

Roteiro 2 - Segurança em Sistemas Operacionais

Beatriz Muniz de Castro e Silva

Exercício 1.1.a: Descubra qual ip do seu alvo.

Utilizando o comando `arp-scan -i eth0 -l` é possível ver todos os ips conectados na rede local. Assim temos uma ideia de que a máquina possui um IP 192.168.86.-, mas pelos nomes das máquinas pode ser difícil identificar qual é a máquina específica que é o nosso alvo.

```
(root@kali)-[/home/kali]
# arp-scan -i eth0 -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:95:bd:54, IPv4: 192.168.86.33
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.86.1      44:07:0b:00:96:86      Google, Inc.
192.168.86.24    50:76:af:a7:65:fc      Intel Corporate
192.168.86.20    44:07:0b:00:96:a7      Google, Inc.
192.168.86.32    08:00:27:35:4c:c8      PCS Systemtechnik GmbH
192.168.86.26    44:07:0b:00:83:ca      Google, Inc.
192.168.86.38    44:d4:c4:56:39:11      ASUSTek COMPUTER INC.
192.168.86.54    d0:d2:b0:97:f9:20      Apple, Inc.
192.168.86.34    7c:61:66:bf:4b:1c      Amazon Technologies Inc.
192.168.86.40    50:de:06:6a:fe:78      Apple, Inc.
192.168.86.36    74:ec:b2:fb:bc:27      (Unknown)
192.168.86.25    54:13:79:1e:c5:59      Hon Hai Precision Ind. Co.,Ltd.
192.168.86.219   44:07:0b:02:e5:58      Google, Inc.
192.168.86.23    7a:a5:fe:e8:a5:d1      (Unknown: locally administered)
192.168.86.249   68:0a:e2:80:64:80      Silicon Laboratories
```

Possuindo então a informação da range em qual o IP do alvo está, podemos rodar o comando `nmap -sV 192.168.86.1-254` (range de IPs que estamos procurando) e confirmamos assim, que o IP do nosso alvo (Metasploitable) é 192.168.86.32.

```
Nmap scan report for 192.168.86.32
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
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)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:35:4C:C8 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Exercício 1.1.b: reconhecendo serviços e portas abertas do alvo.

Para descobrir o nome e versão do processo na porta 21 do alvo sem utilizar uma ferramenta de escaneamento de portas e serviços podemos usar o telnet. Para isso, devemos inserir o comando telnet 192.168.86.32 21 (comando no caso rodado no host pois no kali deu problemas de timeout).

```
C:\Users\biamc\Documents\Insper>telnet 192.168.86.32 21_
```

Isso cria uma conexão com o alvo nesta porta. Ele nos informa que o serviço que está rodando na porta 21 do alvo é o vsFTPD na versão 2.3.4.

```
C:\> Telnet 192.168.86.32
220 (vsFTPD 2.3.4)
```

Exercício 1.1.c:

Utilizando o nmap com o -O, conseguimos mais informações em relação ao sistema operacional do nosso alvo. Rodando então nmap -sV 192.168.86.32 (agora que temos o IP) -O:

```
(root@kali)~# nmap -sV 192.168.86.32 -O
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-10 01:29 EST
Nmap scan report for 192.168.86.32
Host is up (0.00078s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
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)
512/tcp   open  exec?
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:35:4C:C8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 65.76 seconds
```

Vemos que o sistema operacional do host é um Linux entre a versão 2.6.9 - 2.6.33, rodando a distribuição Debian, como evidenciado pelo processo na porta 22.

Exercício 1.1.d : Criação de Escaneamento de Portas com Python.

O arquivo em questão é o portScanner.py. Link do código: <https://github.com/Bilbia/Roteiros-TechHack/blob/main/Roteiro2/portScanner.py>. Código baseado no do site <https://www.vivaolinux.com.br/artigo/Port-Scanner-com-Python> e outras pesquisas.

Exercício 1.1.e – Listar as vulnerabilidades das portas 21 e 445

Utilizando o comando `nmap -sV -script vuln 192.168.68.109` podemos checar vulnerabilidades da máquina.

Vulnerabilidades na porta 21:

```
not shown. 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
| ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPD version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: CVE:CVE-2011-2523 BID:48539
| vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
| Shell command: id
| Results: uid=0(root) gid=0(root)
| References:
| https://www.securityfocus.com/bid/48539
| http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_
```

A porta 21 possui uma vulnerabilidade de backdoor.

Vulnerabilidades na porta 445:

```
445/tcp    open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

A porta 445 não possui vulnerabilidades

Exercício 1.1.f – Encontrar um exploit para uma vulnerabilidade nos serviços testados no exercício anterior.

A vulnerabilidade na porta 21 pode ser explorada através de um script como o encontrado no link <https://www.exploit-db.com/exploits/49757>. Ele usa a backdoor para entrar no shell do alvo.

Exercício 1.1.g – Encontrar uma CVE classificada como alta para os serviços das portas 3306 e 5432.

Uma CVE é classificada como alta quando está entre 7.0 e 8.9:

Severity	Base Score
None	0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Na porta 3306 encontramos a CVE-2009-2446 com valor 8.5 :

```

3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
| vulners:
|   cpe:/a:mysql:mysql:5.0.51a-3ubuntu5:
|   SSV:19118      8.5      https://vulners.com/seebug/SSV:19118      *EXPLOIT*
|   CVE-2009-2446  8.5      https://vulners.com/cve/CVE-2009-2446
|   SAINT:D505D53863BE216621FDAECA22896071  7.5      https://vulners.com/saint/SAINT:D505D53863BE216621FDAECA22896071      *
EXPLOIT*
|   SAINT:A9E0BE0CEF71F1F98D3CB3E95173B3D0  7.5      https://vulners.com/saint/SAINT:A9E0BE0CEF71F1F98D3CB3E95173B3D0      *
EXPLOIT*
|   SAINT:79BA92A57C28E796ADD04A6A8AE158CE  7.5      https://vulners.com/saint/SAINT:79BA92A57C28E796ADD04A6A8AE158CE      *
EXPLOIT*
|   SAINT:3101D21E4D8017EA5B14AF668DC39CAD  7.5      https://vulners.com/saint/SAINT:3101D21E4D8017EA5B14AF668DC39CAD      *
EXPLOIT*
|   PACKETSTORM:85678      7.5      https://vulners.com/packetstorm/PACKETSTORM:85678      *EXPLOIT*
|   PACKETSTORM:82247      7.5      https://vulners.com/packetstorm/PACKETSTORM:82247      *EXPLOIT*
|   MSF:EXPLOIT/WINDOWS/MYSQL/MYSQL_YASSL_HELLO  7.5      https://vulners.com/metasploit/MSF:EXPLOIT/WINDOWS/MYSQL/MYSQL_YASSL_HELLO      *EXPLOIT*
YASSL_HELLO
|   MSF:EXPLOIT/LINUX/MYSQL/MYSQL_YASSL_HELLO  7.5      https://vulners.com/metasploit/MSF:EXPLOIT/LINUX/MYSQL/MYSQL_YA

```

Na porta 5432 encontramos duas com valor alto (CVE-2010-1447 e CVE-2010-1169) além de algumas com valor críticos:

```

5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| vulners:
|   cpe:/a:postgresql:postgresql:8.3:
|   SSV:60718      10.0     https://vulners.com/seebug/SSV:60718      *EXPLOIT*
|   CVE-2013-1903  10.0     https://vulners.com/cve/CVE-2013-1903
|   CVE-2013-1902  10.0     https://vulners.com/cve/CVE-2013-1902
|   SSV:30015      8.5      https://vulners.com/seebug/SSV:30015      *EXPLOIT*
|   SSV:19652      8.5      https://vulners.com/seebug/SSV:19652      *EXPLOIT*
|   POSTGRESQL:CVE-2013-1900      8.5      https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1900
|   POSTGRESQL:CVE-2010-1169      8.5      https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1169
|   CVE-2010-1447  8.5      https://vulners.com/cve/CVE-2010-1447
|   CVE-2010-1169  8.5      https://vulners.com/cve/CVE-2010-1169
|   MSF:ILITIES/LINUXRPM-RHSA-2012-1047/  7.5      https://vulners.com/metasploit/MSF:ILITIES/LINUXRPM-RHSA-2012-1047/
EXPLOIT*
|   MSF:ILITIES/LINUXRPM-RHSA-2012-1046/  7.5      https://vulners.com/metasploit/MSF:ILITIES/LINUXRPM-RHSA-2012-1046/

```

Exercício 1.1.h - Realize uma consulta ao nome www.ietf.org, e responda:

Utilizando o nikto:

```

(root@kali)~[/home/kali]
# nikto -h http://www.ietf.org/
- Nikto v2.1.6

+ Target IP:      104.16.45.99
+ Target Hostname: www.ietf.org
+ Target Port:    80
+ Message:        Multiple IP addresses found: 104.16.45.99, 104.16.44.99
+ Start Time:     2022-03-10 02:22:59 (GMT-5)

+ Server: cloudflare
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differen
t fashion to the MIME type
+ Root page / redirects to: https://www.ietf.org/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7889 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:       2022-03-10 02:25:38 (GMT-5) (159 seconds)

+ 1 host(s) tested

```

a. Qual é o endereço IP associado?

O endereço IP associado é 104.16.45.99

b. Quais são seus servidores DNS?

IPs dos servidores através do nslookup:

```

Non-authoritative answer:
Name:      ietf.org
Addresses: 2001:1900:3001:11::2c
           4.31.198.44

```

Nameservers utilizando o comando whois ietf.org:

```
Name Server: NS0.AMSL.COM
Name Server: NS1.AMS1.AFILIAS-NST.INFO
Name Server: NS1.MIA1.AFILIAS-NST.INFO
Name Server: NS1.SEA1.AFILIAS-NST.INFO
Name Server: NS1.YYZ1.AFILIAS-NST.INFO
Name Server: NS1.HKG1.AFILIAS-NST.INFO
```

O site utiliza servidores da Cloudflare (nikto)

c. Existe algum servidor de e-mail associado ao domínio ietf.org? Qual o seu nome e IP?

Utilizando as ferramentas do site <https://dnschecker.org/>, podemos ver que o domínio possui um servidor de web com nome mail.ietf.org e IP 4.31.198.44

Result for: IETF.ORG

MAIL.IETF.ORG.	
Mx Record	mail.ietf.org.
IP	4.31.198.44 ↗
Owner: Level 3 Parent, LLC  WHOIS AS3356	
IP is not blocked by any blacklists More	

Exercício 1.1.i - Escolha um site na Internet e responda as seguintes perguntas:

Site escolhido: instructables.com

a) Quais servidores DNS são responsáveis por este domínio? (print a sua consulta)

IPs dos servidores através do comando nslookup:

```
Non-authoritative answer:
Name:   instructables.com
Addresses: 151.101.1.105
           151.101.65.105
           151.101.129.105
           151.101.193.105
```

Utilizando o comando whois instructables.com é possível ver os nameservers:

```
Name Server: ns-104.awsdns-13.com
Name Server: ns-557.awsdns-05.net
Name Server: ns-1777.awsdns-30.co.uk
Name Server: ns-1163.awsdns-17.org
```

b) Existem outros domínios ou serviços hospedados no mesmo host (IP)? Quais são?

Os outros domínios ou serviços hospedados no mesmo IP do host, 151.101.129.105 (encontrado através do nikto), são:


- cookingstartshere.com
- instructable.org
- instructables.community

- instructables.net
- instructables.org
- instructablesworkshop.com
- instructible.net
- instructible.org
- instructibles.com
- instructibles.net
- instructibles.org

Informações encontradas através do site <https://dnslytics.com/reverse-ip>

c) Qual o Servidor WEB e Sistema Operacional que hospedam este site? Quais foram as últimas alterações?

O site é hospedado pelo Fastly, como mostra o Netcraft:

Site	http://instructables.com 
Netblock Owner	Fastly
Hosting company	Fastly

E utiliza servidores web da Varnish, mas o Netcraft não consegue reconhecer qual é o sistema operacional utilizado:

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Fastly PO Box 78266 San Francisco CA US 94107	151.101.129.105	unknown	Varnish	7-Jan-2022
Fastly PO Box 78266 San Francisco CA US 94107	151.101.193.105	unknown	Varnish	6-Jan-2022
Fastly PO Box 78266 San Francisco CA US 94107	151.101.1.105	unknown	Varnish	5-Jan-2022
Fastly PO Box 78266 San Francisco CA US 94107	151.101.65.105	unknown	Varnish	4-Jan-2022
Fastly PO Box 78266 San Francisco CA US 94107	151.101.1.105	unknown	Varnish	3-Jan-2022
Fastly PO Box 78266 San Francisco CA US 94107	151.101.193.105	unknown	Varnish	2-Jan-2022
Fastly PO Box 78266 San Francisco CA US 94107	151.101.1.105	unknown	Varnish	1-Jan-2022
Fastly PO Box 78266 San Francisco CA US 94107	151.101.193.105	unknown	Varnish	13-Oct-2021
Fastly PO Box 78266 San Francisco CA US 94107	151.101.129.105	unknown	Varnish	12-Oct-2021
Fastly PO Box 78266 San Francisco CA US 94107	151.101.1.105	unknown	Varnish	11-Oct-2021

Porém dando um ping no site mostra que o TTL é de 56, o que indica que o servidor roda uma distribuição de Linux:

```
C:\Users\biamc\Documents\Inspirer>ping instructables.com

Pinging instructables.com [151.101.129.105] with 32 bytes of data:
Reply from 151.101.129.105: bytes=32 time=4ms TTL=56
Reply from 151.101.129.105: bytes=32 time=6ms TTL=56
Reply from 151.101.129.105: bytes=32 time=5ms TTL=56
Reply from 151.101.129.105: bytes=32 time=5ms TTL=56

Ping statistics for 151.101.129.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 6ms, Average = 5ms
```

d) Quais tecnologias (jquery, utilizadas por este site)?

Site Technology (fetched today)

Network

Any network related service or technology.

Technology	Description	Popular sites using this technology
Amazon Web Services - Route 53 ↗	Cloud based Domain Name System (DNS) service	

HTTP Accelerator

A web accelerator is a proxy server that reduces web site access times.

Technology	Description	Popular sites using this technology
Varnish ↗	An HTTP accelerator for web applications	www.corriere.it , www.homedepot.com , www.gov.uk

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL ↗	A cryptographic protocol providing communication security over the Internet	

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Local Storage	<i>No description</i>	www.primevideo.com , www.google.com , www.amazon.in
JavaScript ↗	Widely-supported programming language commonly used to power client-side dynamic content on websites	

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8 ↗	UCS Transformation Format 8 bit	

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
X-Content-Type-Options ↗	Browser MIME type sniffing is disabled	outlook.live.com , lfacebook.com , mail.google.com
Strict Transport Security ↗	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	en.wikipedia.org , accounts.google.com , web.whatsapp.com
Referrer Policy ↗	Restrict referrer information included in subsequent requests	www.bbc.co.uk , www.startpage.com , www.leboncoin.fr
Content Security Policy ↗	Detect and mitigate attacks in the browser	yandex.ru , vk.com , discord.com
X-XSS-Protection Block ↗	Block pages on which cross-site scripting is detected	www.paypal.com , mail.protonmail.com , mail-redir.mention.com

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5 ↗	Latest revision of the HTML standard, the main markup language on the web	

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	www.msn.com , docs.microsoft.com

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External ↗	Styles defined within an external CSS file	www.baidu.com , www.instagram.com , www.linkedin.com

e) Existe algum WAF protegendo este site? (Print a saída do comando)

Utilizando o comando wafw00f instructables.com vemos que o site não possui nenhum WAF:

```
(root@kali)-[/home/kali]
# wafw00f instructables.com

      ( Woof! )
    ,,,
  ,--'
 /  \
(    )  (    )
 \  /    \  /
  \(_)_/  \(_)_/

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://instructables.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```


f) O Domínio possui um servidor de e-mail configurado? Qual (is) Ip (s)?

O domínio utiliza servidores de email da Google:

Result for: **INSTRUCTABLES.COM**

ASPMX.L.GOOGLE.COM.

Mx Record

aspmx.l.google.com.

IP

74.125.192.27 

Owner: [Google LLC](#)  | [WHOIS](#) | [AS15169](#)

Exercício 1.1.j

Portas abertas no instructables.com (IP 151.101.129.105) (dentre as portas 0 a 300):

```
C:\Users\biamc\Documents\Inspir\TechHack\Roteiros-TechHack\Roteiro2>python3 portScanner.py
```

```
Big's Port  
Scanner
```

```
Insira um IP para ser escaneado: 151.101.129.105
```

```
Insira uma range de ports, separando com - e sem utilizar espaços (ex: 0-65535): 0-300
```

```
Escaneando o IP 151.101.129.105
```

```
A porta 80 está aberta
```

```
Serviço que está rodando na porta 80: http
```

```
Portas abertas: [80]
```

A porta 21 do site não está aberta, portanto não é possível determinar vulnerabilidades do processo já que não há nenhum rodando. Porém é comun que a porta 21 esteja rodando o processo ftp, que pode ser facilmente explorado para abrir uma backdoor ao servidor, possibilitando acesso aos arquivos e ao shell.