A7011E Homework 4

Nico Ferrari (nicfer-0@student.ltu.se)

January 4, 2021

1. analysis of most famous attacks of the last decade

in 2010, a new worm has been discoverd, created in order to affect nuclear installations in Iran. The target of this worm were supervisory control and data acquisition (SCADA) systems in industrial controllers. Stuxnet is based on different zero-day vulnerabilities to infect computers: An automatic process from connected removable drives such as USB flash drives through Windows shortcut files to initiate executable code, a connection with shared printers (addressing the Print Spooler Service) and two other vulnerabilities concerning privilege escalation. The target of the worm were infrastructures using Windows as operating system. In order to run malicious code, Stuxnet used 'stolen' certificates of popular hardware companies. In this way, for the OS the software results not compromised and trusted [4]. This attack had brought direct economical effects for Iran. In facts, around 1000 centrifuges has been destroyed by Stuxnet, which, beside bringing effects in terms of damages, brought delays in production of low enriched uranium. Moreover, in order to avoid this kind of attacks, important investments in new security and cybersecurity measures in the nuclear facilities has been established [7]. In order to contain the malware, the vulnerabilities have been patched by Microsoft in the following months and the companies producing software with the vulnerabilities had to release their patches. Nevertheless some of the vulnerabilities hasn't been completely fixed for years, leaving the system vulnerable.

Many malwares have been then created based on Stuxnet. In 2012 a worm called Shamoon [5], attacked the world's largest oil producer company in Arabia, wiping out data from 30000 computers in the company. The malware is composed by a Dropper (which creates a service that enables it to remain persistent on the infected computer), the Wiper (used to access to the Hard Drive and erase the files) and a Reporter (reports the information about the deleted files to the attackers). Shamoon has been initiated by a phishing email attack to an employee of Saudi Aramco Information Technology, giving access to the attackers into the company's network. In 2016 a new version of this malware has been discovered, presenting new features.

In September 2011, an information stealer rootkit named Duqu has been discovered in a European Company. Duqu presented several similarities with Stuxnet and was targeting MS Windows based PC [3]. Duqu was exploiting a zero day vulnerability in MS Word using kernel components signed with digital signatures from a Taiwanese company.

On October 2013, Adobe announced a data breach in its network , exposing credit and debit cards information of 3 million of customers together with user names, passwords and email addresses for more than 150 millions of peoples. Moreover, the source code of multiple Adobe software products has been stolen.

In 2014, Sony Pictures Entertainment got hacked by a hacking group known as *Guardians of Peace*, linked to North Korea's intelligence apparatus. The purpose of the attack was to stop the release of the movie titled *The Interview*, and after Sony refused so,, hackers destroyed the company's internal network and leaked studio data and private emails online.The unreleased movies that were leaked caused the company to lose a lot of money. Emails from different partners that were leaked exposed a lot of personal information about their partners which would result in them terminating their contracts with Sony [1].

2014 has been signed also by the discovery of a vulnerability in some versions of the OpenSSL software, known as *Heartbleed bug*, with the potential to expose the personal and financial data held by a wide range of online operators. Heartbleed has been introduced in OpenSSL in 2012 and remained undiscovered for nearly two years [2]. Heartbleed exploits, buffer over-read, similar to that of buffer overflow but is typically resulted from insufficient or a lack of bound checking for buffer read. This problem gained attention after the discovery of this bug, and presenting techniques which help its mitigation [10]. After this discovery, Google launched the *Project Zero*, a project with the goal of research zero-day vulnerabilities in order to improve the security.

in 2016 a vulnerability called *Badlock* affecting MS Windows and Samba has been discovered. It allows privilege escalation and using this vulnerability, a man-in-the-middle attacker could intercept communications between a client and a server hosting a SAM database and can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database. Moreover it facilitate DoS attack on services running Samba. This vulnerability has been promptly patched by Microsoft and from the Samba team.

A Security bug called *Cloudbleed* has been discovered in 2017, affecting edge servers of Cloudfare, a leading cloud based security, reverse proxy and optimization company.In some unusual circumstances, the servers were running past the end of a buffer and returning memory that contained private information such as authentication tokens, HTTP POST bodies and other sensitive data. Some of these data has been cached by search engines.

Another zero day vulnerability has been discovered in 2016 affecting the Linux kernel since 2005, allowing privilege escalation. The vulnerability, *Dirty COW (Dirty copy on write)*, allows attackers to escalate the file system protection of Linux Kernel, get root privilege and thus compromise the whole system. Many servers has been affected by this vulnerability, including a large number of financial, educational, health care organization [8].

Another attack against computers running Linux OS has been discovered in 2016/2017. Linux.Encoder.1 (ELF/Filecoder.A or Trojan.Linux.Ransom.A) has been considered the first ransomware trojan aiming Linux, which using a security flow in Magento software, encrypts certain types of files which are set on local and network file systems [9]. Magento patched the software but lot of small e-commerce sites did not apply this critical patch.

This is only a small amount of the security issues encountered during the last decade. As we can see the vulnerabilities affects both Linux and Windows systems. In order to mitigate zero days exploits, Companies such as Google started projects which try to find them. Thanks to these initiatives, companies like Cloudfare solved critical issues in their servers. Some vulnerabilities has been detected with years of delay, and this could cause an incredible damage. Nevertheless, patches are not always applied by the system administrators, leaving their systems vulnerable to known vulnerabilities. Phishing continues to be a common technique used to enter in a company's network, like it happened with the spread of the malware Shamoon. Companies should invest more in awareness training and implementation of security operations in order to keep the system protected and up to date. Especially small companies tend to ignore the security issues leaving their data and the data of their customers not safe. Many data breaches revealed sensible information of thousands of people, including names and passwords. Moreover, the same passwords are used by the user in other services, making them vulnerable. This shows also how important is the use of keys which can be cancelled. Using biometric data as key could compromise the identity of a user in a permanent way in case of leakage. Therefore, multiple studies has been conducted to find alternatives ways of user authentication.

The Last decade has been signed by DoS attack as well. Several IoT devices has been implemented and they have been targeted by several attacks. One of them has been Mirai, a Linux malware which was aiming mainly to routers and IP cameras, trying to bruteforce their passwords through dictionary [6]. The infected devices can then become remotely controlled bots or "zombies". In 2016 a DDoS attack has been performed and the code of Mirai has been quickly released after a week but replicated by cybercriminals, which performed massive attack that brought down the domain registration services provider Dyn. The vulnerability was caused by leaving the default credentials in the installed devices. Many descendants of Mirai has been created, such as *Mukashi* , which leverages a remote execution vulnerability in Zyxel network-attached storage products (NAS). This shows how important is to apply basic security practices when installing new devices and how important is to keep the updated. Zyxel patched the vulnerability the owners of their devices must update the firmware as soon as possible.

2. References

[1] *Analysis from the East-West Center.* Tech. rep.

[2] James Banks. "The Heartbleed bug: Insecurity repackaged, rebranded and resold". In: *Crime, Media, Culture* 11.3 (Dec. 2015), pp. 259–279. ISSN: 17416604. DOI: 10.1177/1741659015592792.

[3] Boldizsár Bencsáth et al. *Duqu: Analysis, Detection, and Lessons Learned Márk Félegyházi.* Vol. 12. 2012. ISBN: 9781450311656. URL: http://www.symantec.com/connect/blogs/.

[4] Anton Cherepanov. *WIN32/INDUSTROYER A new threat for industrial control systems.* Tech. rep.

[5] Zakariya Dehlawi and Norah Abokhodair. "Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident". In: *IEEE ISI 2013 - 2013 IEEE International Conference on Intelligence and Security Informatics: Big Data, Emergent Threats, and Decision-Making in Security Informatics.* 2013, pp. 73–75. ISBN: 9781467362115. DOI: 10.1109/ISI.2013.6578789.

[6] Luis Eduardo Suástegui Jaramillo. "Malware Detection and Mitigation Techniques: Lessons Learned from Mirai DDOS Attack". In: *Journal of Information Systems Engineering & Management* 3.3 (July 2018). DOI: 10.20897/jisem/2655.

[7] "Stuxnet". In: (2017). DOI: 10.3929/ethz-b-000200661. URL: https://doi.org/10.3929/ethz-b-000200661.

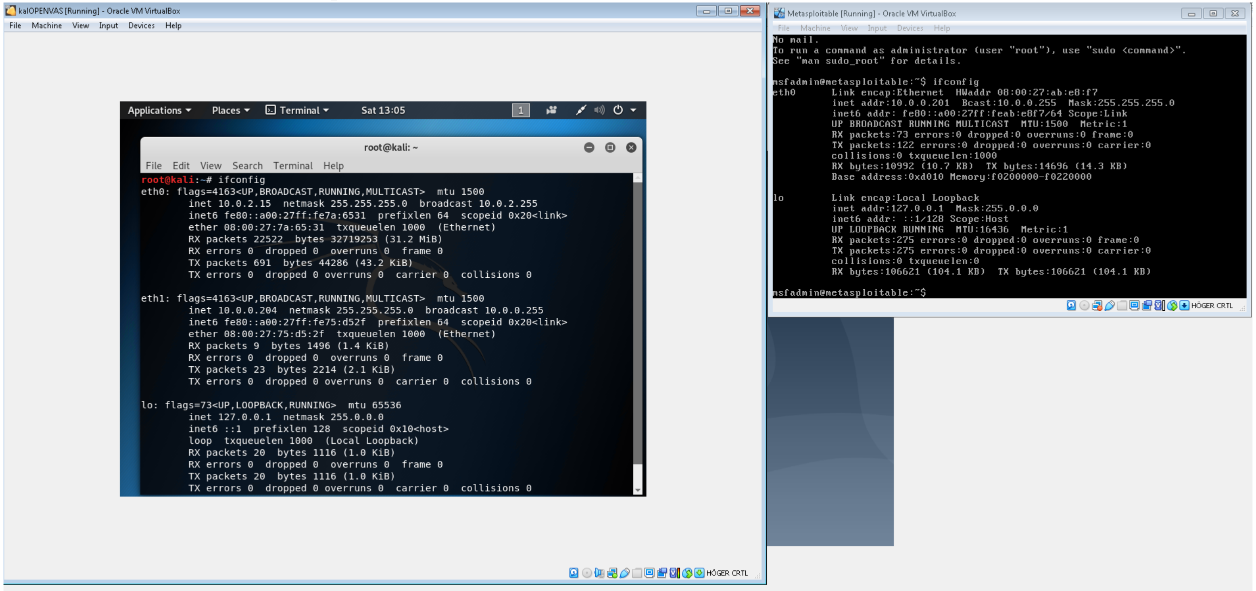
[8] University of Greenwich and Institute of Electrical and Electronics Engineers. *2017 International Conference on Consumer Electronics and Devices (ICCED 2017) : July 14-17, 2017, London, UK.* ISBN: 9781538604038.

[9] Bojan Vujanić, Nemanja Maček, and Saša Adamović. "An Implementation of Ransomware Malicious Software in Python". In: Singidunum University, June 2017, pp. 19–24. DOI: 10.15308/sinteza-2017-19-24.

[10] Jun Wang et al. "Risk Assessment of Buffer 'Heartbleed' Over-Read Vulnerabilities". In: *Proceedings of the International Conference on Dependable Systems and Networks.* Vol. 2015-September. IEEE Computer Society, Sept. 2015, pp. 555–562. ISBN: 9781479986293. DOI: 10.1109/DSN.2015.59.

3. Have you successfully completed Lab assignment (4)

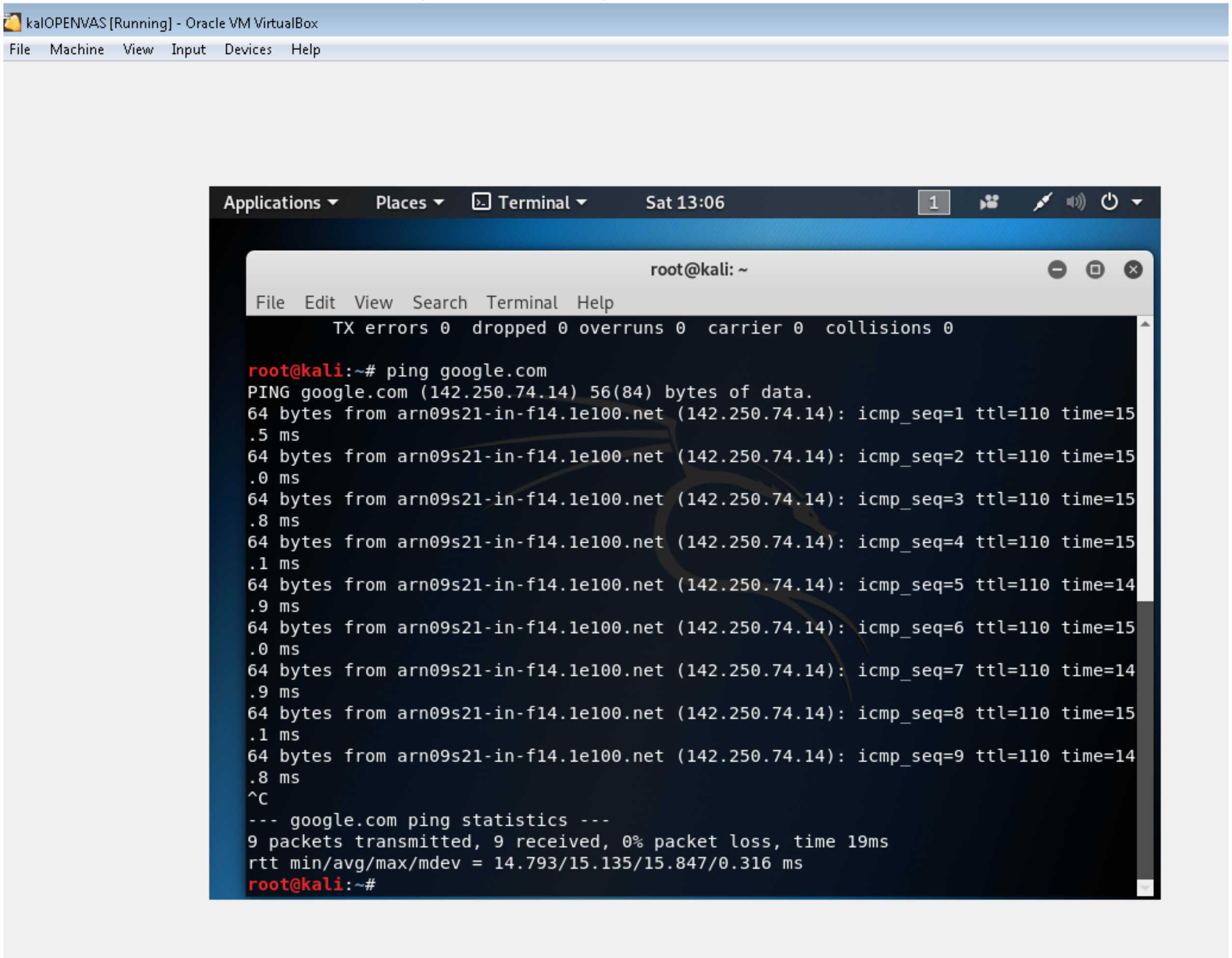
Figure 1: Checking that the metasploitable VM is connected to the right network, getting the IP through DHCP server running in the Debian VM. The Kali VM is using two interfaces, one for Internet access and one to connect to the Metasploitable VM.


kaliOPENVAS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Sat 13:05
root@kali: ~
File Edit View Search Terminal Help
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HÖGER CRTL

```
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:fe7a:6531  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:7a:65:31  txqueuelen 1000  (Ethernet)
        RX packets 22522  bytes 32719253 (31.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 691  bytes 44286 (43.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.204  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::a00:27ff:fe75:d52f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:75:d5:2f  txqueuelen 1000  (Ethernet)
        RX packets 9  bytes 1496 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 2214 (2.1 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
```

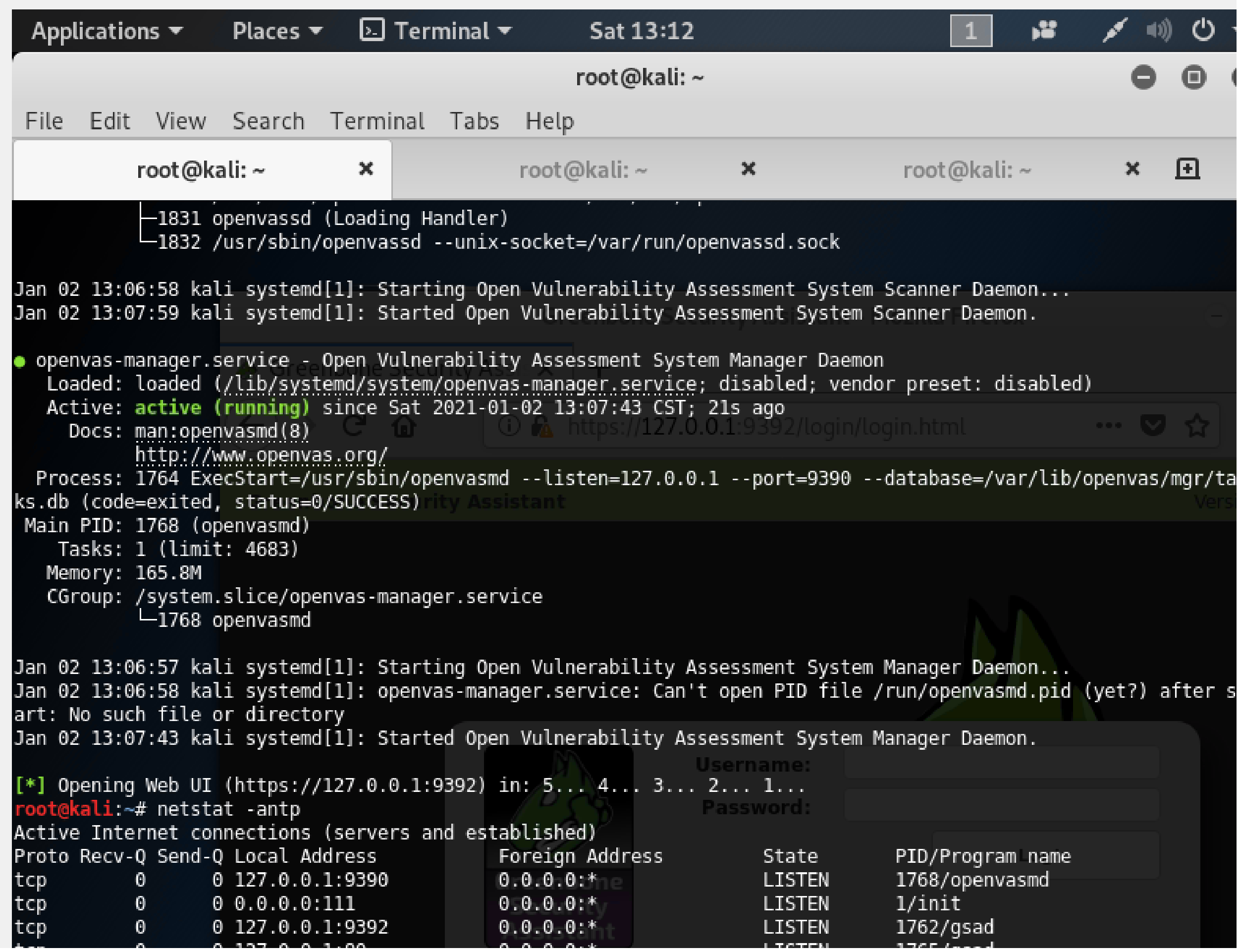
```
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:e8:f7
          inet addr:10.0.0.201  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feab:e8f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:73 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10992 (10.7 KB)  TX bytes:14696 (14.3 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:275 errors:0 dropped:0 overruns:0 frame:0
          TX packets:275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:106621 (104.1 KB)  TX bytes:106621 (104.1 KB)

msfadmin@metasploitable:~$
```

Figure 2: Checking that internet works


kaIOPENVAS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾ Sat 13:06
1
root@kali: ~
File Edit View Search Terminal Help

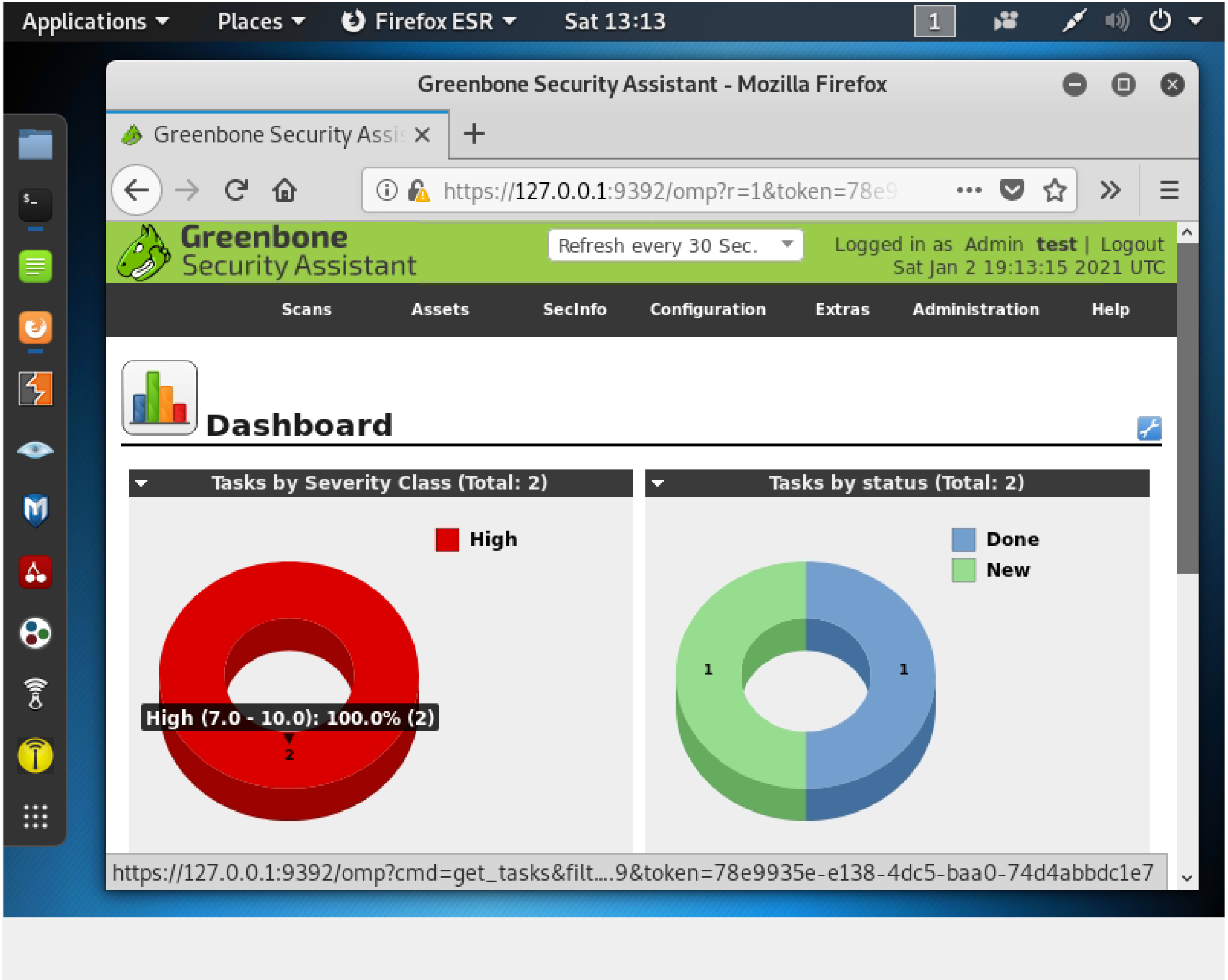
```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# ping google.com
PING google.com (142.250.74.14) 56(84) bytes of data.
64 bytes from arn09s21-in-f14.1e100.net (142.250.74.14): icmp_seq=1 ttl=110 time=15
.5 ms
64 bytes from arn09s21-in-f14.1e100.net (142.250.74.14): icmp_seq=2 ttl=110 time=15
.0 ms
64 bytes from arn09s21-in-f14.1e100.net (142.250.74.14): icmp_seq=3 ttl=110 time=15
.8 ms
64 bytes from arn09s21-in-f14.1e100.net (142.250.74.14): icmp_seq=4 ttl=110 time=15
.1 ms
64 bytes from arn09s21-in-f14.1e100.net (142.250.74.14): icmp_seq=5 ttl=110 time=14
.9 ms
64 bytes from arn09s21-in-f14.1e100.net (142.250.74.14): icmp_seq=6 ttl=110 time=15
.0 ms
64 bytes from arn09s21-in-f14.1e100.net (142.250.74.14): icmp_seq=7 ttl=110 time=14
.9 ms
64 bytes from arn09s21-in-f14.1e100.net (142.250.74.14): icmp_seq=8 ttl=110 time=15
.1 ms
64 bytes from arn09s21-in-f14.1e100.net (142.250.74.14): icmp_seq=9 ttl=110 time=14
.8 ms
^C
--- google.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 19ms
rtt min/avg/max/mdev = 14.793/15.135/15.847/0.316 ms
root@kali:~#
```

Figure 3: launching OpenVAS and checking that is listening on the kali machine. We can see that it is listening on port 9390 with PID 1768.



```
             ├─1831 openvassd (Loading Handler)
             └─1832 /usr/sbin/openvassd --unix-socket=/var/run/openvassd.sock

Jan 02 13:06:58 kali systemd[1]: Starting Open Vulnerability Assessment System Scanner Daemon...
Jan 02 13:07:59 kali systemd[1]: Started Open Vulnerability Assessment System Scanner Daemon.

● openvas-manager.service - Open Vulnerability Assessment System Manager Daemon
   Loaded: loaded (/lib/systemd/system/openvas-manager.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2021-01-02 13:07:43 CST; 21s ago
     Docs: man:openvasmd(8)
           http://www.openvas.org/
  Process: 1764 ExecStart=/usr/sbin/openvasmd --listen=127.0.0.1 --port=9390 --database=/var/lib/openvas/mgr/ta
ks.db (code=exited, status=0/SUCCESS)
 Main PID: 1768 (openvasmd)
    Tasks: 1 (limit: 4683)
   Memory: 165.8M
   CGroup: /system.slice/openvas-manager.service
           └─1768 openvasmd

Jan 02 13:06:57 kali systemd[1]: Starting Open Vulnerability Assessment System Manager Daemon...
Jan 02 13:06:58 kali systemd[1]: openvas-manager.service: Can't open PID file /run/openvasmd.pid (yet?) after s
art: No such file or directory
Jan 02 13:07:43 kali systemd[1]: Started Open Vulnerability Assessment System Manager Daemon.

[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
root@kali:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:9390          0.0.0.0:*               LISTEN      1768/openvasmd
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      1/init
tcp        0      0 127.0.0.1:9392          0.0.0.0:*               LISTEN      1762/gsad
```

Figure 4:

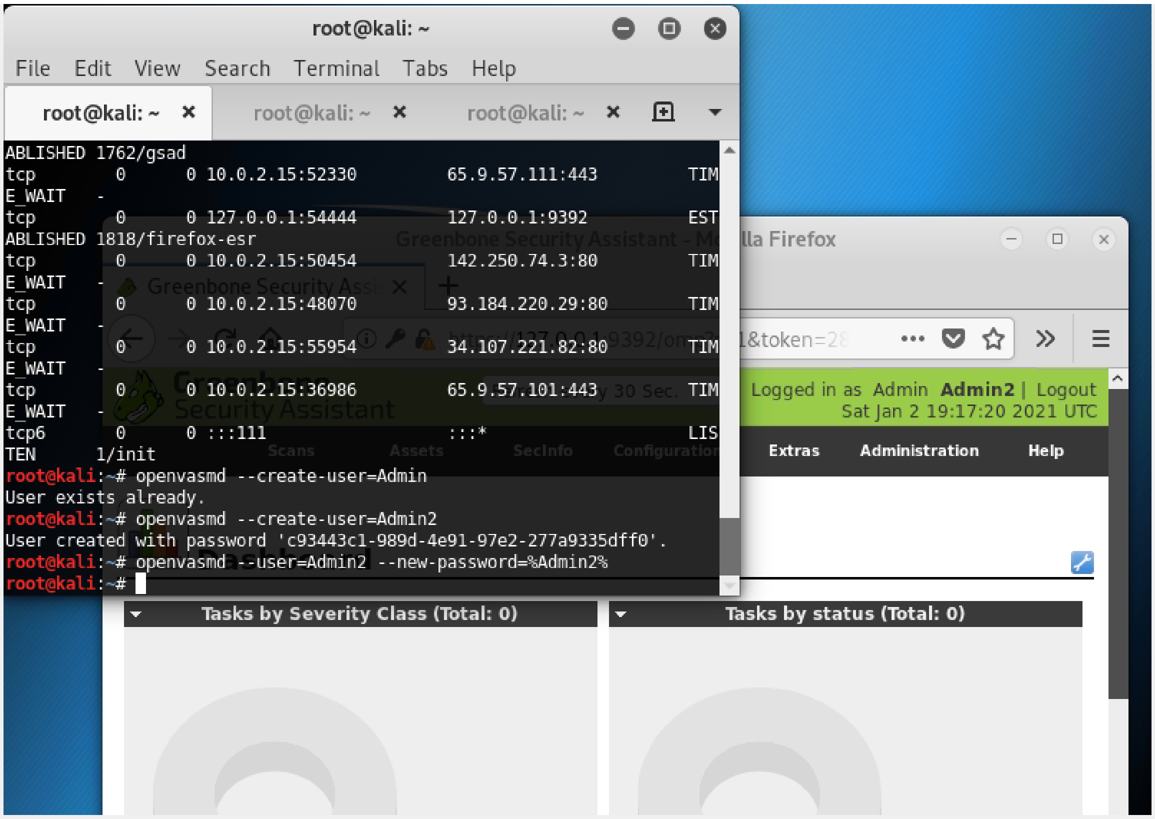


https://127.0.0.1:9392/omp?r=1&token=78e9

Refresh every 30 Sec.

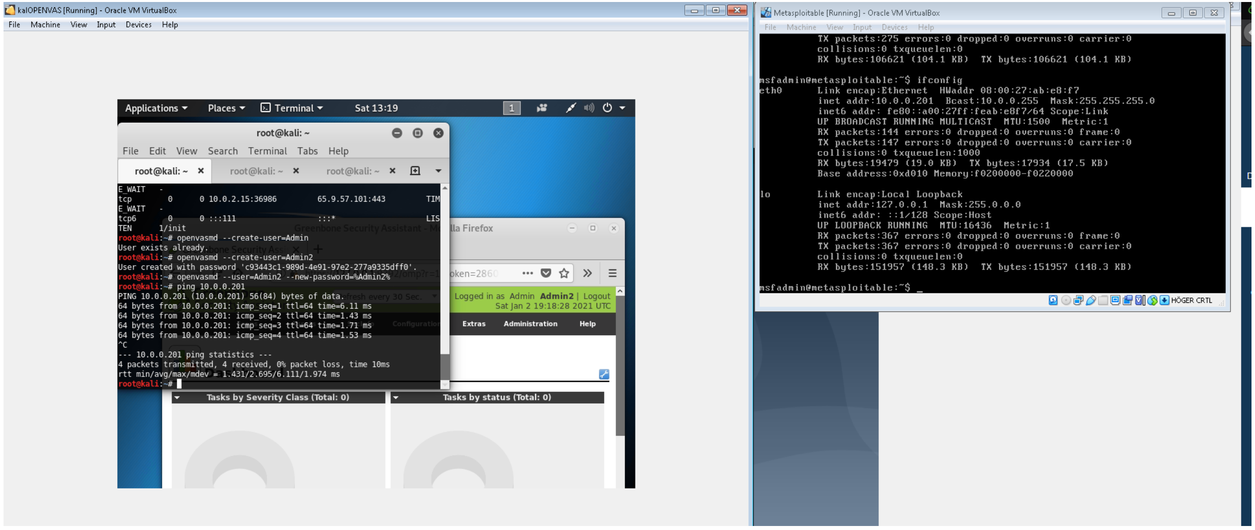
Logged in as Admin **test** | Logout
Sat Jan 2 19:13:15 2021 UTC

https://127.0.0.1:9392/omp?cmd=get_tasks&filt....9&token=78e9935e-e138-4dc5-baa0-74d4abbdc1e7


root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
root@kali: ~
Mozilla Firefox
Logged in as Admin Admin2 | Logout
Sat Jan 2 19:17:20 2021 UTC
Extras Administration Help
Tasks by Severity Class (Total: 0)
Tasks by status (Total: 0)

```
ABLISHED 1762/gsad
tcp        0      0 10.0.2.15:52330         65.9.57.111:443         TIM
E_WAIT   -
tcp        0      0 127.0.0.1:54444         127.0.0.1:9392          EST
ABLISHED 1818/firefox-esr
tcp        0      0 10.0.2.15:50454         142.250.74.3:80         TIM
E_WAIT   -
tcp        0      0 10.0.2.15:48070         93.184.220.29:80        TIM
E_WAIT   -
tcp        0      0 10.0.2.15:55954         34.107.221.82:80        TIM
E_WAIT   -
tcp        0      0 10.0.2.15:36986         65.9.57.101:443         TIM
E_WAIT   -
tcp6       0      0 :::111                  :::*                    LIS
TEN      1/init
root@kali:~# openvasmd --create-user=Admin
User exists already.
root@kali:~# openvasmd --create-user=Admin2
User created with password 'c93443c1-989d-4e91-97e2-277a9335dff0'.
root@kali:~# openvasmd --user=Admin2 --new-password=%Admin2%
root@kali:~# 
```

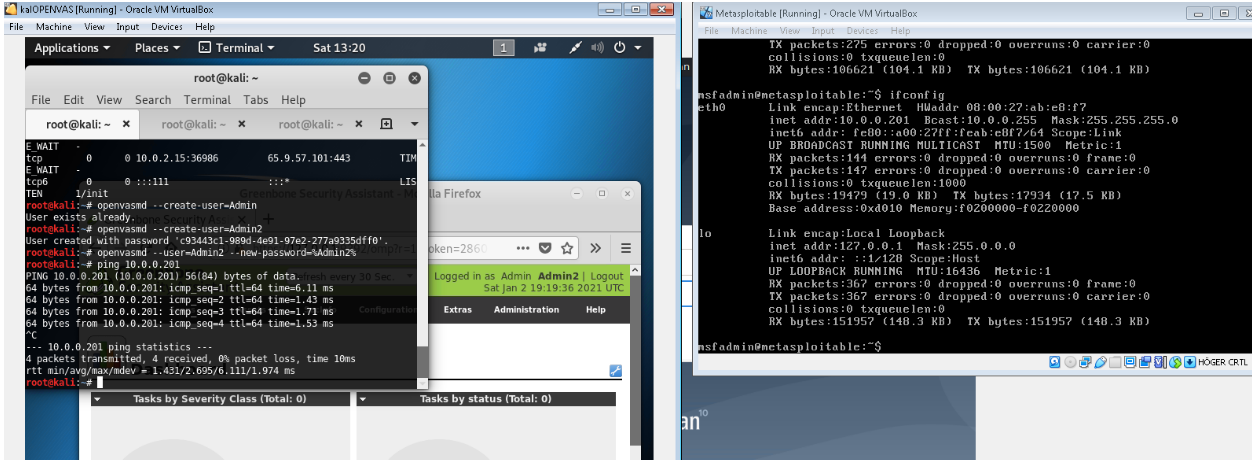
Figure 6:


kaliOPENVAS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Sat 13:19
root@kali: ~
File Edit View Search Terminal Tabs Help
lla Firefox
Logged in as Admin Admin2 | Logout
Sat Jan 2 19:18:28 2021 UTC
Extras Administration Help
Tasks by Severity Class (Total: 0)
Tasks by status (Total: 0)
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HÖGER CRTL

```
E_WAIT   -
tcp        0      0 10.0.2.15:36986         65.9.57.101:443         TIM
E_WAIT   -
tcp6       0      0 :::111                  :::*                    LIS
TEN      1/init
root@kali:~# openvasmd --create-user=Admin
User exists already.
root@kali:~# openvasmd --create-user=Admin2
User created with password 'c93443c1-989d-4e91-97e2-277a9335dff0'.
root@kali:~# openvasmd --user=Admin2 --new-password=%Admin2%
root@kali:~# ping 10.0.0.201
PING 10.0.0.201 (10.0.0.201) 56(84) bytes of data.
64 bytes from 10.0.0.201: icmp_seq=1 ttl=64 time=6.11 ms
64 bytes from 10.0.0.201: icmp_seq=2 ttl=64 time=1.43 ms
64 bytes from 10.0.0.201: icmp_seq=3 ttl=64 time=1.71 ms
64 bytes from 10.0.0.201: icmp_seq=4 ttl=64 time=1.53 ms
^C
--- 10.0.0.201 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 10ms
rtt min/avg/max/mdev = 1.431/2.695/6.111/1.974 ms
root@kali:~# 
```

```
          TX packets:275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:106621 (104.1 KB)  TX bytes:106621 (104.1 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:e8:f7
          inet addr:10.0.0.201  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feab:e8f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:144 errors:0 dropped:0 overruns:0 frame:0
          TX packets:147 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19479 (19.0 KB)  TX bytes:17934 (17.5 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:367 errors:0 dropped:0 overruns:0 frame:0
          TX packets:367 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:151957 (148.3 KB)  TX bytes:151957 (148.3 KB)

msfadmin@metasploitable:~$ _
```

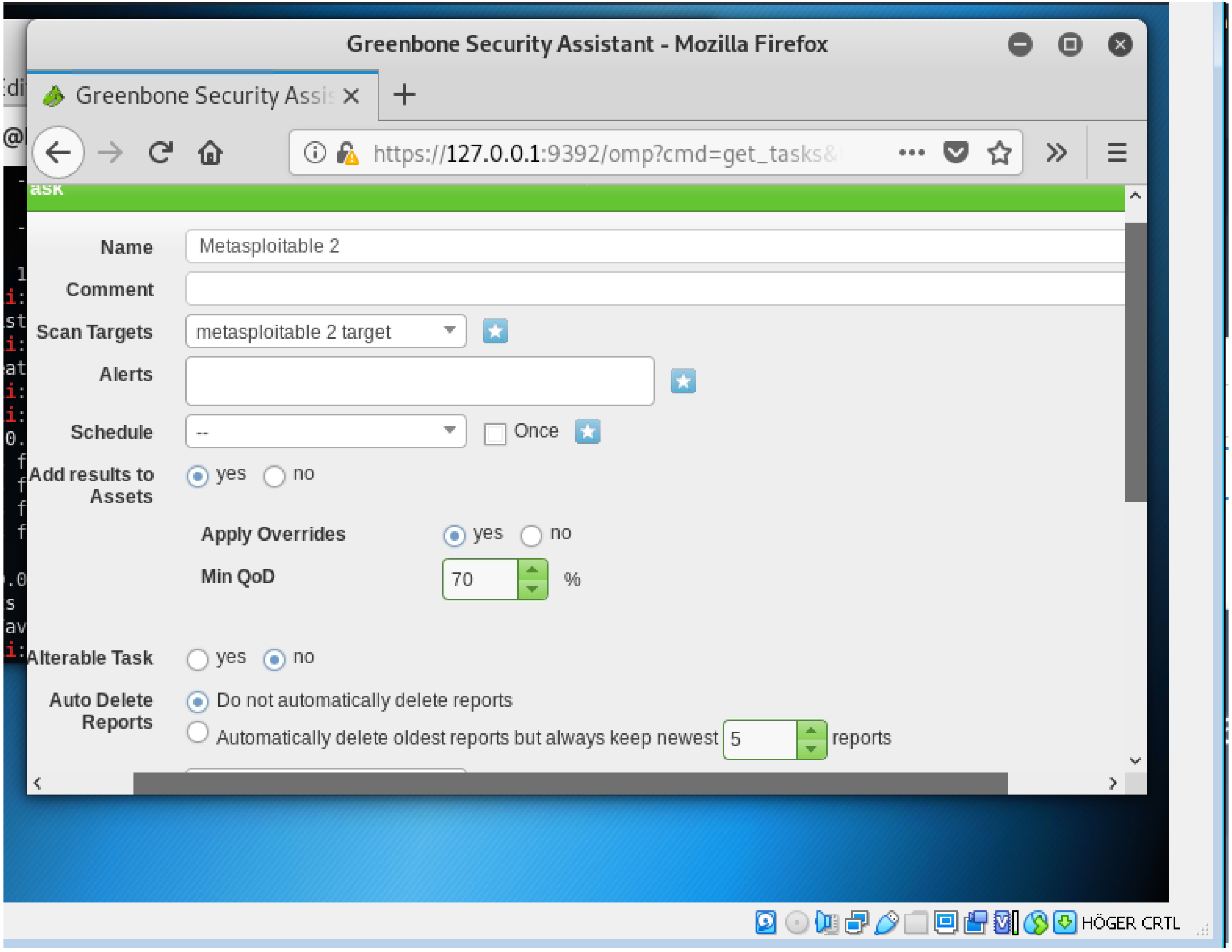
Figure 7:


kalOPENVAS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Sat 13:20
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
Logged in as Admin Admin2 | Logout
Sat Jan 2 19:19:36 2021 UTC
Extras Administration Help
Tasks by Severity Class (Total: 0)
Tasks by status (Total: 0)
Metasploitable [Running] - Oracle VM VirtualBox
HÖGER CRTL

```
E_WAIT   -
tcp        0      0 10.0.2.15:36986         65.9.57.101:443         TIM
E_WAIT   -
tcp6       0      0 :::111                  :::*                    LIS
TEN      1/init
root@kali:~# openvasmd --create-user=Admin
User exists already.
root@kali:~# openvasmd --create-user=Admin2
User created with password 'c93443c1-989d-4e91-97e2-277a9335dff0'.
root@kali:~# openvasmd --user=Admin2 --new-password=%Admin2%
root@kali:~# ping 10.0.0.201
PING 10.0.0.201 (10.0.0.201) 56(84) bytes of data.
64 bytes from 10.0.0.201: icmp_seq=1 ttl=64 time=6.11 ms
64 bytes from 10.0.0.201: icmp_seq=2 ttl=64 time=1.43 ms
64 bytes from 10.0.0.201: icmp_seq=3 ttl=64 time=1.71 ms
64 bytes from 10.0.0.201: icmp_seq=4 ttl=64 time=1.53 ms
^C
--- 10.0.0.201 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 10ms
rtt min/avg/max/mdev = 1.431/2.695/6.111/1.974 ms
root@kali:~# 
```

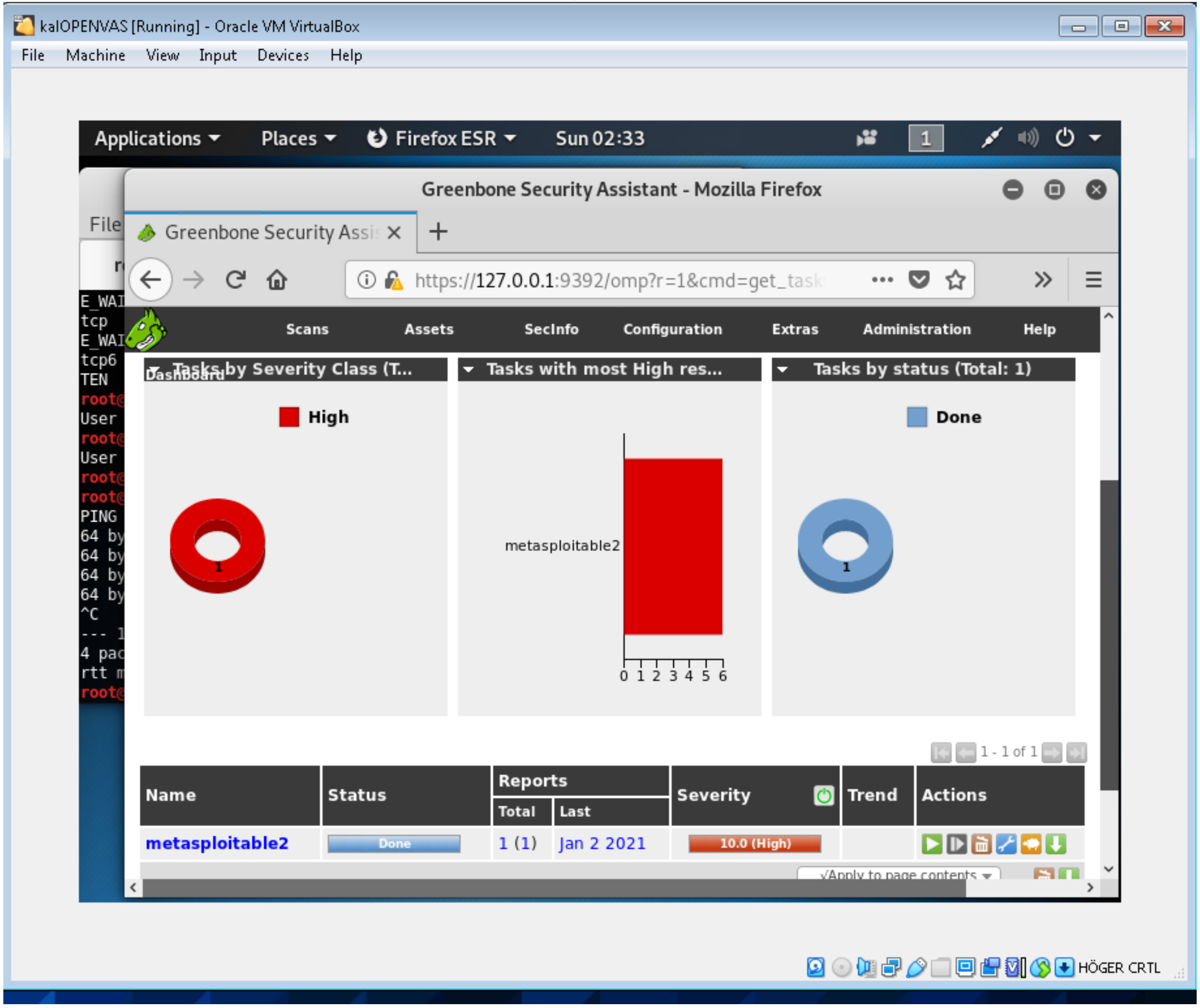
```
          TX packets:275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:106621 (104.1 KB)  TX bytes:106621 (104.1 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:e8:f7
          inet addr:10.0.0.201  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feab:e8f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:144 errors:0 dropped:0 overruns:0 frame:0
          TX packets:147 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19479 (19.0 KB)  TX bytes:17934 (17.5 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:367 errors:0 dropped:0 overruns:0 frame:0
          TX packets:367 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:151957 (148.3 KB)  TX bytes:151957 (148.3 KB)

msfadmin@metasploitable:~$
```

Figure 8: create new task and target


Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=get_tasks&
ask
HÖGER CRTL

Name	Metasploitable 2
Comment	
Scan Targets	metasploitable 2 target
Alerts	
Schedule	-- □ Once
Add results to Assets	● yes ○ no
Apply Overrides	● yes ○ no
Min QoD	70 %
Alterable Task	○ yes ● no
Auto Delete Reports	● Do not automatically delete reports ○ Automatically delete oldest reports but always keep newest 5 reports

Figure 9:

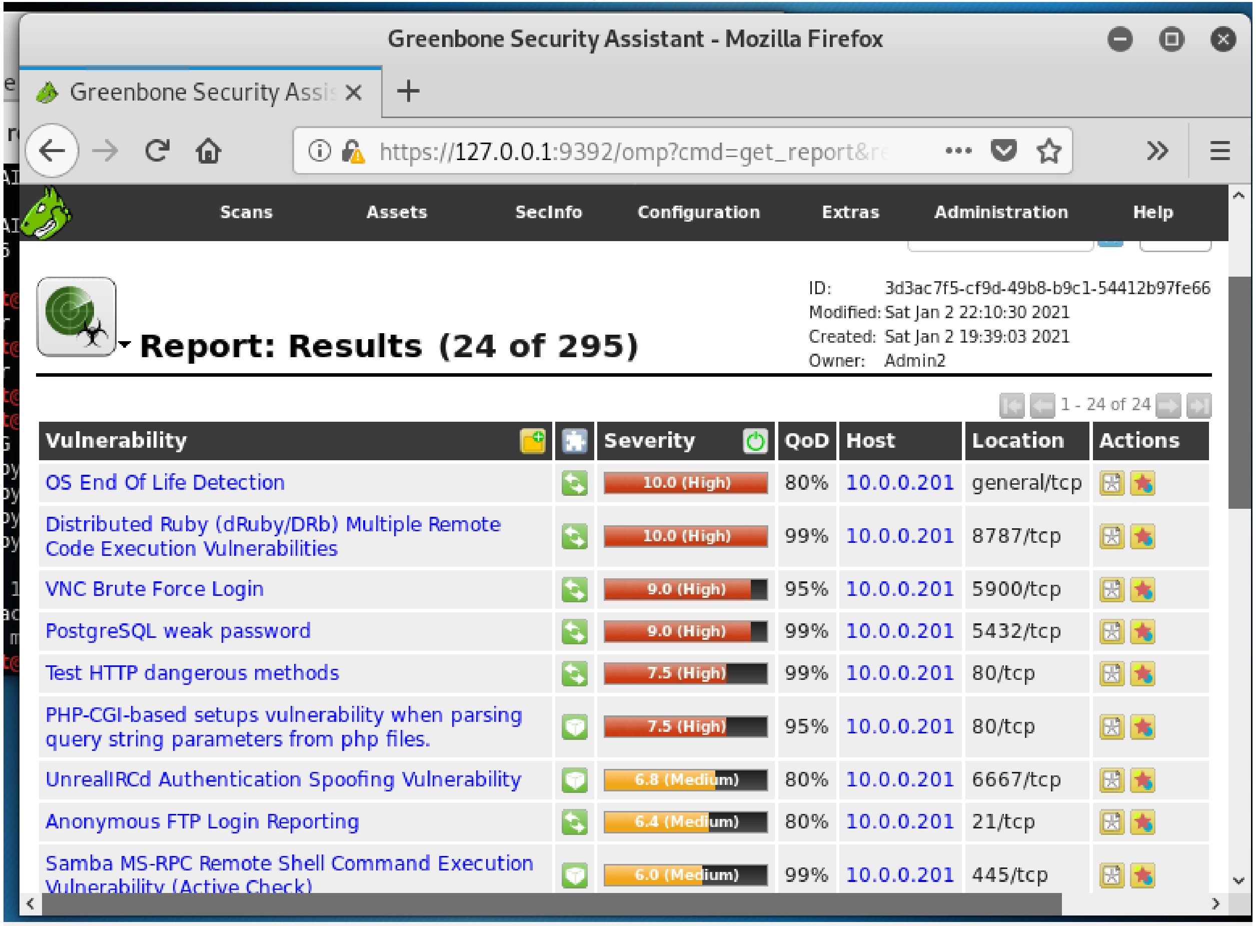


kalOPENVAS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Firefox ESR Sun 02:33
Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assis
https://127.0.0.1:9392/omp?r=1&cmd=get_task
Scans Assets SecInfo Configuration Extras Administration Help
Dashboard
Tasks by Severity Class (T...
High
1
Tasks with most High res...
metasploitable2
0 1 2 3 4 5 6
Tasks by status (Total: 1)
Done
1
1 - 1 of 1
√Apply to page contents
HÖGER CRTL

```
E_WAI
tcp
E_WAI
tcp6
TEN
root
User
root
User
root
root
PING
64 by
64 by
64 by
64 by
^C
--- 1
4 pac
rtt m
root
```

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
metasploitable2	Done	1 (1)	Jan 2 2021	10.0 (High)		

Figure 10:



Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=get_report&r
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help

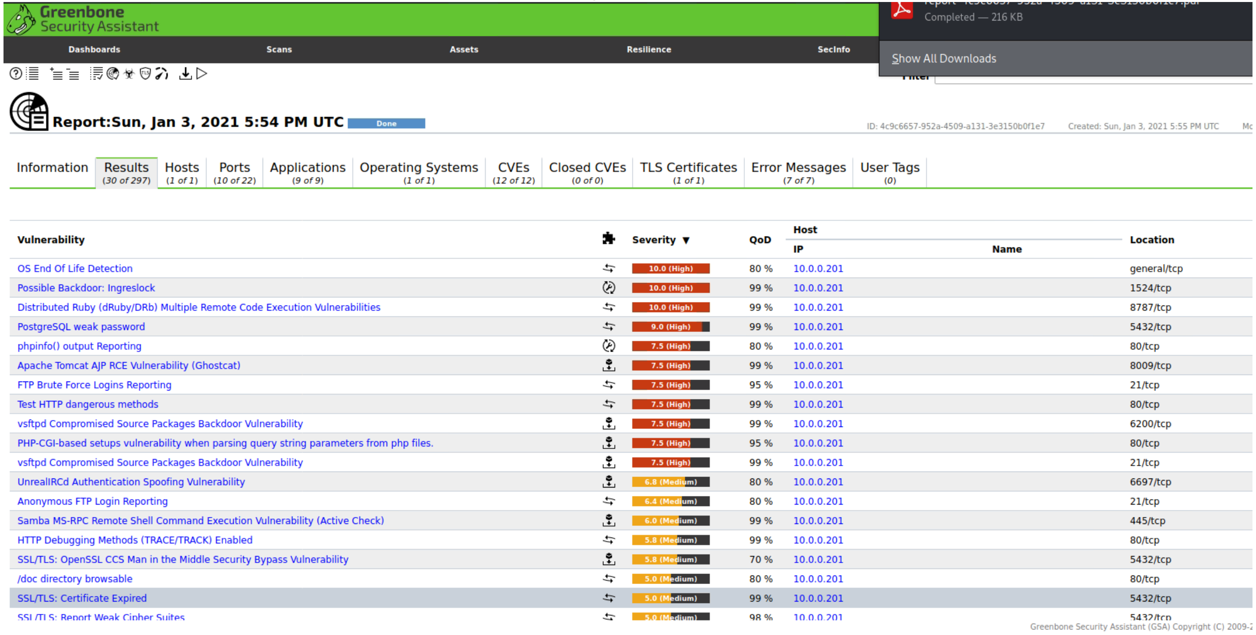
Report: Results (24 of 295)

ID: 3d3ac7f5-cf9d-49b8-b9c1-54412b97fe66
Modified: Sat Jan 2 22:10:30 2021
Created: Sat Jan 2 19:39:03 2021
Owner: Admin2

1 - 24 of 24

Vulnerability		Severity	QoD	Host	Location	Actions
OS End Of Life Detection		10.0 (High)	80%	10.0.0.201	general/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%	10.0.0.201	8787/tcp	
VNC Brute Force Login		9.0 (High)	95%	10.0.0.201	5900/tcp	
PostgreSQL weak password		9.0 (High)	99%	10.0.0.201	5432/tcp	
Test HTTP dangerous methods		7.5 (High)	99%	10.0.0.201	80/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	10.0.0.201	80/tcp	
UnrealIRCd Authentication Spoofing Vulnerability		6.8 (Medium)	80%	10.0.0.201	6667/tcp	
Anonymous FTP Login Reporting		6.4 (Medium)	80%	10.0.0.201	21/tcp	
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)		6.0 (Medium)	99%	10.0.0.201	445/tcp	

Figure 11:



Report:Sun, Jan 3, 2021 5:54 PM UTC

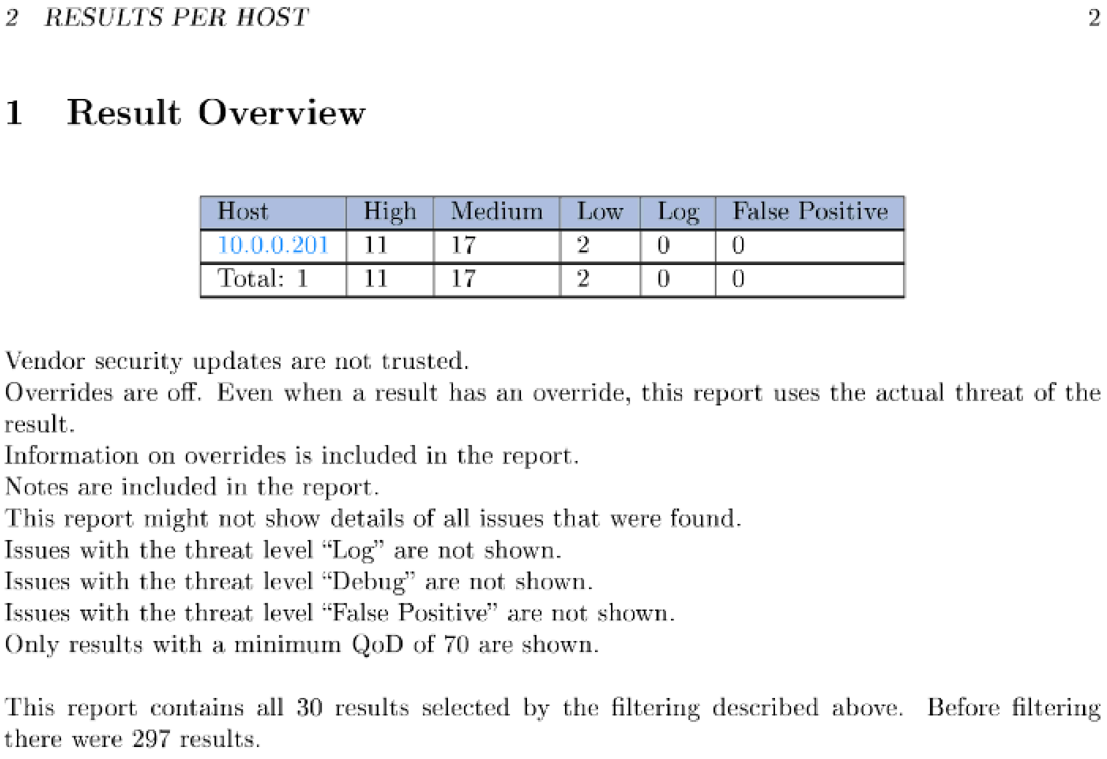
ID: 4c9c6657-952a-4509-a131-3e3150b0f1e7 Created: Sun, Jan 3, 2021 5:55 PM UTC

Information | Results (30 of 297) | Hosts (1 of 1) | Ports (10 of 22) | Applications (9 of 9) | Operating Systems (1 of 1) | CVEs (12 of 12) | Closed CVEs (0 of 0) | TLS Certificates (1 of 1) | Error Messages (7 of 7) | User Tags (0)

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location
OS End Of Life Detection	⇆	10.0 (High)	80 %	10.0.0.201		general/tcp
Possible Backdoor: Ingreslock	◎	10.0 (High)	99 %	10.0.0.201		1524/tcp
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	⇆	10.0 (High)	99 %	10.0.0.201		8787/tcp
PostgreSQL weak password	⇆	9.0 (High)	99 %	10.0.0.201		5432/tcp
phpinfo() output Reporting	◎	7.5 (High)	80 %	10.0.0.201		80/tcp
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	⤓	7.5 (High)	99 %	10.0.0.201		8009/tcp
FTP Brute Force Logins Reporting	⇆	7.5 (High)	95 %	10.0.0.201		21/tcp
Test HTTP dangerous methods	⇆	7.5 (High)	99 %	10.0.0.201		80/tcp
vsftpd Compromised Source Packages Backdoor Vulnerability	⤓	7.5 (High)	99 %	10.0.0.201		6200/tcp
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	⤓	7.5 (High)	95 %	10.0.0.201		80/tcp
vsftpd Compromised Source Packages Backdoor Vulnerability	⤓	7.5 (High)	99 %	10.0.0.201		21/tcp
UnrealIRCd Authentication Spoofing Vulnerability	⤓	6.8 (Medium)	80 %	10.0.0.201		6697/tcp
Anonymous FTP Login Reporting	⇆	6.4 (Medium)	80 %	10.0.0.201		21/tcp
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	⤓	6.0 (Medium)	99 %	10.0.0.201		445/tcp
HTTP Debugging Methods (TRACE/TRACK) Enabled	⇆	5.8 (Medium)	99 %	10.0.0.201		80/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	⤓	5.8 (Medium)	70 %	10.0.0.201		5432/tcp
/doc directory browsable	⇆	5.0 (Medium)	80 %	10.0.0.201		80/tcp
SSL/TLS: Certificate Expired	⇆	5.0 (Medium)	99 %	10.0.0.201		5432/tcp
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	10.0.0.201		5432/tcp

Greenbone Security Assistant (GSA) Copyright (C) 2009-

Figure 12: The scan found 11 high risk threats on the VM and 17 Medium.



2 RESULTS PER HOST 2

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.0.201	11	17	2	0	0
Total: 1	11	17	2	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 30 results selected by the filtering described above. Before filtering there were 297 results.

Explanation of three HIGH threat vulnerabilities:

- PostgreSQL weak Password: PostgreSQL is an open source object relational database. This vulnerability refers to the weakness of a user password, which can be easily exploited with techniques such as rainbow tables. In order to solve this problem is necessary to change the password and choosing a strong password according to good practicescould result in a sufficent protection against this kind of attack. This attack can lead to problems in therms of availability (a user could shoutdown the database or make unavailable the data by deleting them), integrity (compromising the databases) and confidentiality (disclosing the information).
- OS End of Life Detection: The OS used in the VM is Ubuntu version 8.04, with an End Of Life date which is mid 2013. This means that the OS is not receiving any feature, maintenance or security updates since more than 7 years. After the EOL date, the software might be vulnerable to vulnerabilities and not receive any update. Moreover this can lead to instability and cause threats to availability of the system. in order to mitigate this threat is necessary to upgrade the system to a supported version and patch it with the necessary security updates.
- vsftpd Compromised Source Packages Backdoor Vulnerability: vsftpd version 2.3.4 results containing a vulnerability which allows remote code execution. The vulnerability has been fixed by the vendor, releasing a new version which needs to be installed. it is suggested to verify the signature of the package in order to be sure of not downloading a compromised package and to verify its authenticity.

CVE:

- CVE-2020-1938: Apache Tomcat AJP RCE Vulnerability (Gostcat)
- CVE-2012-1823/2311/2336/2335: PHP-CGI-based setups vulnerability when parsing query string parameters from php
- CVE-2007-2447: Samba MS-RPC Remote Shell Command Execution Vulnerability

4. thoughts about this week

interesting the setting up part of a vulnerable system. It took long time to setup OpenVAS on my own Kali VM.

identification	Network IP	High Threats	Medium Threats	Low Threats	Vulnerability Insight	Solution
Possible Backdoor: Ingreslock	10.0.0.201	HIGH (CVSS:10.0)			The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root)	A whole cleanup of the infected system is recommended.
vsftpd Compromised Source Packages Backdoor Vulnerability	10.0.0.201	HIGH (CVSS:7.5)			Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.	VendorFix
phpinfo() output Reporting	10.0.0.201	HIGH (CVSS:7.5)			Some of the information that can be gathered from this file includes: The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.	Delete the listed files or restrict access to them.
Test HTTP dangerous methods	10.0.0.201	HIGH (CVSS:7.5)			Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files.	Use access restrictions to these dangerous HTTP methods or disable them completely.
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	10.0.0.201	HIGH (CVSS:7.5)			PHP is prone to an information-disclosure vulnerability.	PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.
OS End Of Life Detection	10.0.0.201	HIGH (CVSS:10.0)			The Operating System on the remote host has reached the end of life and should not be used anymore.	Upgrade the Operating System on the remote host to a version which is still supported and receiving security updates by the vendor.
PostgreSQL weak password	10.0.0.201	HIGH (CVSS:9.0)			It was possible to login into the remote PostgreSQL as user postgres using weak credentials.('postgres')	Change the password as soon as possible.
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0.0.201	HIGH (CVSS:10.0)			The service is running in $SAFE >= 1 mode. However it is still possible to run arbitrary syscall commands on the remote host. Sending an invalid syscall the service returned the following response: Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in `syscall'"0/usr/lib/ruby/1.8/drb/drb.rb:1555:in `send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in `__send__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in `perform_without_block'"3/usr/lib/ruby/1.8/drb/drb.rb:1515:in `perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in `main_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in `loop'"5/usr/lib/ruby/1.8/drb/drb.rb:1585:in `main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in `start'"5/usr/lib/ruby/1.8/drb/drb.rb:1581:in `main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:1430:in `run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in `start'"//usr/lib/ruby/1.8/drb/drb.rb:1427:in `run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in `initialize'"//usr/lib/ruby/1.8/drb/drb.rb:1627:in `new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in `start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not implemented	Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include: - Implementing taint on untrusted input - Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate) - Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts
FTP Brute Force Logins Reporting	10.0.0.201	HIGH (CVSS:7.5)			It was possible to login into the remote FTP server using weak/known credentials. msfadmin:msfadmin postgres:postgres service:service user:user	Change the password as soon as possible.

vsftpd Compromised Source Packages Backdoor Vulnerability	10.0.0.201	HIGH (CVSS:7.5)			Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.	The repaired package can be downloaded from the referenced link. Please validate the package with its signature.
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	10.0.0.201	HIGH (CVSS:7.5)			It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.	Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later. For other products using Tomcat please contact the vendor for more information on fixed versions.
HTTP Debugging Methods (TRACE/TRACK) Enabled	10.0.0.201		Medium(CVSS:5.8)		Debugging functions are enabled on the remote web server. The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.	Disable the TRACE and TRACK methods in your web server configuration. Please see the manual of your web server or the references for more information.
UnrealIRCd Authentication Spoofing Vulnerability	10.0.0.201		Medium(CVSS:6.8)		This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability.	Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.
Anonymous FTP Login Reporting	10.0.0.201		Medium(CVSS:6.4)		Reports if the remote FTP Server allows anonymous logins.	If you do not want to share files, you should disable anonymous logins.
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	10.0.0.201		Medium(CVSS:6)		Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.	Updates are available. Please see the referenced vendor advisory.
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	10.0.0.201		Medium(CVSS:5.8)		OpenSSL is prone to security-bypass vulnerability.	Updates are available. Please see the references for more information.
/doc directory browsable	10.0.0.201		Medium(CVSS:5		The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.	Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf: <Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory>
SSL/TLS: Certificate Expired	10.0.0.201		Medium(CVSS:5		The remote server's SSL/TLS certificate has already expired.	Replace the SSL/TLS certificate by a new one.
SSL/TLS: Report Weak Cipher Suites	10.0.0.201		Medium(CVSS:5		This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.	The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.
FTP Unencrypted Cleartext Login	10.0.0.201		4.8		The remote host is running a FTP service that allows cleartext logins over unencrypted connections.	Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Cleartext Transmission of Sensitive Information via HTTP	10.0.0.201		4.8		The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.	Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	10.0.0.201		4.3		It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.
SSH Weak Encryption Algorithms Supported	10.0.0.201		4.3		The remote SSH server is configured to allow weak encryption algorithms.	Disable the weak encryption algorithms.
jQuery < 1.6.3 XSS Vulnerability	10.0.0.201		4.3		Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.	Update to version 1.6.3 or later or apply the patch.
jQuery < 1.9.0 XSS Vulnerability	10.0.0.201		4.3		jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.	Update to version 1.9.0 or later.
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	10.0.0.201		4.3		This host is prone to an information disclosure vulnerability.	Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	10.0.0.201		4		The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).	Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	10.0.0.201		4		The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.	Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to

						obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.
TCP timestamps	10.0.0.201			LOW (CVSS:2.6)	It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 8588357 Packet 2: 8588465	To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
SSH Weak MAC Algorithms Supported	10.0.0.201			LOW (CVSS:2.6)	The following weak client-to-server MAC algorithms are supported by the remote service: hmac-md5 hmac-md5-96 hmac-sha1-96 The following weak server-to-client MAC algorithms are supported by the remote service: hmac-md5 hmac-md5-96 hmac-sha1-96	Disable the weak MAC algorithms.