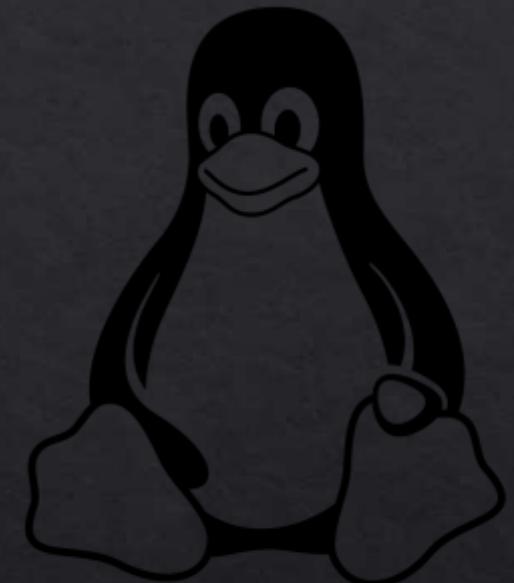


# HUNTER PENGUIN

## NO REST FOR BAD GUYS

01/12/2021

Hacker Club - Beco do Exploit



Linux

FIAP

B E C O  
D O  
E X P L O I T

B E C O  
D O  
E X P L O I T



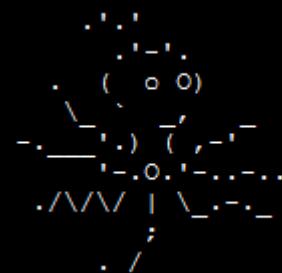
# PROJECT OCT0PS

| Fundador: C41Tx90 - Victor de Queiroz

| Inicio do projeto: 03/09/2021

## Proposta de Assuntos para a Seleção:

- [ - ] Binary Exploitation
- [ - ] Windows Internals
- [ - ] Kernel Linux
- [ - ] Reverse Engineering
- [ - ] Mobile Security
- [ - ] WEB Security
- [ - ] Wireless
- [ - ] IoT
- [ - ] ICS
- [ - ] Malware
- [ - ] Network/telecom
- [ - ] Cloud
- [ - ] Análise de Memória
- [ - ] Anti-Forense
- [ - ] OSINT
- [ - ] Exfiltração de Dados
- [ - ] Obfuscation
- [ - ] Criptografia
- [ - ] Esteganografia
- [ - ] Anonimato





HACKING  
CLUB  
BECO DO EXPLOIT

B E C O  
D O  
E X P L O I T

becodoexploit.com

## DESAFIO – 30 MÁQUINAS EM 30 DIAS

- 0x02 Edições

### PODCAT

- 1  #podCATx01 Desenvolvimento de Malware feat SALEMA {C41tx90 + SWaNk} CATx003\_ 1:05:05
- 2  #podCATx02 Mindset Ofensivo - feat Vinicius Vieira e Ulisses Alves {C41TX90 + Odisseus+V1N1V131R4} CATx003\_ 1:05:12
- 3  #podCATx03 Anti-forense - Feat Eder {C41Tx90 + ΣΔΞÎR Lu1D1} CATx003\_ 57:13
- 4  #podCATx04 Espionagem e Hardware Hacking - Feat Julio Della Flora {C41Tx90 + JULIODELLAFLORA} CATx003\_ 2:10:06

<https://www.youtube.com/c/CATx003/>

[HTTPS://T.ME/BECODOXPL](https://t.me/becodoxpl)



## BECO DO EXPLOIT

[www.becodoexploit.com](http://www.becodoexploit.com)

### EMAIL

[contato@becodoexploit.com](mailto:contato@becodoexploit.com)

### TELEGRAM

[t.me/becodoxpl](https://t.me/becodoxpl)

# SEXTA HACK NO BECO

/\*TODA SEXTA\*/

**B E C O  
D O  
E X P L O I T**

TODA SEXTA AS 24H OU SABADO AS  
00H , VOCÊ QUEM MANDA.

TRAGA SUA BEBIDA

VENHA JOGAR UM CTF OU BATER UM PAPO OU QUALQUER  
COISA QUE ESTIVER ROLANDO...

COMEÇA AS 00H

# \$ CAT .AGENDA

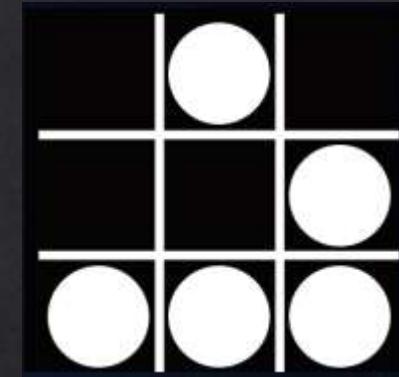
- ❖ Disclaimer && whoami && objetivo
- ❖ Contexto
- ❖ Filesystem Hierarchy Standard
- ❖ Gerenciamento e Processamento de logs;
- ❖ A linguagem dos daemons (Serviços);
- ❖ Buscando Anomalias;
  - ❖ Anomalias no FileSystem, how detect and evade
  - ❖ Anomalias em arquivos de log: Detectando ataques
  - ❖ Padrão em arquivos
- ❖ Automação do processo (IDS, IPS)
- ❖ The next level
- ❖ Time to play

# ./DISCLAIMER

- ❖ I don't speak on behalf of my employer.
- ❖ All the ideas and information presented here are from myself.
- ❖ All the external documents, images and papers referenced here will be linked on “References”, a big thanks for the security professionals and they researches.
- ❖ I do not take any responsibility for the usage of this documentation for improper ends.

# MORE ~/.PROFILE

- ❖ Real Name: Felippe Foppa
- ❖ Area de atuação: Redteamer, Pentester and Security Researcher
- ❖ Current Role: Especialista de Segurança Ofensiva na GlobalHitss
- ❖ Certifications: LPI1, LPI2, OSCP, CRTP, eWPTXv2, ISO27k, ITILv4
- ❖ CVE's: 2021-39375, 2021-39376
- ❖ Blog: <https://diesec.home.blog/>
- ❖ Linkedin: <https://www.linkedin.com/in/felippe-foppa-6b1434108/>
- ❖ Github: <https://github.com/d34dfr4m3>
- ❖ Material da Palestra vai ser compartilhado em:
  - ❖ <https://github.com/d34dfr4m3/Contributions/>



# echo \$OBJETIVO

- ❖ Essa talk não tem como objetivo aprofundar em temas de auditoria de ambientes Linux, resposta à incidente, forense ou threat hunting.
- ❖ A expectativa, é que no pouco tempo de duração de agenda, os participantes obtenham os insumos necessários para entender alguns aspectos de serviços, o papel dos logs, buscar por anomalias que podem revelar potenciais ameaças e melhores práticas de escalabilidade do processo de monitoramento/auditoria.
- ❖ Vendor Free!
- ❖ Distro Free!

# Contexto

Porque Linux é relevante?

Best operating system for hack

[Todas](#) [Notícias](#) [Vídeos](#) [Shopping](#) [Imagens](#) [Mais](#)

Aproximadamente 68.400.000 resultados (0,74 segundos)

**Top 10 Operating Systems for Ethical Hackers and Penetration Testers (2024)**

- Kali Linux. ...
- BackBox. ...
- Parrot Security Operating System. ...
- DEFT Linux. ...
- Network Security Toolkit. ...
- BlackArch Linux. ...
- Cyborg Hawk Linux. ...
- GnackTrack.

[Mais itens...](#)

why linux is |

Why Linux Is Better For Programming  
Cancão

why linux is **better than windows**

why linux is **faster than windows**

why linux is **best for developers**

why linux is **not unix**

why linux is **portable**

why linux is **case sensitive**

why linux is **more secure**

why linux is **more secure than windows**

why linux is **virus free**

Nota Importante: Linux não é vírus free....



8 https://www.quickstart.com/blog/why-linux-runs-90-percent-of-the-public-cloud-workload/

Looking to accelerate your career growth and increase your income?

## Why Linux Runs 90 percent of the Public Cloud Workload

March 03, 2020 | Author: Faisal Khwaja



Right now, Linux is one of the most powerful operating systems dominating clouds and servers all over the globe. As of 2019, 100% of the supercomputers in the world were operated by Linux. The percentage might seem hard to believe, but research has proven this to be true. It does not just end here! Out of every 25 websites, 23 are using Linux, and this further strengthens the credibility of Linux. It is the number one choice for the best cloud hosts today, and it is continuously making waves around the globe.

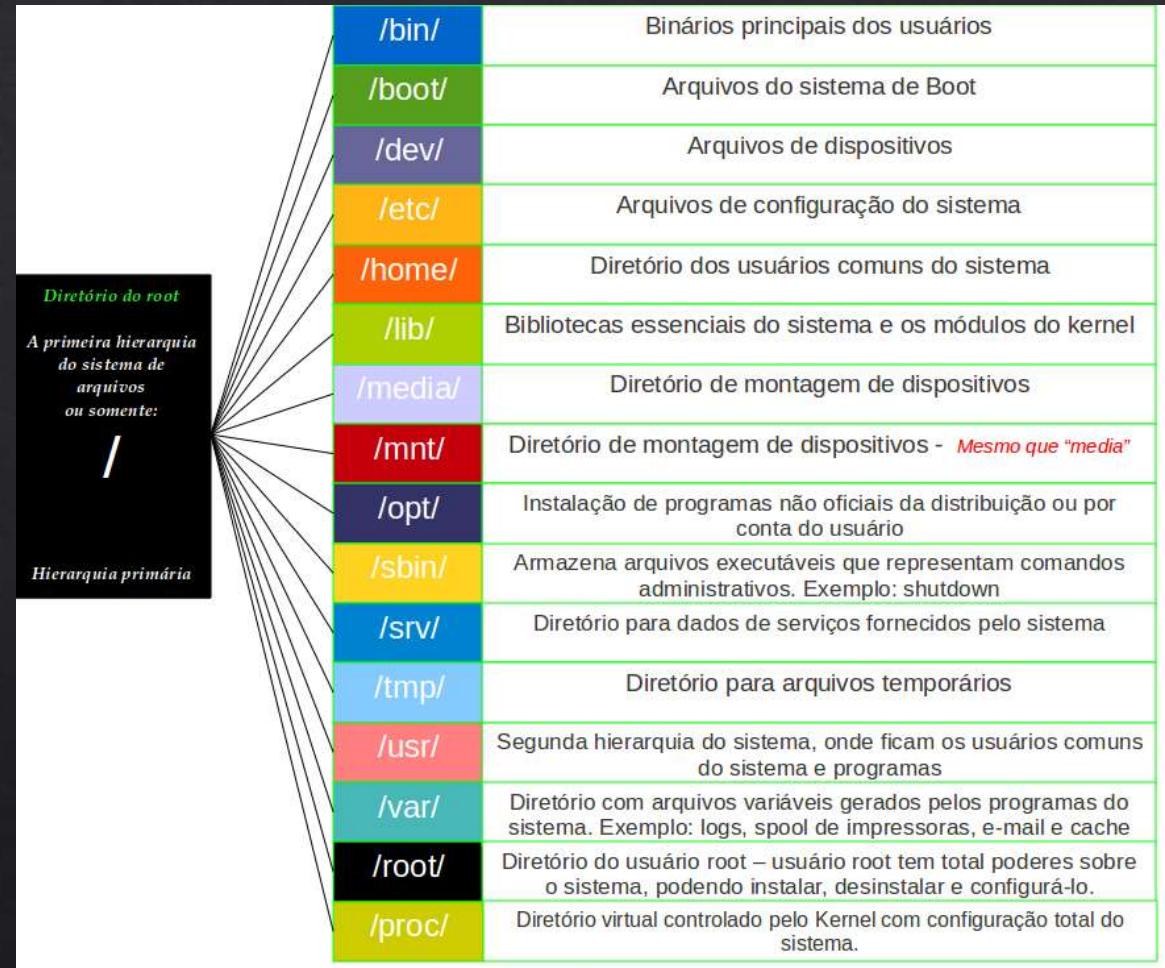
<https://www.quickstart.com/blog/why-linux-runs-90-percent-of-the-public-cloud-workload/>

# FILESYSTEM HIERARCHY STANDARD

Visão Geral

# Filesystem Hierarchy Standard

- ❖ O Filesystem Hierarchy Standard (padrão para sistema de arquivos hierárquico), ou FHS, **define os principais diretórios, e o seu conteúdo, em um sistema operacional** Linux ou do tipo Unix. A versão atual é a 3.0, anunciada em 3 de junho de 2015
- ❖ O FHS é mantido pela **Linux Foundation**, uma organização sem fins lucrativos formada por importantes empresas de hardware e software, como HP, Red Hat, IBM e Dell.
- ❖ Ainda hoje, algumas maioria das distribuições Linux, incluindo membros da Linux Foundation, não adotam o padrão proposto. Em particular, diretórios (paths) criados pelo FHS, como o /srv/, não foram adotados em grande escala. Alguns sistemas Unix e Linux rompem com o padrão FHS.
- ❖ [https://pt.wikipedia.org/wiki/Filesystem\\_Hierarchy\\_Standard](https://pt.wikipedia.org/wiki/Filesystem_Hierarchy_Standard)



[https://samthngs.files.wordpress.com/2017/11/hierarquia\\_linux.png](https://samthngs.files.wordpress.com/2017/11/hierarquia_linux.png)

# Gerenciamento de log

Visão Geral

# Logs everywhere

- ◊ Os logs do Linux fornecem uma linha de tempo dos eventos para o kernel Linux, aplicativos e sistema e são uma valiosa ferramenta de solução de problemas quando você encontra problemas. Essencialmente, a análise de arquivos de log é a primeira coisa que um administrador precisa fazer quando um problema é descoberto.
- ◊ Para problemas específicos do aplicativo da área de trabalho, os arquivos de log são escritos em locais diferentes. Por exemplo, o Chrome grava relatórios de falhas em ‘`~/.chrome/Crash Reports`’.
- ◊ Os arquivos são armazenados em texto simples e podem ser encontrados no diretório `/var/log` e subdiretório. Existem logs do Linux para tudo (que tenha minimo de boas práticas): sistema, kernel, gerenciadores de pacotes, processos de inicialização, Xorg, Apache, MySQL.

# Linux log Files and Usage

- ❖ /var/log/messages : General message and system related stuff
- ❖ /var/log/auth.log : Authentication logs
- ❖ /var/log/kern.log : Kernel logs
- ❖ /var/log/cron.log : Crond logs (cron job)
- ❖ /var/log/maillog : Mail server logs
- ❖ /var/log/qmail/ : Qmail log directory (more files inside this directory)
- ❖ /var/log/httpd/ : Apache access and error logs directory
- ❖ /var/log/lighttpd/ : Lighttpd access and error logs directory
- ❖ /var/log/nginx/ : Nginx access and error logs directory
- ❖ /var/log/apt/ : Apt/apt-get command history and logs directory
- ❖ /var/log/boot.log : System boot log
- ❖ /var/log/mysqld.log : MySQL database server log file
- ❖ /var/log/secure or /var/log/auth.log : Authentication log
- ❖ /var/log/utmp or /var/log/wtmp : Login records file
- ❖ /var/log/yum.log or /var/log/dnf.log: Yum/Dnf command log file.

# Utilitários de Console

- ❖ less command
- ❖ more command
- ❖ cat command
- ❖ grep command
- ❖ tail command
- ❖ zcat command
  - ❖ Arquivos comprimidos em gzip
- ❖ zgrep command
  - ❖ Procura padrões (regex) em arquivos comprimidos
- ❖ zmore command
- ❖ dmesg command
- ❖ journalctl command

# Exemplos

- ❖ # less /var/log/messages
- ❖ # more -f /var/log/messages
- ❖ # cat /var/log/messages
- ❖ # tail -f /var/log/messages
- ❖ # grep -i error /var/log/messages
- ❖ # head -n 10 /var/log/messages
- ❖ # tac /var/log/messages | head -n 10

# Printing the Linux kernel ring buffer messages

- ❖ sudo dmesg
- ❖ sudo dmesg | grep 'error'
- ❖ sudo dmesg | grep -i -E 'error|warn|failed'
- ❖ sudo dmesg | more

# How it works, exactly?

- ❖ Os **daemons de log** do sistema **registram as mensagens de saída do kernel (klogd)** e **sistema (syslogd)** nos arquivos em `/var/log` .
- ❖ Syslogd : Este daemon **controla o registro de logs do sistema**.
- ❖ Klogd: **Este daemon controla o registro de mensagens do kernel**. Ele monitora as mensagens do kernel e as envia para o daemon de monitoramento syslogd, por padrão.
- ❖ Journalctl: é um core do systemd, portanto, é instalado automaticamente em qualquer sistema operacional usando o systemd. O **Journal fornece registro estruturado e indexado, enquanto fornece um certo grau de compatibilidade** com implementações clássicas de syslog.
- ❖ A principal diferença é que o journal, além de outras ferramentas baseadas em syslog é que ele **armazena logs ou mensagens em formato binário**, que não pode ser lido por humanos. Os logs do journal são geralmente processados pela aplicação journalctl

# Log Levels

- ❖ Um nível de log ou gravidade de log é uma informação que indica a importância de uma determinada mensagem de log. É uma maneira simples, mas muito poderosa, de distinguir eventos de log entre si. Se os níveis de log forem usados corretamente em seu aplicativo, tudo o que você precisa é examinar primeiro a gravidade. Ele dirá se você pode continuar dormindo durante a noite de plantão ou se precisa pular da cama imediatamente e bater outro recorde pessoal ao correr entre o quarto e o laptop.
- ❖ O Syslog surgiu com a ideia dos níveis de criticidade, que agora são definidos no padrão syslog. O Syslog vem com os seguintes níveis de criticidade:
  - ❖ Emergency – Sistema inutilizável
  - ❖ Alert – Ações devem ser tomadas imediatamente
  - ❖ Critical – Condições de operação em níveis críticos
  - ❖ Error – Erros não críticos
  - ❖ Warning – Condições de alertas que devem ser tratadas.
  - ❖ Notice - Nível normal de log, eventos significantes
  - ❖ Informational – Informativo, não requer ações
  - ❖ Debug – Exibido pelo kernel se for habilitado.

# Meet Logger

- ❖ Este comando permite enviar uma mensagem nos log do sistema. A mensagem é enviada aos logs via daemon syslogd ou via soquete do sistema, é possível especificar a prioridade, nível, um nome identificando o processo, etc. Seu uso é muito útil em shell scripts ou em outros eventos do sistema.

```
logger -p kern.emerg KERNEL PANIC, DONT LET ME DIE. just kidding bro
```

```
Jan 7 23:06:19 masterslave-dns centos: KERNEL PANIC, DONT LET ME DIE. just kidding bro
```

# Collateral Effect: Disk usage - Logrotate

- ❖ Usado para fazer backups dos logs atuais do sistema (programado via cron, ou outro daemon com a mesma função) e criando novos arquivos de logs que serão usados pelo sistema. Opcionalmente os arquivos de logs antigos serão compactados para diminuir a utilização de espaço em disco ou enviados por e-mail ao administrador. A rotação dos arquivos de logs proporciona maior agilidade quando precisamos encontrar algum detalhe útil (que seria mais difícil de se achar em um arquivo de log de 10MB ou maior).
- ❖ /etc/logrotate.conf

# Entendendo os Daemons

Apache2 Logs

# Apache2 Case

## Common Log Format

A typical configuration for the access log might look as follows.

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common  
CustomLog logs/access_log common
```

This defines the *nickname* `common` and associates it with a particular log format string. The format string consists of percent characters (%), which are replaced by specific information about each request. The quote character ("") must be escaped by placing a backslash before it. It also includes escape sequences for new-line (\n) and tab (\t).

The `CustomLog` directive sets up a new log file using the defined *nickname*. The filename for the access log is relative to the server's working directory.

The above configuration will write log entries in a format known as the Common Log Format (CLF). This standard format can produce output like this:

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

<https://httpd.apache.org/docs/2.4/logs.html>

- ❖ 127.0.0.1 (%h) - This is the IP address of the client (remote host)
- ❖ (%l) - Identity of the client determined by identd on the clients machine; (Highly unreliable)
- ❖ frank (%u) - This is the userid of the person requesting the document as determined by HTTP authentication
- ❖ (%>r%) – The request
- ❖ 200 (%>s) - This is the status code that the server sends back to the client
- ❖ 2326 (%b) - The last part indicates the size of the object returned to the client

# Buscando Anomalias

Daemons e FileSystem

# The Pattern Finder

- ❖ A09:2021 – Security Logging and Monitoring Failures
- ❖ Manipulação de arquivos
  - ❖ Buscando anomalias em logs, ataques de força bruta de diretórios, tentativas de autenticação etc.
  - ❖ Buscando divergência de padrão
  - ❖ Utilitários (wc, find, sort, uniq, cut, sed etc)
- ❖ Filesystem
  - ❖ Caçando alterações no disco, cenário de pós exploração.
  - ❖ Utilitários (Stat, touch, find)

# A09:2021 – Security Logging and Monitoring Failures

The screenshot shows a web browser displaying the OWASP Top 10 2021 page for category A09. The title bar reads "A09 Security Logging and Monitoring Failures". The main content area starts with a brief description: "expands beyond CWE-778 Insufficient Logging to include CWE-117 Improper Output Neutralization for Logs, CWE-223 Omission of Security-relevant Information, and CWE-532 Insertion of Sensitive Information into Log File." Below this is a section titled "Description" which states: "Returning to the OWASP Top 10 2021, this category is to help detect, escalate, and respond to active breaches. Without logging and monitoring, breaches cannot be detected. Insufficient logging, detection, monitoring, and active response occurs any time:". To the right of this text is a vertical sidebar with several links: "Table of Contents", "Factors", "Overview", "Description", "How to Detect", "Examples", "References", and "List of References". At the bottom of the content area is a bulleted list of eight items describing specific failure types:

- Auditable events, such as logins, failed logins, and high-value transactions, are not logged.
- Warnings and errors generate no, inadequate, or unclear log messages.
- Logs of applications and APIs are not monitored for suspicious activity.
- Logs are only stored locally.
- Appropriate alerting thresholds and response escalation processes are not in place or effective.
- Penetration testing and scans by dynamic application security testing (DAST) tools (such as OWASP ZAP) do not trigger alerts.
- The application cannot detect, escalate, or alert for active attacks in real-time or near real-time.

# A09:2021 – Security Logging and Monitoring Failures

The screenshot shows a web browser displaying the OWASP Top 10 2021 page for A09: Security Logging and Monitoring Failures. The URL in the address bar is [https://owasp.org/Top10/pt\\_BR/A09\\_2021-SecurityLogging\\_and\\_Monitoring\\_Failures](https://owasp.org/Top10/pt_BR/A09_2021-SecurityLogging_and_Monitoring_Failures). The page has a blue header with the title "A09 Security Logging and Monitoring Failures". Below the header, there is a sub-header "or an attacker (see A01:2021-Broken Access Control)". The main content section is titled "How to Prevent" and contains a bulleted list of eight items providing guidance on how to prevent these failures. At the bottom of the page, there is a note about commercial and open-source application protection frameworks.

or an attacker (see A01:2021-Broken Access Control).

## How to Prevent

Developers should implement some or all the following controls, depending on the risk of the application:

- Ensure all login, access control, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts and held for enough time to allow delayed forensic analysis.
- Ensure that logs are generated in a format that log management solutions can easily consume.
- Ensure log data is encoded correctly to prevent injections or attacks on the logging or monitoring systems.
- Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.
- DevSecOps teams should establish effective monitoring and alerting such that suspicious activities are detected and responded to quickly.
- Establish or adopt an incident response and recovery plan, such as National Institute of Standards and Technology (NIST) 800-61r2 or later.

There are commercial and open-source application protection frameworks such as the OWASP ModSecurity Core Rule Set, and open-source log correlation software, such as the Elasticsearch, Logstash, Kibana (ELK) stack, that feature custom dashboards and alerting.

# HTTP Status Code

A screenshot of a web browser displaying the MDN Web Docs page for HTTP Status Codes. The URL in the address bar is <https://developer.mozilla.org/pt-BR/docs/Web/HTTP>Status>. The page title is "HTTP Status Code". In the top left, there are navigation icons for back, forward, and refresh. On the right side of the header are a star icon and a "Change language" button. Below the header, there is a note: "This page was translated from English by the community. Learn more and join the MDN Web Docs community." A "Table of contents" link is also present. The main content features a large, bold heading "Códigos de status de respostas HTTP". Below it, a text block states: "Os códigos de *status* das respostas HTTP indicam se uma requisição HTTP foi corretamente concluída. As respostas são agrupadas em cinco classes:" followed by a numbered list of five categories. At the bottom, a note says: "Os status abaixo são definidos pela [seção 10 da RFC 2616](#). Você pode encontrar uma versão atualizada da especificação na [RFC 7231](#).

## Códigos de status de respostas HTTP

Os códigos de *status* das respostas HTTP indicam se uma requisição HTTP foi corretamente concluída. As respostas são agrupadas em cinco classes:

1. Respostas de informação ( 100 - 199 ),
2. Respostas de sucesso ( 200 - 299 ),
3. Redirecionamentos ( 300 - 399 )
4. Erros do cliente ( 400 - 499 )
5. Erros do servidor ( 500 - 599 ).

Os status abaixo são definidos pela [seção 10 da RFC 2616](#). Você pode encontrar uma versão atualizada da especificação na [RFC 7231](#).

# Apache2 (Web Server) Case – Attack Types

- ◊ Negação de Serviço baseado em consumo de recursos;
  - ◊ Problema de Frequência de iteração ou CWE-799 (<https://cwe.mitre.org/data/definitions/799.html>)
- ◊ Ataques de força bruta em autenticação de usuários;
  - ◊ Frequência de Iteração? Sim, além disso, HTTP STATUS CODE? PICK ONE! 40X? 401? 403?
- ◊ Enumeração de Diretórios (Força Bruta);
  - ◊ Frequência de Iteração? Sim, além disso? HTTP STATUS CODEE? PICK ONE! GO 3.2.1
- ◊ Injeção de SQL (A1:2017) (A3:2021)
  - ◊ Frequência de Iteração? Sim, mas não, além disso?
- ◊ Cross Site Script (A7:2017) (A3:2021)
  - ◊ Answer this question really quick

# Apache2 (Web Server) Case - BadRobots?

- ◊ Metadados de Ferramentas
- ◊ User Agents?!
- ◊ Quais anomalias podemos ver?

```
operador@remember:~$ sudo nmap -sS -sV --script=http-enum.nse 192.168.1.8
Starting Nmap 7.60 ( https://nmap.org ) at 2021-11-30 22:10 -03
Nmap scan report for 192.168.1.8
Host is up (0.0088s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:15:5D:42:E1:08 (Microsoft)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

p.org/book/nse.html)"
192.168.1.70 - - [01/Dec/2021:01:11:08 +0000] "GET /xGB/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.70 - - [01/Dec/2021:01:11:08 +0000] "GET /xml/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.70 - - [01/Dec/2021:01:11:08 +0000] "GET /XSL/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.70 - - [01/Dec/2021:01:11:08 +0000] "GET /xtemp/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.70 - - [01/Dec/2021:01:11:08 +0000] "GET /xymon/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.70 - - [01/Dec/2021:01:11:08 +0000] "GET /zb41/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.1.70 - - [01/Dec/2021:01:11:08 +0000] "GET /zipfiles/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

# Apache2 (Web Server) Case - BadRobots?

- ❖ Pelo menos 3?!

```
p.org/book/nse.html)"
192.168.1.70 -- [01/Dec/2021:01:11:08 +0000] "GET /xGB/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org
/book/nse.html)"
192.168.1.70 -- [01/Dec/2021:01:11:08 +0000] "GET /xml/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org
/book/nse.html)"
192.168.1.70 -- [01/Dec/2021:01:11:08 +0000] "GET /XSL/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org
/book/nse.html)"
192.168.1.70 -- [01/Dec/2021:01:11:08 +0000] "GET /xtemp/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.o
rg/book/nse.html)"
192.168.1.70 -- [01/Dec/2021:01:11:08 +0000] "GET /xymon/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.o
rg/book/nse.html)"
192.168.1.70 -- [01/Dec/2021:01:11:08 +0000] "GET /zb41/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nma
p.org/book/nse.html)"
192.168.1.70 -- [01/Dec/2021:01:11:08 +0000] "GET /zipfiles/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nma
```

# Apache2 (Web Server) Case - BadRobots?

## ❖ DirSearch?

```
operador@remember:~$ dirsearch -u http://192.168.1.8 -e
dirsearch v0.3.8
Extensions: [ | HTTP method: get | Threads: 10 | Error Log: /opt/dirsearch/logs/errors-21-11-30_21-34-14.log | Target: http://192.168.1.8 | Starting: [22:34:13] Starting:
[22:34:14] 403 - 276B - ./hta
[22:34:14] 403 - 276B - ./ht_wsr.txt
[22:34:14] 403 - 276B - ./htaccess-dev
[22:34:14] 403 - 276B - ./htaccess-marco
[22:34:14] 403 - 276B - ./htaccess-local
[22:34:14] 403 - 276B - ./htaccess_BAK
[22:34:14] 403 - 276B - ./htaccess.old
[22:34:14] 403 - 276B - ./htaccess.bak1
[22:34:14] 403 - 276B - ./htaccess.orig
[22:34:14] 403 - 276B - ./htaccess.sample
[22:34:14] 403 - 276B - ./htaccess.save
[22:34:14] 403 - 276B - ./htaccess.txt
[22:34:14] 403 - 276B - ./htaccess_extra
[22:34:14] 403 - 276B - ./htaccess_orig
[22:34:14] 403 - 276B - ./htaccess_sc
[22:34:14] 403 - 276B - ./htaccessBAK
[22:34:14] 403 - 276B - ./htaccessOLD
[22:34:14] 403 - 276B - ./htaccess-
[22:34:14] 403 - 276B - ./htaccessOLD2
[22:34:14] 403 - 276B - ./htgroup
[22:34:14] 403 - 276B - ./htpasswd-old
[22:34:14] 403 - 276B - ./htpasswd-test
[22:34:14] 403 - 276B - ./htusers
[22:34:14] 403 - 276B - ./index.html
[22:34:28] 200 - 11KB - /index.html
, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /xmlrpc.php HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /xmlrpc_server.php HTTP/1.1" 404 488 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /xphpMyAdmin/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /xsl/ HTTP/1.1" 404 453 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /xsl/_common.xsl HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /XSQLConfig.xml HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /yaml.log HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /xsl/common.xsl HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /yaml_cron.log HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /yonetici HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /xsql/lib/XSQLConfig.xml HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /yonetici.html HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /yonetici.php HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /yonetim HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:34:39 +0000] "GET /yonetim.html HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1468.0 Safari/537.36"
```

# Apache2 (Web Server) Case – SQL Injection?

- ❖ Sqlmap?

```
Gecko) Chrome/28.0.1468.0 Safari/537.36"
192.168.1.70 - - [01/Dec/2021:01:39:08 +0000] "GET / HTTP/1.1" 200 3440 "-" "sqlmap/1.4.7.25#dev (http://sqlmap.org)"
192.168.1.70 - - [01/Dec/2021:01:39:09 +0000] "GET /?PnWd=5852%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%
2%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..
2F..%2Fetc%2Fpasswd%27%29%23 HTTP/1.1" 200 3440 "-" "sqlmap/1.4.7.25#dev (http://sqlmap.org)"
192.168.1.70 - - [01/Dec/2021:01:39:09 +0000] "GET / HTTP/1.1" 200 3440 "-" "sqlmap/1.4.7.25#dev (http://sqlmap.org)"
```

# Apache2 (Web Server) Case – SQL Injection?

## ❖ SQL Injection Signatures?

```
202FHY HTTP/1.1" 404 453 "-" "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%20NULL%2CNULL%20NULL%2CNULL%2CNULL%2C  
NULL--%20Bech HTTP/1.1" 404 453 "-" "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%20NULL%2CNULL%20NULL%2CNULL%2C  
NULL%2CNULL--%20B0SP HTTP/1.1" 404 453 "-" "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20ORDER%20BY%201--%201Joo HTTP/1.1" 404 453 "-" "sqlmap/1.4.7.25#dev (http://sqlmap.  
org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20ORDER%20BY%201--%201Joo HTTP/1.1" 404 453 "-" "sqlmap/1.4.7.25#dev (http://sqlmap.  
org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL--%20pW12 HTTP/1.1" 404 453 "-" "sqlmap/1.4.7.25#dev (h  
ttp://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL--%20evng HTTP/1.1" 404 453 "-" "sqlmap/1.4.7.25  
#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL--%20l4uz HTTP/1.1" 404 453 "-" "sqlmap/1.  
4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL--%20mhzk HTTP/1.1" 404 453 "-" "s  
qlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL--%20ppUj0 HTTP/1.1" 404 453  
"- "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL--%20dxFy HTTP/1.1"  
404 453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL--%20grov HT  
T/1.1" 404 453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL--%20200  
$0 HTTP/1.1" 404 453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2C  
NULL--%20fRm HTTP/1.1" 404 453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL--%20X0FFI  
HTTP/1.1" 404 453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20ORDER%20BY%201--%20kbH1 HTTP/1.1" 404 453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.org  
)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20ORDER%20BY%204279--%20qubv HTTP/1.1" 404 453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.  
org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20UNION%20ALL%20SELECT%20NULL--%206fnt HTTP/1.1" 404 453 "- "sqlmap/1.4.7.25#dev (ht  
tp://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20UNION%20ALL%20SELECT%20NULL%2CNULL--%20Pkyb HTTP/1.1" 404 453 "- "sqlmap/1.4.  
7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL--%20ewQ HTTP/1.1" 404 453 "- "sql  
map/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL--%20oyz HTTP/1.1" 404 453 "- "sql  
map/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL--%20FEM HTTP/1.1" 404 453 "- "sql  
map/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL--%20ed0f HTTP/1.1" 404  
453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL--%20je1p HTTP/1.  
1" 404 453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL--%20B0BG  
HTTP/1.1" 404 453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL--%20ueX  
HTTP/1.1" 404 453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.org)"  
192.168.1.70 - - [01/Dec/2021:01:40:23 +0000] "GET /id=1%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2C  
NULL--%20CapP HTTP/1.1" 404 453 "- "sqlmap/1.4.7.25#dev (http://sqlmap.org)"
```

# Apache2 (Web Server) Case – SQL Injection?

- ❖ GET Parameters Example
- ❖ Estou sendo atacado?

- ❖ grep -iE "select|table|union" /var/log/apache2/access.log --color

- ❖ Quantas tentativas?
  - ❖ wc -l
- ❖ E de onde vem?
  - ❖ cut -d ' ' -f 1 | uniq -c

```
[root@fiap-linux-websrv:~# grep -iE "select|table|union" /var/log/apache2/access.log --color | wc -l
102
root@fiap-linux-websrv:~#
```

```
[root@fiap-linux-websrv:~# grep -iE "select|table|union" /var/log/apache2/access.log --color | cut -d ' ' -f 1 | uniq -c
102 192.168.1.70
...]
```

# Apache2 (Web Server) Case – XSS?

- ❖ GET Parameters Example
  - ❖ Signature?

# Apache2 (Web Server) Case – XSS?

- ❖ GET Parameters Example
  - ❖ Grep -iE “onhelp|alert|<script|<|>” /var/log/apache2/access.log

# Apache2 (Web Server) Case – Sentindo Falta de Algo?!

- ❖ E como fica o POST?
- ❖ Não é logado por default no Apache2.....
- ❖ Wait what?
  - ❖ a2enmod dump\_io
- ❖ Melhor solução? Nah.

# SSH Case

- ❖ Caçando ataques de força bruta.
- ❖ grep "Failed password" /var/log/auth.log
- ❖ egrep "Failed|Failure" /var/log/auth.log

```
Dec  1 01:59:37 fiap-linux-websrv sshd[3003]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.70 user=operador
Dec  1 01:59:39 fiap-linux-websrv sshd[3003]: Failed password for operador from 192.168.1.70 port 37394 ssh2
Dec  1 01:59:45 fiap-linux-websrv sshd[3003]: message repeated 2 times: [ Failed password for operador from 192.168.1.70 port 37394 ssh2]
Dec  1 01:59:45 fiap-linux-websrv sshd[3003]: Connection closed by authenticating user operador 192.168.1.70 port 37394 [preauth]
Dec  1 01:59:45 fiap-linux-websrv sshd[3003]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.70 user operador
Dec  1 01:59:48 fiap-linux-websrv sshd[3006]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.70 user=operador
Dec  1 01:59:50 fiap-linux-websrv sshd[3006]: Failed password for operador from 192.168.1.70 port 37396 ssh2
Dec  1 01:59:56 fiap-linux-websrv sshd[3006]: message repeated 2 times: [ Failed password for operador from 192.168.1.70 port 37396 ssh2]
Dec  1 01:59:56 fiap-linux-websrv sshd[3006]: Connection closed by authenticating user operador 192.168.1.70 port 37396 [preauth]
Dec  1 01:59:56 fiap-linux-websrv sshd[3006]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.70 user operador
root@fiap-linux-websrv:~#
```

<https://security.stackexchange.com/questions/110706/am-i-experiencing-a-brute-force-attack>  
<https://linoxide.com/enable-sshd-logging/>

# Tools

- ❖ wc
- ❖ sort
- ❖ uniq
- ❖ sed
- ❖ cut
- ❖ Regex (egrep) (grep -E) (<https://regex101.com/>)

# FileSystem - Hunting

- ❖ Find, algumas dicas, mas o caminho é sempre rtfm

```
# Identificando arquivos com 777
find . -type f -perm 0777 -print
# Sticky Bit Files (551)
find / -perm 1551
# SUID Files
find / -perm /u=s
# Read-Only Files
find / -perm /u=r
# Executable Files
find / -perm /a=x
```

```
# Seek and destroy
find . -type f -name "*.txt" -exec rm -f {} \;
# Files from user
find / -user fiapstudent
# Files from group
find /home -group developer
```

# FileSystem - Hunting

- ❖ Mas o ponto é, no linux tudo é um arquivo e todo arquivo tem um timestamp.
- ❖ O que é Unix TimeStamp ou Unix Time ou POSIX TIME ou UNIX Epoch?
- ❖ Primeiramente, é a mesma coisa.
- ❖ Segundamente, é o número de segundos que se passaram desde 01/01/1970, literalmente o Unix Time 0 é meia noite de 01/01/1970.

1 Hora	3600 segundos
1 Dia	86400 segundos
1 Semana	604800 Segundos
1 mês	2629743 Segundos
1 Ano	31556926 Segundos

```
date +%s -d"Jan 1, 1980 00:00:01"
date -d @1520000000
```

# FileSystem – Hunting

- ❖ Identificar arquivos modificados em -50 dias
  - ❖ find / -mtime 50
- ❖ Identificar arquivos acessados em -50 dias
  - ❖ find / -atime 50
- ❖ Identificar arquivos modificados entre 50 e 100 dias
  - ❖ find / -mtime +50 -mtime -100
- ❖ Identificar Alterações em arquivos em menos de 1h
  - ❖ find / -cmin -60
- ❖ Identificar arquivos modificados em 1h
  - ❖ find / -mmin -60
- ❖ Identificar arquivos acessados em 1 hr
  - ❖ find / -amin -60

```
root@fiap-linux-websrv:~# stat /var/www/html/LEAVE-ME_HERE
  File: /var/www/html/LEAVE-ME_HERE
  Size: 13          Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d  Inode: 1441985      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    33/www-data)  Gid: (    33/www-data)
Access: 2021-12-01 00:11:38.142282260 +0000
Modify: 2021-12-01 00:11:38.142282260 +0000
Change: 2021-12-01 00:11:44.648694889 +0000
 Birth: -
```

```
root@fiap-linux-websrv:~# find /var/www -mmin -10
/var/www/html
/var/www/html/LEAVE-ME_HERE
root@fiap-linux-websrv:~#
```

```
root@fiap-linux-websrv:~# find /var/www -mmin -10 -exec cat {} +
cat: /var/www/html: Is a directory
lalala_haxor
root@fiap-linux-websrv:~#
```

```
root@fiap-linux-websrv:~# stat /var/www/html/LEAVE-ME_HERE
  File: /var/www/html/LEAVE-ME_HERE
  Size: 13          Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d  Inode: 1441985      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    33/www-data)  Gid: (    33/www-data)
Access: 2021-12-01 00:21:17.131236469 +0000
Modify: 2021-12-01 00:11:38.142282260 +0000
Change: 2021-12-01 00:11:44.648694889 +0000
 Birth: -
```

```
stat /path/to/file
```

# FileSystem – Hunting: Limpando Rastros

- ❖ Cenário: Exploração Web, log poisoning, WebShell, upload de arquivo malicioso usando wget, execução de arquivo, reverse shell, shell spawn em /var/www/public/
- ❖ No logs No Crimes?
- ❖ Log do HTTPd/apache2;
- ❖ Arquivo anômalo em diretório conhecido;
- ❖ Conexão de rede anômala;
- ❖ Processos filhos anômalos.
- ❖ Onde mais?

# FileSystem – Hunting: Limpando Rastros

- ❖ Vai apagar o log inteiro do apache2? rm –rf /var/log/apache2/? Não? Vai fazer o que?
  - ❖ Supondo que você tenha acesso): sed '/192.168.1.2/d' access.log
- ❖ E sobre o arquivo novo no diretório? Vai deletar sua reverse shell? Não? Medo de ficar sem acesso? Vai Fazer o que?
  - ❖ Fileless payloads
  - ❖ TimeStamp?
    1. Get the timestamp pattern from other files using stat
    2. Change the timestamp using touch
  - ❖ Pray (ou adote backdoors mais elaborados – weevely?)
- ❖ E a conexão reversa de rede? Vai matar a conexão? Não? Vai fazer o que?
  - ❖ The Problem
- ❖ E aquele processo com o nome revshell.py com seu IP no ‘ps aux’? Vai matar o Processo? Ta com Pena? Não?
- ❖ Onde mais?

# FileSystem – Hunting: Curiosidade

- ❖ Usado IRL?
- ❖ Sim, o blackhat PHINEAS FISHER publicou um vídeo de uma intrusão não autorizada em um órgão do governo vinculado à policiamento.
- ❖ Na gravação, durante a pós exploração, ele realiza a alteração do timestamp dos arquivos como técnica anti-forense.

# Automação do processo (IDS, IPS)

The wayy you go

# Local Stuff

- ❖ IDS/IPS
- ❖ ModSecurity – WAF de baixo custo? Não, é de graça! funciona? Depende de você.
- ❖ Mod Evasive – Mitigação de DDoS/DoS
- ❖ Fail2Ban – IPS Local, atua em conjunto com o firewall para bloquear endereços de origem;
- ❖ Tripware – Mapeia modificações no filesystem com base em hashes de arquivos e monitora periodicamente.
- ❖ Snort? NIDS de baixo custo
- ❖ Suricata? IPS



# Apache WAF

- ❖ ModSecurity, IDS, IPS. Signature based
- ❖ What are signatures? Regex?
- ❖ Wait what? Brace yourselves

# Apache WAF – Big reveal

## Step 5: Analyzing the alert messages

So we are looking at 13,000 alerts. And even if the format of the entries in the error log may be clear, without a tool they are very hard to read, let alone analyze. A simple remedy is to use a few *shell aliases*, which extract individual pieces of information from the entries. They are stored in the alias file we discussed in the log format in Tutorial 5.

```
$> cat ~/.apache-modsec.alias
...
alias meldata='grep -o "[data ^]*" | cut -d\" -f2'
alias melfile='grep -o "[file ^]*" | cut -d\" -f2'
alias melhostname='grep -o "[hostname ^]*" | cut -d\" -f2'
alias melid='grep -o "[id ^]*" | cut -d\" -f2'
alias melip='grep -o "[client ^]*" | cut -b9-'
alias melidmsg='sed -e "s/.*\[id \///" -e "s/\([0-9]*\).*\[msg \"/\1 /" -e "s/\"].*//" -e "s/(Total .*/(Total ... ...) .../" -e "s/Incoming and Outgoing Score: [0-9]* [0-9]*/Incoming and Outgoing Score: .../"
alias melline='grep -o "[line ^]*" | cut -d\" -f2'
alias melmatch='grep -o " at [^ ]*\.\[file" | sed -e "s/\.\. \[file//" | cut -b5-
alias melmsg='grep -o "[msg ^]*" | cut -d\" -f2'
alias meltimestamp='cut -b2-25'
alias melunique_id='grep -o "[unique_id ^]*" | cut -d\" -f2'
alias meluri='grep -o "[uri ^]*" | cut -d\" -f2'
...
...
```

# Apache WAF – REMOTE COMMAND EXEC?

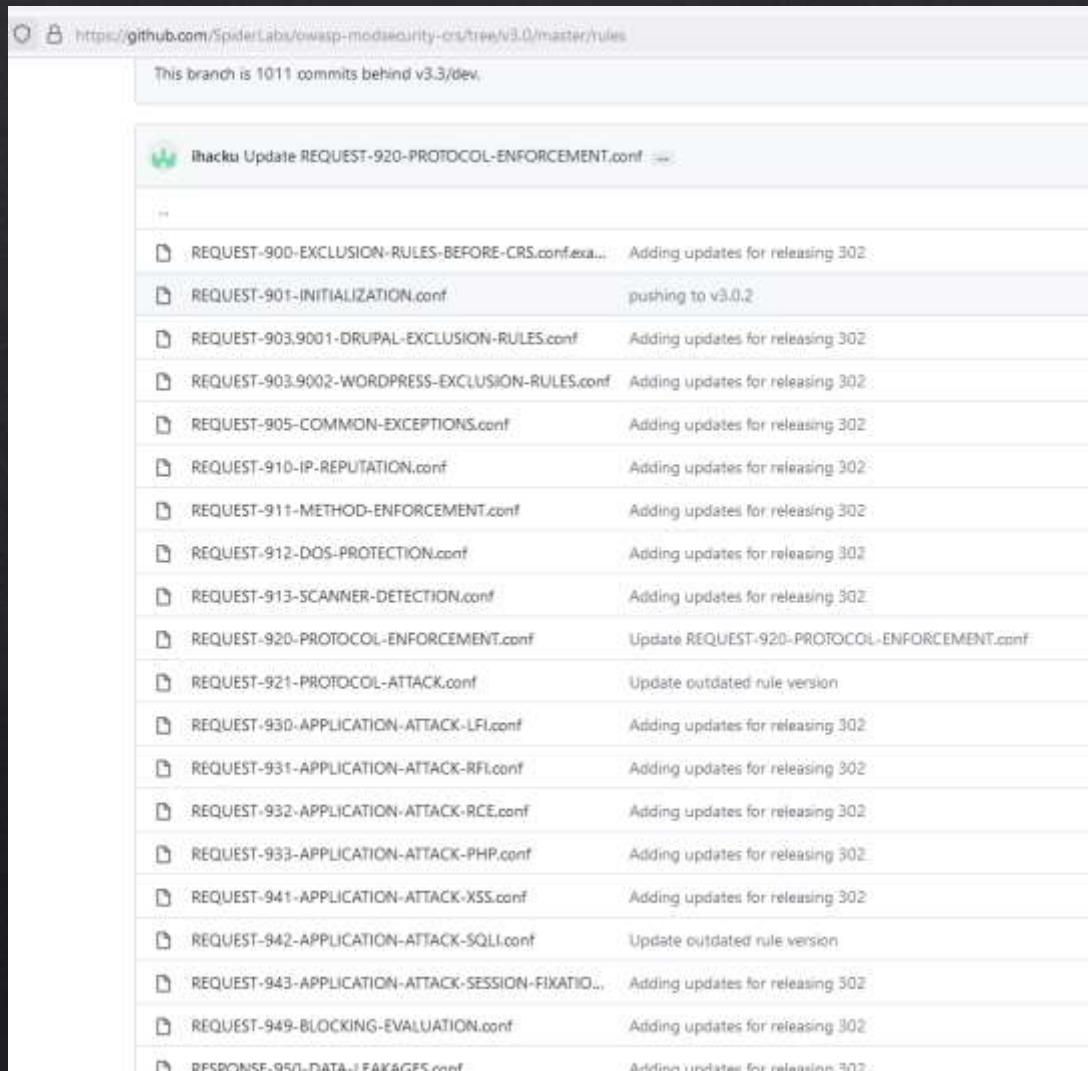
```
362 # [ Unix direct remote command execution ]
363 #
364 # Detects Unix commands at the start of a parameter (direct RCE).
365 # Example: foo=wget%20www.example.com
366 #
367 # This case is different from command injection (rule 932100), where
368 # command string is appended (injected) to a regular parameter, and
369 # passed to a shell unescaped.
370 #
371 # Due to a higher risk of false positives, the following changes have
372 # made relative to rule 932100:
373 # 1) the set of commands is smaller
374 # 2) we require a trailing space (denoting command parameters) or carriage
375 #    separator character after the command
376 #
377 # To rebuild the word list regexp:
378 #   cd util/regexp-assemble
379 #   cat regexp-932150.txt | ./regexp cmdline.py unix | ./regexp-assemble
380 #
381 # Then insert the assembled regexp into this template:
382 #
383 # -----
384 # SecRule REQUEST_COOKIES|!REQUEST_COOKIES:/__utm|REQUEST_COOKIES_NAMES|ARGS_NAMES|ARGS|XML:/* "@rx (?:^=)\s*(?:{||\s*"
385 #     "msg:'Remote Command Execution: Direct Unix Command Execution',\
386 #     phase:request,\\
387 #     rev:'1',\
388 #     ver:'OWASP CRS/3.0.0',\
389 #     maturity:'1',\
390 #     accuracy:'7',\
391 #     capture,\\
392 #     t:none,\\
393 #     ctl:auditLogParts=+E,\\
394 #     block,\\
395 #     id:932150,\\
396 #     tag:'application-multi',\
397 #     tag:'language-shell',\
398 #     tag:'platform-unix',\
399 #     tag:'attack-rce',\
400 #     tag:'OWASP CRS/WEB_ATTACK/COMMAND_INJECTION',\
401 #     tag:'WASC TC/WASC-31',\
402 #     tag:'OWASP_TOP_10/A1',\
403 #     tag:'PCI/6.5.2',\
404 #     logdata:'Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}',\
405 #     severity:'CRITICAL',\
406 #     setvar:'tx.msg=%{rule.msg}',\
407 #     setvar:tx.rce_score=+ %{tx.critical_anomaly_score},\
408 #     setvar:tx.anomaly_score=+ %{tx.critical_anomaly_score},\
409 #     setvar:tx.%{rule.id}-OWASP CRS/WEB_ATTACK/RCE-%{matched_var_name}=%{tx.0}"
410 #
411 #
412 #
413 # -----
```

# Here we go



# Remember rce rule?

# Want more?



<https://github.com/SpiderLabs/owasp-modsecurity-crs/tree/v3.0/master/rules>

# E a nível de camada 3 e 4?



The following is a list of the rule categories that TALOS includes in the download pack along with an explanation of the content in each rule file. More categories can be added at any time, and if that occurs a notice will be placed on the [Snort.org blog](#).

- **app-detectrules** - This category contains rules that look for, and control, the traffic of certain applications that generate network activity. This category will be used to control various aspects of how an application behaves.
- **blocklist.rules** - This category contains URL, USER-AGENT, DNS, and IP address rules that have been determined to be indicators of malicious activity. These rules are based on activity from the TALOS virus sandboxes, public list of malicious URLs, and other data sources.
- **browser-chromerules** - This category contains detection for vulnerabilities present in the Chrome browser. (This is separate from the "browser-webkit" category, as Chrome has enough vulnerabilities to be broken out into its own, and while it uses the Webkit rendering engine, there's a lot of other features to Chrome.)
- **browser-firefoxrules** - This category contains detection for vulnerabilities present in the Firefox browser, or products that have the "Gecko" engine. (Thunderbird email client, etc)
- **browser-ie.rules** - This category contains detection for vulnerabilities present in the Internet Explorer browser (Trident or Tasman engines)
- **browser-webkit** - This category contains detection of vulnerabilities present in the Webkit browser engine (aside from Chrome) this includes Apple's Safari, RIM's mobile browser, Nokia, KDE, Webkit itself, and Palm
- **browser-other** - This category contains detection for vulnerabilities in other browsers not listed above.
- **browser-plugins** - This category contains detection for vulnerabilities in browsers that deal with plugins to the browser. (Example: ActiveX)
- **content-replace** - This category contains any rule that utilizes the "replace" functionality inside of Snort.
- **deleted** - When a rule has been deprecated or replaced it is moved to this categories. Rules are never totally removed from the ruleset, they are moved here.
- **exploit** - This is an older category which will be deprecated soon. This category looks for exploits against software in a generic form.
- **exploit-kit** - This category contains rules that are specifically tailored to detect exploit kit activity. This does not include "post-compromise" rules (as those would be dropped as result of visiting an exploit kit) would be in their respective file category.
- **file-executable** - This category contains rules for vulnerabilities that are found or are delivered through executable files, regardless of platform.
- **file-flash** - This category contains rules for vulnerabilities that are found or are delivered through flash files. Either compressed or uncompressed, regardless of what is attacked.
- **file-image** - This category contains rules for vulnerabilities that are found inside of images files. Regardless of delivery method, software being attacked, or file extension (png, gif, bmp, etc)
- **file-identify** - This category is to identify files through file extension, the content in the file (file magic), or header found in the traffic. This information is usually used to then trigger a different rule.
- **file-java** - This category contains rules for vulnerabilities present inside of Java files (.jar)

# E a nível de camada rede?

```
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Trojan.FileEncoder IP geolocation checkin attempt"; flow:to_server,established; isdataat:213; isdataat:!214; urilen:1; content:"GET / HTTP/1.1|0D 0A|User-Agent: Mozilla/4.0 (compatible|3B| MSIE 6.0|3B| Windows NT 5.1|3B| SV1|3B| .NET4.0C|3B| .NET4.0E|3B| .NET CLR 2.0.50727|3B| .NET CLR 3.0.4506.2152|3B| .NET CLR 3.5.30729)|0D 0A|Host: ip-addr.es|0D 0A|Cache-Control: no-cache|0D 0A 0D 0A|"; fast_pattern:only; metadata:impact_flag red, ruleset community, service http; reference:url,www.virustotal.com/en/file/17edf82c40df6c7268191def7cbff6e60e78d7388018408800d42581567f78cf/analysis/; classtype:trojan-activity; sid:33449; rev:3;)
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Trojan.FileEncoder variant outbound connection"; flow:to_server,established; content:"POST"; http_method; content:"="; depth:2; http_client_body; content:"Content-Length: 128|0D 0A|"; fast_pattern:only; http_header; content:"Content-Type: application/x-www-form-urlencoded|0D 0A|"; http_header; content:"|3B 20|MSIE|20|"; http_header; content:!"Accept-Language:"; http_header; pcre:"/[a-z]\x3d[a-f\d]{126}/P"; metadata:impact_flag red, ruleset community, service http; reference:url,www.virustotal.com/en/file/17edf82c40df6c7268191def7cbff6e60e78d7388018408800d42581567f78cf/analysis/; classtype:trojan-activity; sid:33449; rev:3;)
# alert udp any 53 -> $HOME_NET any (msg:"PROTOCOL-DNS glibc getaddrinfo A record stack buffer overflow attempt"; flow:to_client; dsiz>2000; byte_test:1,&,2,2; byte_test:1,&,0x80,2; byte_test:1,!&,0x78,2; content:"|00 01|"; depth:2; offset:4; content:"|00 00 01 00 01|"; fast_pattern:only; metadata:policy max-detect-ips drop, policy security-ips drop, ruleset community, service dns; reference:cve,2015-7547; reference:url,googleonlinesecurity.blogspot.com/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html; classtype:attempted-user; sid:37730; rev:5;)
# alert udp any 53 -> $HOME_NET any (msg:"PROTOCOL-DNS glibc getaddrinfo AAAA record stack buffer overflow attempt"; flow:to_client; dsiz>2000; byte_test:1,&,2,2; byte_test:1,&,0x80,2; byte_test:1,!&,0x78,2; content:"|00 01|"; depth:2; offset:4; content:"|00 00 01 00 01|"; fast_pattern:only; metadata:policy max-detect-ips drop, policy security-ips drop, ruleset community, service dns; reference:cve,2015-7547; reference:url,googleonlinesecurity.blogspot.com/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html; classtype:attempted-user; sid:37731; rev:5;)
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Trojan.Dridex dropper variant"; flow:to_server,established; content:"/gt.jpg?"; fast_pattern; http_uri; content:"="; within:1; distance:1; http_header; metadata:impact_flag red, ruleset community, service http; reference:url,www.virustotal.com/en/file/8a80760f60f42ce5574a8020c08123a6a8fc2a12d28e8802f3d5101f72c2ad0c/analysis/; classtype:trojan-activity; sid:37733; rev:2;)
```



# Next Level

Centralização dos logs, monitoramento e orquestração (SIEM and SOAR)

# Centralização de logs

- ❖ Centralização ou descentralização nativa
  - ❖ É recomendado que os logs sejam armazenados em mais de um lugar (A10:2017?).
  - ❖ O processos pode ser feito utilizando integrações nativas dos gerenciadores de logs do próprio Linux através do RSYSLOG por exemplo.
  - ❖ Escalável? TLDR? Nope
  - ❖ Gestão centralizada? TLDR? Nope
  - ❖ Fácil auditoria? TLDR? Nope
  - ❖ Funciona? TLRD? Sim

# Monitoramento

- ❖ Eventos são quaisquer ações.
- ❖ Dado um determinado conjuntos de eventos (rules? Remember that?), alertas são criados e endereçados para equipes responsáveis. (Na teoria)

# SIEM?

- ❖ SIEM é a combinação de gerenciamento de eventos de segurança (**SEM** – security event management) e gerenciamento de informações de segurança (**SIM** – security information management).
- ❖ Com eventos de segurança, alertas e etc, o SIEM é capaz de detectar ameaças de segurança já existentes...
  - ❖ Dado a configuração correta das rules e correlações, sim.
- ❖ E eventos Desconhecidos?
- ❖ Hmm IA? Machine Learning? Patterns everywhere?

# Orquestração?

- ❖ Então você coleta eventos e garante que todos (relevantes) estão sendo coletados,
- ❖ E determinados eventos geram alertas?
- ❖ Então uma equipe irá atuar no alerta? Sim
- ❖ Todo um processo de investigação é feito, documentado e arquivado (playbooks) e podem ser usados em próximos cenários semelhantes ou idênticos.
- ❖ E se uma vez documentados, as respostas/tratativas fossem automatizadas?

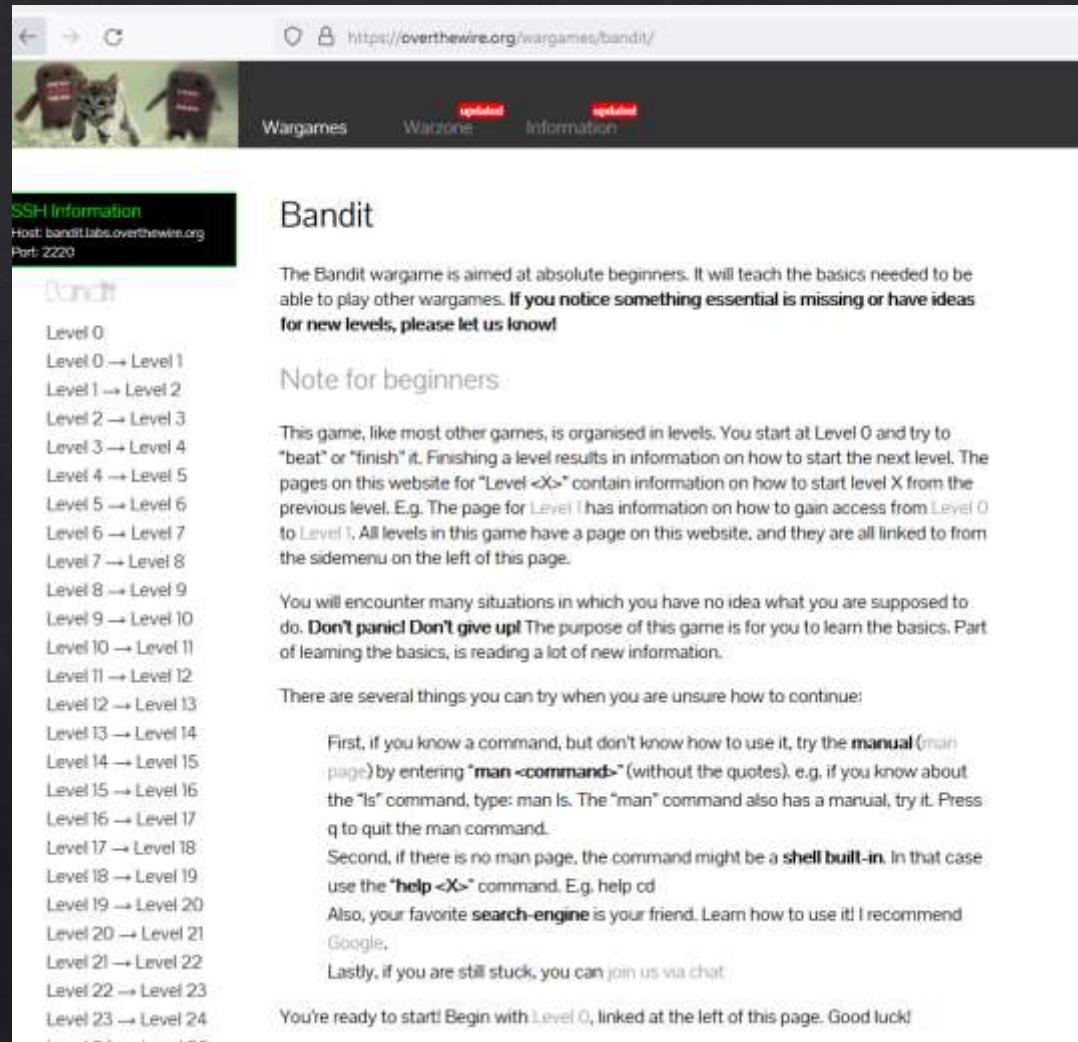
# Like it or not, meet SOAR

- ❖ Security Orchestration, Automation and Response (SOAR)

# Time to Play Around

Meet Bandit

# BACK TO TUX



The screenshot shows a web browser displaying the OverTheWire Wargames Bandit level page. The URL in the address bar is <https://overthewire.org/wargames/bandit/>. The page features a header with three tuxedo cat icons and navigation links for "Wargames", "Warzone", and "Information". Below the header, there's a sidebar titled "SSH Information" with host details: Host: bandit.labs.overthewire.org, Port: 2220. The main content area is titled "Bandit" and contains information about the game's purpose and levels. It includes a note for beginners, instructions for navigating levels, and tips for troubleshooting. At the bottom, it encourages users to start with Level 0.

**SSH Information**  
Host: bandit.labs.overthewire.org  
Port: 2220

**Bandit**

The Bandit wargame is aimed at absolute beginners. It will teach the basics needed to be able to play other wargames. If you notice something essential is missing or have ideas for new levels, please let us know!

**Note for beginners**

This game, like most other games, is organised in levels. You start at Level 0 and try to "peat" or "finish" it. Finishing a level results in information on how to start the next level. The pages on this website for "Level <X>" contain information on how to start level X from the previous level. E.g. The page for Level 1 has information on how to gain access from Level 0 to Level 1. All levels in this game have a page on this website, and they are all linked to from the sidemenu on the left of this page.

You will encounter many situations in which you have no idea what you are supposed to do. Don't panic! Don't give up! The purpose of this game is for you to learn the basics. Part of learning the basics, is reading a lot of new information.

There are several things you can try when you are unsure how to continue:

First, if you know a command, but don't know how to use it, try the **manual** ([man page](#)) by entering "**man <command>**" (without the quotes). e.g. if you know about the "ls" command, type: man ls. The "man" command also has a manual, try it. Press q to quit the man command.

Second, if there is no man page, the command might be a **shell built-in**. In that case use the "**help <X>**" command. E.g. help cd

Also, your favorite **search-engine** is your friend. Learn how to use it! I recommend Google.

Lastly, if you are still stuck, you can [join us via chat](#).

You're ready to start! Begin with [Level 0](#), linked at the left of this page. Good luck!

<https://overthewire.org/wargames/bandit/>

# Referências

- ❖ <https://sempreupdate.com.br/como-funciona-os-logs-no-linux/>
- ❖ <https://diesec.home.blog/2018/01/07/centralizando-logs-com-rsyslog/>
- ❖ <https://www.ppgia.pucpr.br/pt/arquivos/techdocs/linux/foca-avancado/ch-log.html>
- ❖ <https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs-pt>
- ❖ <https://httpd.apache.org/docs/2.4/logs.html>
- ❖ <https://www.geeksforgeeks.org/find-command-in-linux-with-examples/>

Thank you security community!

# Dúvidas?

Muito Obrigado!

XOR “Vale mais 7 horas de debug do que 15 minutos de man pages”