Table of Contents

Scan OpenVAS RHEL 7.3

I want to know how Firewall, SELinux or NFS services affects scan vulnerability tests.

Scenario

- Debian Sid unstable hypervisor with KVM 4.1 with libvirt 5.6
- Three virtual machines
  - RHEL 7.3 client
    - 1GB RAM
    - 10GB SDD
    - 1 vCPU
    - IP 192.168.122.254
  - RHEL 7.3 NFS Server:
    - 1GB RAM
    - 10 GB SDD
    - 1 vCPU
    - IP 192.168.122.14
  - Greenbone OS 5.0
    - 4GB RAM
    - 10GB SDD
    - 1 vCPU
    - IP 192.168.122.254

I will run several scans with OpenVAS to the RHEL 7.3 client, I provided the root password to OpenVAS:

- 1. RHEL 7.3 with Firewall up and SELinux enforcing, without NFS mount as client, without Chronyd started
- 2. RHEL 7.3 with firewall down and SELinux enforcing, without NFS mount as client, without Chronyd started
- 3. RHEL 7.3 with Firewall down and SELinux enforcing, without NFS mount as client, with Chronyd started
- 4. RHEL 7.3 with Firewall down and SELinux enforcing, with NFS mount as client, with Chronyd started
- 5. RHEL 7.3 with Firewall down and SELinux permissive, with NFS mount as client, with Chronyd started
- 6. RHEL 7.3 with Firewall down and SELinux permissive, with NFS mount as client, with Chronyd started with fixed founded problems

Finally I will export scan results as CSV with the option: “CSV Results”. With diff I will try to find differences beetween scans. I removed all columns except: IP, Hostname, Port, Port Protocol, CVSS, Severity,Solution Type, NVT Name.

I also want to obviate package updates.

Results

Boring numbers

Result number	Amount of Results	Amount of Results without logs	Amount of Results without update problems	Difference between previous result
1	204	176	3	NA
2	206	176	3	0
3	209	177	3	0
4	209	177	3	0
5	209	177	3	0
6	205	174	-3	0

Boring differentes

I compared first result with 2, 3, 4 and 5 scan respectively.

- 2nd scan:

```
15a16
> 192.168.122.254,,111,tcp,0.0,Log,,Obtain list of all port mapper
registered programs via RPC
137a139
> 192.168.122.254,,111,tcp,0.0,Log,,RPC portmapper (TCP)
```

- 3rd scan:

```
15a16
> 192.168.122.254,,111,tcp,0.0,Log,,Obtain list of all port mapper
registered programs via RPC
20a22,23
> 192.168.122.254,,,,5.0,Medium,VendorFix,QEMU <= 3.1.50 Denial of Service
Vulnerability
> 192.168.122.254,,,,0.0,Log,,QEMU Version Detection (Linux)
137a141
> 192.168.122.254,,111,tcp,0.0,Log,,RPC portmapper (TCP)
145a150
> 192.168.122.254,,,,0.0,Log,,Sun/Oracle OpenJDK Version Detection
```

- 4th scan:

```
15a16
> 192.168.122.254,,111,tcp,0.0,Log,,Obtain list of all port mapper
registered programs via RPC
20a22,23
> 192.168.122.254,,,,5.0,Medium,VendorFix,QEMU <= 3.1.50 Denial of Service
Vulnerability
> 192.168.122.254,,,,0.0,Log,,QEMU Version Detection (Linux)
137a141
> 192.168.122.254,,111,tcp,0.0,Log,,RPC portmapper (TCP)
145a150
```

```
> 192.168.122.254,,,,0.0,Log,,Sun/Oracle OpenJDK Version Detection
```

- 5th scan:

```
15a16
> 192.168.122.254,,111,tcp,0.0,Log,,Obtain list of all port mapper
registered programs via RPC
20a22,23
> 192.168.122.254,,,,5.0,Medium,VendorFix,QEMU <= 3.1.50 Denial of Service
Vulnerability
> 192.168.122.254,,,,0.0,Log,,QEMU Version Detection (Linux)
137a141
> 192.168.122.254,,111,tcp,0.0,Log,,RPC portmapper (TCP)
145a150
> 192.168.122.254,,,,0.0,Log,,Sun/Oracle OpenJDK Version Detection
```

Fixing sins

Disable tcp timestamps:

```
echo "net.ipv4.tcp_timestamps = 0" >> /etc/sysctl.d/99-sysctl.conf
sysctl -p
```

Restrict rpcbind:

```
echo "rpcbind: 192.168.122.14" >> /etc/hosts.allow
echo "rpcbind: ALL" >> /etc/hosts.deny
```

SSH weak encryption and MAC algorithms:

```
MACs hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-
etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-
etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-
sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-
sha2-512,hmac-ripemd160

Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-
gcm@openssh.com,chacha20-poly1305@openssh.com
```

Conclusion

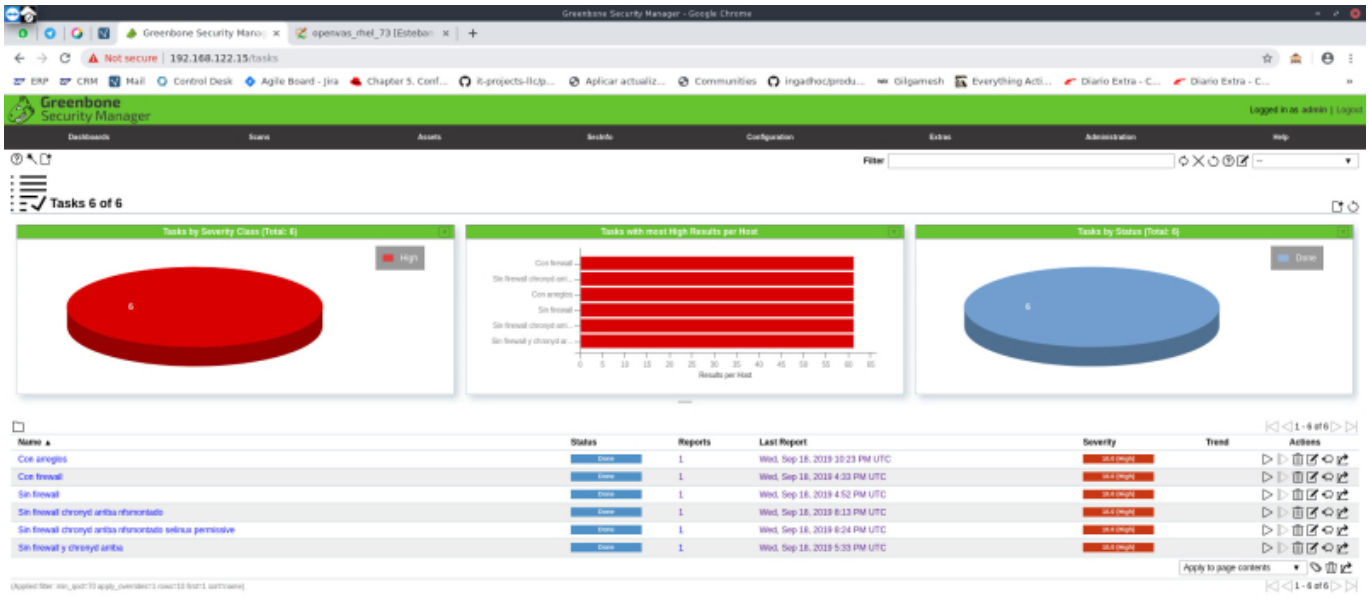
I noticed that with firewall up the scan can obtain the list of port mapper registered programs via RPC. I can fix those with TCP Wrappers instead firewall.

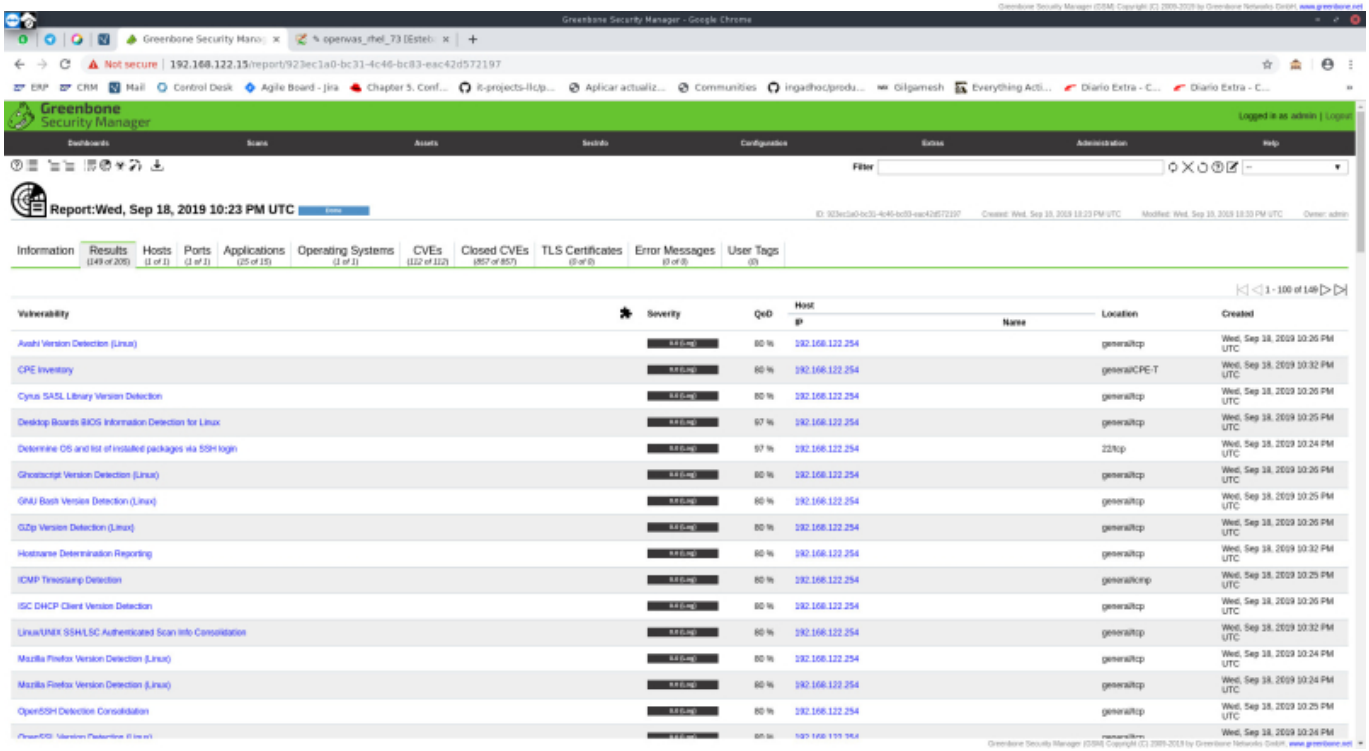
I noticed that SELinux doesn't make difference.

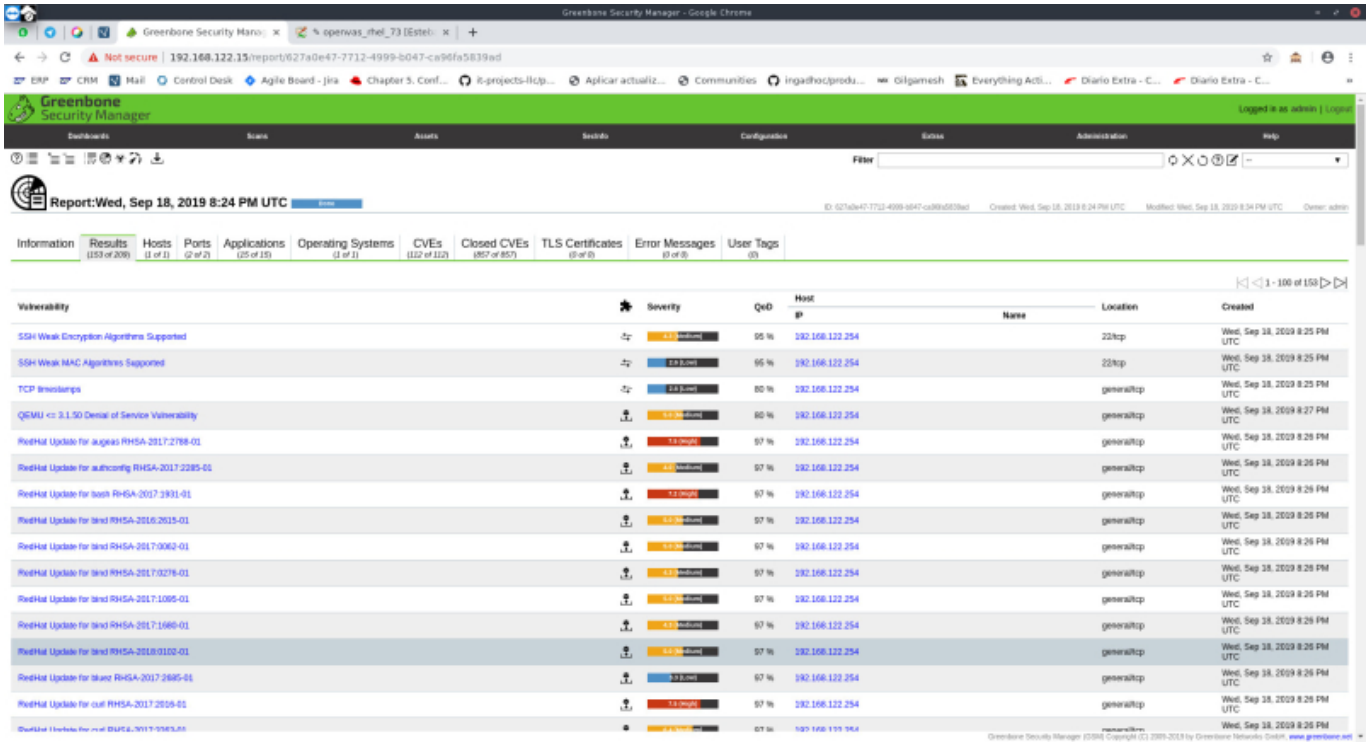
Recommendations

- Make a better penetration tests, because SELinux is not correctly tested with OpenVAS
- The scenario was a controlled environment without real applications, I need test Oracle Database, Tomcat or WebLogic

Useless Screenshots







Resources

- Original CSVs:

original.tar.gz

- Filtered CSVs:

filtered.tar.gz

- https://tipstricks.itmatrix.eu/making-rpcbindpreviously-portmap-port-111-more-secure/
- https://www.thegeekdiary.com/how-to-disable-md5-based-hmac-algorithms-for-ssh/