1

2

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

RECONHECIMENTO E COLETA DE INFORMAÇÕES

4

Reconhecimento e coleta de informações

FIAP

- Primeiro passo para descobrir se um alvo (equipamento, como um servidor de um website) está com recursos de hardware ou software vulneráveis

- Duas formas:
  - Footprint
  - Fingerprint

5

Reconhecimento e coleta de informações

FIAP

- **Footprinting**
  - Processo inicial de **coleta de informações ampla** sobre um **alvo**
    - **Visão geral: IPs, domínios, funcionários, tecnologias adotadas, entre outros**
  - **Passiva** (sem interagir diretamente com os sistemas-alvo)
  - **Objetivo:**
    - Mapear a "superfície de ataque“
  - Exemplos:
    - whois, consultas DNS, informações publicamente disponíveis
    - Descobrir que uma empresa usa o **servidor web Apache**, tem um domínio **exemplo.com** e IPs na faixa **192.168.1.0/24**

6

Reconhecimento e coleta de informações

- **Fingerprinting**
  - Identificação de **detalhes técnicos específicos** sobre um alvo (sistema, serviço ou dispositivo)
  - **Ativa**, normalmente
  - **Objetivo:**
    - Obter informações detalhadas como:
      - Versões de serviços e sistemas operacionais
      - Detecção de qual servidor web está em uso
      - Configurações de rede

7

Reconhecimento e coleta de informações

- **Fingerprinting (*cont.*)**
  - Ativo:
    - Envio de pacotes ao alvo para analisar a resposta (ex: Nmap).
    - Porém, gera alarme em sistemas de detecção
  - Passivo:
    - análise do tráfego de rede (ex: Wireshark).
  - Realizada após o footprinting, quando o alvo já foi delimitado.
  - Exemplos:
    - Identificar que o servidor web Apache é a **versão 2.4.41** rodando **em um Ubuntu 18.04**.

8

Reconhecimento e coleta de informações

- Observe as afirmações e assinale:
- a) nmap (identificar serviços e versões em execução em um host remoto)
- b) whois (consultas públicas de registros de domínios)
- c) dig (consulta DNS para observar hosts de um domínio)
- d) traceroute (mapear o caminho até um servidor-alvo)
- e) wireshark (reconhecimento das características do navegador de um usuário)

9

Common Vulnerabilities and Exposures (CVE)

10

Common Vulnerabilities and Exposures

- O ataque que não se via
- CurveBall (CVE-2020-0601): o cadeado HTTPS enganava
- Falha na criptografia do Windows 10
- Permitia falsificar certificados digitais
- Atacantes podiam criar sites "seguros" forjados

11

CVE

- É um identificador único para falhas de segurança
- Mantido pelo MITRE e catalogado pelo NVD (NIST)
- Ajuda pesquisadores, empresas e governos a se comunicarem sobre vulnerabilidades
- Ex.:

CVE-2021-44228

Nome: Log4Shell

Gravidade: 10.0

Afeta: Java Log4j < 2.15

12

Tipos de CVEs comuns

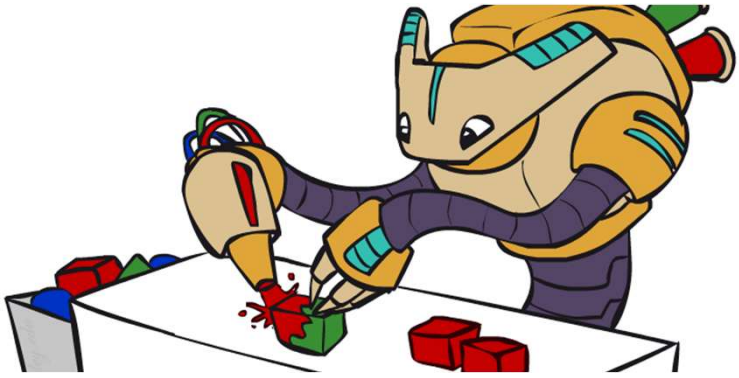
FIAP

- RCE: Remote Code Execution
  - Execução de código pelo atacante na máquina alvo
- XSS: Cross-site Scripting
- SQLi: SQL Injection
- DoS/DDoS: Negacão de serviço
- Privilege Escalation

13

FIAP

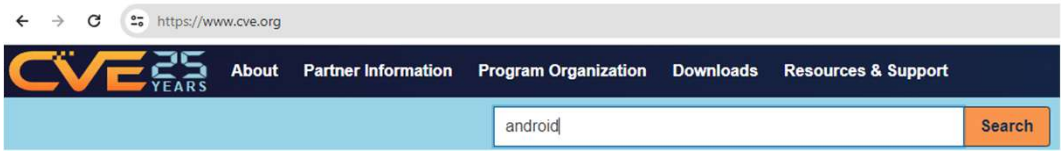
HANDS ON!



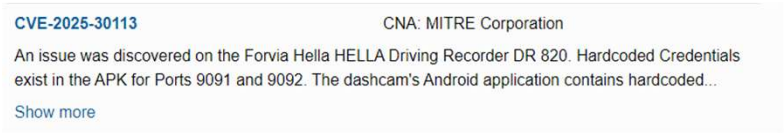
14

CVE

- Site: https://www.cve.org/
- Busque por: ***android***



- Clique no CVE-2025-30113



15

CVE

- Site: https://nvd.nist.gov/
- Vulnerabilites->Search & Statistics: Busque por: ***android rce***
- Clique no CVE-2023-42801

Vuln ID	Summary	CVSS Severity
CVE-2023-42801	Moonlight-common-c contains the core GameStream client code shared between Moonlight clients. Moonlight-common-c is vulnerable to buffer overflow starting in commit f57bd745b4cbed577ea654fad4701bea4d38b44c. A malicious game streaming server could exploit a buffer overflow vulnerability to crash a moonlight client. Achieving RCE is possible but unlikely, due to stack canaries in use by modern compiler toolchains. The published binaries for official clients Qt, Android, iOS/tvOS, and Embedded are built with stack canaries, but some unofficial clients may not use stack canaries. This vulnerability takes place after the pairing process, so it requires the client to be tricked into pairing to a malicious host. It is not possible to perform using a man-in-the-middle due to public key pinning that takes place during the pairing process. The bug was addressed in commit b2497a3918a6d79808d9fd0c04734786e70d5954. **Published:** December 14, 2023; 12:15:07 PM -0500	*V4.0:*(not available) *V3.1:* 7.6 HIGH *V2.0:*(not available)

16

CVE

- Observe:
  - Qual o código da CVE?
  - O que ela permite?
  - Qual CVSS (gravidade)?
  - Qual CWE (recurso explorado)?
  - Qual software/versão afetado?

17

CVE - Recap

- CVEs identificam falhas
- Se sistemas não forem corrigidos...
- Eles ficam visíveis na Internet
- Atacantes usam isso para ataques direcionados

18

CVE e Zero day

FIAP

Qual a diferença entre CVE e Zero-Day?

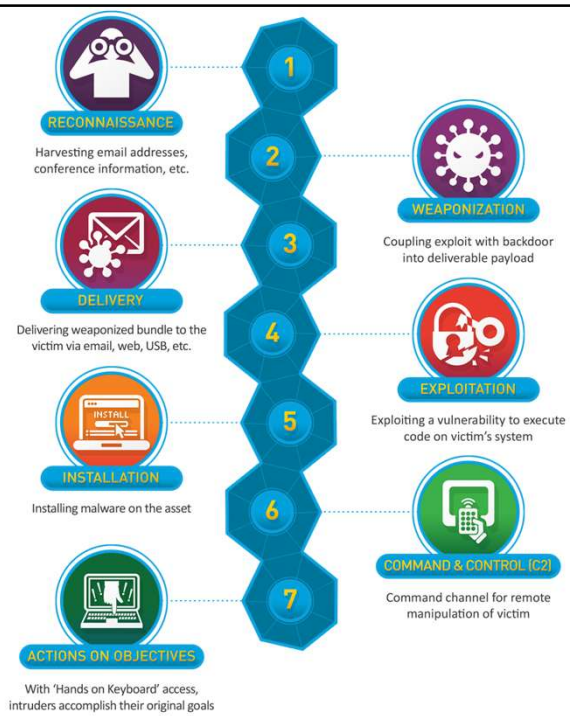
19

FIAP

CADEIA DE ATAQUE

20

Cyber Kill Chain



21

Cyber Kill Chain

1. Reconhecimento (Reconnaissance)
2. Armamento (Weaponization)
3. Entrega (Delivery)
4. Exploração (Exploitation)
5. Instalação (Installation)
6. Comando e Controle (Command & Control)
7. Ações no Objetivo (Actions on Objectives)

22

Cyber Kill Chain

FIAP

- Em 2 minutos:
  - https://www.youtube.com/watch?v=jdOph6kNNCA
- Cisco Lab completo (evidências de como executar um ataque completo considerando os elementos da Cyber Kill Chain):
  - https://learningnetwork.cisco.com/s/article/Cisco-Full-Attack-Continuum-and-Cyber-Kill-Chain-Lab--Case-Study

23

FIAP

Opensource Intelligence

24

Opensource Intelligence (OSINT)

- Coleta e análise de informações disponíveis publicamente para fins de inteligência
  - Para sites, por exemplo:
    - https://who.is
- Relevância:
  - Identificação de ameaças
  - Identificação de vulnerabilidades

25

OSINT

- Ética:
  - Não é porque está disponível que eu posso/devo acessar
  - Respeitar a privacidade
  - Manter aderência às leis vigentes durante as investigações

26

OSINT

- Cenários envolvendo dilemas éticos no uso do OSINT
- Debate :
  - Cenário:
    - Imagine que você encontra um banco de dados exposto publicamente contendo informações pessoais de clientes de uma empresa (nomes, e-mails e telefones). Você não quebrou nenhuma senha, não invadiu nada – apenas usou uma pesquisa OSINT.
  - Perguntas:
    - Você deveria informar a empresa sobre essa exposição?
    - Se você divulgar o problema publicamente para alertar os usuários, estaria fazendo um bem ou prejudicando ainda mais?
    - O que faria se uma empresa se recusasse a corrigir a falha?

27

OSINT

- Conclusão:
  - O uso responsável de OSINT deve priorizar a proteção das pessoas envolvidas, não a exploração de falhas para benefício próprio.

28

OSINT

FIAP

- **Caso real 1:**
  - **Vazamento da Cloud Bucket da Verizon (2017)**
  - **Resumo:** Em 2017, a empresa de telecomunicações **Verizon** expôs informações pessoais de **14 milhões de clientes** devido a uma configuração incorreta em um **Amazon S3 Bucket**.
  - **Como foi descoberto?** Pesquisadores de segurança da **UpGuard** utilizaram técnicas OSINT para encontrar o bucket **publicamente acessível** usando ferramentas como **Shodan** e buscas avançadas no Google. Os dados incluíam: Nomes completos; Endereços de e-mail; Números de telefone; PINs de conta (que poderiam ser usados para engenharia social)

- **Lição:**
  - Configurações incorretas em servidores na nuvem são um dos erros mais comuns explorados por pesquisadores OSINT. O **Google Dorks** pode revelar diretórios mal configurados, enquanto o **Shodan** pode detectar buckets expostos.

29

OSINT

FIAP

- **Caso real 2:**
  - **Vazamento de 533 milhões de usuários do Facebook (2021)**
  - **Resumo:** Em abril de 2021, um banco de dados com informações de **533 milhões de usuários do Facebook** vazou e ficou publicamente disponível em fóruns de hackers.
  - **Como foi descoberto?** Pesquisadores de OSINT monitoram fóruns da dark web e Telegram para rastrear dados vazados. Neste caso, **Alon Gal**, um pesquisador de segurança cibernética, identificou os dados expostos em fóruns antes que fossem amplamente divulgados. Os dados incluíam: Nomes completos; Números de telefone; E-mails; Datas de nascimento. O Facebook alegou que os dados haviam sido **coletados via scraping**, uma técnica OSINT que utiliza robôs para extrair informações de páginas públicas.

- **Lição:**
  - Informações públicas **podem ser coletadas em massa** e reutilizadas para ataques de phishing e engenharia social. Sites como **Have I Been Pwned** permitem verificar se seus dados vazaram.

30

OSINT na prática

31

OSINT na prática

- Have I Been Pwned?
  - https://haveibeenpwned.com/
- Google Dorking
  - Dorks - tags de pesquisa
- Shodan

32

Google Dorks

FIAP

- Dorking:
  - Strings de busca com tags definidas pelo Google
  - Intenção inicial era facilitar a busca, refinando os critérios para encontrar itens específicos, porém...
- Strings de busca:
  - Arquivos confidenciais possivelmente expostos:
    - filetype:pdf | doc | xls | ppt site:example.com
      - Lista arquivos de um domínio
    - filetype:env intext:DB_PASSWORD
      - Arquivos .env (muito usados em arquiteturas cloud - docker, Kubernetes) com senha de acesso a banco de dados
    - intitle:index.of passwd
      - Diretórios mal configurados que podem expor senhas

33

Google Dorks

FIAP

- Strings de busca (cont.):
  - Painéis administrativos mal configurados:
    - intitle:"index of /admin“
      - Diretórios abertos com nome admin (possivelmente ambiente de administração)
    - inurl:view/index.shtml
      - Câmeras de segurança e IoT abertas
  - Credenciais e senhas em texto claro:
    - intext:"password" filetype:xls | txt | log
      - Busca senhas em arquivos específicos
    - filetype:log intext:login
      - Logs com autenticações registradas.

34

Google Dorks

FIAP

- Strings de busca (cont.):
  - Combinação:
    - site:github.com "password" AND ("mysql" OR "smtp") AND ("root" OR "admin")
      - Busca no site github.com por senhas que sejam de banco de dados mysql ou de e-mail e que tenham usuário root ou admin

35

Shodan

FIAP

- Introdução ao Shodan
  - O “Google” dos dispositivos conectados
  - Busca dispositivos conectados à Internet
    - Ex: servidores web, câmeras IP, roteadores, sistemas SCADA
  - Ética e cuidado ao usar: observação e pesquisa, não invasão

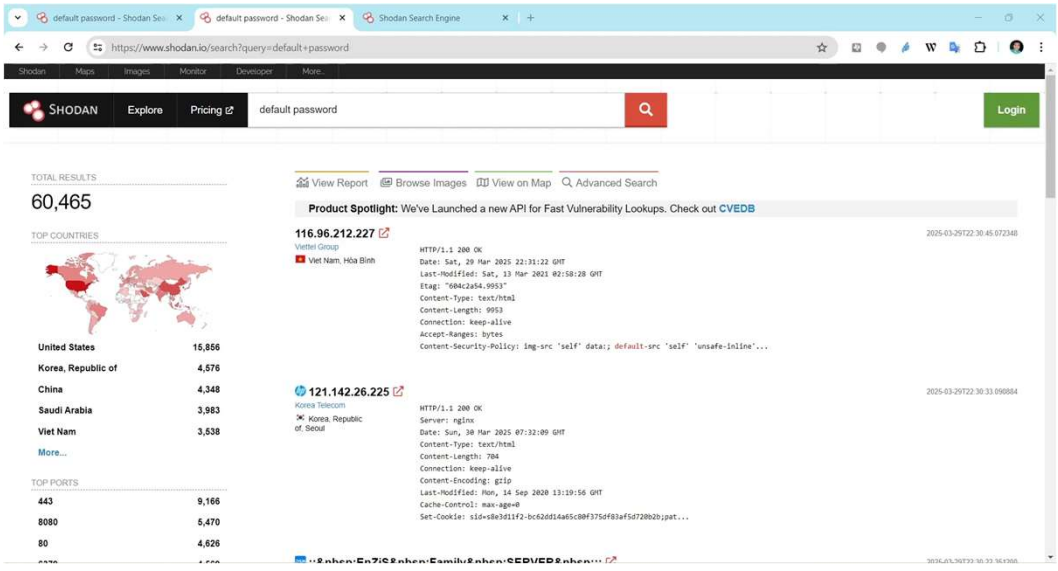
36

Shodan

- Coleta informações públicas
- Site:
  - https://www.shodan.io
- Conta gratuita:
  - permite algumas buscas por dia
- **Real impacto de exposição acidental e configuração incorreta de sistemas**

37

Shodan



38

Shodan

FIAP

- Procure por sistemas/softwares reconhecidamente vulneráveis:
  - Windows 7
  - OpenSSL 1.0.1e
  - log4j (log4shell) - 2.0-beta9 a 2.14.1
  - Linux 2.6
  - Microsoft-IIS/6.0
  - Android 10

39

Shodan

FIAP

- Similar ao Dorks
- Strings de busca:
  - Câmeras de segurança
    - port:554 has_screenshot:true
      - Sem autenticação ou com padrão
    - "NetSurveillance Web" country:"BR“
      - Interface padrão de câmeras IP genéricas (principalmente em uso doméstico)
  - Interface administrativa de servidores Web:
    - http.title:"phpMyAdmin" country:"BR"
      - PHPMyAdmin

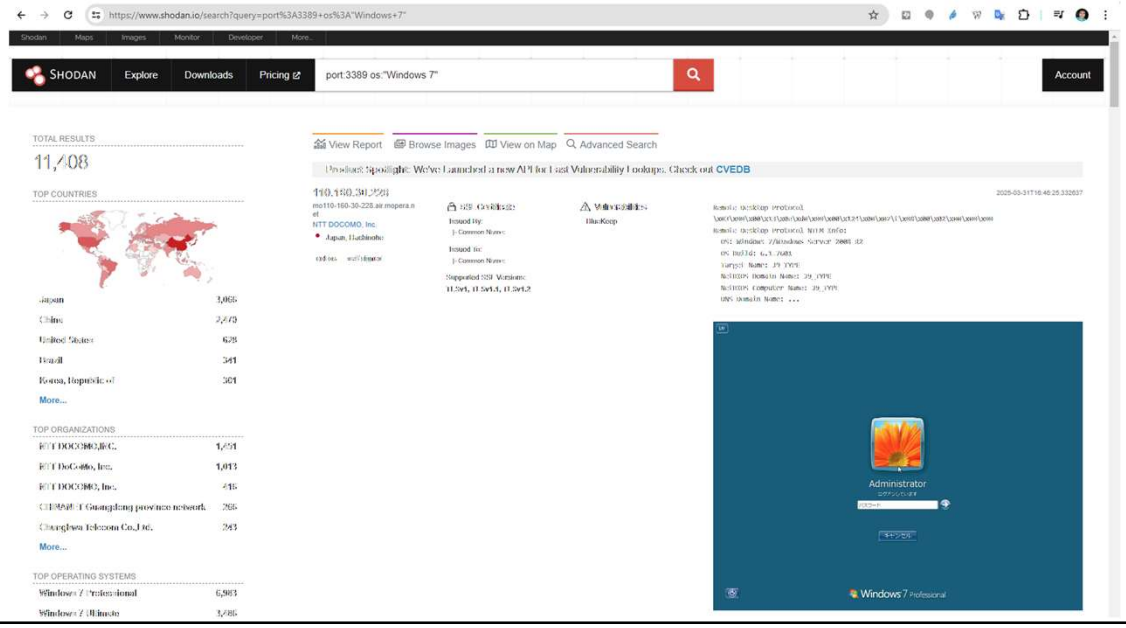
40

Shodan

- Strings de busca (cont.):
  - Bancos de dados expostos (sem autenticação):
    - port:27017 "MongoDB Server Information"
      - Servidores MongoDB expostos sem senha — muito comum!
  - IoT:
    - title:"RouterOS router configuration page"
      - Interface de dispositivos Mikrotik sem senha ou desprotegidos
  - Acesso remoto (SSH) disponível via Internet:
    - port:22 os:"Linux"
      - Porta 22 aberta na Internet
  - Sem autenticação:
    - authentication: disabled
      - Sistemas sem autenticação

41

Shodan



42

OSINT framework

- https://osintframework.com/

43

Contramedidas

44

Riscos

- Riscos de Sistemas Desatualizados:
  - Ausência de atualizações de segurança
  - Ausência de criptografia forte/recomendada
  - Credenciais padrão
  - Superfície de ataque ampliada

45

Checklist de boas práticas

- Atualização constante dos sistemas
- Troca de senhas padrão
- Uso de autenticação forte - Multi-Factor Authentication (MFA)
- Segmentação de redes e uso de VPNs
- Firewall e controle de acesso

46

Contramedidas

- **Contramedidas**
  - Configurar robots.txt
    - Arquivo que fica na raiz do website e informa quais informações devem (e não devem) ser indexadas nos buscadores como Google, Bing, etc.
  - Ocultar diretórios
  - Restringir IPs (firewall)
  - Evitar nomear arquivos com palavras como "senha“, “password” ou "confidencial"

47

Contramedidas

- robots.txt

https://www.youtube.com/robots.txt

```
# robots.txt file for YouTube
# Created in the distant future (the year 2000) after
# the robotic uprising of the mid 90's which wiped out all humans.

User-agent: Mediapartners-Google*
Disallow:

User-agent: *
Disallow: /api/
Disallow: /comment
Disallow: /feeds/videos.xml
Disallow: /get_video
Disallow: /get_video_info
Disallow: /get_midroll_info
Disallow: /live_chat
Disallow: /login
```

https://www.uol.com.br/robots.txt

```
# robots.txt
#
User-agent: *
Sitemap: https://www.uol.com.br/carros/sitemap/v2/news-01.xml
Sitemap: https://www.uol.com.br/ecoa/sitemap/news-01.xml
Sitemap: https://www.uol.com.br/esporte/sitemap/v2/news-01.xml
Sitemap: https://www.uol.com.br/nossa/sitemap/news-01.xml
Sitemap: https://www.uol.com.br/splash/sitemap/news-01.xml
Sitemap: https://www.uol.com.br/tilt/sitemap/news-01.xml
Sitemap: https://www.uol.com.br/universa/sitemap/v2/news-01.xml
Sitemap: https://www.uol.com.br/vivabem/sitemap/v2/news-01.xml
Sitemap: https://www.uol.com.br/apostas/api/?resource-id=sitemap&source=apostas/v1/articles.xml
Sitemap: https://www.uol.com.br/apostas/api/?resource-id=sitemap&source=apostas/v1/authors.xml
Sitemap: https://www.uol.com.br/apostas/api/?resource-id=sitemap&source=apostas/v1/content.xml
Sitemap: https://www.uol.com.br/apostas/api/?resource-id=sitemap&source=apostas/v1/news.xml
Sitemap: https://c.jsuol.com.br/assets/jupiter-news/?resource-id=sitemap&source=toca/index.xml
Allow: /
Disallow: /carros/dev/
User-agent: GPTBot
Disallow: /
User-agent: Google-Extended
Disallow: /
```

48

Mapa mental

- Recap da aula

49

FIAP GRADUAÇÃO

50