SHELL SCRIPT

SEU ALIADO NO PENTEST!

#> QUEM SOU EU

LET'S HACK

MATEUS BUOGO

FORMACAO

- REDES DE COMPUTADORES
- MBA ADMINISTRACAO DE TI
- MESTRANDO EM ADMINISTRACAO

PROFISSIONAL

- ANALISTA DE SEGURANCA
- PROFESSOR

CONTATO

MBUOGORS@GMAIL.COM

MATEUSBUOGO@LETSHACK.COM.BR

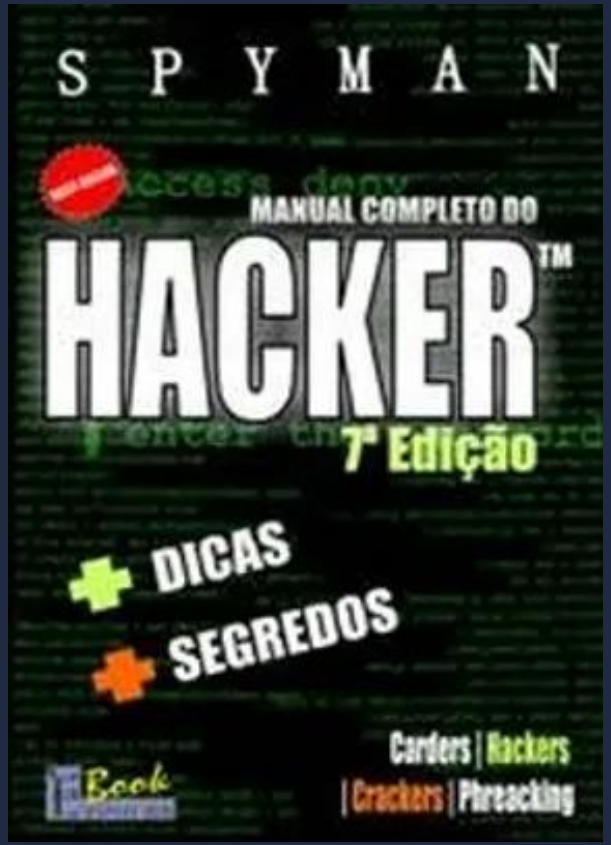
LET'S HACK

HTTPS://LETSHACK.COM.BR

#> SEGURANCA OFENSIVA

LET'S HACK

ONDE TUDO COMECOU?



#> SEGURANCA OFENSIVA

LET'S HACK

NOME BONITO PARA UTILZAR TECNICAS DE HACKING PARA IDENTIFICAR VULNERABILIDADE EM SISTEMAS CORPORATIVOS.

#> ESTAMOS EXPOSTOS?

LET'S HACK

O DESAFIO DA CIBERSEGURANCA NA SAUDE

PARA CLAUDIO BANNWART, COUNTRY MANAGER DA CHECK POINT NO BRASIL, OS BAIXOS NIVEIS DE SEGURANCA QUE OS HOSPITAIS APRESENTAM FACILITAM O ACESSO A UM ENORME VOLUME DE INFORMACOES SENSIVEIS, O QUE POR SUA VEZ PERMITE A OBTENCAO DE ELEVADOS PROVEITOS FINANCEIROS POR PARTE DOS ATACANTES.

PORTAL SECURITY REPORT - 25/09/2019

#> ESTAMOS EXPOSTOS?

LET'S HACK

DISPOSITIVOS DE SAUDE PODEM ACARRETAR RISCOS PARA A SEGURANCA CIBERNETICA

AS PRINCIPAIS AMEACAS CIBERNETICAS QUE ATINGEM OS DISPOSITIVOS DE SAUDE PODEM SER DIVIDIDAS EM TRES TIPOS: AQUELAS QUE VIOLAM A PRIVACIDADE DOS DADOS, AS QUE COMPROMETEM A INTEGRIDADE DESTES E AS QUE ATACAM SUA DISPONIBILIDADE.

PORTAL SECURITY REPORT - 18/01/2019

#> ESTAMOS EXPOSTOS?

LET'S HACK

VIOLACOES DE DADOS COMPROMETERAM 4,5 BILHOES DE REGISTROS NO PRIMEIRO SEMESTRE

QUANDO COMPARADO AO MESMO PERIODO EM 2017, O NUMERO DE REGISTROS PERDIDOS, ROUBADOS OU COMPROMETIDOS AUMENTOU EM 133%; A SAUDE CONTINUA A LIDERAR EM NUMERO DE INCIDENTES (27%).

PORTAL SECURITY REPORT - 10/10/2018

#> ESTAMOS EXPOSTOS?

LET'S HACK

PESQUISADORES DESCOBREM FALHAS QUE PERMITEM FALSIFICAR SINAIS VITAIS DE PACIENTE

TIME DA MCAFEE DESCOBRIU UMA FRAQUEZA NO PROTOCOLO RWHAT USADO PELOS DISPOSITIVOS MEDICOS; SE UM HACKER EXPLORAR ESSA VULNERABILIDADE, ELE PODERA FORNECER INFORMACOES FALSAS A EQUIPE MEDICA EM TEMPO REAL

PORTAL SECURITY REPORT - 14/08/2018

#> ESTAMOS EXPOSTOS?

LET'S HACK

HACKERS VENDEM DADOS DE 127 MILHOES DE CONTAS NA DARK WEB

MAIS 127 MILHOES DE SENHAS DE OITO SITES SURGIRAM A VENDA NO DREAM MARKET, UM MERCADO DE PRODUTOS ILEGAIS QUE FUNCIONA NA DARK WEB. A DESCOBERTA FOI FEITA PELO SITE BRITANICO THE REGISTER, NA ULTIMA QUINTA-FEIRA (14), QUE RELATOU QUE PACOTE COMPLETO DE INFORMACOES ROUBADAS PODIA SER OBTIDO PELO EQUIVALENTE A R$ 54 MIL EM BITCOIN.

PORTAL TECH TUDO - 16/02/2019

#> SEGURANCA OFENSIVA

LET'S HACK

VULNERABILITY MANAGEMENT IS A CORE ELEMENT IN MODERN INFORMATION TECHNOLOGY (IT) COMPLIANCE.

#> SEGURANCA OFENSIVA

LET'S HACK

CENARIO ATUAL

- LAG DE TECNOLOGIA
- SKILL GAP
- ASSIMETRIA ATAQUE E DEFESA
- MONETIZACAO MALWARES
- IOT
- CLOUD
- FERRAMENTAS DE ATAQUE

#> SEGURANCA OFENSIVA

LET'S HACK

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.

OPENVAS.ORG

#> SEGURANCA OFENSIVA

LET'S HACK

RANSOMWARE WANNACRY

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.

INF246X - ENTERPRISE SECURITY FUNDAMENTALS - EDX.ORG

#> $ $ $ $ $

LET'S HACK

THE COST OF A BREACH IS ALWAYS AN ESTIMATE. EVEN AFTER A BREACH OCCURS, THE ACTUAL COST OF THE BREACH MAY NEVER BE ACCURATELY DETERMINED. ON TOP OF THE DISRUPTION TO THE BUSINESSES PROCESSES, IT IS DIFFICULT TO ASSESS THE VALUE OF INTANGIBLES SUCH AS REPUTATIONAL DAMAGE, THE COST OF REHABILITATING COMPROMISED SYSTEMS, THE COST OF INVESTIGATING THE BREACH ITSELF AND THE COST OF ANY FINES OR PENALTIES THAT MAY NEED TO BE PAID TO THE RELEVANT AUTHORITY.

INF246X - ENTERPRISE SECURITY FUNDAMENTALS - EDX.ORG

#> $ $ $ $ $

LET'S HACK

O CUSTO DA *PREVENCAO* E SEMPRE MENOR QUE O CUSTO DA *REMEDIACAO*.

#> ETHICAL HACKER

LET'S HACK

UM **HACKER** ETICO E UM **ESPECIALISTA** EM SISTEMAS E REDES DE COMPUTADORES QUE CONHECE AS **TECNICAS** E METODOS UTILIZADOS PARA SE **ENCONTRAR** VULNERABILIDADES DE SEGURANCA EM SOFTWARES E REDES CORPORATIVAS.

HTTP://PROFISSAOHACKER.COM/

#> SEGURANCA OFENSIVA

HACKING
IS NOT A CRIME

#> SEGURANCA OFENSIVA

LET'S HACK

CERTIFICACOES

EXIN Ethical Hacking
Certified by EXIN

C|EH™ Certified Ethical Hacker

DESEC INFORMATION SECURITY

OFFENSIVE® security OSCP

#> SEGURANCA OFENSIVA

LET'S HACK

RED TEAM

BLUE TEAM

#> LEGISLACAO

LET'S HACK

LGPD

GDPR

A SEGURNACA OFENSIVA FAZ PARTE DO SEU ESCOPO?

#> MAO NA MASSA

LET'S HACK

MAS CHEGA DE LERO LERO!
VAMOS AOS SCRIPTS!

#> MAO NA MASSA

LET'S HACK

https://github.com/mbuogo

#> ENCERRAMENTO

LET'S HACK

A PERGUNTA NAO E "SE" VAMOS SER INVADIDOS, MAS SIM "QUANDO" SEREMOS.

#> ENCERRAMENTO

LET'S HACK

TUDO E UMA QUESTAO DE TEMPO, DINHEIRO E OPORTUNIDADE.

#> ENCERRAMENTO

OBRIGADO

LET'S HACK