



Teoria e Prática de Ataques de Segurança

2025/2026

André Baptista
andre.baptista@fc.up.pt

Miguel Regala
miguel.regala@fc.up.pt

<https://tpas.alunos.dcc.fc.up.pt>



Parte 1

Apresentação



Agenda

- Funcionamento
- Horário
- Avaliação
- Programa
- Bibliografia
- Requisitos laboratoriais



Funcionamento

- Aulas teóricas (Presenciais, algumas poderão ser virtuais via Zoom)
- Aulas práticas (Lab. Redes)
- Palestras/workshops de convidados
- Guias, desafios e trabalhos práticos
- Apresentações dos alunos
- Conteúdos disponibilizados no Moodle: <https://moodle2526.up.pt/course/view.php?id=6071>
- Algumas regras:
 - Presença física e mental
 - Ética



Horário

- **Aula Teórica:** Quinta-feira, 16h00-17h30
 - Intervalo 15 mins
- **Aula Prática:** Quinta-feira, 17h45-19h30
- **Horário de atendimento: N/A** - Email disponível para comunicação e esclarecimento de dúvidas pontuais



Avaliação

- Avaliação contínua ao longo do semestre **sem exame escrito final**
- **Componentes:**
 - A: Trabalho laboratorial (50%)
 - 1: Apresentações e motivação (10%)
 - 2: Teste prático (25%)
 - 3: Desafios de TPAS (15%)
 - B: Projeto semestral (50%)
- Nota final = .1*A1 + .25*A2 + .15*A3 + .5*B



Componente laboratorial

- Trabalhos de grupo e apresentações
- Semanalmente serão lançados desafios e guiões de laboratório
 - Alguns deles serão realizados nos laboratórios, outros em casa
 - Cada aluno deverá submeter soluções ou relatórios individualmente
 - Os pontos serão atribuídos na plataforma de desafios:
<https://tpas-desafios.alunos.dcc.fc.up.pt/>
- No final do semestre haverá um teste prático individual de *penetration test* (VM com serviços vulneráveis)
- Nota individual agregada sobre toda a informação recolhida durante o semestre



Projecto semestral

- Projecto obrigatório em grupo (2 alunos) desenvolvido durante o semestre
 - **Até dia 16/10/2025:** escolha do grupo e tema
 - Acompanhamento presencial e slots virtuais
 - **TBD Janeiro 2026:** Apresentações e entrega de relatórios



Programa

- Conceitos básicos de segurança da informação
- Reconhecimento e recolha de informação
- *Scanning, sniffing* e evasão
- *Network hacking*
- Análise de *malware*: *trojans* e outras aplicações maliciosas



Programa

- Ataques a sistemas operativos e software
- *Reverse engineering*
- Utilização e desenvolvimento de exploits
- *Web exploitation*: servidores e aplicações + introdução a bug bounties
- Testes de penetração



Bibliografia

- Hacking: The Art of Exploitation, 2nd Edition
 - Jon Erickson
- CEH: Certified Ethical Hacker Bundle, Third Edition (All-in-One)
 - Matt Walker
- The Hacker Playbook: Practical Guide to Penetration Testing
 - Peter Kim
- Unauthorized Access: Physical Penetration Testing for IT Security Teams
 - Kevin Mitnick
- Web Hacking 101
 - Peter Yaworski



Racional

- Um tratamento exaustivo desta temática nas aulas é impossível:
 - Demasiadas tecnologias e vulnerabilidades
 - Demasiados ataques, vectores
 - Demasiadas ferramentas
- Nas aulas veremos os conceitos fundamentais e ferramentas representativas
- Os trabalhos avaliam **não só** a aplicação de ferramentas estudadas nas aulas
- Mas também a iniciativa e o trabalho fora das aulas na exploração de outras ferramentas e técnicas



Requisitos laboratoriais

- Laboratório de redes: FC6137 @ DCC
- O uso de computador pessoal é altamente recomendado
- Distribuição Linux - **Ubuntu**, ou baseada em **Debian** são recomendadas (dual-boot ou VM)



Parte 2

Background



Agenda

- Elementos de segurança da informação
- Políticas de segurança
- *Ethical hacking*
 - Terminologia
 - Tipos de ataques
 - Fases de um ataque



hack'er



hack'er

/'ha-ker/

noun

one who enjoys the intellectual challenge of creatively overcoming limitations

hackerone



Teste de terminologia

- Vulnerabilidade
- *Exploit*
- *Payload*
- *Exploit chain*
- *Zero-day*
- *Target-of-Evaluation* (ToE)
- *Doxing*



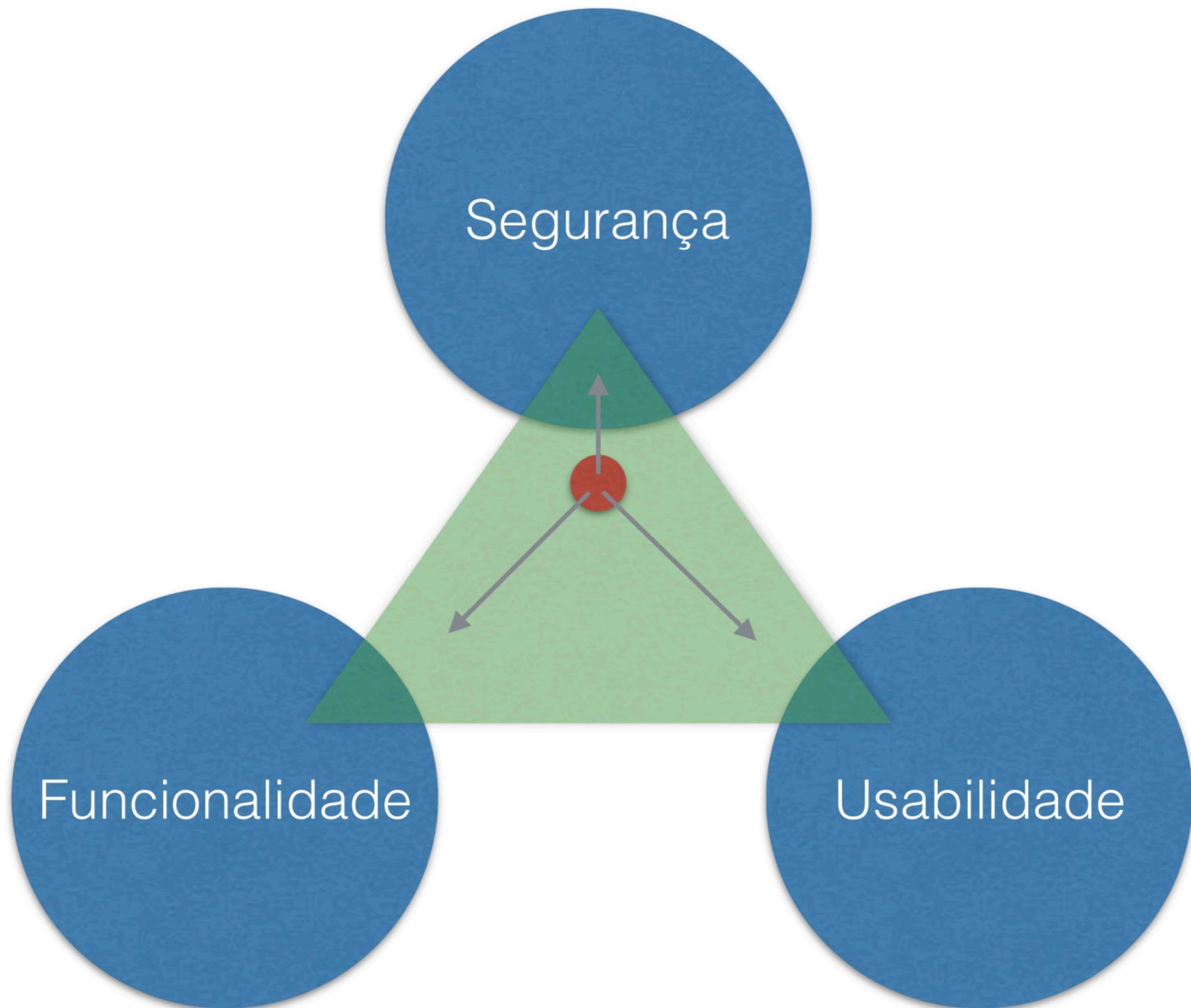
Segurança da Informação

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Não-repúdio





Compromissos: Um Triângulo





Vectores de ataque

- Ciber-crime organizado
- Software desactualizado
- *Malware* direcccionado
- Engenharia social
- Ameaças internas
- *Botnets*
- *Exploits* (incluindo *0days*)



Vectores de ataque

- Falta de profissionais especializados
- Aplicações de rede
- Políticas de segurança desadequadas
- Dispositivos móveis
- Hacktivismo
- Adopção de tecnologias imaturas



Estrutura de um ataque

- **Motivação:** perturbação, roubo de informação
- **Vulnerabilidade:** algo que pode ser explorado
- **Método:** forma de explorar a vulnerabilidade



Assets e ameaças

- Uma análise de segurança começa com a identificação de **assets (ativos)** e **threats (ameaças)**
- Estas permitem iniciar uma análise de risco
- Um ativo é algo com valor para a organização e que pode motivar um ataque
- Uma ameaça representa uma origem possível (agente, circunstância, etc) de danos aos assets



Ameaças

- Ameaças naturais
 - Desastres naturais (planos de contingência)
- Ameaças à segurança física
 - Perda ou destruição de equipamento
 - Intrusão física, sabotagem, espionagem
- Ameaças humanas
 - *Insider/outsider*
 - *Black hats*, hacktivismo, engenharia social, falta de preparação



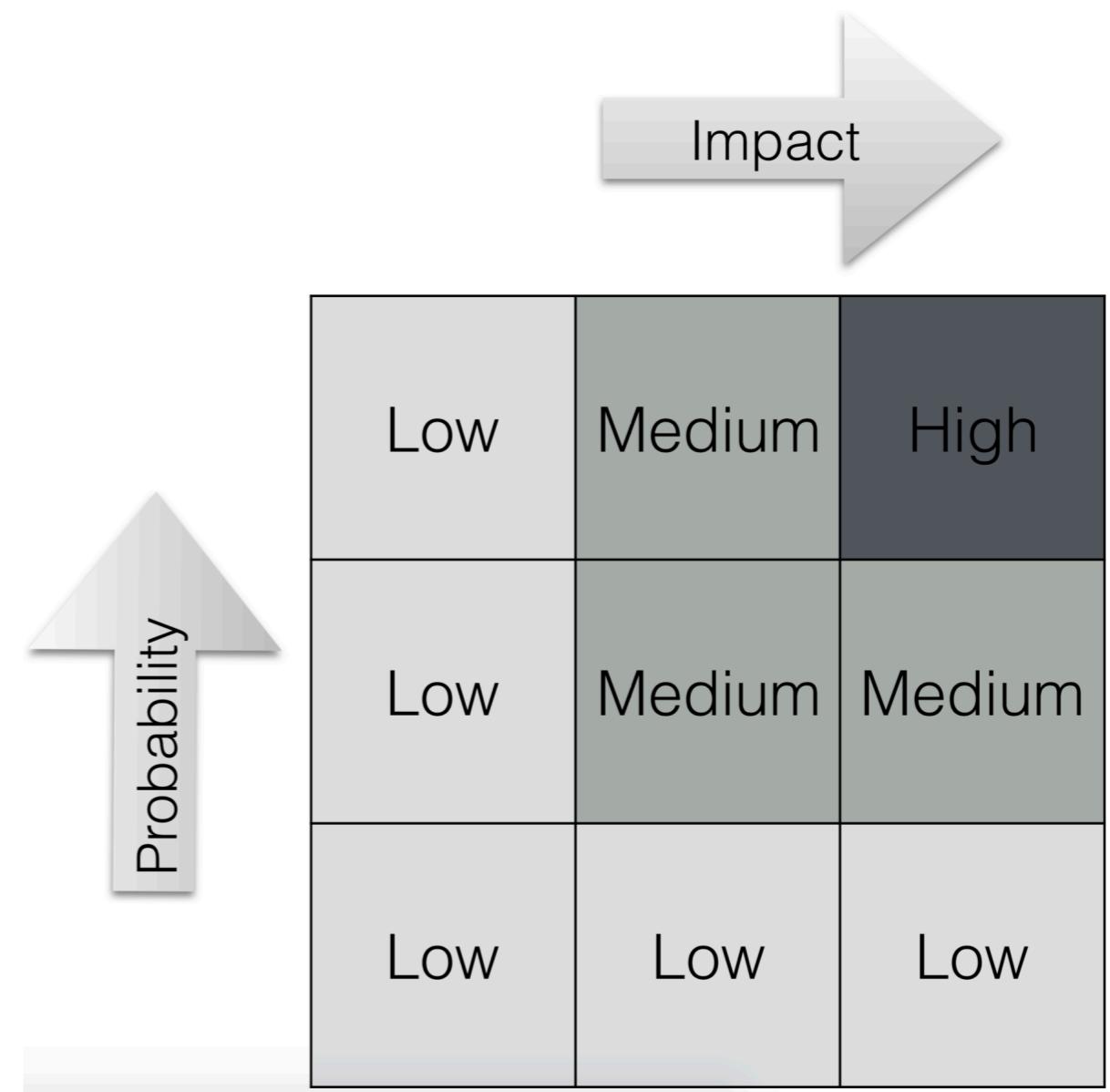
Ameaças humanas

- Ameaças à rede: largo espectro
 - Recolha de informação, *sniffing, spoofing, hijacking*, etc
- Ameaças à máquina: direcionadas
 - *Malware, DoS, intrusão física, remote exploits*, etc
- Ameaças à aplicação
 - Validação de inputs, criptografia fraca, *memory corruption*



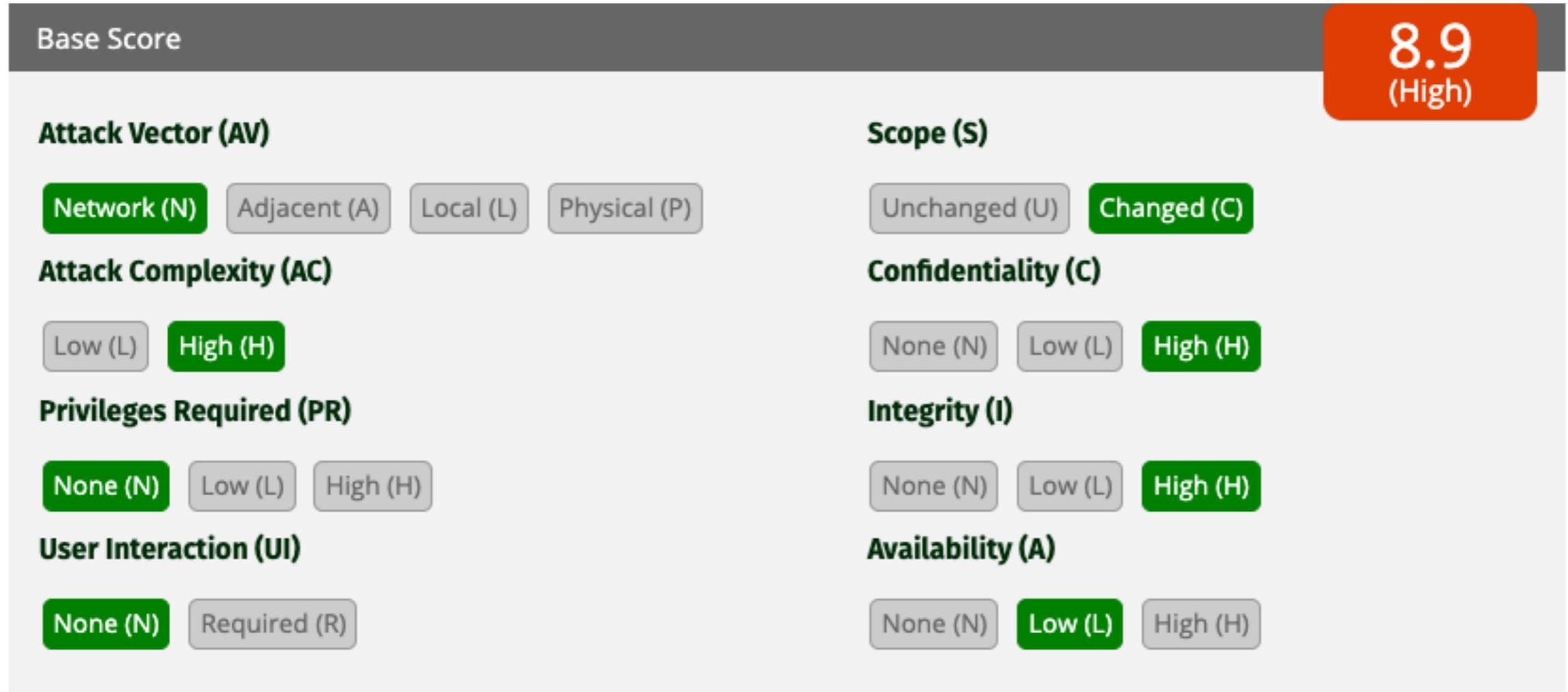
Análise de risco

- A acção a tomar depende de dois factores críticos:
 - Potencial impacto
 - Probabilidade de materialização
- Cada ameaça tem que ser avaliada nestes dois eixos
- A decisão de mitigação depende do risco avaliado





CVSS



Vector String -

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:L/E:P

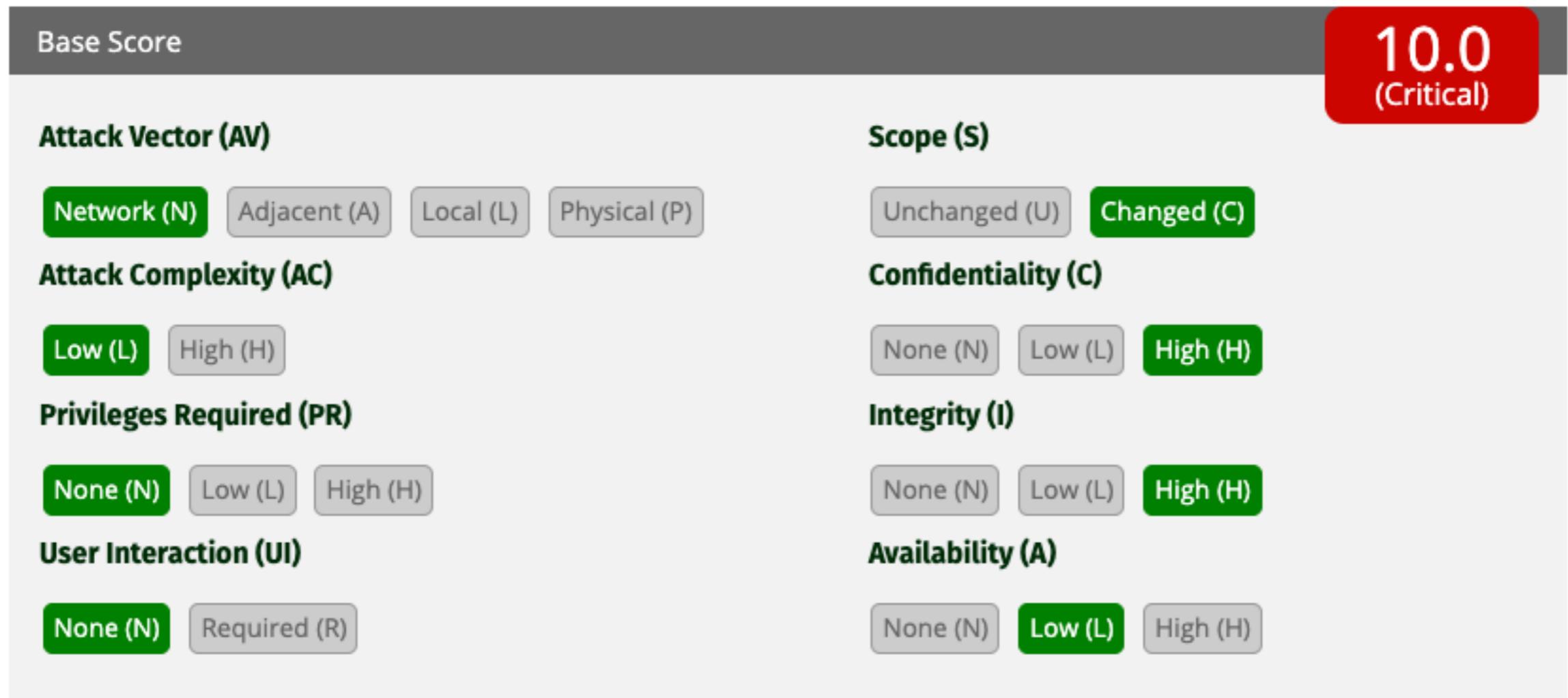
Ver: <https://www.first.org/cvss/calculator/3.1>



FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO



CVSS



Vector String -

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L/E:P



CVSS

- Versão 4.0 vai começar a ser adoptada progressivamente
- Diferenças principais:
 - Pontuação contextual: probabilidade de materialização
 - Complexidade do ataque: mais granular, requisitos
 - Métricas temporais (maturidade e existência de patch)
 - Mais informação: <https://www.first.org/cvss/v4.0/specification-document>



Defesas em profundidade

- Aplicação
- Máquina
- Rede interna
- Perímetro
- Física
- Políticas, procedimentos e consciencialização



Mecanismos de controlo

- Físicos
 - guardas, câmaras, cofres
- Técnicos
 - smartcards, biometria, ACLs
- Administrativos
 - penalizações, formação
- Preventivos / correctivos



Políticas de segurança

- Descrição dos controlos de segurança
- Mapa para a gestão da segurança da informação
- Gestão de responsabilidade
- Gerir equilíbrio entre serviço prestado e recursos
- Evitar acessos ou modificações não autorizados
- Redução de risco de danos
- Clarificar os privilégios dos actores



Tipos de políticas de segurança

- Gestão de utilizadores (e.g., passwords, email)
- Gestão IT (e.g., *backups*, configuração, etc)
- Responsabilidades
- Parceiros
- Específicas (e.g. segurança física)



U. Construção de políticas de segurança

- Análise de risco
- Enquadramento em normas/standards
- Diálogo com a gestão
- Definição de penalizações
- Implementação e formação



Gestão de incidentes

- Preparação
- Detecção e análise
- Classificação e priorização
- Notificação
- Capacidade de resposta
- Contenção
- Investigação forense
- Erradicação e recuperação
- Actividades pós-incidente



“Ciberguerra”

- Defensiva
 - “Prevenção”?
 - Alertas, detecção
 - Prontidão, resposta
- Ofensiva
 - Ataques a aplicações e servidores
 - Ataques com *malware* ou *phishing*
 - Ataques MitM (e.g., dentro da infra-estrutura)



Cybersecurity DRAFT

Offensive Defensive

Plates represent distinct fields of knowledge

Labels represent specializations

Signals

Business Model

Operation Management

Signals

Legislation

traces

evidence

DoS

marketing

ransom

mining

reputation

put everything together

C&C

exfil

control agent

stealth

to the root cause

antivirus

botnet hacking

regulation

persistence

covers

payload

control agent

stealth

DFIR

leverage for scale

botnet hacking

regulation

signals

Infrastructure

Exploit

Vuln

Patch

o

Vulnerability is
the core of entire
industry

Focus on the
core

This is an
adversarial model
of my industry

© Alisa Esage (www.zerodayengineering.com)

Zero Day Engineering



FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO



Ethical Hacking

- A distinção está nas intenções
- **Hacking Cracking:** geralmente não autorizado, ilegal, intenção de utilizar o sistema para fins não previstos e/ou causar dano
- **(Ethical) hacking:** autorizado, intenção de efectuar diagnóstico, encontrar vulnerabilidades (pode causar dano), com o fim de melhorar a protecção
- Excelentes conhecimentos ofensivos levam a uma melhor capacidade de defesa



Enquadramento legal

- Lei 109/2009 - ciber-crime
- Lei 67/ 1998 - proteção de dados pessoais
- Lei 41/2004 - regula a proteção de dados pessoais no sector das Comunicações Eletrónicas
- Convenção de Budapeste (Convenção sobre ciber-crime do Conselho da Europa)
- Decisão-Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação
- Diretiva 95/46/CE – Diretiva de Proteção de Dados Pessoais Diretiva
- 2002/58/CE – Diretiva das Comunicações Eletrónicas
- Diretiva 2006/24/CE – relativa à conservação de dados das comunicações eletrónicas e que altera a Diretiva 2002/58/CE

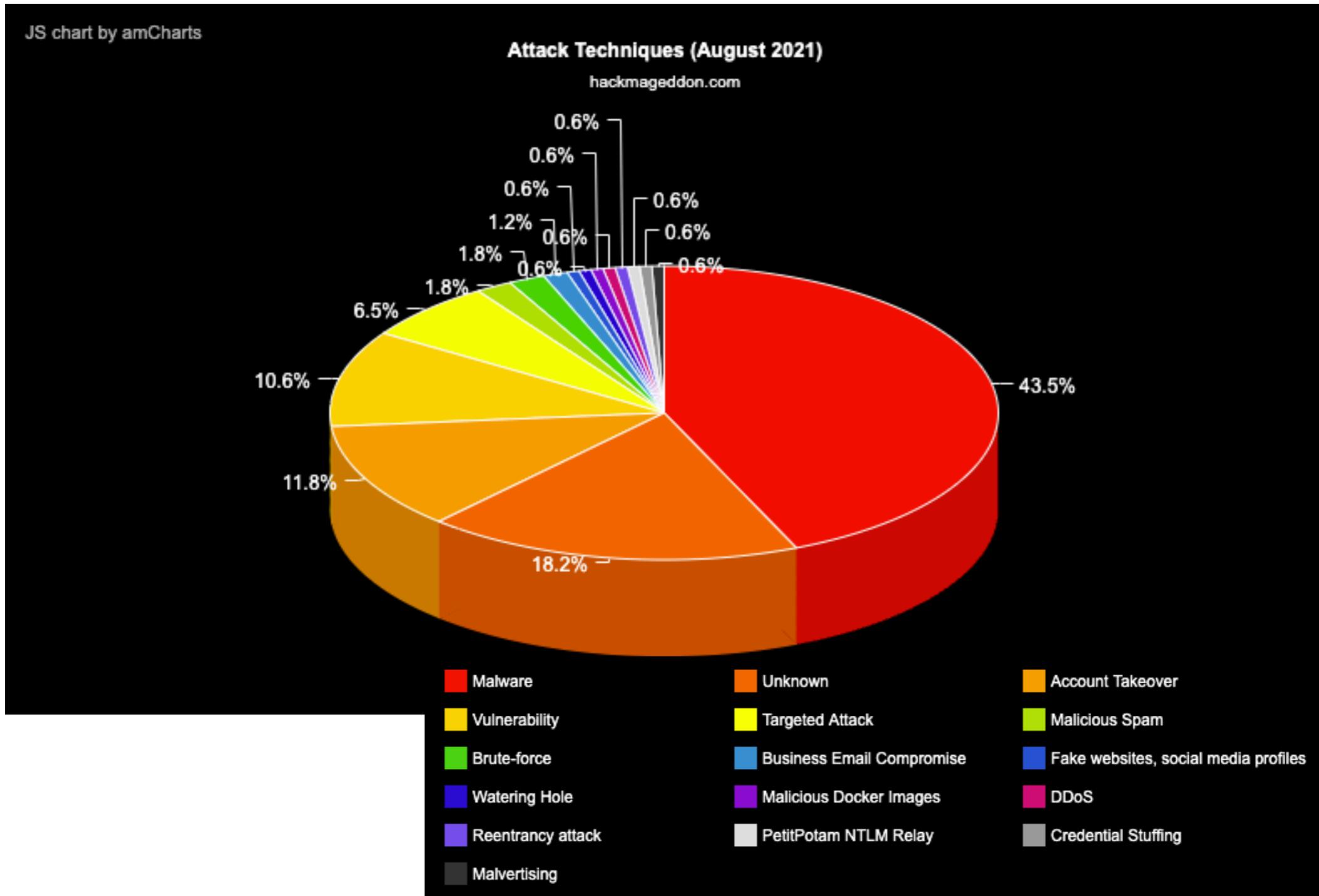


Impacto do cracking

- Perda/divulgação não desejada de informação
- Perda de valor (e.g., botnets, DoS e down-time)
- Perda de negócio (e.g. propriedade intelectual)
- Danos na reputação (defacing; imagem, confiança)
- Tudo somado: \$10.5 triliões por ano (Cybersecurity Ventures)
- <https://www.hackmageddon.com/>
- <https://www.ic3.gov/>



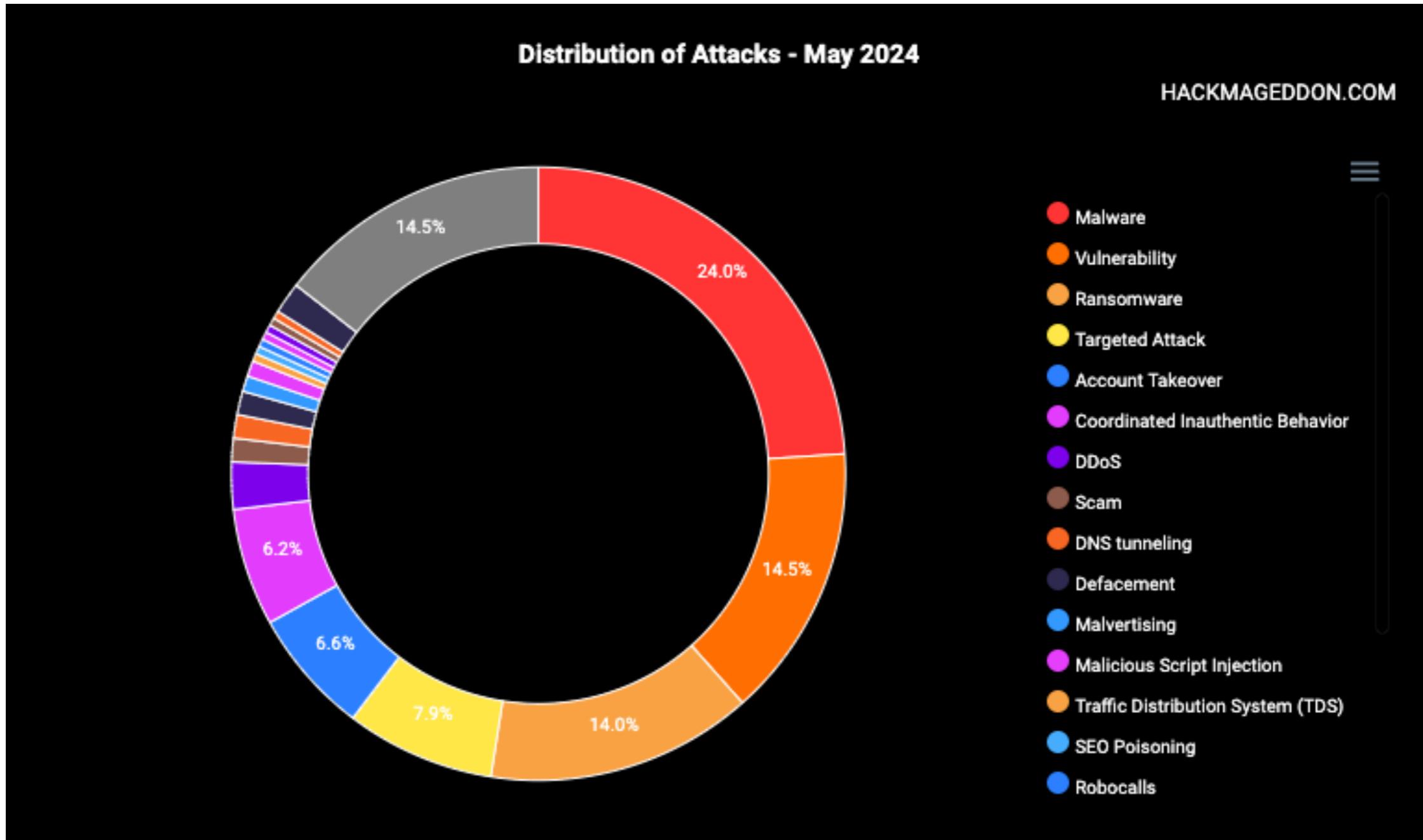
Impacto do cracking



Fonte: [hackmageddon](https://hackmageddon.com)



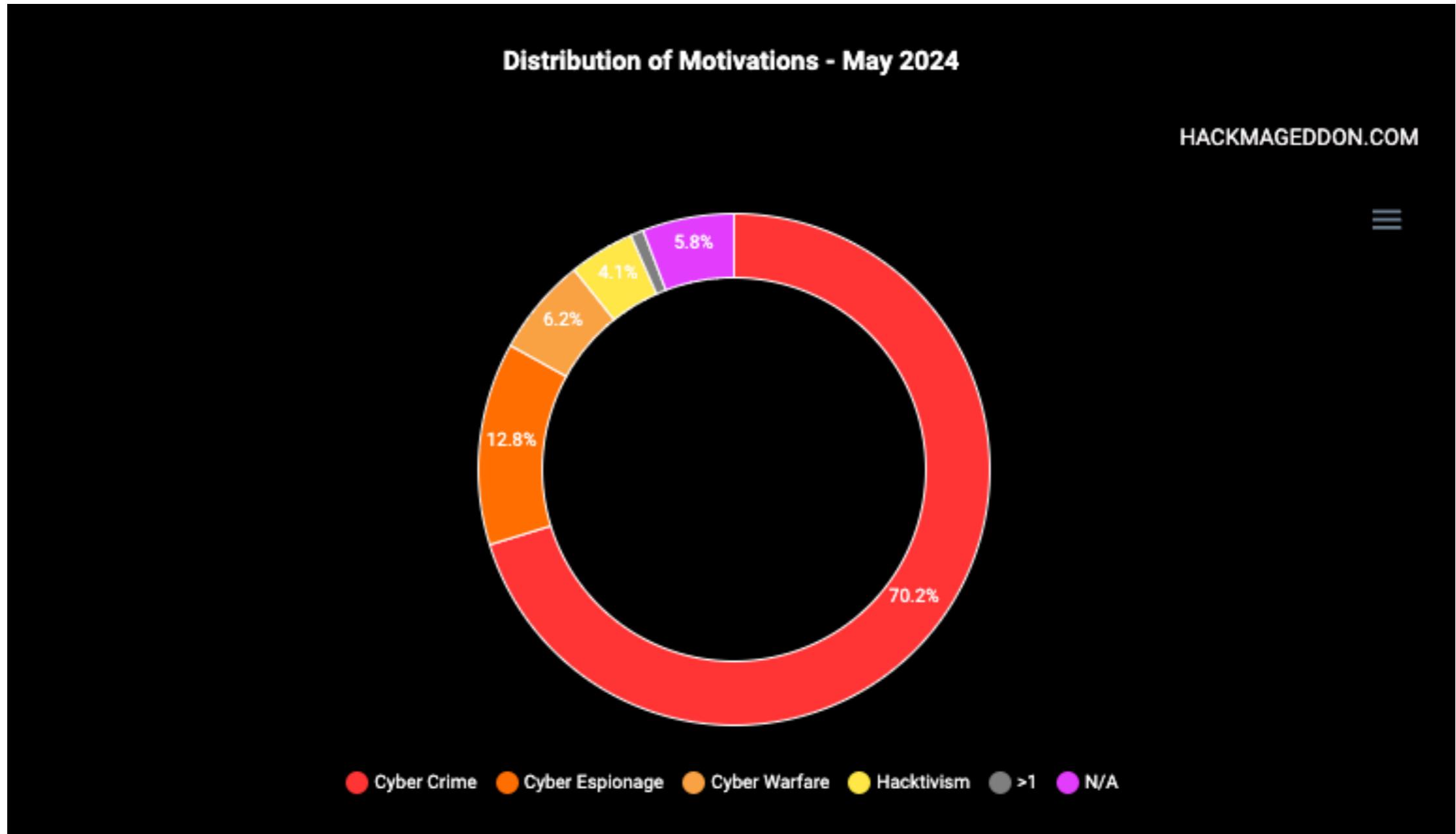
Impacto do cracking



Fonte: [hackmageddon](https://hackmageddon.com)



Impacto do cracking



Fonte: [hackmageddon](https://hackmageddon.com)



Perfil de um *hacker*

- Indivíduos inteligentes, criativos e com *computer expertise*
- Muitas vezes é um *hobby*, um desafio
- Intenção pode ser obter conhecimento ou utilizar recursos para efectuar operações ilegais
- Pode haver valor interínseco na informação obtida (e.g., cartões de crédito, passwords, etc)
- Conhecimentos: redes, sistemas operativos, aplicações, criptografia, *hardware*, *exploitation*, *reverse engineering*



Tipos de hackers/crackers

- *Black-hat*
- *White-hat*
- *Script-kiddies*
- Hackers patrocinados por estados (*state actors*)
- Hacktivistas



Fases do hacking

- **Reconhecimento passivo/activo, levantamento**
 - Social engineering, DNS records, procura de informações na internet, identificação da superfície de ataque, enumeração de subdomínios, *port scanning, content discovery*
- **Identificação de vulnerabilidades**
 - Uso da informação obtida na fase de *recon* para identificar vulnerabilidades
 - Cuidados com sistemas de detecção de intrusões, (e.g., WAFs)



Fases do hacking

- **Exploração da vulnerabilidade(s)**
 - Através de uma ou várias, explorar a vulnerabilidade com o exploit apropriado
- **Acesso**
 - A partir da exploração da vulnerabilidade
 - Obter acesso a uma rede, máquina ou aplicação para:
 - Escalar privilégios ou causar danos imediatos
- **Manter acesso**
 - Assegurar acesso futuro, *low profile*
 - Apagar evidências



Tipos de vulnerabilidades

- Sistema operativo, e.g., vulnerabilidades em serviços desactualizados
- Aplicação, e.g., XSS, buffer overflows, SQL injection...
- Código off-the-shelf (shrink-wrap code)
- (Des)configuração
- ...



Testes de penetração

- Método de avaliação do nível de segurança de um sistema
- Simulação de um ataque de procura de vulnerabilidade que poderiam ser exploradas
- *Black box*: semelhante a um ataque real
- *White box*: com conhecimento privilegiado
- O valor está nos relatórios, passos para reproduzir e recomendações finais



Catálogo de vulnerabilidades

- Há quem encontre vulnerabilidades
- Há quem explore vulnerabilidades
- Há quem recolha e mantenha essa informação:
 - Common Vulnerabilities and Exposures: <https://cve.mitre.org>
 - Security Focus: <https://www.securityfocus.com>
 - National Vulnerability Database: <https://nvd.nist.gov>
- Os sites de CERT (Computer Emergency Response Team) são também úteis:
 - <https://www.us-cert.gov>
 - <https://cert.europa.eu>
 - <https://www.cncs.gov.pt/pt/notificacao-incidentes/>



CVE

- “*CVE is a dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, databases, and services) with these definitions. CVE Entries are comprised of an identification number, a description, and at least one public reference.*”



Trabalho de grupo - CVE

- Grupos de 2 elementos
- Cada grupo deve informar o decente da sua constituição e a vulnerabilidade escolhida (*first-come first-served basis*) através do link:
<https://forms.gle/mUGWuCkSAjkMLjks8> **até dia 26/09**
- Cada grupo deve utilizar o site <https://cve.mitre.org> (Common Vulnerability Database) para:
 - **Identificar uma vulnerabilidade com severidade >= High**
 - Investigar: **contexto, teoria, técnicas/exploit, demonstração (i.e. POC)** (se possível), **impacto e contramedidas**
 - Aulas de **09/10/2025** - virtual (zoom link via email):
flash presentation, máximo 10 minutos por grupo



Parte 3

Apresentação da equipa xSTF

<https://xstf.pt>