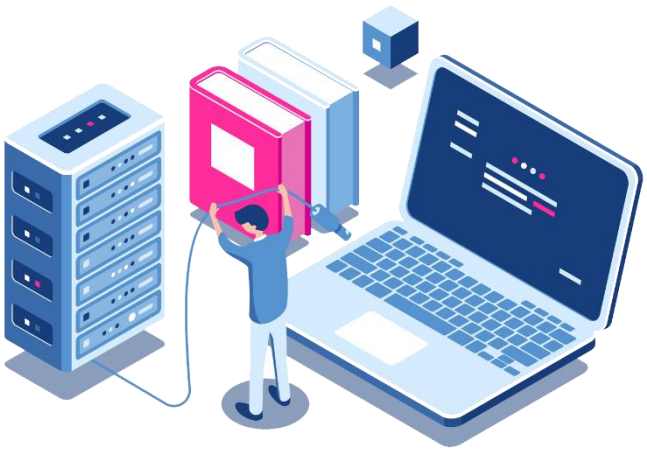
P.PORTO

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

Licenciatura Segurança Informática em Redes e Computadores

Relatório Trabalho Prático Auditória Informática

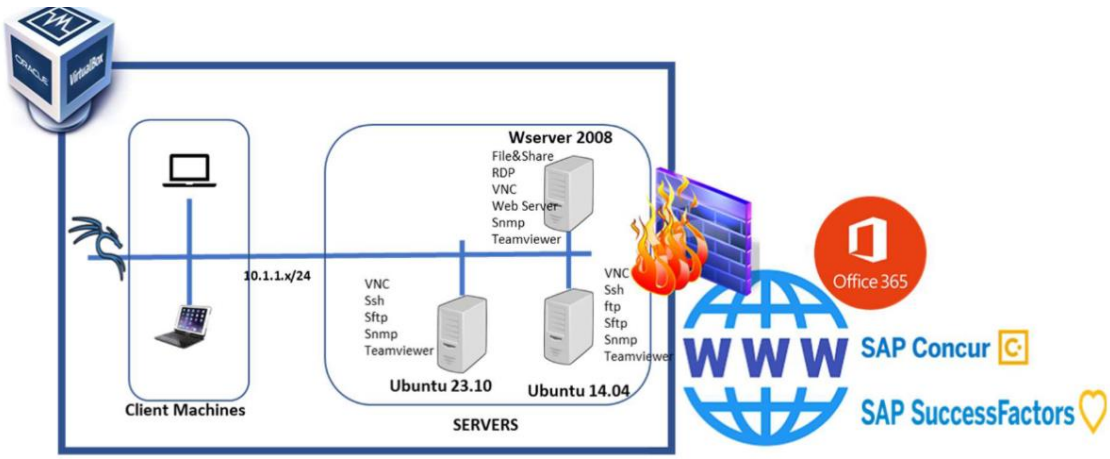


Fábio da Cunha 8210619

ESTG, abril de 2024

1. Introdução

No âmbito da disciplina de Auditória Informática foi-nos solicitado um trabalho prático cujo objetivo é fazer uma auditoria a um cenário que nos foi proposto, onde devemos instalar alguns serviços nas máquinas disponíveis, donde alguns serão servidores e outros máquinas clientes, sendo este auditoria toda ela baseada nos dados da empresa TRANSPORT RT que se pretende auditar, neste relatório irei demostrar todo os processos efetuados, bem como os comandos utilizados.



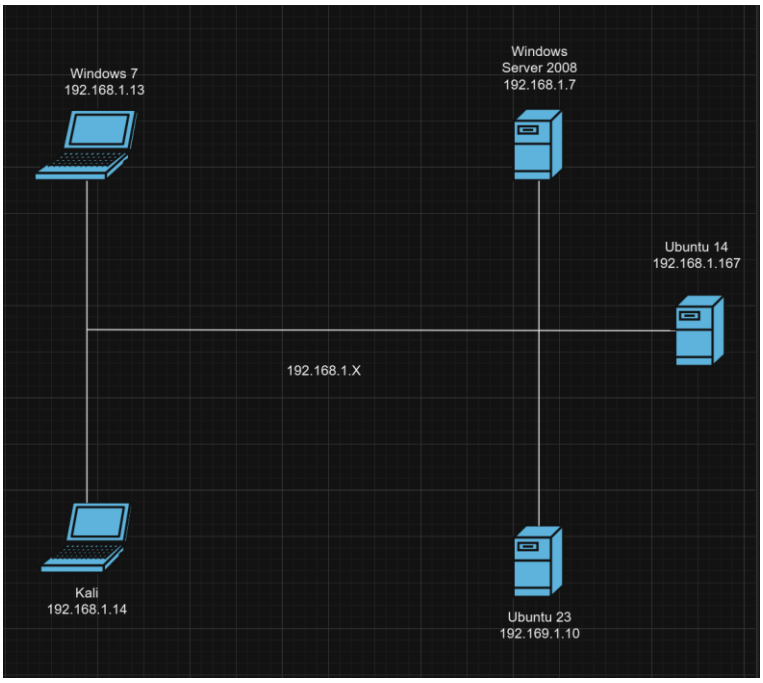
Este é o cenário proposto.

2. Lista de Ativos e Desenho da Rede

Servidores: WebServer 2008, Ubuntu 22.10, Ubuntu Server 14.04

Clientes: Kali Linux e Windows 7

Não cheguei a usar o Windows 10 no trabalho



Desenho da rede

Lista de Ativos:
Windows 7

```
C:\Users\john>systeminfo

Host Name:                 JOHN-PC
OS Name:                   Microsoft Windows 7 Ultimate
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          john
Registered Organization:
Product ID:                00426-292-0000007-85919
Original Install Date:     19-03-2021, 23:00:41
System Boot Time:          28-04-2024, 23:11:56
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 25 Model 80 Stepping 0 AuthenticAMD
```

Kali Linux

```
┌──(kali㉿kali)-[~/Downloads]
└─$ uname -a
Linux kali 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-04-09) x86_64 GNU/Linux
```

Windows Server 2008

```
Host Name:                 WIN-CMV7HKGHRJL
OS Name:                   Microsoft Windows Server 2008 R2 Standard
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00477-001-0000347-84491
Original Install Date:     3/30/2020, 12:15:10 AM
System Boot Time:          4/28/2024, 6:36:30 PM
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAM
```

Ubuntu Server 14.04

```
ubuntulab@ubuntulab:~$ uname -a
Linux ubuntulab 4.4.0-142-generic #168~14.04.1-Ubuntu SMP Sat Jan 19 11:26:28 UTC 2019 x86_64 x86_64
 x86_64 GNU/Linux
ubuntulab@ubuntulab:~$
```

Ubuntu Server 23.10

```
fabio@fabio-VirtualBox:~$ uname -a
Linux fabio-VirtualBox 6.5.0-28-generic #29~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC T
hu Apr  4 14:39:20 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
fabio@fabio-VirtualBox:~$
```

3. Acessos por serviço

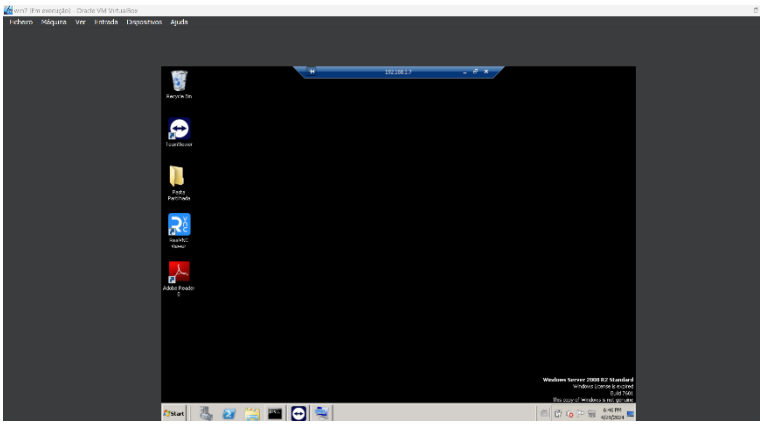
Conexão sftp entre Kali e o Ubuntu 23

```
┌──(kali㉿kali)-[~]
└─$ sftp fabio@192.168.1.10
fabio@192.168.1.10's password:
Connected to 192.168.1.10.
sftp>
```

Conexão ftp entre Kali e Ubuntu Server 14

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.167
Connected to 192.168.1.167.
220 (vsFTPd 3.0.2)
Name (192.168.1.167:kali): ubuntulab
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

No Windows 7 fiz uma ligação RDP para o servidor Windows 8

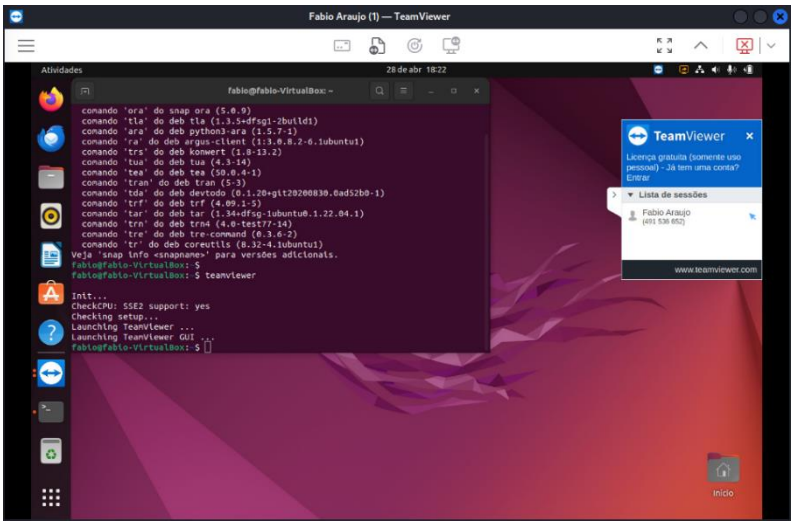


Conexão SSH entre o Kali Linux e a máquina Ubuntu

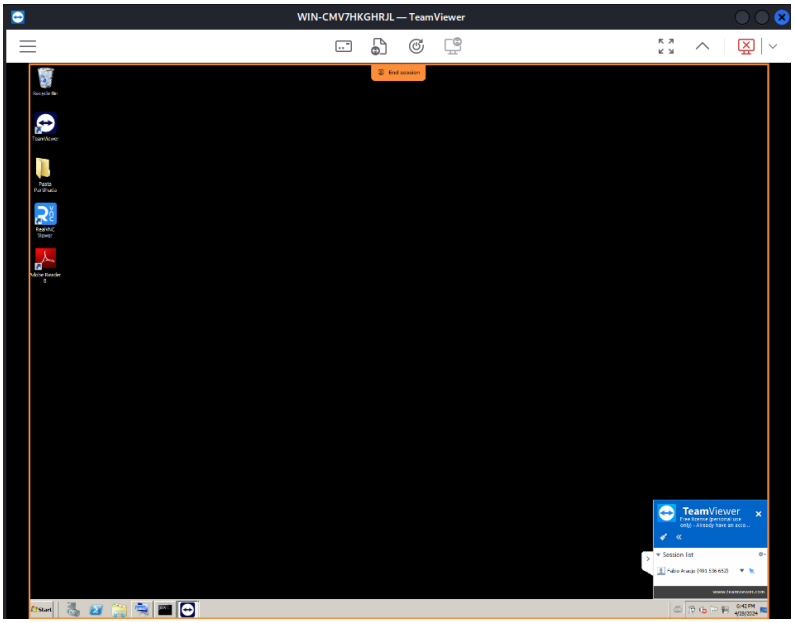
Conexão SSH entre o Kali e o Ubuntu Server 14

```
┌──(kali㉿kali)-[~]
└─$ ssh ubuntulab@192.168.1.167
The authenticity of host '192.168.1.167 (192.168.1.167)' can't be established.
ED25519 key fingerprint is SHA256:jvTYdgKMYiQFPkQFMhabyPhOJdisVvTjTzRBjNn1dYA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.167' (ED25519) to the list of known hosts.
ubuntulab@192.168.1.167's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sun Apr 28 16:30:29 WEST 2024

  System load:  0.52              Processes:           112
  Usage of /:   22.3% of 8.73GB   Users logged in:     0
  Memory usage: 22%               IP address for eth0: 192.168.1.167
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Sun Apr 28 16:30:29 2024
ubuntulab@ubuntulab:~$
```

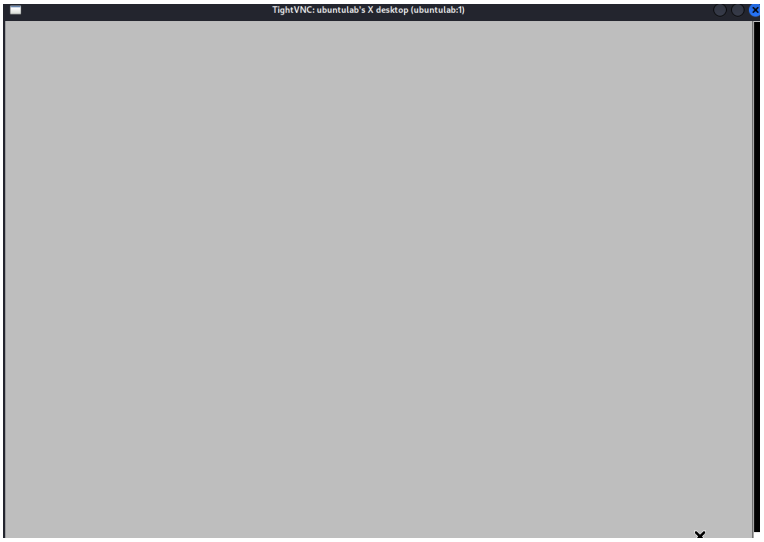
Usando o teamviewer estabeleci uma ligação do cliente Kali com o servidor Ubuntu 23



Usando o teamviewer estabeleci uma ligação do cliente Kali com o servidor Windows 8



Só consegui estabelecer uma ligação Vnc entre o Kali e o Ubuntu Server 14, mas só aparecia essa tela cinza, não sei o porquê



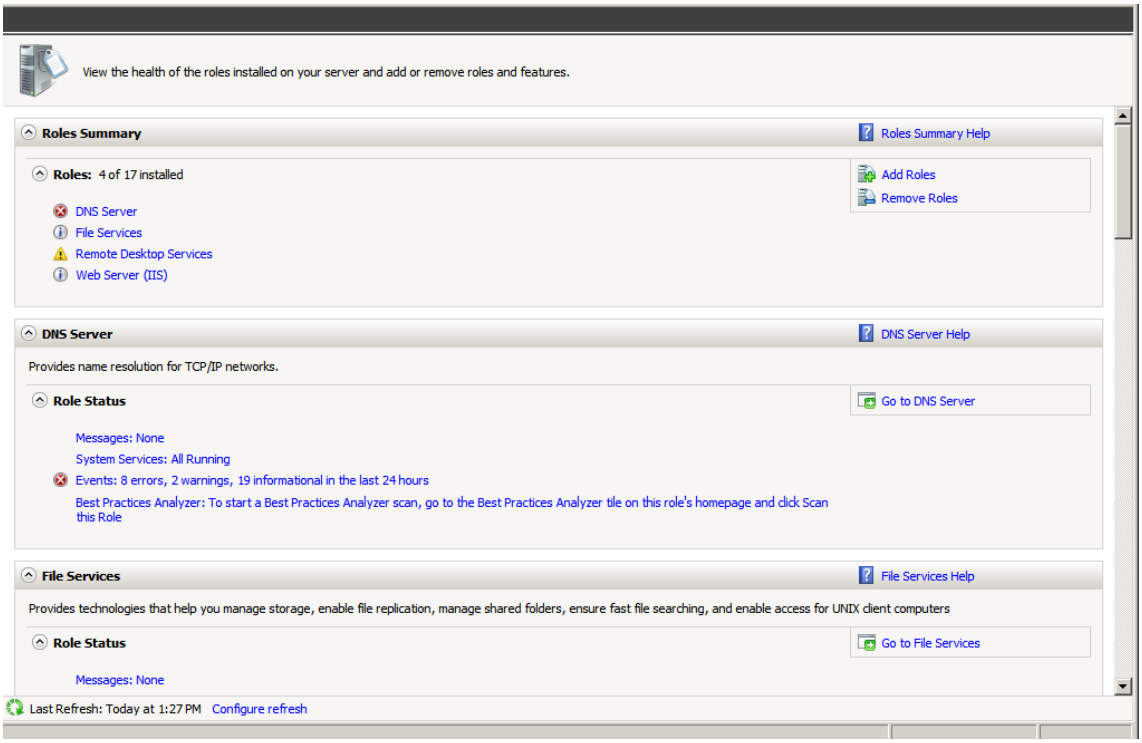
4. Serviços instalados nos servidores

Ubuntu 14

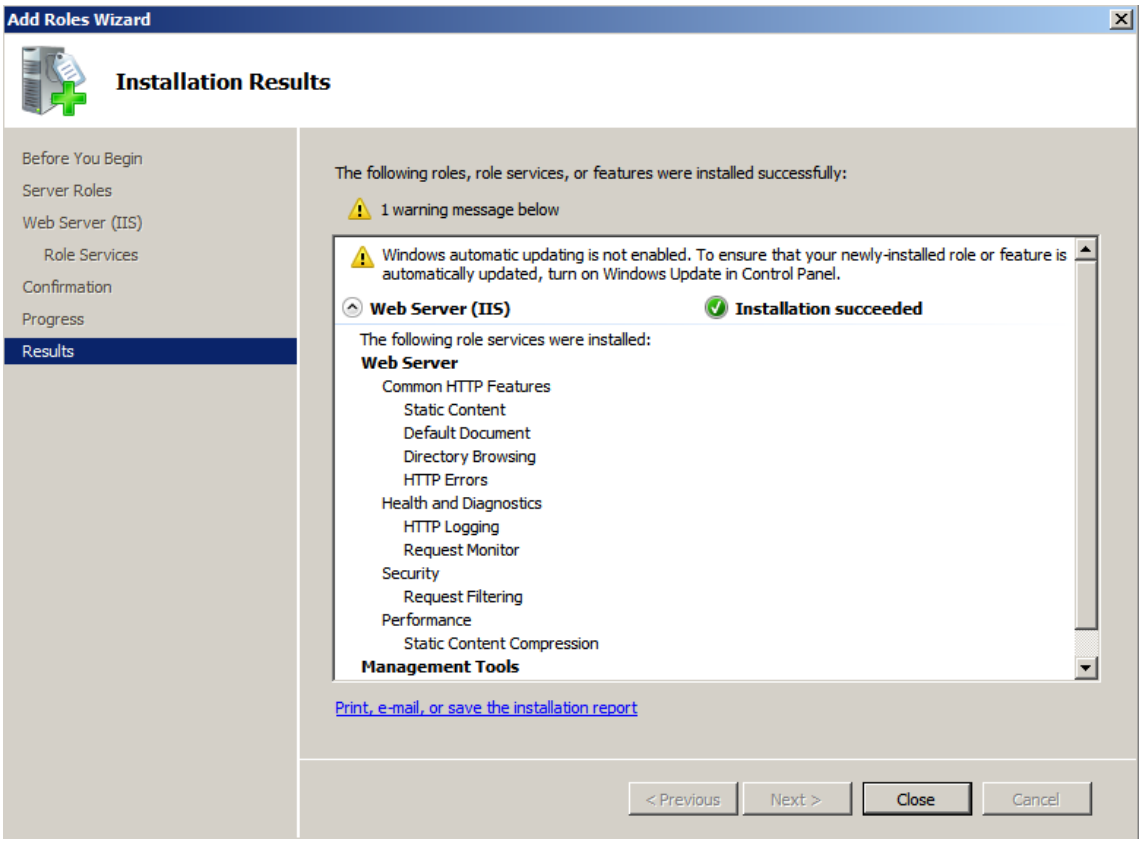
Ubuntu 23

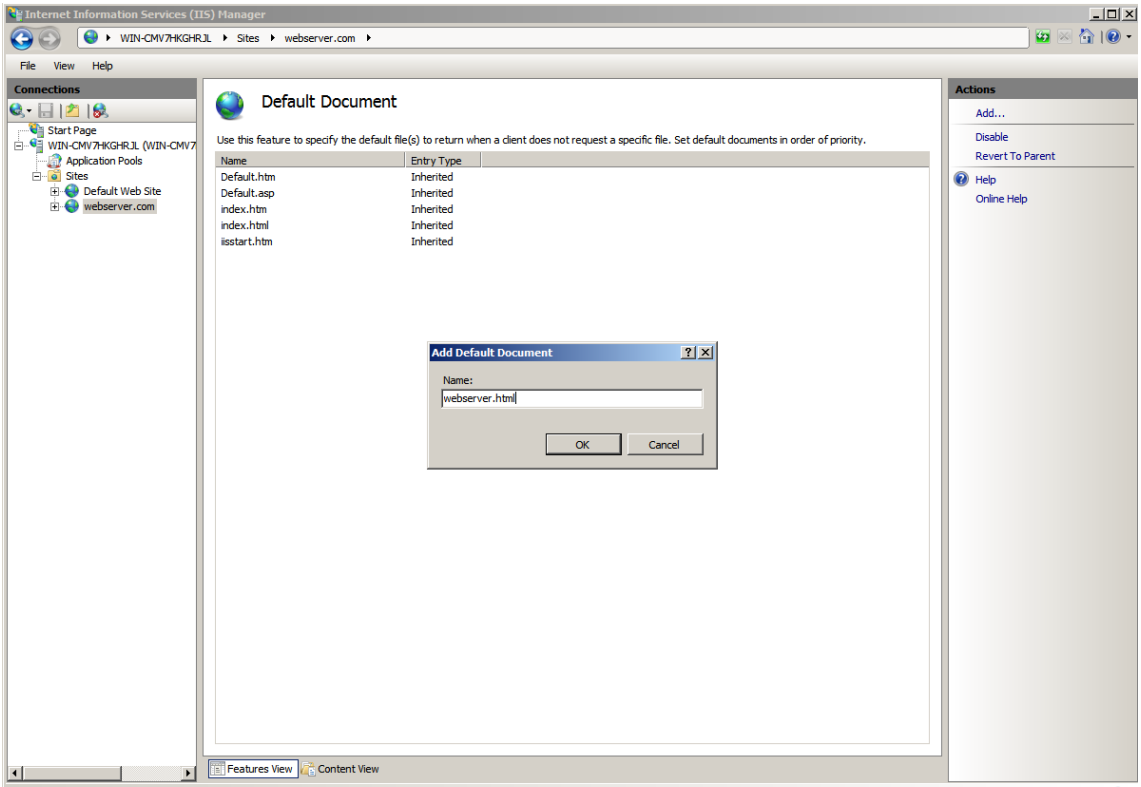
```
fabio@fabio-VirtualBox:~$ dpkg -l | grep sftp
ii  openssh-sftp-server                     1:8.9p1-3ubuntu0.7
      amd64        secure shell (SSH) sftp server module, for SFTP access from
remote machines
fabio@fabio-VirtualBox:~$ snmpd -v

NET-SNMP version:  5.9.1
Web:               http://www.net-snmp.org/
Email:             net-snmp-coders@lists.sourceforge.net

fabio@fabio-VirtualBox:~$
fabio@fabio-VirtualBox:~$ ssh -V
OpenSSH_8.9p1 Ubuntu-3ubuntu0.7, OpenSSL 3.0.2 15 Mar 2022
fabio@fabio-VirtualBox:~$ teamviewer -version

 TeamViewer                          15.53.6  (DEB)

fabio@fabio-VirtualBox:~$
fabio@fabio-VirtualBox:~$ vncserver -version

Warning: fabio-VirtualBox:1 is taken because of /tmp/.X1-lock
Remove this file if there is no X server fabio-VirtualBox:1
Couldn't start Xtightvnc; trying default font path.
Please set correct fontPath in the vncserver script.
Couldn't start Xtightvnc process.

Xvnc version TightVNC-1.3.10
Xvnc version TightVNC-1.3.10

fabio@fabio-VirtualBox:~$

fabio@fabio-VirtualBox:~$ wireshark -v
Wireshark 3.6.2 (Git v3.6.2 packaged as 3.6.2-2)

Copyright 1998-2022 Gerald Combs <gerald@wireshark.org> and contributors.
License GPLv2+: GNU GPL version 2 or later <https://www.gnu.org/licenses/gpl-2.0
.html>
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) using GCC 11.2.0, with Qt 5.15.2, with libpcap, with POSIX
capabilities (Linux), with libnl 3, with GLib 2.71.2, with zlib 1.2.11, with Lua
5.2.4, with GnuTLS 3.7.3 and PKCS #11 support, with Gcrypt 1.9.4, with MIT
Kerberos, with MaxMind DB resolver, with nghttp2 1.43.0, with brotli, with LZ4,
with Zstandard, with Snappy, with libxml2 2.9.12, with libsmi 0.4.8, with
QtMultimedia, without automatic updates, with SpeexDSP (using system library),
with Minizip.

Running on Linux 6.5.0-28-generic, with AMD Ryzen 5 5600H with Radeon Graphics
(with SSE4.2), with 1959 MB of physical memory, with GLib 2.72.4, with zlib
1.2.11, with Qt 5.15.3, with libpcap 1.10.1 (with TPACKET_V3), with c-ares
1.18.1, with GnuTLS 3.7.3, with Gcrypt 1.9.4, with nghttp2 1.43.0, with brotli
1.0.9, with LZ4 1.9.3, with Zstandard 1.4.8, with libsmi 0.4.8, with
LC_TYPE=pt_PT.UTF-8, binary plugins supported (0 loaded).
fabio@fabio-VirtualBox:~$
```

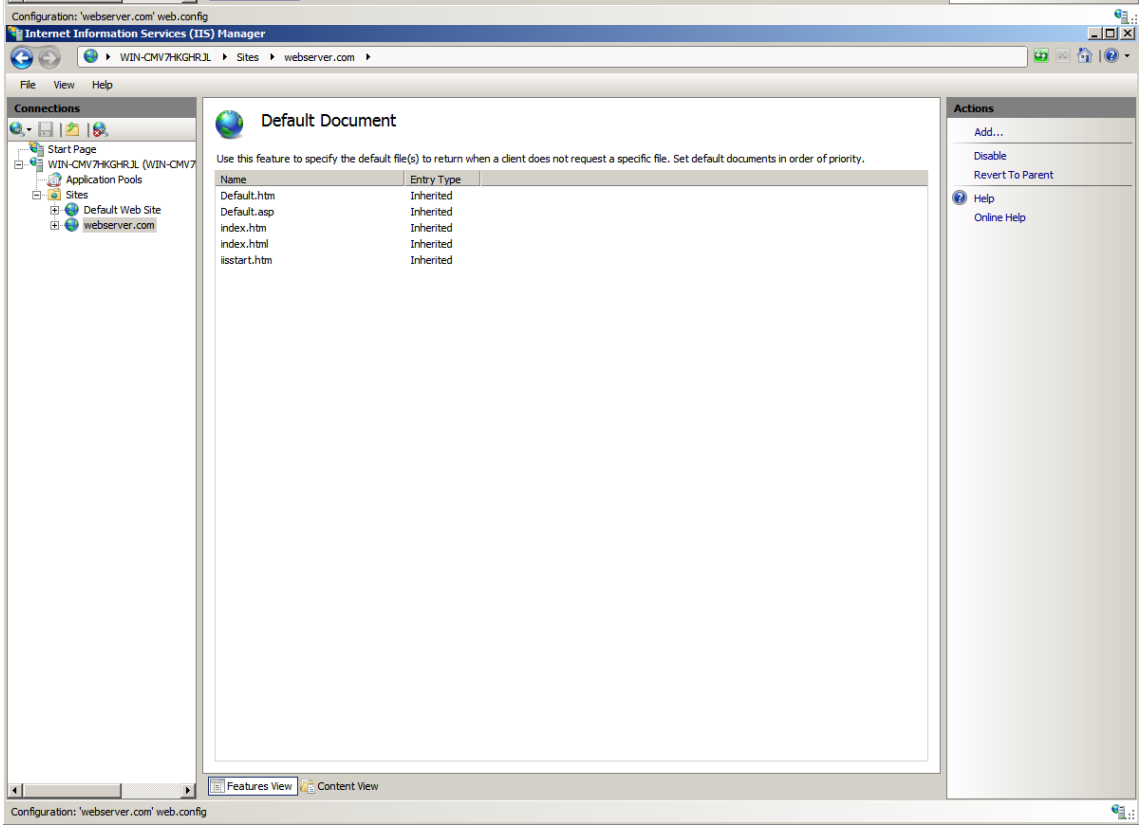
Windows Server 2008

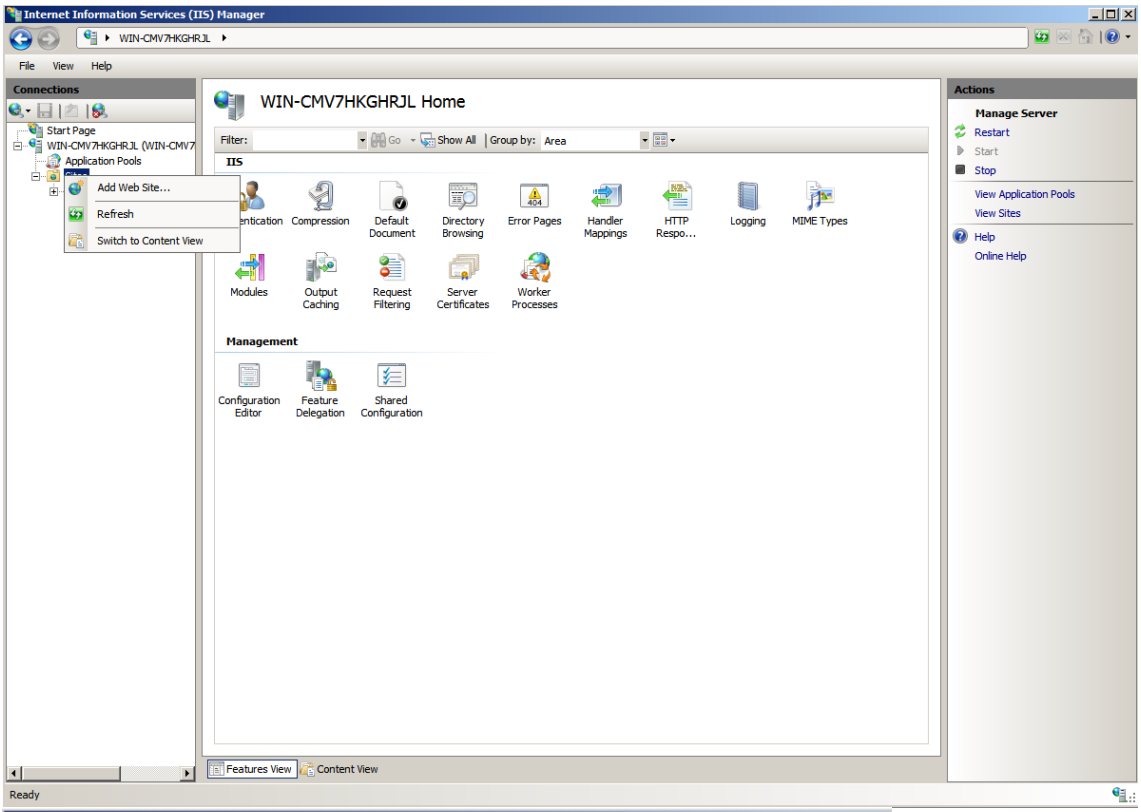


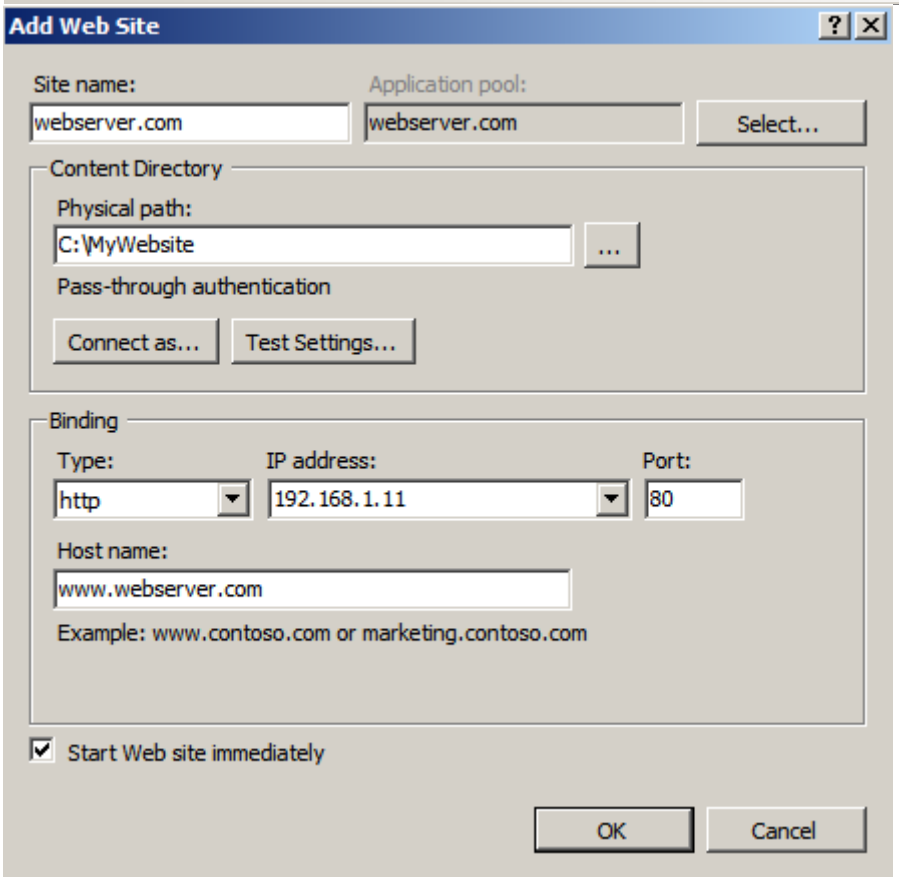
5. Web Server (Windows Server 2008)

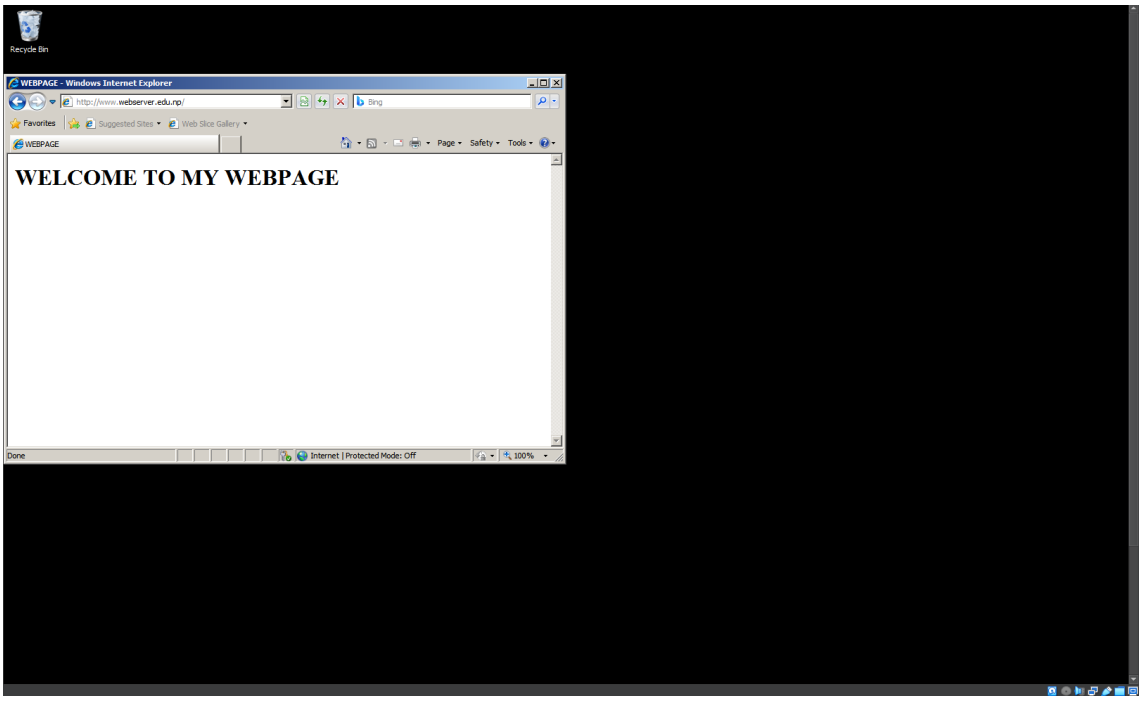

Add Roles Wizard
Installation Results
Before You Begin
Server Roles
Web Server (IIS)
Role Services
Confirmation
Progress
Results
The following roles, role services, or features were installed successfully:
1 warning message below
Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update in Control Panel.
Web Server (IIS)
Installation succeeded
The following role services were installed:
Web Server
Common HTTP Features
Static Content
Default Document
Directory Browsing
HTTP Errors
Health and Diagnostics
HTTP Logging
Request Monitor
Security
Request Filtering
Performance
Static Content Compression
Management Tools
Print, e-mail, or save the installation report
< Previous
Next >
Close
Cancel


Internet Information Services (IIS) Manager
WIN-CMV7HKGHRJL ▸ Sites ▸ webserver.com ▸
File View Help
Connections
Start Page
WIN-CMV7HKGHRJL (WIN-CMV7
Application Pools
Sites
Default Web Site
webserver.com
Default Document
Use this feature to specify the default file(s) to return when a client does not request a specific file. Set default documents in order of priority.
Name
Entry Type
Default.htm Inherited
Default.asp Inherited
index.htm Inherited
index.html Inherited
iisstart.htm Inherited
Add Default Document
Name:
webserver.html
OK
Cancel
Actions
Add...
Disable
Revert To Parent
Help
Online Help
Features View
Content View
Configuration: 'webserver.com' web.config


Internet Information Services (IIS) Manager
WIN-CMV7HKGHRJL ▸ Sites ▸ webserver.com ▸
File View Help
Connections
Start Page
WIN-CMV7HKGHRJL (WIN-CMV7
Application Pools
Sites
Default Web Site
webserver.com
Default Document
Use this feature to specify the default file(s) to return when a client does not request a specific file. Set default documents in order of priority.
Name
Entry Type
Default.htm Inherited
Default.asp Inherited
index.htm Inherited
index.html Inherited
iisstart.htm Inherited
Actions
Add...
Disable
Revert To Parent
Help
Online Help
Features View
Content View
Configuration: 'webserver.com' web.config


Internet Information Services (IIS) Manager
WIN-CMV7HKGHRJL
File View Help
Connections
Start Page
WIN-CMV7HKGHRJL (WIN-CMV7
Application Pools
Add Web Site...
Refresh
Switch to Content View
WIN-CMV7HKGHRJL Home
Filter:
Go
Show All
Group by: Area
IIS
Compression
Default Document
Directory Browsing
Error Pages
Handler Mappings
HTTP Respo...
Logging
MIME Types
Modules
Output Caching
Request Filtering
Server Certificates
Worker Processes
Management
Configuration Editor
Feature Delegation
Shared Configuration
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Help
Online Help
Features View
Content View
Ready


Add Web Site
Site name:
webserver.com
Application pool:
webserver.com
Select...
Content Directory
Physical path:
C:\MyWebsite
...
Pass-through authentication
Connect as...
Test Settings...
Binding
Type:
http
IP address:
192.168.1.11
Port:
80
Host name:
www.webserver.com
Example: www.contoso.com or marketing.contoso.com
Start Web site immediately
OK
Cancel



6. Scan aos servidores apartir do cliente Kali Linux

a. Nmap

Kali Linux – Ubuntu 14(Não sei o porquê do snmp não estar a aparecer como um dos serviços ativos, mas na máquina ele está ativo).

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.167
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 19:04 WEST
Nmap scan report for ubuntulab.home (192.168.1.167)
Host is up (0.0020s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
53/tcp   open  domain      ISC BIND 9.9.5-3ubuntu0.19 (Ubuntu Linux)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
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)
5901/tcp open  vnc         VNC (protocol 3.8)
6001/tcp open  X11         (access denied)
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: UBUNTULAB; 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 11.52 seconds
```

```
ubuntulab@ubuntulab:~$ sudo service snmpd status
 * snmpd is running
```

Kali Linux – Ubuntu 23.10

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 19:14 WEST
Nmap scan report for fabio-VirtualBox.home (192.168.1.10)
Host is up (0.0023s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.5
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
5902/tcp open  vnc     VNC (protocol 3.8)
6002/tcp open  X11     (access denied)
Service Info: 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 6.59 seconds
```

Kali Linux – Windows 7

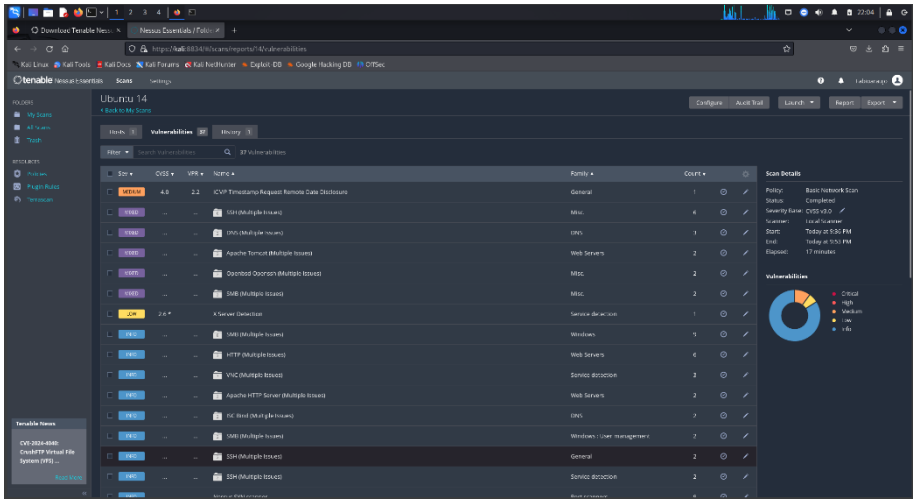
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.1.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 18:51 WEST
Nmap scan report for john-PC.home (192.168.1.13)
Host is up (0.0020s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE            VERSION
3389/tcp open  ssl/ms-wbt-server?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 84.67 seconds
```

Kali Linux – Windows Server 8

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-2
8 18:48 WEST
Nmap scan report for WIN-CMV7HKGHRJL.home (192.168.1.7)
Host is up (0.0021s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE            VERSION
53/tcp    open  domain             Microsoft DNS 6.1.76
01 (1DB1446A) (Windows Server 2008 R2 SP1)
80/tcp    open  http               Microsoft IIS httpd
7.5
135/tcp   open  msrpc              Microsoft Windows RP
C
139/tcp   open  netbios-ssn        Microsoft Windows ne
tbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Se
rver 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
49154/tcp open  msrpc              Microsoft Windows RP
C
49155/tcp open  msrpc              Microsoft Windows RP
C
49156/tcp open  msrpc              Microsoft Windows RP
C
Service Info: OSs: Windows, Windows Server 2008 R2 - 20
12; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, c
pe:/o:microsoft:windows

Service detection performed. Please report any incorrec
t results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 84.95 se
conds
```

b. Nessus

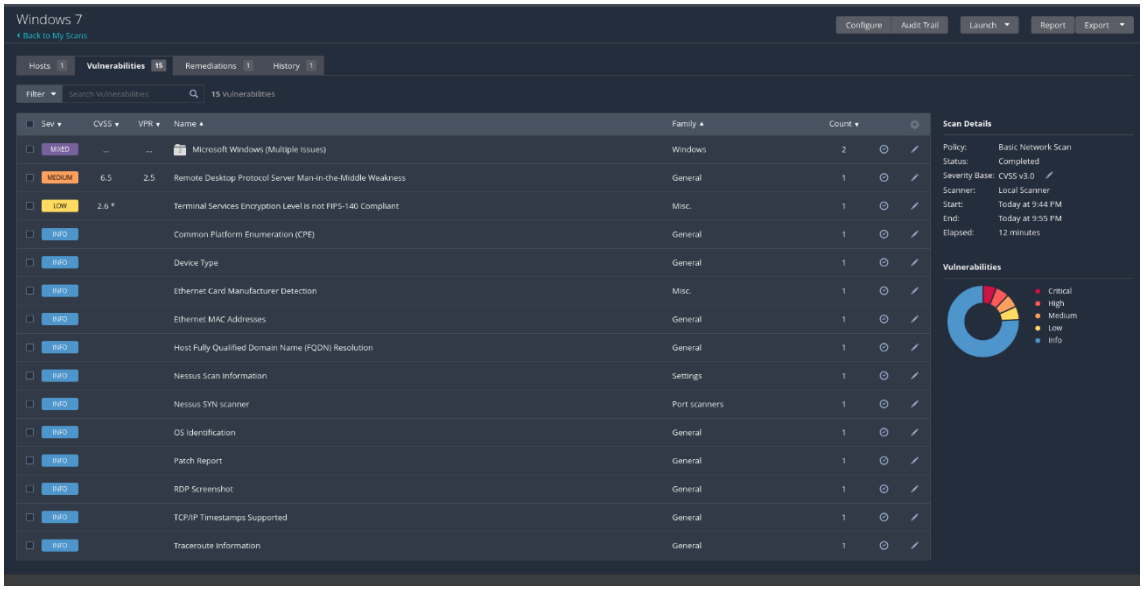
Ubuntu 14.04



Finding 1

i. Tipo de Finding: Descoberta de serviços e informações do sistema operacional.
ii. Descrição do Finding: O scan identificou vários serviços em execução no host, incluindo FTP (vsftpd), SSH (OpenSSH), DNS (BIND), HTTP (Apache httpd), NetBIOS (Samba), e Apache Tomcat.
- Os serviços HTTP estão hospedando páginas identificáveis ("My Web Page" no Apache httpd e "Apache Tomcat" no Apache Tomcat) e o serviço BIND está executando uma versão específica.
- As portas abertas indicam uma variedade de serviços disponíveis no sistema.
iii. Nível de Risco: O risco varia dependendo da configuração e da finalidade do servidor. Por exemplo, a presença de serviços como SSH e FTP pode representar um risco de acesso não autorizado, enquanto a exposição de serviços HTTP pode indicar uma superfície de ataque para vulnerabilidades relacionadas à web.
iv. Recomendação: Recomenda-se revisar e reforçar a segurança dos serviços expostos, como garantir que as versões dos serviços estejam atualizadas, implementar autenticação forte quando aplicável e restringir o acesso a serviços sensíveis a partir de fontes confiáveis. Além disso, é importante monitorar regularmente a atividade do sistema para detectar e responder a possíveis ameaças.

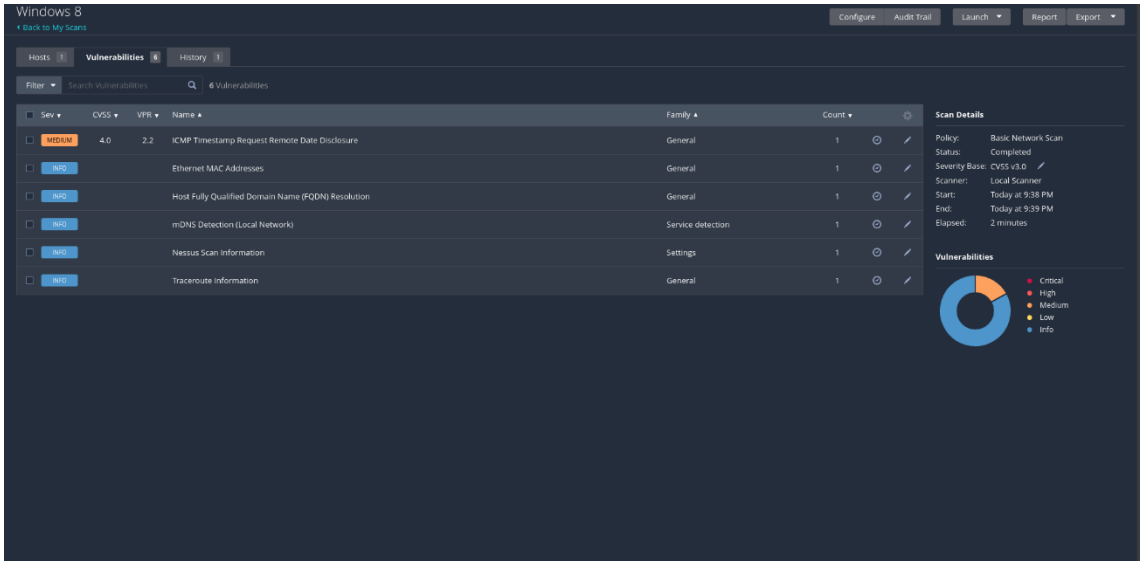
Windows 7



Finding 1:

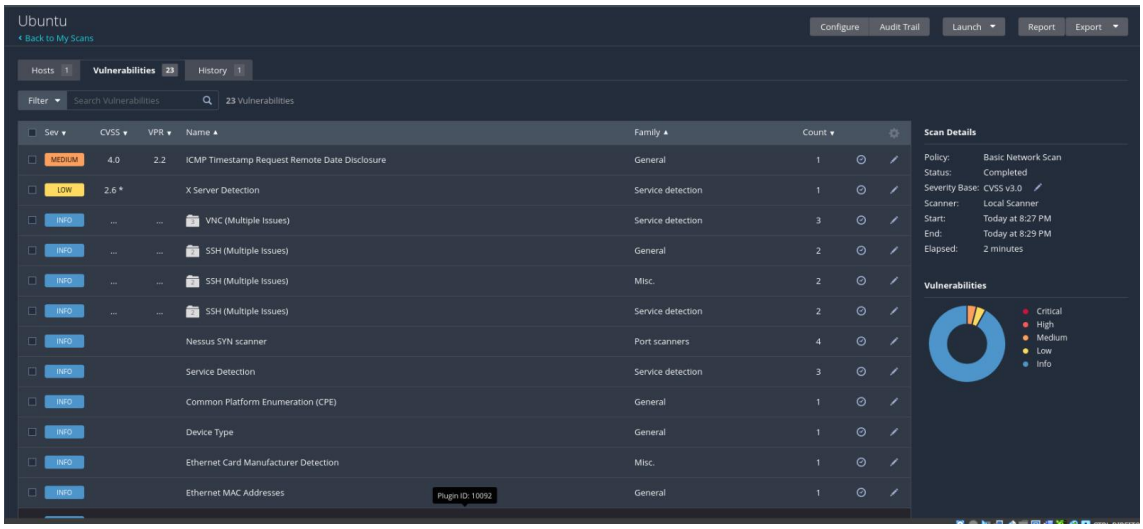
Referência do Finding: CVE-2019-0708
Tipo de Finding: Vulnerabilidade de Execução Remota de Código (RCE)
Descrição do Finding: A vulnerabilidade CVE-2019-0708 afeta o Protocolo de Área de Trabalho Remota (RDP) da Microsoft. Um atacante remoto não autenticado pode explorar isso por meio de uma série de solicitações especialmente elaboradas para executar código arbitrário.
Nível de Risco: Crítico
Recomendação: Aplicar os patches de segurança fornecidos pela Microsoft para sistemas afetados, incluindo Windows XP, 2003, 2008, 7 e 2008 R2.
Especificar Plano de Ação: Implementar imediatamente os patches fornecidos pela Microsoft para mitigar o risco de exploração dessa vulnerabilidade. Além disso, monitorar atentamente a rede em busca de atividades suspeitas relacionadas a tentativas de exploração dessa vulnerabilidade.

Windows Server 8



Finding 1:
Tipo de Finding: Serviço em Execução - Microsoft DNS.
Descrição do Finding com evidências: O Nmap identificou o serviço de DNS (Domain Name System) rodando na porta 53/tcp.
Nível de Risco: Baixo.
Recomendação: Certificar-se de que o serviço DNS esteja configurado corretamente e que apenas consultas autorizadas sejam permitidas.

Ubuntu 23.10



Finding 1

Tipo de Finding: Porta SSH Aberta (22/tcp).
Descrição do Finding com evidências: A porta 22/tcp está aberta, indicando que o serviço SSH está em execução no host.
Nível de Risco: Baixo.
Recomendação: Verificar se o serviço SSH está configurado corretamente e se é necessário limitar o acesso apenas a usuários autorizados.

8. **Riscos do Colaborador com Privilégios de Administração:**
   - Vazamento de dados sensíveis.
   - Instalação de software não autorizado.
   - Ataques internos.
   - Exploração de vulnerabilidades.

   Medidas sugeridas:
   - Princípio do menor privilégio.
   - Monitoramento de atividades.
   - Treinamento em segurança da informação.
   - Revisão periódica de acessos.
   - Implementação de controles adicionais.

9. **Riscos de Access Point Wi-Fi não Autorizado:**
    - Aumento da superfície de ataque.
    - Potencial de acesso não autorizado.
    - Interceptação de dados.
    - Exploração de vulnerabilidades.

    Medidas sugeridas:
    - Identificação e remoção do Access Point.
    - Reforço da segurança da rede.
    - Monitoramento contínuo da rede.
    - Políticas de segurança claras.
    - Educação e conscientização dos funcionários.

10. **Riscos do Túnel VPN LAN-LAN:**
    - Acesso não autorizado.
    - Exposição a ataques.
    - Riscos de compartilhamento de recursos.

    Medidas sugeridas:
    - Controles de acesso rigorosos.
    - Monitoramento de atividades.
    - Segregação de rede.
    - Criptografia forte.
    - Auditorias regulares de segurança.

11. **Ao implementar o Kubernetes para orquestrar containers, é crucial considerar os seguintes riscos de segurança**:

Vulnerabilidades do Kubernetes: Atualizações regulares são essenciais para corrigir falhas de segurança.

Acesso não autorizado: Controle de acesso rigoroso é necessário para evitar acessos indevidos.

Vazamento de informações sensíveis: Configurações inadequadas podem expor dados confidenciais.

Ataques de negação de serviço (DoS): Proteções devem ser implementadas para prevenir sobrecargas maliciosas.

Ataques de lateralidade: Isolamento entre contêineres é vital para conter possíveis ataques.

Configurações inadequadas de rede: Erros podem aumentar a superfície de ataque.

Falhas na gestão de identidade e acesso: Controle preciso de privilégios é essencial para evitar escaladas.

Práticas de segurança como atualizações regulares, políticas de acesso estritas e monitoramento de atividades são cruciais para mitigar esses riscos.

12. **Riscos do Chatbot com IA:**
    - Privacidade e segurança dos dados.
    - Viés e discriminação.
    - Falhas no aprendizado.

    Medidas sugeridas:
    - Avaliação abrangente de risco.
    - Políticas claras de segurança e privacidade.
    - Treinamento adequado para colaboradores.
    - Implementação de medidas de monitoramento.

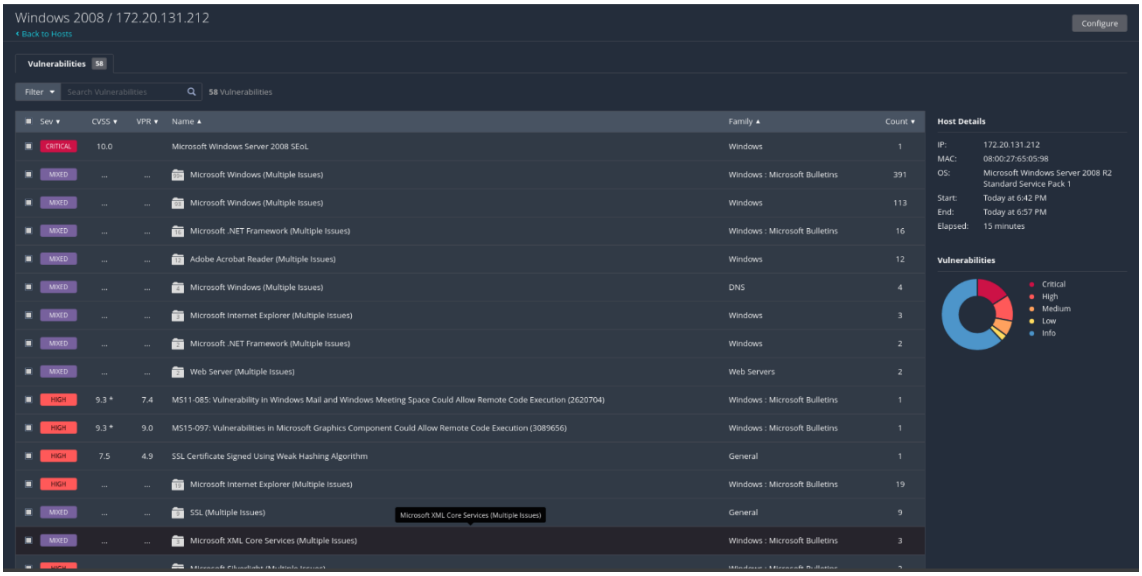
13. **Recomendações para Proteção de Perímetro Interno e Externo:**
    - Segmentação de Rede.
    - Firewalls Avançados.
    - VPN Segura.
    - Monitoramento de Tráfego.
    - Atualizações de Segurança.
    - Autenticação Forte.
    - Controle de Acesso.
    - Auditoria e Monitoramento de Acesso.
    - Educação e Conscientização em Segurança.
    - Revisão da Arquitetura de Rede.

14. **Proposta de próximas ações**

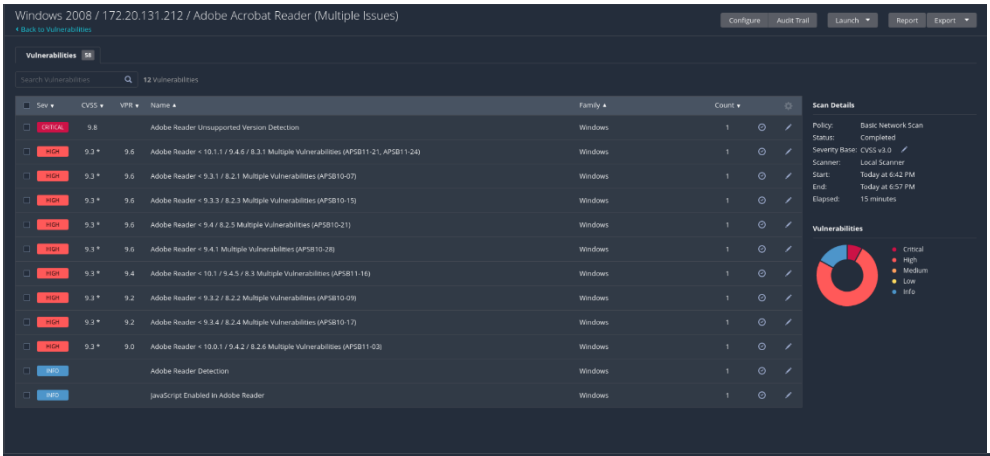
    a. Implementar segmentação de rede: Recomendamos segmentar a rede empresarial da TRANSPORT RT para limitar o acesso dos usuários e proteger os serviços críticos.
    b. Atualizar sistemas operacionais: É crucial atualizar os sistemas operacionais para versões mais recentes e suportadas, especialmente o Ubuntu 14.04 e o Windows Server 2008, que estão fora do suporte.
    c. Fortalecer configurações de segurança: Recomendamos revisar e fortalecer as configurações de segurança dos servidores, incluindo políticas de senha, firewall e permissões de usuário.
    d. Implementar criptografia forte: É essencial implementar criptografia forte em todos os serviços, como SSL/TLS para a aplicação web e SFTP, para proteger a comunicação de dados confidenciais.
    e. Remover serviços desnecessários: Recomendamos desativar ou remover serviços desnecessários, como SNMP, quando não forem essenciais para operações comerciais.
    f. Monitorar regularmente a rede: Propomos estabelecer um sistema de monitoramento contínuo da rede para identificar e responder rapidamente a atividades suspeitas ou ameaças cibernéticas.
    g. Educação em segurança da informação: Promover treinamentos regulares de conscientização em segurança da informação para todos os funcionários, a fim de reduzir o risco de violações causadas por práticas inadequadas.

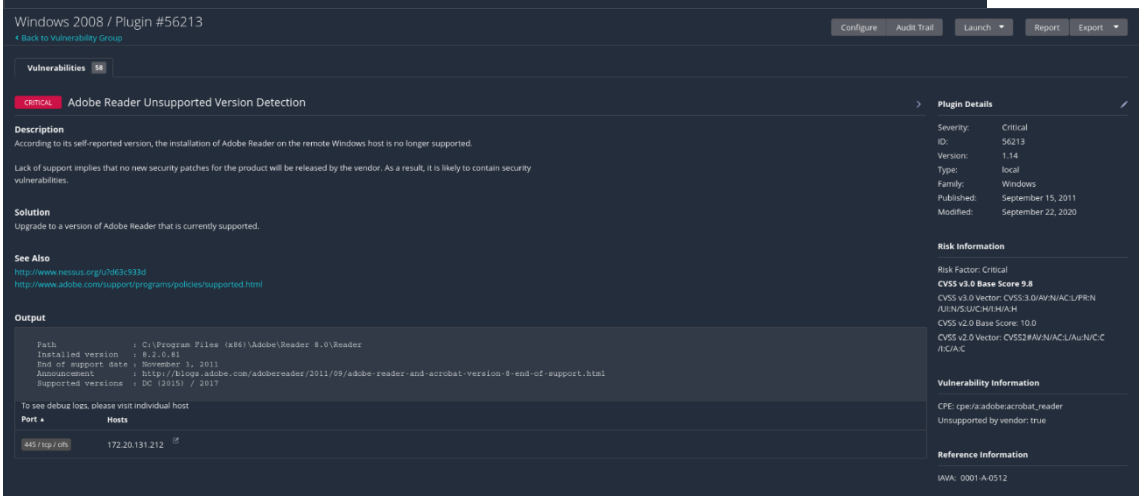
Scans Autenticado com o Nessus

Windows Server 2008

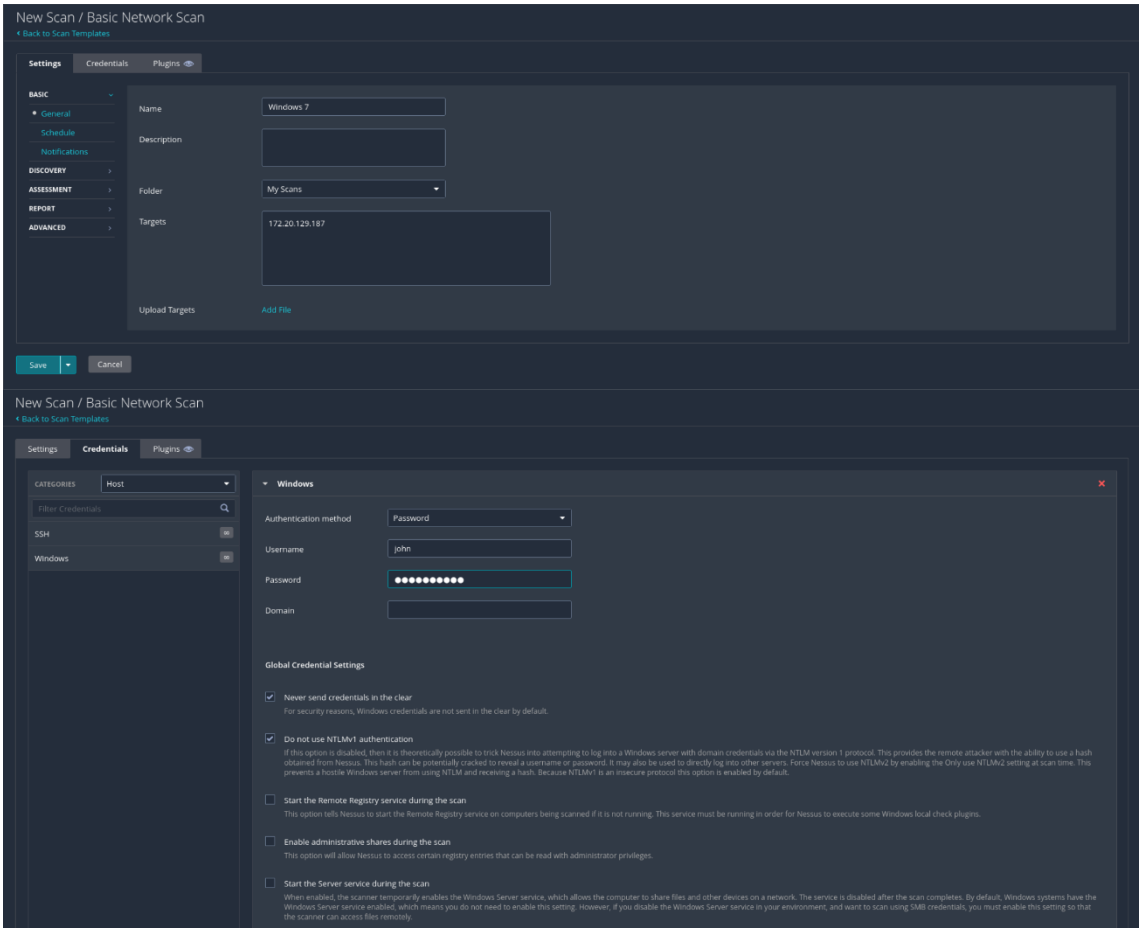


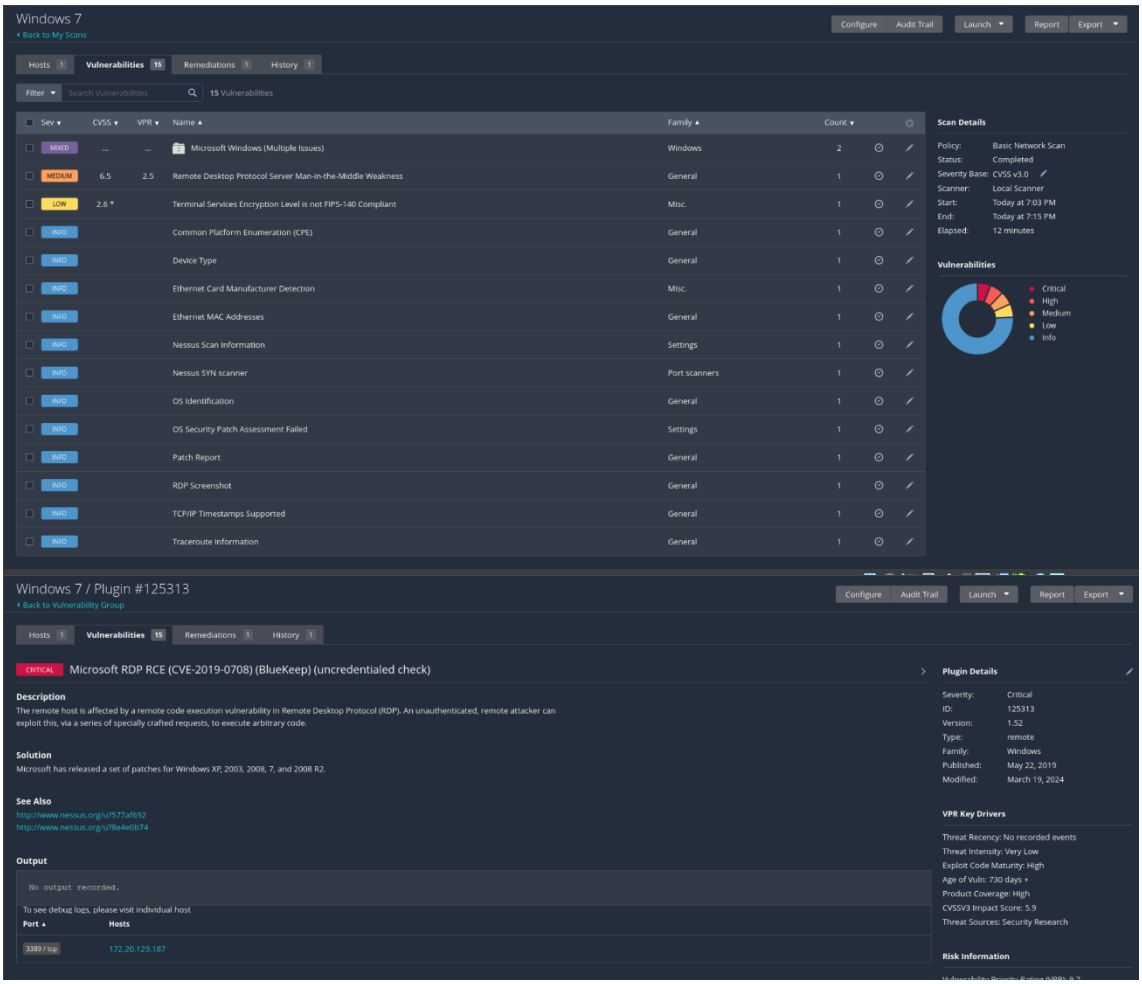
Fazendo scans autenticados é possível ver vulnerabilidades dos softwares instalados na máquina, por exemplo, foi-nos pedido para instalar o Adobe na máquina Windows 2008, fazendo o scan foi possível detetar as vulnerabilidades desse software



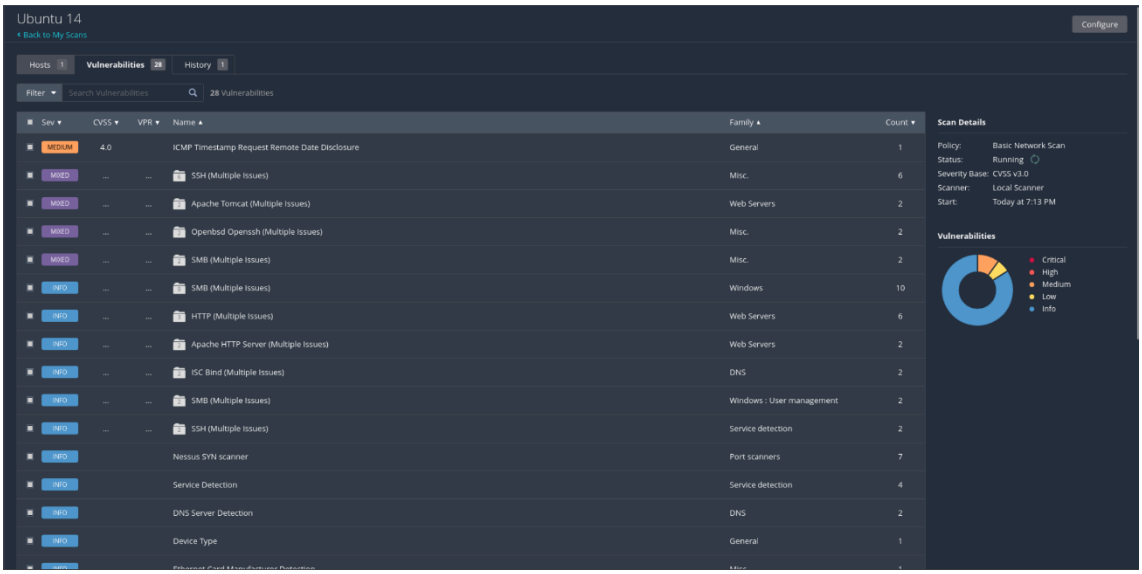


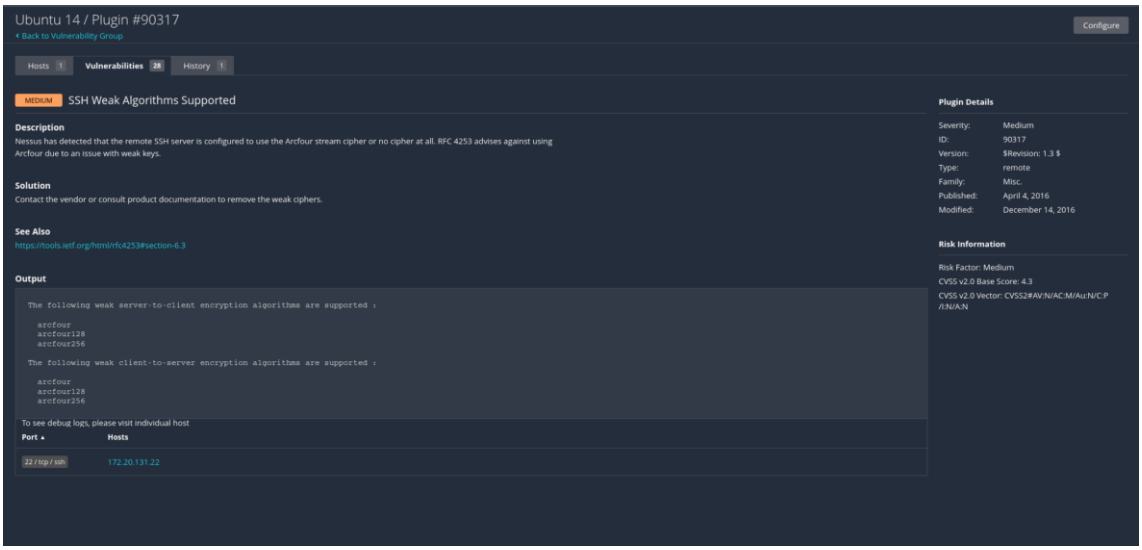
Windows 7


New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Windows 7
Description
Folder
My Scans
Targets
172.20.129.187
Upload Targets
Add File
Save
Cancel
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
CATEGORIES
Host
Filter Credentials
SSH
Windows
Windows
Authentication method
Password
Username
john
Password
Domain
Global Credential Settings
Never send credentials in the clear
For security reasons, Windows credentials are not sent in the clear by default.
Do not use NTLMv1 authentication
If this option is disabled, then it is theoretically possible to trick Nessus into attempting to log into a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a hash obtained from Nessus. This hash can be potentially cracked to reveal a username or password. It may also be used to directly log into other servers. Force Nessus to use NTLMv2 by enabling the Only use NTLMv2 setting at scan time. This prevents a hostile Windows server from using NTLM and receiving a hash. Because NTLMv1 is an insecure protocol this option is enabled by default.
Start the Remote Registry service during the scan
This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Nessus to execute some Windows local check plugins.
Enable administrative shares during the scan
This option will allow Nessus to access certain registry entries that can be read with administrator privileges.
Start the Server service during the scan
When enabled, the scanner temporarily enables the Windows Server service, which allows the computer to share files and other devices on a network. The service is disabled after the scan completes. By default, Windows systems have the Windows Server service enabled, which means you do not need to enable this setting. However, if you disable the Windows Server service in your environment, and want to scan using SMB credentials, you must enable this setting so that the scanner can access files remotely.

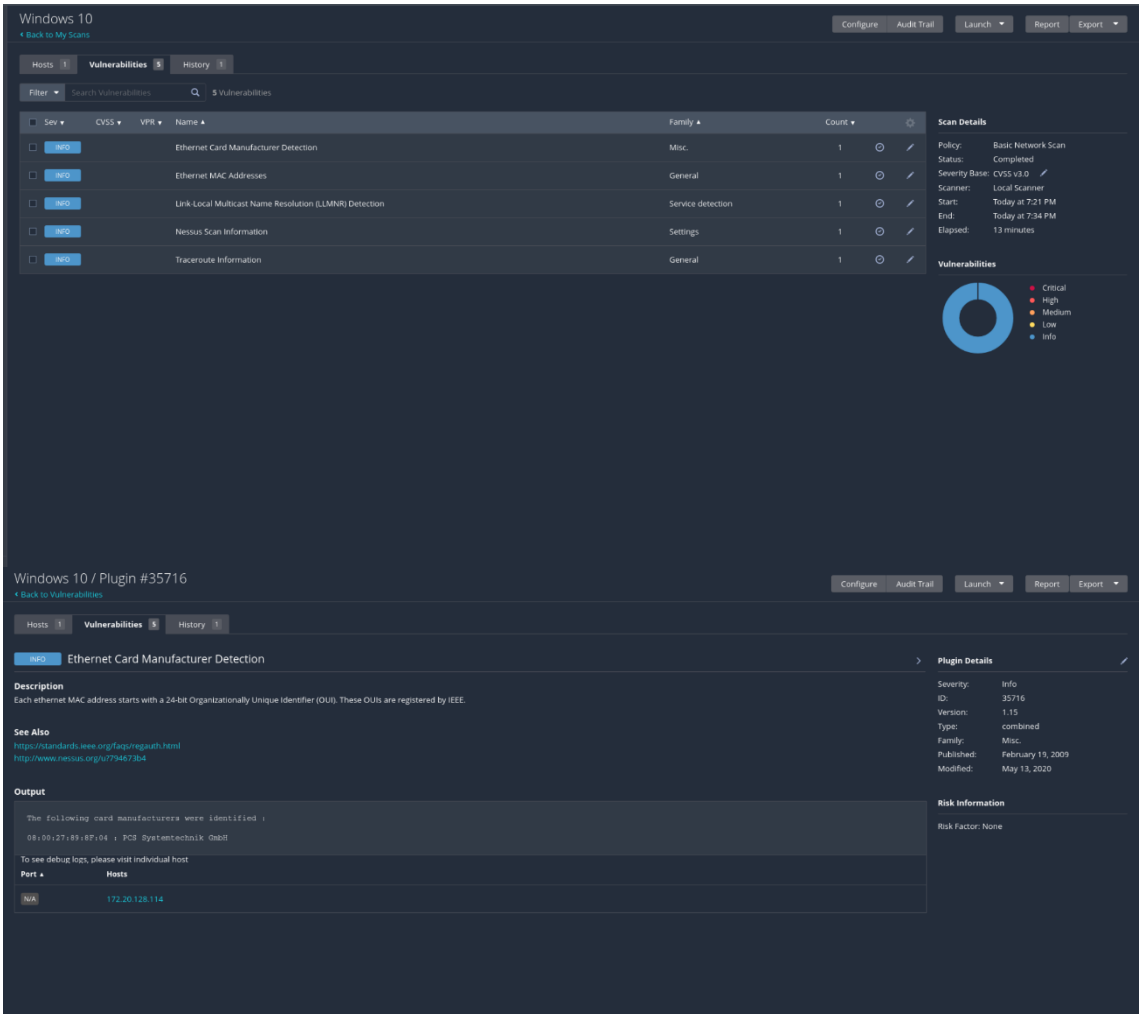

Windows 7
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 15
Remediations 1
History 1
Filter
Search Vulnerabilities
15 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MIXED Microsoft Windows (Multiple Issues) Windows 2
MEDIUM 6.5 2.5 Remote Desktop Protocol Server Man-in-the-Middle Weakness General 1
LOW 2.6 * Terminal Services Encryption Level is not FIPS-140 Compliant Misc. 1
INFO Common Platform Enumeration (CPE) General 1
INFO Device Type General 1
INFO Ethernet Card Manufacturer Detection Misc. 1
INFO Ethernet MAC Addresses General 1
INFO Nessus Scan Information Settings 1
INFO Nessus SYN scanner Port scanners 1
INFO OS Identification General 1
INFO OS Security Patch Assessment Failed Settings 1
INFO Patch Report General 1
INFO RDP Screenshot General 1
INFO TCP/IP Timestamps Supported General 1
INFO Traceroute Information General 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:03 PM
End: Today at 7:15 PM
Elapsed: 12 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Windows 7 / Plugin #125313
Back to Vulnerability Group
CRITICAL Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
Description
The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.
Solution
Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.
See Also
http://www.nessus.org/u?577af692
http://www.nessus.org/u?8e4e0b74
Output
No output recorded.
To see debug logs, please visit individual host
Port
Hosts
3389 / tcp
172.20.129.187
Plugin Details
Severity: Critical
ID: 125313
Version: 1.52
Type: remote
Family: Windows
Published: May 22, 2019
Modified: March 19, 2024
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: High
Age of Vuln: 730 days +
Product Coverage: High
CVSSV3 Impact Score: 5.9
Threat Sources: Security Research
Risk Information

Ubuntu 14.04


Ubuntu 14
Back to My Scans
Configure
Hosts 1
Vulnerabilities 28
History 1
Filter
Search Vulnerabilities
28 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MEDIUM 4.0 ICMP Timestamp Request Remote Date Disclosure General 1
MIXED SSH (Multiple Issues) Misc. 6
MIXED Apache Tomcat (Multiple Issues) Web Servers 2
MIXED Openbsd Openssh (Multiple Issues) Misc. 2
MIXED SMB (Multiple Issues) Misc. 2
INFO SMB (Multiple Issues) Windows 10
INFO HTTP (Multiple Issues) Web Servers 6
INFO Apache HTTP Server (Multiple Issues) Web Servers 2
INFO ISC Bind (Multiple Issues) DNS 2
INFO SMB (Multiple Issues) Windows : User management 2
INFO SSH (Multiple Issues) Service detection 2
INFO Nessus SYN scanner Port scanners 7
INFO Service Detection Service detection 4
INFO DNS Server Detection DNS 2
INFO Device Type General 1
Scan Details
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:13 PM
Vulnerabilities
Critical
High
Medium
Low
Info



Windows 10



Observando os scans feitos constatei que o Windows 10 tem menos vulnerabilidades que o Windows 7