Ethical Hacking

Ferramentas OpenSource para Pentest

Pentester Mateus Buogo

Quem sou eu?

Nome: Mateus Buogo

Formação: Redes de Computadores – UNIFTEC / MBA Administração de TI – UNISINOS / Mestrando em Administração - UCS

Cursos: ITIL Avançado; ISO27001 e ISO27002; Configuring and Troubleshooting a Windows Server; Administração de Servidores Linux; Ethical Hacking, Enterprise Security Fundamentals (Microsoft), Formação de Pentester (DESEC)

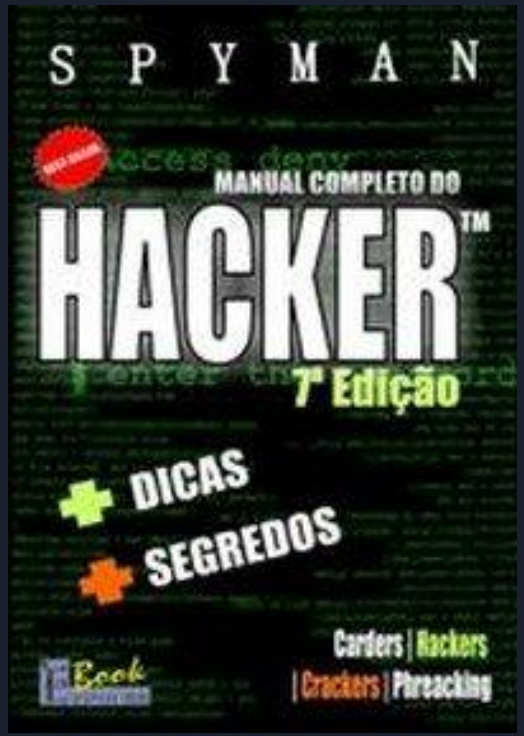
Experiência Profissional: Analista de Segurança

Experiência Acadêmica: Segurança em Redes, Sistemas Operacionais, Governança de TI, Serviços de Redes e Segurança da Informação

DCPT


DESEC
CERTIFIED
PROFESSIONAL
MATEUS BUOGO
Concluiu com êxito o exame para a Certificação Penetration Tester Desec Security
DCPT
DESEC CERTIFIED PENETRATION TESTER
CHAVE: UJYA-CSJUK-BSUU
20 de maio de 2019
Ricardo Longatto
Diretor Executivo
Para validar este certificado acesse desecsecurity.com e informe a chave.

Onde tudo começou...



Ethical Hacking

Vulnerability management is a core element in modern information technology (IT) compliance. IT compliance is defined as the adherence to legal, corporate and contractual rules and regulations as they relate to IT infrastructures. Within its context IT compliance mainly relates to information security, availability, storage and privacy. Companies and agencies have to comply with many legal obligations in this area.

http://www.openvas.org/

Ethical Hacking

- Technology lag
- Application development security
- Skill gap
- Asymmetry of attack and defense
- Increasing availability and sophistication of attack tools
- Monetization of malware
- Automation of Detection
- Internet of Things
- Transition to the cloud
- Increasing regulation

Ethical Hacking

When considering the cybersecurity landscape, it's important to note that the versions of products that organizations have deployed exist on a spectrum, **with a small number of organizations running the latest versions, most organizations running older but still supported versions, and a substantial number of organizations running information systems that are no longer supported by the vendor.**

It's usually the organizations running outdated or unsupported products that you hear about when a large cybersecurity incident occurs. For example, the 2017 **WannaCry ransomware attack disproportionally impacted organizations that had servers running the Windows Server 2003 operating system** where the ports that are used for SMB storage protocol were exposed to the internet.

Ethical Hacking

The recent Global Information and Security Workforce Study by the Center for Cyber Safety and Education projected a global **shortfall of 1.8 million information security workers by 2020.**

HACKING
IS NOT
A CRIME

Ethical Hacking

Um Hacker Ético é um especialista em sistemas e redes de computadores que conhece as técnicas e métodos utilizados para se encontrar vulnerabilidades de segurança em **softwares e redes corporativas**.

Antes de mais nada, um hacker é um especialista em sistemas e redes de computadores. Ele conhece muito bem a base teórica e prática do funcionamento de **sistemas e redes.**

http://profissaohacker.com/

Ethical Hacking

Pen Tester: Salário médio de 2015: R$6.500 – 14.000

Desenvolvedor: Salário médio de 2015: R$6.500 – 12.000

Profissional de infraestrutura: Salário médio de 2015: R$4.000 – 7.000

http://aratuonline.com.br/noticias/mundo-hacker-conheca-os-perfis-salarios-e-como-esta-o-mercado-para-profissionais-da-tecnologia/?utm_content=bufferbc9f4&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer

Ethical Hacking

Nível 1 – Júnior - Tool based Penetration

Nível 2 - Pleno Coding based Penetration

Nível 3 – Sênior Vulnerability Researcher

Ethical Hacking

EXIN ETHICAL HACKING

C|EH Certified Ethical Hacker

GIAC CERTIFIED PENETRATION TESTER GPEN

OFFENSIVE® security OSCP

GIAC WEB APP PEN TESTER GWAPT

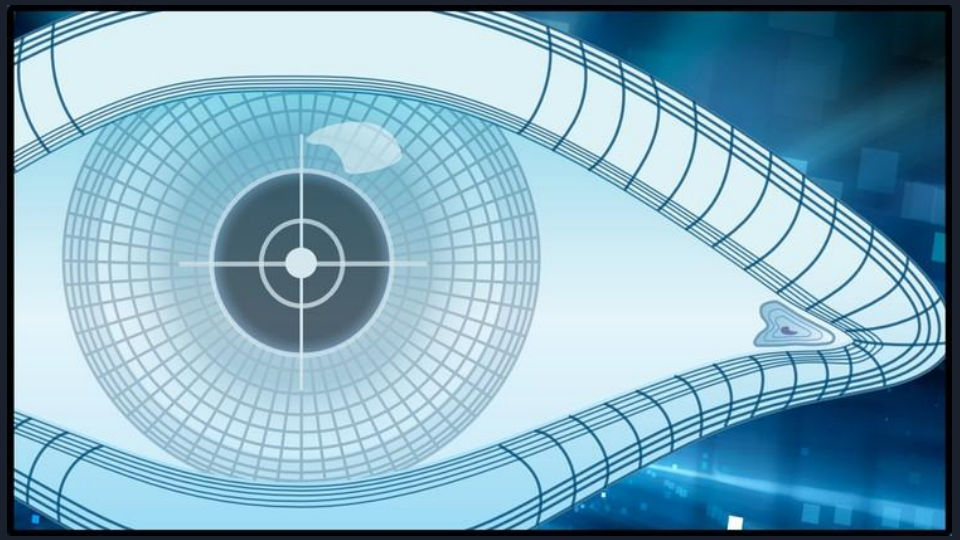
DESEC INFORMATION SECURITY

24 horas de exame.

Ferramentas

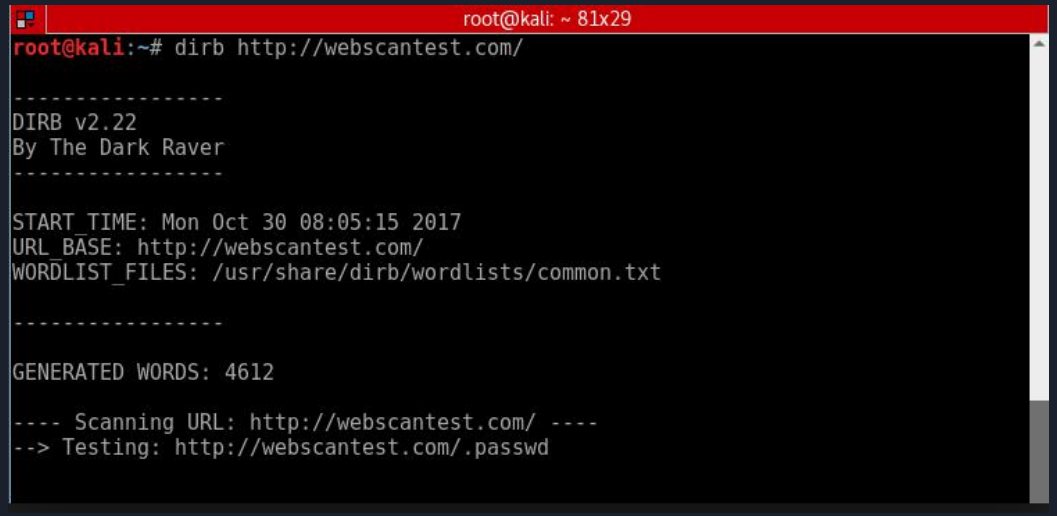
- DIRB
- NMAP
- NETCAT
- METASPLOIT (só para conhecimento, não dependa dela!)

NMAP



NETCAT

DIRB


root@kali: ~ 81x29
root@kali:~# dirb http://webscantest.com/

DIRB v2.22
By The Dark Raver

START_TIME: Mon Oct 30 08:05:15 2017
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
---- Scanning URL: http://webscantest.com/ ----
--> Testing: http://webscantest.com/.passwd

NETCAT

Ethical Hacking

contato: mbuogors@gmail.com
site: https://letshack.com.br