receiver=3.3.0]

Releasing lock on /var/lib/gvm/feed-update.lock

[*] Checking Default scanner
08b69003-5fc2-4037-a479-93b440211c73  OpenVAS  /run/ospd/ospd.sock  0  OpenVAS Default
[i] No need to alter default scanner

[+] Done
[i] Admin user already exists for GVM
[i] If you have forgotten it, you can change it. See gvmd manpage for more information

[>] You can now run gvm-check-setup to make sure everything is correctly configured
```

- Start gvm: ***"sudo gvm-start"***

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo gvm-start
[sudo] password for kali:
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
     Active: active (running) since Fri 2024-10-25 04:40:04 CDT; 12ms ago
 Invocation: 163941aca98748c8b5f239c7ef96bd89
       Docs: man:gsad(8)
             https://www.greenbone.net
   Main PID: 35685 (gsad)
      Tasks: 1 (limit: 4606)
     Memory: 1.2M (peak: 1.2M)
        CPU: 3ms
     CGroup: /system.slice/gsad.service
             └─35685 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Oct 25 04:40:04 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gs
ad)...
Oct 25 04:40:04 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsa
d).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/usr/lib/systemd/system/gvmd.service; disabled; preset: disabled)
     Active: active (running) since Fri 2024-10-25 04:39:59 CDT; 5s ago
 Invocation: 4288261ec4f44d9fa419eea364b04625
       Docs: man:gvmd(8)
    Process: 35577 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_
gvm (code=exited, status=0/SUCCESS)
   Main PID: 35578 (gvmd)
      Tasks: 2 (limit: 4606)
     Memory: 6.5M (peak: 9.3M)
        CPU: 2.277s
```

```
kali@kali: ~
File  Actions  Edit  View  Help
   Main PID: 35578 (gvmd)
      Tasks: 2 (limit: 4606)
     Memory: 6.5M (peak: 9.3M)
        CPU: 2.277s
     CGroup: /system.slice/gvmd.service
             ├─35578 "gvmd: Waiting " --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
             └─35607 gpg-agent --homedir /var/lib/gvm/gvmd/gnupg --use-standard-socket --daemon

Oct 25 04:39:56 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon
(gvmd)...
Oct 25 04:39:56 kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) aft
er start: No such file or directory
Oct 25 04:39:59 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (
gvmd).

● ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
     Loaded: loaded (/usr/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
     Active: active (running) since Fri 2024-10-25 04:39:55 CDT; 8s ago
 Invocation: e574947ba93e42f193a3acc5d03d56d0
       Docs: man:ospd-openvas(8)
             man:openvas(8)
    Process: 35513 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-con
fig /etc/gvm/ospd-logging.conf (code=exited, status=0/SUCCESS)
   Main PID: 35548 (ospd-openvas)
      Tasks: 5 (limit: 4606)
     Memory: 60.7M (peak: 101.5M)
        CPU: 1.852s
     CGroup: /system.slice/ospd-openvas.service
             ├─35548 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf
--log-config /etc/gvm/ospd-logging.conf
             └─35551 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf
--log-config /etc/gvm/ospd-logging.conf

Oct 25 04:39:53 kali systemd[1]: Starting ospd-openvas.service - OSPd Wrapper for the OpenVAS Sc
anner (ospd-openvas)...
Oct 25 04:39:55 kali systemd[1]: Started ospd-openvas.service - OSPd Wrapper for the OpenVAS Sca
nner (ospd-openvas).
```


Greenbone Security Assis
https://127.0.0.1:9392/login
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone
Sign in to your account
Username
admin
Password
Sign In
Greenbone
Community
EDITION


Greenbone Security Assis
https://127.0.0.1:9392
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone
Security Assistant
Kali Forums
https://forums.kali.org/
Dashboards
Help
Tasks by Severity Class (Total: 0)
Tasks by Status (Total: 0)
CVEs by Creation Time
Created CVEs
Total CVEs
# of created CVEs
Total CVEs
Time
NVTs by Severity Class (Total: 145285)
Log
High
Low
50685
86289

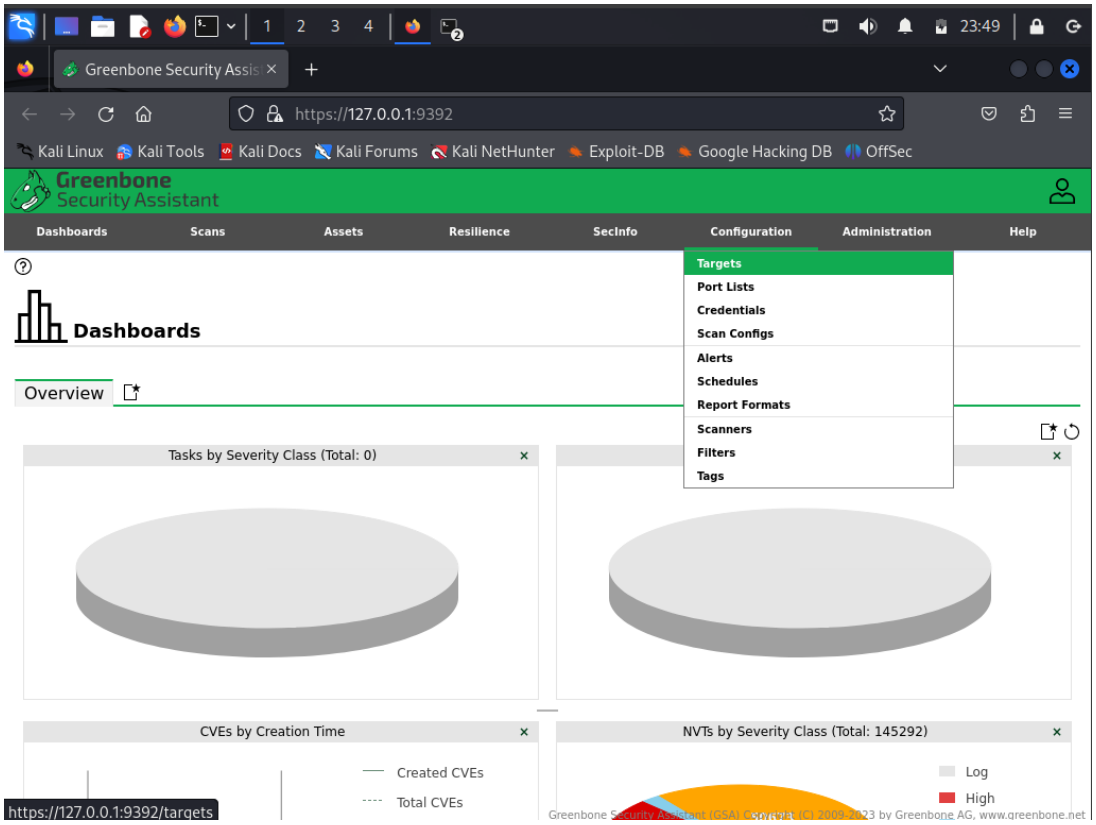
- Check if GVM start successfully: ***"sudo ss -lntp"***

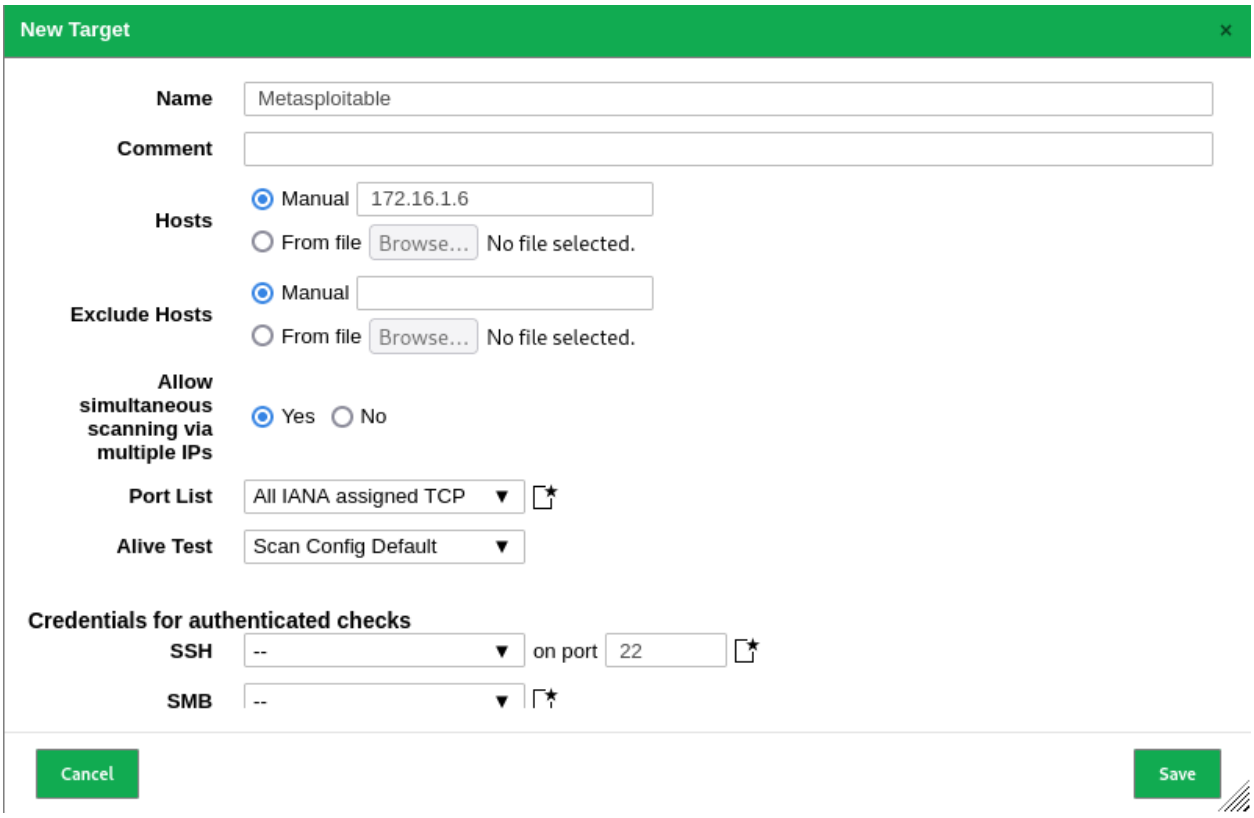
```
┌──(kali㉿kali)-[~]
└─$ sudo ss -lntp
State   Recv-Q  Send-Q   Local Address:Port   Peer Address:Port Process
LISTEN  0       244          127.0.0.1:5432        0.0.0.0:*     users:(("postgres",pid=5907,
LISTEN  0       4096         127.0.0.1:9392        0.0.0.0:*     users:(("gsad",pid=25645,fd=
LISTEN  0       4096         127.0.0.1:80          0.0.0.0:*     users:(("gsad",pid=25646,fd=
LISTEN  0       244              [::1]:5432           [::]:*     users:(("postgres",pid=5907,
```

- Stop GVM: ***"sudo gvm-stop"***

```
┌──(kali㉿kali)-[~]
└─$ sudo gvm-stop
[>] Stopping GVM services
○ gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:gsad(8)
             https://www.greenbone.net

Oct 25 21:41:26 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Oct 25 21:41:26 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).
Oct 25 21:54:40 kali systemd[1]: Stopping gsad.service - Greenbone Security Assistant daemon (gsad)...
Oct 25 21:54:40 kali systemd[1]: gsad.service: Deactivated successfully.
Oct 25 21:54:40 kali systemd[1]: Stopped gsad.service - Greenbone Security Assistant daemon (gsad).

○ gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/usr/lib/systemd/system/gvmd.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:gvmd(8)

Oct 25 21:41:08 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Oct 25 21:41:08 kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: No such fil
rectory
Oct 25 21:41:21 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).
Oct 25 21:54:40 kali systemd[1]: Stopping gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Oct 25 21:54:40 kali systemd[1]: gvmd.service: Deactivated successfully.
Oct 25 21:54:40 kali systemd[1]: Stopped gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).

○ ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
     Loaded: loaded (/usr/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:ospd-openvas(8)
             man:openvas(8)

Oct 25 21:40:53 kali systemd[1]: Starting ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas).
Oct 25 21:40:57 kali systemd[1]: Started ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas).
Oct 25 21:54:40 kali systemd[1]: Stopping ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas).
Oct 25 21:54:40 kali systemd[1]: ospd-openvas.service: Deactivated successfully.
Oct 25 21:54:40 kali systemd[1]: Stopped ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas).
```

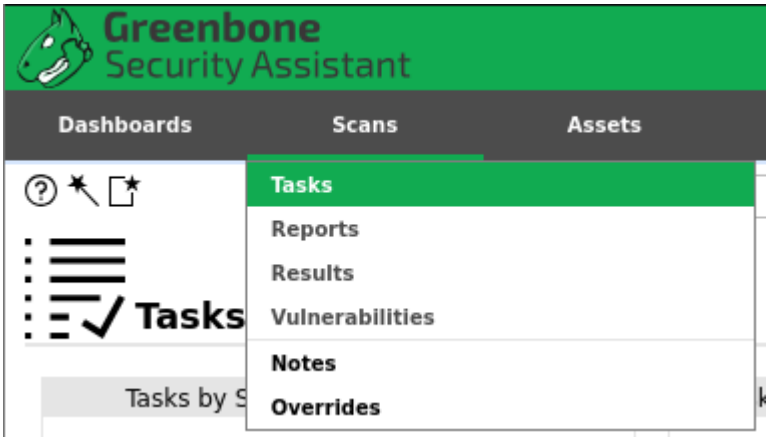
- GVM – Usage
  - Create a target


Greenbone Security Assistant
https://127.0.0.1:9392
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Targets
Port Lists
Credentials
Scan Configs
Alerts
Schedules
Report Formats
Scanners
Filters
Tags
Dashboards
Overview
Tasks by Severity Class (Total: 0)
CVEs by Creation Time
Created CVEs
Total CVEs
NVTs by Severity Class (Total: 145292)
Log
High
https://127.0.0.1:9392/targets

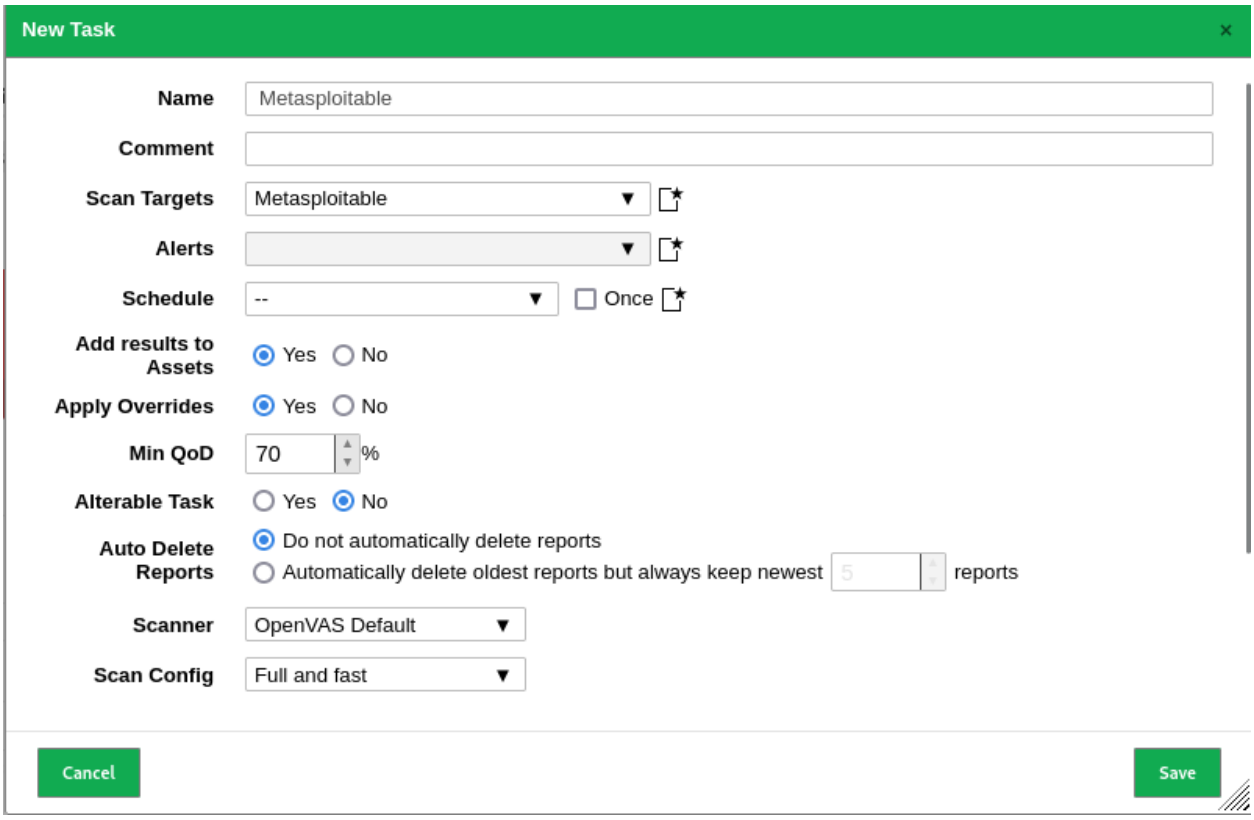

New Target
Name
Metasploitable
Comment
Hosts
Manual
172.16.1.6
From file
Browse...
No file selected.
Exclude Hosts
Manual
From file
Browse...
No file selected.
Allow simultaneous scanning via multiple IPs
Yes
No
Port List
All IANA assigned TCP
Alive Test
Scan Config Default
Credentials for authenticated checks
SSH
--
on port
22
SMB
--
Cancel
Save

- As can be seen, my Metasploitable machine has IP 172.16.1.6 and it's OpenSSH connection is at port 22
- Port List using: All IANA assigned TCP (can check at Port Lists in Configuration tab)

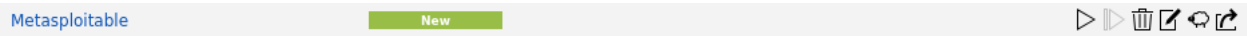
- Create a task



- Navigate to Scans tab, choose "Tasks" and click to "*" icon to create a new task

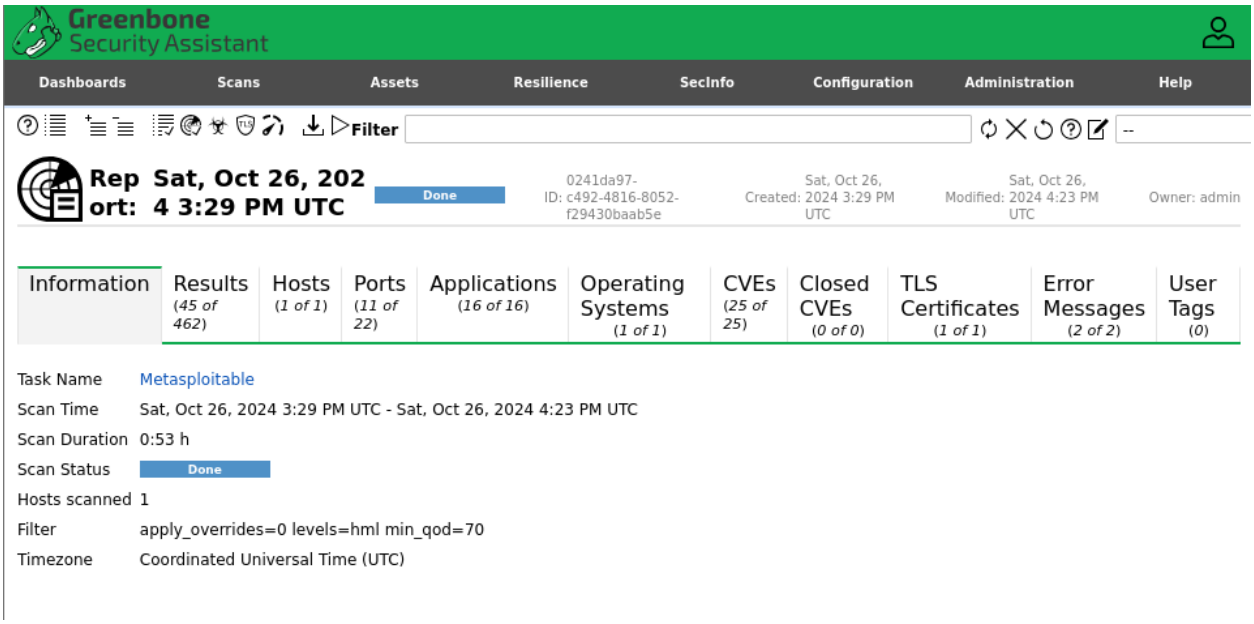


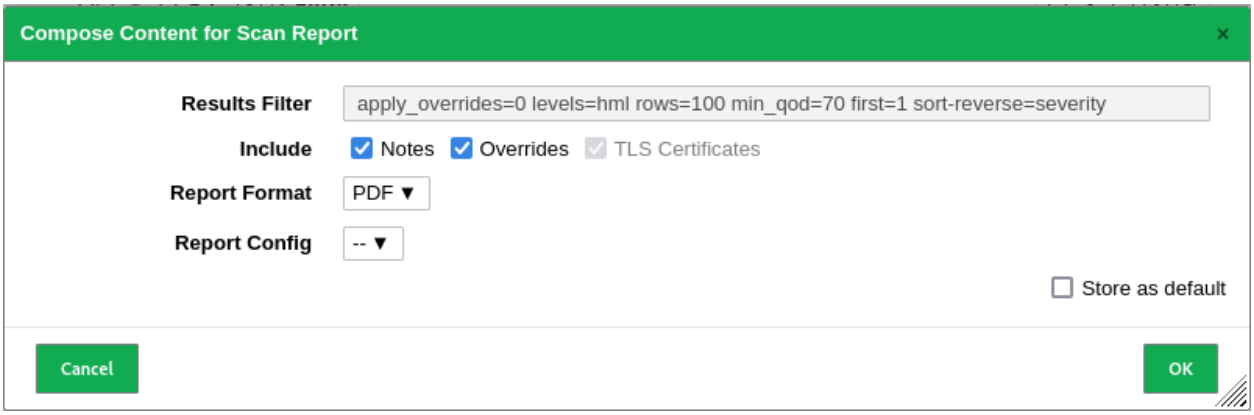
- In Scan Targets, choose the target you have just created.

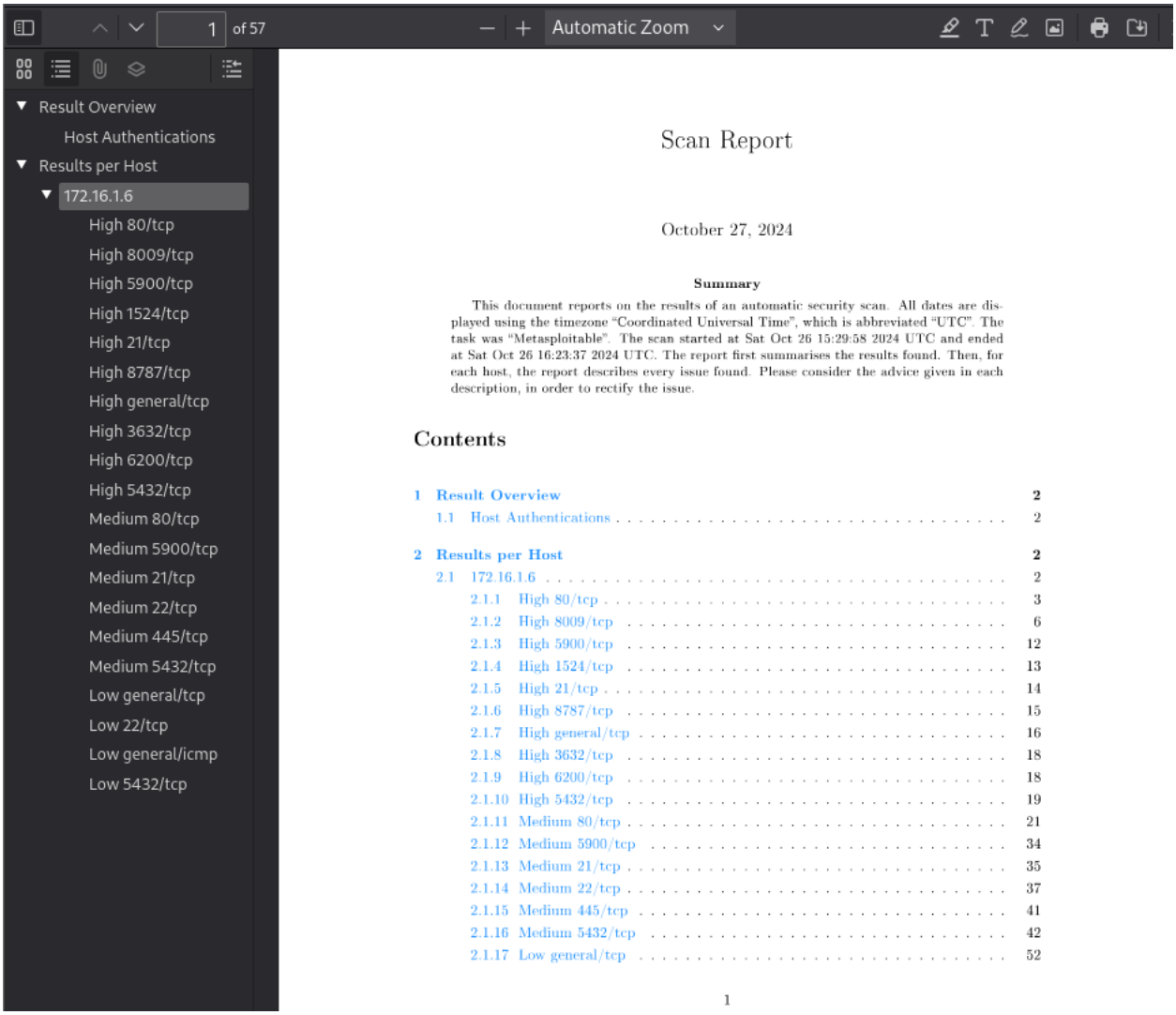


- Start the task
  - To run this task, click on the “start” button (triangle one)
  - After the task is started, the web UI of GVM will automatically refresh about the progress of the scan.

- Report







3. Exploitation **NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)**
   - Connect to Metasploitable VM using SSH
     - Start SSH in Metasploitable by using command ***"sudo nano /etc/rc.local"***, and then add a line ***"/etc/init.d/ssh start"*** to start SSH service each time Metasploitable VM is booted.
     - In Kali, because Kali cannot detect and matching host key, so we have to use command ***"ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa msfadmin@172.16.1.6"*** to connect to Metasploitable VM using SSH service.

```
┌──(kali㉿kali)-[~]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa msfa
dmin@172.16.1.6
The authenticity of host '172.16.1.6 (172.16.1.6)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.1.6' (RSA) to the list of known hosts.
msfadmin@172.16.1.6's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Oct 28 14:14:41 2024
msfadmin@metasploitable:~$ ls
vulnerable
```

- Start Metasploit Framework
  - Metasploit relies on a database to speed up searches. Ensure the database is started with
    - ***"sudo service postgresql start"***
    - ***"sudo msfdb init"***
  - Using command ***"msfconsole"*** to start Metasploit framework

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

       =[ metasploit v6.4.32-dev                          ]
+ -- --=[ 2458 exploits - 1264 auxiliary - 430 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

- Using ***"search ssh"***

```
   0    exploit/linux/http/acronis_cyber_infra_cve_2023_45249          2024-07-24    excellent  Yes   Acronis Cybe
r Infrastructure default password remote code execution
   1       \_ target: Unix/Linux Command                               .             .          .     .
   2       \_ target: Interactive SSH                                  .             .          .     .
   3    exploit/linux/http/alienvault_exec                             2017-01-31    excellent  Yes   AlienVault O
SSIM/USM Remote Code Execution
   4    auxiliary/scanner/ssh/apache_karaf_command_execution           2016-02-09    normal     No
 Default Credentials Command Execution
   5    auxiliary/scanner/ssh/karaf_login                              .             normal     No
 Login Utility
   6    exploit/apple_ios/ssh/cydia_default_ssh                        2007-07-02    excellent  No    Apple iPhone
fault SSH Password Vulnerability
   7    exploit/unix/ssh/arista_tacplus_shell                          2020-02-02    great      Yes   Arista restr
icted shell escape (with privesc)
   8    exploit/unix/ssh/array_vxag_vapv_privkey_privesc               2014-02-03    excellent  No    Array Networ
ks vAPV and vXAG Private Key Privilege Escalation Code Execution
   9    exploit/linux/ssh/ceragon_fibeair_known_privkey                2015-04-01    excellent  No    Ceragon Fibe
Air IP-10 SSH Private Key Exposure
   10   auxiliary/scanner/ssh/cerberus_sftp_enumusers                  2014-05-27    normal     No    Cerberus FTP
 Server SFTP Username Enumeration
   11   auxiliary/dos/cisco/cisco_7937g_dos                            2020-06-02    normal     No    Cisco 7937G
Denial-of-Service Attack
   12   auxiliary/admin/http/cisco_7937g_ssh_privesc                   2020-06-02    normal     No    Cisco 7937G
SSH Privilege Escalation
   13   exploit/linux/http/cisco_asax_sfr_rce                          2022-06-22    excellent  Yes   Cisco ASA-X
with FirePOWER Services Authenticated Command Injection
   14      \_ target: Shell Dropper                                    .             .          .     .
   15      \_ target: Linux Dropper                                    .             .          .     .
   16   auxiliary/scanner/http/cisco_firepower_login                   .             normal     No    Cisco Firepo
wer Management Console 6.0 Login
   17   exploit/linux/ssh/cisco_ucs_scpuser                            2019-08-21    excellent  No    Cisco UCS Di
rector default scpuser password
   18   auxiliary/scanner/ssh/eaton_xpert_backdoor                     2018-07-18    normal     No    Eaton Xpert
Meter SSH Private Key Exposure Scanner
   19   exploit/linux/ssh/exagrid_known_privkey                        2016-04-07    excellent  No    ExaGrid Know
n SSH Key and Default Password
   20   exploit/linux/ssh/f5_bigip_known_privkey                       2012-06-11    excellent  No    F5 BIG-IP SS
H Private Key Exposure
   21   exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684  2022-10-10    excellent  Yes   Fortinet For
tiOS, FortiProxy, and FortiSwitchManager authentication bypass.
   22   auxiliary/scanner/ssh/fortinet_backdoor                        2016-01-09    normal     No    Fortinet SSH
 Backdoor Scanner
   23   post/windows/manage/forward_pageant                            .             normal     No    Forward SSH
Agent Requests To Remote Pageant
   24   exploit/windows/ssh/freeftpd_key_exchange                      2006-05-12    average    No    FreeFTPd 1.0
.10 Key Exchange Algorithm String Buffer Overflow
   25      \_ target: Windows 2000 SP0-SP4 English                     .             .          .     .
   26      \_ target: Windows 2000 SP0-SP4 German                      .             .          .     .
   27      \_ target: Windows XP SP0-SP1 English                       .             .          .     .
   28      \_ target: Windows XP SP2 English                           .             .          .     .
   29   exploit/windows/ssh/freesshd_key_exchange                      2006-05-12    average    No    FreeSSHd 1.0
.9 Key Exchange Algorithm String Buffer Overflow
   30      \_ target: Windows 2000 Pro SP4 English                     .             .          .     .
```

```
 Network Information
   52   exploit/linux/local/ptrace_traceme_pkexec_helper               2019-07-04    excellent  Yes   Linux Polkit
 pkexec helper PTRACE_TRACEME local root exploit
   53   exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey     2014-03-17    excellent  No    Loadbalancer
.org Enterprise VA SSH Private Key Exposure
   54   exploit/multi/http/git_submodule_command_exec                  2017-08-10    excellent  No    Malicious Gi
t HTTP Server For CVE-2017-1000117
   55   exploit/linux/ssh/mercurial_ssh_exec                           2017-04-18    excellent  No    Mercurial Cu
stom hg-ssh Wrapper Remote Code Exec
   56   exploit/linux/ssh/microfocus_obr_shrboadmin                    2020-09-21    excellent  No    Micro Focus
 Operations Bridge Reporter shrboadmin default password
   57   post/multi/gather/ssh_creds                                    .             normal     No    Multi Gather
 OpenSSH PKI Credentials Collection
   58   exploit/solaris/ssh/pam_username_bof                           2020-10-20    normal     Yes   Oracle Solar
is SunSSH PAM parse_user_name() Buffer Overflow
   59      \_ target: SunSSH 1.1.5 / Solaris 10u11 1/13 (x86) / VMware  .             .          .     .
   60      \_ target: SunSSH 1.1.5 / Solaris 10u11 1/13 (x86) / VirtualBox  .         .          .     .
   61   auxiliary/gather/prometheus_api_gather                         2016-07-01    normal     No    Prometheus A
PI Information Gather
   62   exploit/windows/ssh/putty_msg_debug                            2002-12-16    normal     No    PuTTY Buffer
 Overflow
   63      \_ target: Windows 2000 SP4 English                         .             .          .     .
   64      \_ target: Windows XP SP2 English                           .             .          .     .
   65      \_ target: Windows 2003 SP1 English                         .             .          .     .
   66   post/windows/gather/enum_putty_saved_sessions                  .             normal     No    PuTTY Saved
 Sessions Enumeration Module
   67   auxiliary/gather/qnap_lfi                                      2019-11-25    normal     Yes   QNAP QTS and
 Photo Station Local File Inclusion
   68   exploit/linux/ssh/quantum_dxi_known_privkey                    2014-03-17    excellent  No    Quantum DXi
V1000 SSH Private Key Exposure
   69   exploit/linux/ssh/quantum_vmpro_backdoor                       2014-03-17    excellent  No    Quantum vmPR
O Backdoor Command
   70   auxiliary/fuzzers/ssh/ssh_version_15                           .             normal     No    SSH 1.5 Vers
ion Fuzzer
   71   auxiliary/fuzzers/ssh/ssh_version_2                            .             normal     No    SSH 2.0 Vers
ion Fuzzer
   72   auxiliary/fuzzers/ssh/ssh_kexinit_corrupt                      .             normal     No    SSH Key Exch
ange Init Corruption
   73   post/linux/manage/sshkey_persistence                           .             excellent  No    SSH Key Pers
istence
   74   post/windows/manage/sshkey_persistence                         .             good       No    SSH Key Pers
istence
   75   auxiliary/scanner/ssh/ssh_login                                .             normal     No    SSH Login Ch
eck Scanner
   76   auxiliary/scanner/ssh/ssh_identify_pubkeys                     .             normal     No    SSH Public K
ey Acceptance Scanner
   77   auxiliary/scanner/ssh/ssh_login_pubkey                         .             normal     No    SSH Public K
ey Login Scanner
   78   exploit/multi/ssh/sshexec                                      1999-01-01    manual     No    SSH User Cod
e Execution
   79      \_ target: Linux Command                                    .             .          .     .
   80      \_ target: Linux x86                                        .             .          .     .
   81      \_ target: Linux x64                                        .             .          .     .
```

```
   126     \_ target: 6.4_collector                                  .                .          .      .
   127     \_ target: 6.4_platform                                   .                .          .      .
   128     \_ target: 6.5_collector                                  .                .          .      .
   129     \_ target: 6.5_platform                                   .                .          .      .
   130     \_ target: 6.6_collector                                  .                .          .      .
   131     \_ target: 6.6_platform                                   .                .          .      .
   132     \_ target: 6.7_collector                                  .                .          .      .
   133     \_ target: 6.7_platform                                   .                .          .      .
   134     \_ target: 6.8_collector                                  .                .          .      .
   135     \_ target: 6.8_platform                                   .                .          .      .
   136     \_ target: 6.9_collector                                  .                .          .      .
   137     \_ target: 6.9_platform                                   .                .          .      .
   138     \_ target: 6.10_collector                                 .                .          .      .
   139     \_ target: 6.10_platform                                  .                .          .      .
   140     \_ target: All                                            .                .          .      .
   141  exploit/linux/ssh/vmware_vdp_known_privkey                   2016-12-20       excellent  No     VMware VDP K
nown SSH Key
   142  exploit/multi/http/vmware_vcenter_uploadova_rce              2021-02-23       manual     Yes    VMware vCent
er Server Unauthenticated OVA File Upload RCE
   143     \_ target: VMware vCenter Server ≤ 6.7 Update 1b (Linux)  .                .          .      .
   144     \_ target: VMware vCenter Server ≤ 6.7 Update 3j (Windows) .               .          .      .
   145  exploit/linux/ssh/vyos_restricted_shell_privesc              2018-11-05       great      Yes    VyOS restric
ted-shell Escape and Privilege Escalation
   146  post/windows/gather/credentials/whatsupgold_credential_dump  2022-11-22       manual     No     WhatsUp Gold
 Credentials Dump
   147     \_ action: Decrypt                                        .                .          .      Decrypt What
sUp Gold database export CSV file
   148     \_ action: Dump                                           .                .          .      Export Whats
Up Gold database and perform decryption
   149     \_ action: Export                                         .                .          .      Export Whats
Up Gold database without decryption
   150  post/windows/gather/credentials/mremote                      .                normal     No     Windows Gath
er mRemote Saved Password Extraction
   151  exploit/windows/local/unquoted_service_path                  2001-10-25       great      Yes    Windows Unqu
oted Service Path Privilege Escalation
   152  exploit/linux/http/zyxel_lfi_unauth_ssh_rce                  2022-02-01       excellent  Yes    Zyxel chaine
d RCE using LFI and weak password derivation algorithm
   153     \_ target: Unix Command                                   .                .          .      .
   154     \_ target: Linux Dropper                                  .                .          .      .
   155     \_ target: Interactive SSH                                .                .          .      .
   156  auxiliary/scanner/ssh/libssh_auth_bypass                     2018-10-16       normal     No     libssh Authe
ntication Bypass Scanner
   157     \_ action: Execute                                        .                .          .      Execute a co
mmand
   158     \_ action: Shell                                          .                .          .      Spawn a shel
l
   159  exploit/linux/http/php_imap_open_rce                         2018-10-23       good       Yes    php imap_ope
n Remote Code Execution
   160     \_ target: prestashop                                     .                .          .      .
   161     \_ target: suitecrm                                       .                .          .      .
   162     \_ target: e107v2                                         .                .          .      .
   163     \_ target: Horde IMP H3                                   .                .          .      .
   164     \_ target: custom                                         .                .          .      .
```

- Set up the brute-force module

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.16.1.6
RHOSTS => 172.16.1.6
msf6 auxiliary(scanner/ssh/ssh_login) >
```

- Using command ***"show options"*** to check for everything that has been changed.

```
sudo: msfadmin: command not found
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   ANONYMOUS_LOGIN  false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS  false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED 5                yes       How fast to bruteforce, from 0 to 5
   CreateSession    true             no        Create a new session for every successful login
   DB_ALL_CREDS     false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS      false            no        Add all passwords in the current database to the list
   DB_ALL_USERS     false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING none             no        Skip existing credentials stored in the current database (Accepted: none
                                               , user, user&realm)
   PASSWORD         msfadmin         no        A specific password to authenticate with
   PASS_FILE                         no        File containing passwords, one per line
   RHOSTS           172.16.1.6       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
                                               t/basics/using-metasploit.html
   RPORT            22               yes       The target port
   STOP_ON_SUCCESS  false            yes       Stop guessing when a credential works for a host
   THREADS          1                yes       The number of concurrent threads (max one per host)
   USERNAME         msfadmin         no        A specific username to authenticate as
   USERPASS_FILE                     no        File containing users and passwords separated by space, one pair per lin
                                               e
   USER_AS_PASS     false            no        Try the username as the password for all users
   USER_FILE                         no        File containing usernames, one per line
   VERBOSE          false            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 172.16.1.6:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

- Searching for currently running SSH sessions
  - Using command ***"sessions -l"***

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 172.16.1.6:22 - Starting bruteforce
[+] 172.16.1.6:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24
(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(ms
fadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 3 opened (10.10.1.6:46571 → 172.16.1.6:22) at 2024-10-30 22:55:12 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l

Active sessions
===============

  Id  Name  Type          Information  Connection
  --  ----  ----          -----------  ----------
  2         shell linux   SSH kali @   10.10.1.6:32805 → 172.16.1.6:22 (172.16.1.6)
  3         shell linux   SSH kali @   10.10.1.6:46571 → 172.16.1.6:22 (172.16.1.6)
```

- Interaction with the currently running SSH connections
  - Using command ***"session -i [session_id]"***

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

adsasd
-bash: line 2: adsasd: command not found
ls
vJbcYFYq
vulnerable
ls
vJbcYFYq
vulnerable
ls
vJbcYFYq
vulnerable
clear
lTERM environment variable not set.
ls
-bash: line 7: lls: command not found
cd vulnerable
ls
mysql-ssl
samba
tikiwiki
twiki20030201
cd
```

- As can be seen, I can interact with the SSH connection from outside of the main user terminal, it means that I can also interact with any SSH connections that are connected to the Metasploitable VM, and of course steal or cat data from them.

III. Labwork 3: Mitigation and Prevention

1. Detection (Next Lab)
2. Prevention (Block the port 22 immediately / Blocking Hacker's IP)
   - Blocking the port 22 immediately
     - Using Iptables to set rule for the Ubuntu server (firewall) to block all SSH connections to the Metasploitable2 VM
       - Command: ***"sudo iptables -A FORWARD -d 172.16.1.6 -p tcp --dport 22 -j REJECT"***

```
ubuntu@ubuntu:~$ sudo iptables -A FORWARD -d 172.16.1.6 -p tcp --dport 22 -j REJECT
[sudo] password for ubuntu:
ubuntu@ubuntu:~$
```

➔ Result:

```
┌──(kali㉿kali)-[~]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa msfa
dmin@172.16.1.6
ssh: connect to host 172.16.1.6 port 22: Connection refused
```

     - Optional: We can also set the allow IP that can SSH to the machine by using command: ***"sudo iptables -I FORWARD -s 10.10.1.6 -d 172.16.1.6 -p tcp --dport 22 -j ACCEPT"***

➔ Result: The machine with IP 10.10.1.6 (In my case is Kali) now can SSH to the Metasploitable2 machine while others still be rejected.

   - Save the rules
     - Command: ***"sudo netfilter-persistent save"***
     - The iptables-persistent service will automatically load saved rules on boot. If you want to manually reload saved rules, you can use: ***"sudo netfilter-persistent reload"***
     - Save rule manually: ***"sudo iptables-save > /etc/iptables/rules.v4"***
     - Load Rules on Boot Using "/etc/rc.local": ***"iptables-restore < /etc/iptables/rules.v4"***
     - Check if rules are in place: ***"sudo iptables -L -v -n"***

```
ubuntu@ubuntu:~$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 4 packets, 336 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2   120 REJECT     6    --  *      *       0.0.0.0/0            172.16.1.6           tcp dpt:22 reject
rt-unreachable

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

    - Do not need to block each hackers' IPs, but no one can freely access the server through SSH connections except when the server allow an specific IP to connect to.
- Blocking directly hackers' Ips
    - Using tcmdump to catch all the SSH connections that are sending to the Metasploitable2 VM

```
00:44:37.372177 IP 172.16.1.6.ssh > 172.16.1.8.54062: P 161:201(40) ack 200 win
136 <nop,nop,timestamp 691766 2098248579>
00:44:37.373030 IP 172.16.1.8.54062 > 172.16.1.6.ssh: . ack 201 win 249 <nop,nop
,timestamp 2098248580 691766>
00:44:37.388130 IP 172.16.1.6.ssh > 172.16.1.8.54062: P 201:353(152) ack 200 win
 136 <nop,nop,timestamp 691768 2098248580>
00:44:37.389632 IP 172.16.1.6.ssh > 172.16.1.8.54062: P 353:409(56) ack 200 win
136 <nop,nop,timestamp 691768 2098248580>
00:44:37.389981 IP 172.16.1.8.54062 > 172.16.1.6.ssh: . ack 353 win 249 <nop,nop
,timestamp 2098248597 691768>
00:44:37.390827 IP 172.16.1.8.54062 > 172.16.1.6.ssh: . ack 409 win 249 <nop,nop
,timestamp 2098248598 691768>
00:44:42.195202 IP localhost.57770 > localhost.57770: UDP, length 64
00:44:47.296827 IP localhost.57770 > localhost.57770: UDP, length 20
00:44:47.300575 IP localhost.57770 > localhost.57770: UDP, length 944
00:44:47.300631 IP localhost.57770 > localhost.57770: UDP, length 760
00:44:47.300678 IP localhost.57770 > localhost.57770: UDP, length 208
```

    - Here I have two VMs with IP 172.16.1.6 and 172.16.1.8 are SSH to Metasploitable2, and we can see that there are these IPs' log show on the tcpdump.
    - Use iptables log to log the hackers' IPs: ***"sudo iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "SSH attempt: " --log-level 4"***
    - Blocking hackers' IPs by using command: ***"sudo iptables -A INPUT -s 172.16.1.8 -j DROP"*** or ***"sudo iptables -A INPUT -s 172.16.1.9 -j DROP"***
    - Do not need to block the whole port 22, but each time being attacked, we have to log again to check the hackers' IPs and block them.

C. Conclusion

1. Vulnerability Description:
    - This NVT detects SSH configurations using weak or outdated cryptographic algorithms, such as low-bit RSA or DSS (DSA) keys, and hash algorithms like MD5 or SHA-1.
2. Technical Mechanism:
    - SSH keys with insufficient bit strength (e.g., RSA < 2048 bits) or deprecated algorithms (e.g., DSS/DSA) are easier to attack due to advancements in computing power and known cryptographic weaknesses.

3. Impact
   - Man-in-the-Middle (MitM) Risk: Weak algorithms allow attackers to intercept or impersonate SSH connections.
   - Brute-Force Susceptibility: Weaker encryption makes SSH connections more vulnerable to brute-force attacks.
   - Data Confidentiality and Integrity Threat: Compromised encryption endangers the security of data transferred over SSH.
   - Compliance Risks: Weak algorithms may violate security standards like PCI-DSS or GDPR.
   - System Access Vulnerability: Weak host keys can potentially allow attackers to bypass authentication, leading to unauthorized access.
4. Mitigation
   - Update the SSH configuration to use strong algorithms (e.g., ecdsa-sha2-nistp256, ed25519) and a minimum of RSA-2048 if RSA keys are used.
   - Block SSH port 22 at the firewall if SSH access is unnecessary to prevent exploitation.
5. Practical Example
   - Setup a system with Kali Linux as client (attacker), Ubuntu as a firewall, and Metasploitable2 as the target, blocking SSH traffic on the firewall or updating SSH settings on Metasploitable2 (if possible) could mitigate the risk of exploitation.

D. References

https://www.rfc-editor.org/rfc/rfc8332

https://www.rfc-editor.org/rfc/rfc8709

https://www.rfc-editor.org/rfc/rfc4253#section-6.6

http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.117687

https://www.linkedin.com/pulse/weak-host-key-algorithm-vulnerability-mikrotiks-ssh-alves-pereira

https://security.stackexchange.com/questions/131010/which-host-key-algorithm-is-best-to-use-for-ssh