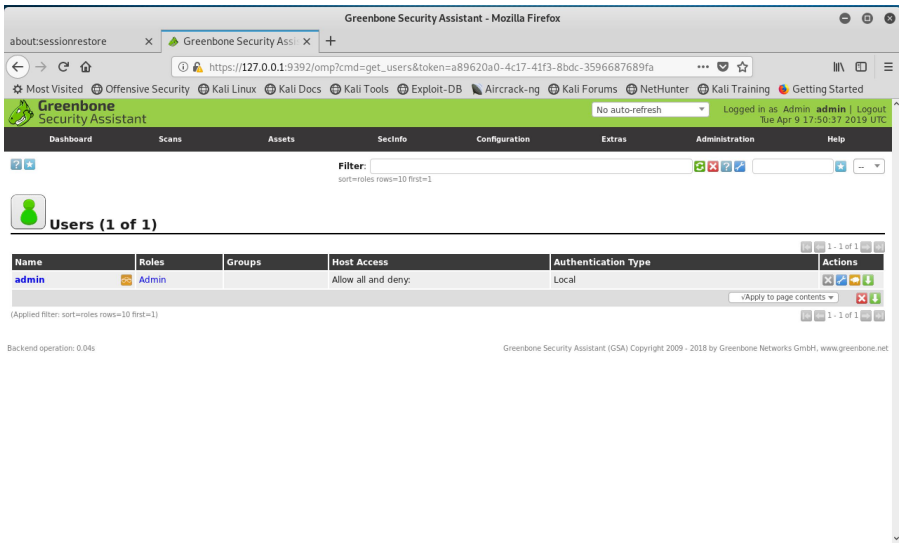
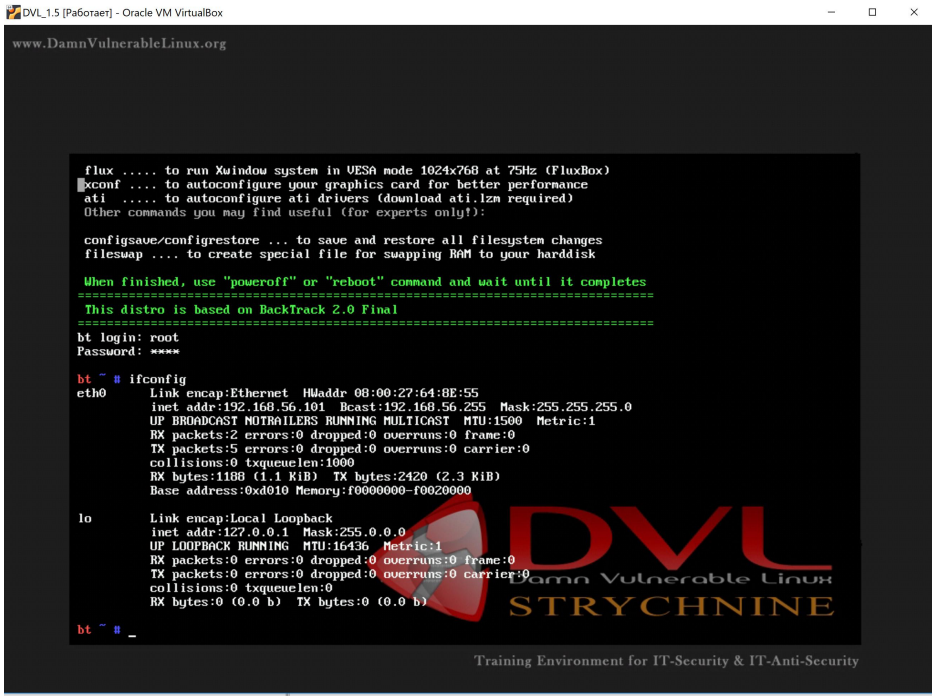
1. Установить OpenVAS в Kali Linux.

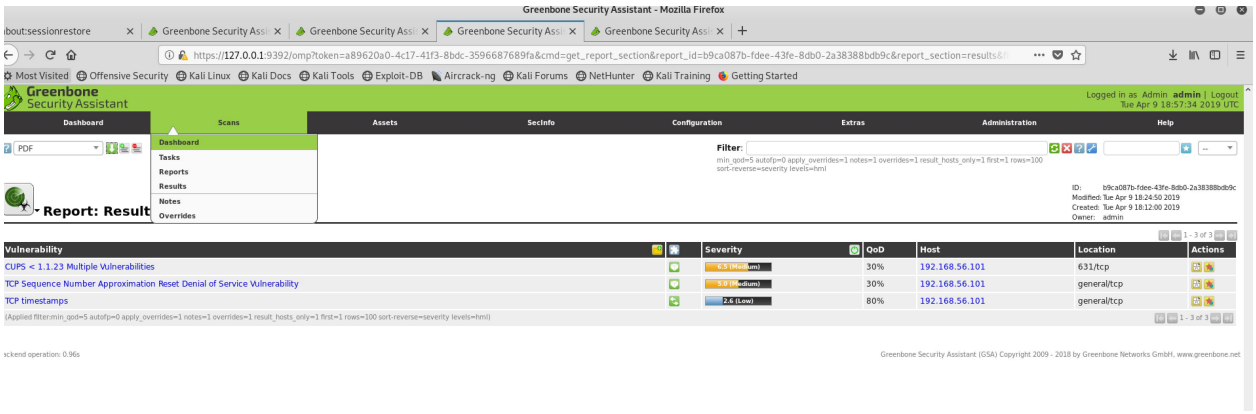


2. Установить систему DVL Linux в качестве виртуальной машины, настроить сетевой доступ к ней со стороны Kali Linux и просканировать систему DVL Linux на наличие уязвимостей.

DVL установил и настроил сеть.



Сканирование было относительно быстрым. Нашел всего 3 уязвимости.



1) Уровень medium. Оценка уязвимости 6.3. Связана с сервером печати. В качестве решения проблемы предложен VendorFix обновить CUPS до версии 1.1.23 или выше

2 Results per Host

2.1 192.168.56.101

Host scan start Tue Apr 9 18:12:13 2019 UTC
Host scan end Tue Apr 9 18:24:50 2019 UTC

Service (Port)	Threat Level
631/tcp	Medium
general/tcp	Medium
general/tcp	Low

2.1.1 Medium 631/tcp

Medium (CVSS: 6.5) NVT: CUPS < 1.1.23 Multiple Vulnerabilities
Product detection result cpe:/a:apple:cups:1.1 Detected by CUPS Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900348)
Summary ...continues on next page ...

2) Уровень medium. Оценка уязвимости 5.0. Уязвимость в TCP-стеке. Сбрасывается соединение отправлением пакета с указанием фиктивного IP адреса, без необходимости подбора номера последовательности. В качестве решения – тоже VendorFix, только я не уверен, что для DVL выпускаются патчи. Ниже написано, ознакомиться с ссылками, но они как-то не очень информативны. В интернете советуют настроить файерволл (стандартные меры борьбы со спуфингом).

2.1.2 Medium general/tcp

Medium (CVSS: 5.0) NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability
Summary The host is running TCP services and is prone to denial of service vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.
Solution **Solution type:** VendorFix Please see the referenced advisories for more information on obtaining and applying fixes.
Affected Software/OS TCP/IP v4
Vulnerability Insight The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack

3) Уровень low. Оценка уязвимости 2.6. Если я правильно понял, то эта уязвимость позволяет определить время работы хоста. В качестве решения предлагают отключить временные метки в linux “net.ipv4.tcp_timestamps = 0”

2.1.3 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 920731
Packet 2: 920983

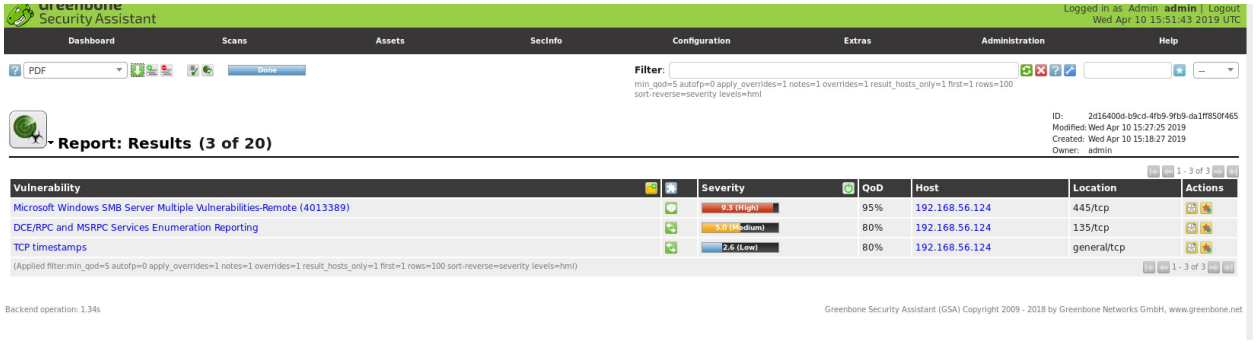
Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
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.

Отчет выгрузил в pdf.

3. * Установить виртуальную машину на базе Windows 7 (8, 8.1 или 10), активировать сетевой доступ к общим папкам. Просканировать ВМ при помощи OpenVAS с использованием данных протокола SMB.

Создал несколько папок с общим доступом. Результат:



1) Уровень high. Оценка уязвимости 9.3. Уязвимость позволяет удаленно выполнять код. Решение – VendorFix установка обновления.

2.1.1 High 445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

2) Уровень medium. Оценка уязвимости 5.0. Подключившись к порту 135 можно найти все работающие службы и собрать информацию о хосте. В качестве решения предлагают фильтровать трафик к этим портам

2.1.2 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary

... continues on next page ...

... continued from previous page ...

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
      UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
      Endpoint: ncacn_ip_tcp:192.168.56.124[49152]
Port: 49153/tcp
      UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1
      Endpoint: ncacn_ip_tcp:192.168.56.124[49153]
      Annotation: Security Center
      UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
      Endpoint: ncacn_ip_tcp:192.168.56.124[49153]
      Annotation: NRP server endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
      Endpoint: ncacn_ip_tcp:192.168.56.124[49153]
      Annotation: DHCP Client LRPC Endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
      Endpoint: ncacn_ip_tcp:192.168.56.124[49153]
      Annotation: DHCPv6 Client LRPC Endpoint
      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:192.168.56.124[49153]
      Annotation: Event log TCPIP
Port: 49154/tcp
      UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
      Endpoint: ncacn_ip_tcp:192.168.56.124[49154]
      Annotation: IP Transition Configuration endpoint
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.56.124[49154]
      UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
      Endpoint: ncacn_ip_tcp:192.168.56.124[49154]
      Annotation: XactSrv service
Port: 49155/tcp
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.56.124[49155]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
Port: 49156/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.56.124[49156]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

3) Уровень low. Оценка уязвимости 2.6. Уязвимость позволяет определить время работы хоста. В качестве решения предлагают отключить временные метки в Windows 'netsh int tcp set global timestamps=disabled'

2.1.3 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 67192
Packet 2: 67293
```

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

Solution type: Mitigation

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.

Affected Software/OS

TCP/IPv4 implementations that implement RFC1323.

... continues on next page ...