# Instruções de remoção de ameaças cibernéticas

Feito por:

ECHOSEC

inteli

GAMELAB

# Instruções gerais

- É recomendado que a navegação pelo sistema seja feita pelo terminal, já que facilita as análises;
- Neste manual, você encontrará instruções de como analisar arquivos maliciosos e usuários não autorizados na sua rede, a utilização de cada comando pode ser encontrada no tópico **‘Comandos’** ou nos tópicos de cada ferramenta;
- Enquanto um hacker estiver na sua rede, ele possivelmente pode injetar arquivos no seu sistema;
- É necessário ser preciso ao utilizar os comandos, cuidado com erros de digitação;
- Os arquivos maliciosos geralmente ficam nas pastas “System32” e “Program Files”;

# Comandos

## Comandos básicos

- ls: listar arquivos na pasta em que você está;
- cd [nome do diretório]: navegar ao diretório;
    - Para voltar à pasta anterior: “cd ..” ;
- rm [diretório ou arquivo]: remover arquivos ou diretórios;
- find [nome do arquivo]: busca arquivos em diretórios;

## Comandos para análise/mitigação

- exiftool: análise de arquivos;
- nmap: scan na rede local, e as portas expostas de usuários;
- users-ls: lista de usuários do seu sistema;
- frw: gerenciamento do firewall da sua rede;
- config: listagem de configurações e especificações do seu sistema;
- help: lista de comandos disponíveis;

# Sobre arquivos maliciosos

## Exiftool

Para analisar arquivos, utilize a ferramenta `Exiftool`, e identifique padrões para remover os arquivos.

### Utilização:

```
exiftool [ nome do arquivo ]
```

#### Output exemplo

```
Version Number                  : 11.16
File Name                       : example.jpg
Directory                       : /caminho/do/arquivo
File Size                       : 245 kB
File Modification Date/Time     : 2022:01:16 15:30:45-05:00
File Access Date/Time           : 2022:01:16 15:30:45-05:00
File Inode Change Date/Time     : 2022:01:16 15:30:45-05:00
File Permissions                : rw- r-- r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Author                          : Microsoft
```

### Padrões possíveis em um arquivo malicioso

- O campo **`File Permissions`** estar modificado, você pode observar que existem 3 sequências de letras nesse campo, a terceira sequência não

pode possuir a letra `x`, ela significa que o arquivo pode ser executado por qualquer usuário (inclusive, pode estar sendo executado nesse momento).
- O campo **`Author`** deve conter um dos usuários do seu sistema. Nesse caso, se atente aos arquivos de imagem, eles podem conter autores diferentes, por serem de origem externa ao seu sistema.
- Se atente ao campo **`File Type`** , já que é onde você pode olhar o tipo de arquivo analisado, segue a lista de tipos de arquivos e possivelmente maliciosos:
    - EXE
    - SHELL
    - PHPP
    - FPY

## Observações

- Caso o arquivo se enquadre em uma dessas regras, ele não é necessariamente malicioso, mas fique atento, muitos hackers habilidosos podem disfarçar algumas configurações de arquivos, e assim passam despercebidos.
- Não remova um arquivo sem que você tenha certeza de que ele é malicioso. Remover um arquivo pode ser fatal para sua máquina.

# Sobre usuários na sua rede

## Nmap

Para analisar os usuários que estão utilizando sua rede, utilize a ferramenta `Nmap`, e para remover um usuário suspeito, utilize o comando `frw`.

### Utilização

```
nmap 192.168.1.0/24
```

### Output exemplo

```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-18 12:00 UTC

Nmap scan report for 192.168.1.1
Host is up (0.001s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 192.168.1.2
Host is up (0.002s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.1.3
Host is up (0.003s latency).
Not shown: 998 closed ports
PORT  STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.1.6
```

```
Host is up (0.002s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
22/tcp  open  ssh
```

## Como identificar um usuário invasor

- Ao fazer o scan na sua rede, você pode observar que a ferramenta retorna um relatório para cada IP (em negrito no output acima), e nos mostra quais portas estão expostas. Essas portas devem estar de acordo com a tabela a seguir:

| PORT | SERVICE |
|---|---|
| 21 | ftp (File Transfer Protocol) |
| 22 | ssh (Secure Shell Protocol) |
| 53 | dns (Domain Name System name resolver) |
| 80 | http (Hypertext Transfer Protocol) |
| 106 | macOS (macOS Server) |
| 139 | NetBios (NetBIOS Session Service) |
| 443 | https (Hypertext Transfer Protocol Secure) |

Se alguma dessas portas ou serviços não estiverem correspondentes à tabela, é possível que seja um invasor

- Fique muito atento às portas com valores numéricos altos, elas podem pertencer à invasores.

# Frw

A ferramenta `frw` serve para utilizar o firewall de sua rede para remover um usuário.

## Como remover um usuário da sua rede

Para remover o usuário invasor, utilize o comando `frw`, referenciando o IP do usuário suspeito.

## Utilização

```
frw -r [IP do usuário]
```

## Observações

- Ambos comandos podem demorar para serem executados.
- NÃO REMOVA UM USUÁRIO ERRADO DA SUA REDE.
- Por mais que possa parecer que o usuário foi removido da rede, alguns hackers têm a habilidade de voltar para a rede de algumas formas, então faça esse procedimento periodicamente.