Prova de Aptidão Profissional

CYBER SECURITY

Técnico de informática sistemas

Samuel Sousa
12º7 Nº18
2025

Agradecimentos

Gostaria de expressar minha profunda gratidão a todos que contribuíram direta ou indiretamente para a realização deste trabalho.

Em primeiro lugar, agradeço aos meus professores, que ao longo do curso compartilharam não apenas seus conhecimentos técnicos, mas também valores éticos fundamentais para a prática segura e responsável da segurança da informação. Sua dedicação e comprometimento foram essenciais para o meu aprendizado e crescimento acadêmico.

Aos meus colegas de classe, agradeço pela parceria, troca de experiências e apoio mútuo durante os desafios que enfrentamos juntos. A convivência e o trabalho em equipe contribuíram significativamente para o desenvolvimento deste projeto e tornaram o processo de aprendizagem mais rico e motivador.

Aos meus pais, deixo um agradecimento especial por todo o apoio, incentivo e compreensão ao longo da minha trajetória. Sua presença constante e o suporte emocional foram fundamentais para que eu pudesse me dedicar com seriedade aos estudos e superar os obstáculos com confiança.

Reconheço que nenhum conhecimento se constrói sozinho, e sou verdadeiramente grato a todos que, de alguma forma, fizeram parte dessa jornada. Esse trabalho é fruto da colaboração, da paciência e do esforço coletivo.

Muito obrigado!

Indice

Índice de Ilustrações

Resumo

Desde criança tive contato com computadores, o que despertou meu interesse pela área. No secundário, escolhi o curso de Técnico de Informática – Sistemas, onde aprendi montagem, configuração e programação, começando com Python.

No 12º ano, estagiei na empresa Sofvoice, onde, junto com um colega, desenvolvi um software em Java para automatizar a contagem de equipamentos do armazém. Trabalhei na parte visual do programa, que foi concluído com sucesso. Projeto: GitHub - Softvoice Scanner

Após essa experiência, comecei a me interessar pela área de Cibersegurança, que hoje é o meu principal foco.

Nesse relatório, farei uma simulação de um ataque de pentest ou hacking, ensinando passo a passo de como o fazer e como se defender.

Tudo nesse relatório é totalmente legal e feito num abiente controlado para o próprio.

Introdução

Comeci a me interessar por cyber segurança pouco a pouco. Quando eu era criança, via meu pai a trabalhar nos computadores devido a um curso que ele estava fazendo, via ele montando e desmontando, parafusando e configurando, e sem perceber, estava cada vez mais interessado naquilo.

Terminei o 9º ano, ao ingressar no secundario, tinha que escolher que curso que iria me "especializar". Escolhi TECNICO DE INFORMATICA – SISTEMAS. Nesse curso, fiz oque meu pai fazia, montar, desmontar, configurar e até montar um cabo de rede. Mas olhando mais pra frente me perguntei, È isso que quero fazer? E nesse mesmo curso que conheci a programação. Algo muito importante para o ramo de TI, mas também dependendo da linguagem, dificil .Nas aula, começamos a programar em python, uma liguagem simples e sintaxes compreendiveis. Começamos com o basico, como fazer o computador mostrar algo na tela. Nisso percebi o real valor da aplicaçoes, porque um simples "ola mundo" na tela de um computador podia ser algo muito complicado para um iniciante como eu na altura.

Ao longo do tempo, fui aprendendo cada vez mais, porque eu estava decidido a ser um programador. No ultimo ano (12º ano), estagiei numa empresa chamada Sofvoice. Era uma empresa onde disponibilizava maquinas e apps para melhorar o funcionamento das lojas. Foi um trabalho mais pratico, como testar impressoras, tanto limpar quanto desmontar computadores. Mas o "chefe" tinha um "problema".

----ele disse:

Temos muitos equipamentos no armazem, tanto coisa novas quanto coisas que já deveriam ter indo embora. Queremos fazer uma contagem de tudo que temos aqui, Mas seria muito dificil contar a mao tudo que temos aqui. Quero que voces desenvolvem um programa que faça contagem automaticamente.

E foi quando eu e o meu colega começamos o desenvolimento do sofware. Foi algo bem interessante, pois algo que realmente aconteceria numa empresa de desenvolvimento (programação). Fizemos o programa em JAVA, perfeito para esse tipo de trabalho. Meu colega cuidou da parte da logica do programa, e eu da estetica. Quase terminando o estagio, finalizamos o programa, e funcionava perfeitamente. Projeto: https://github.com/manteiga25/Softvoice_scanner.git

Logo um tempo depois, ao terminar o estagio, comecei a pensar sobre esse tipo de trabalho que enfrentaria ao longo da minha carreira. Mas não desanimando, continuei o estudo na area. Ao procurar Areas como sugundas opcões, encontrei algo chamado CYBERSECURITY. Foi quando tudo começou.

CYBERSECURITY

A partir de agora, vou mostrar como foi todo o meu processo de aprendizado e evolução na área de cibersegurança.

Descobrimento

Descobrimento, foi marcado pela motivação e curiosidade. Antes de começar qualquer prática, pesquisei bastante em diversas plataformas sobre as vantagens e desvantagens dessa área. Queria entender bem no que estava me envolvendo — quais conhecimentos seriam necessários, quais ferramentas são mais usadas, e quais desafios eu poderia enfrentar. Foi um momento essencial para me preparar mentalmente e traçar os primeiros passos da minha jornada.

Figura 1_img_descobrimento

Ao me aprofundar, entendi que cibersegurança não se resume apenas ao termo 'cyber' — envolve uma ampla gama de conceitos técnicos, como redes, criptografia, sistemas operacionais e análise de vulnerabilidades.

Descobrindo o Mundo Hacker

Naquele dia, tive a certeza de que queria seguir carreira na área de cibersegurança. Com isso em mente, comecei a procurar maneiras de dar os primeiros passos de forma prática e eficiente. Foi então que encontrei a ferramenta ideal para iniciantes e profissionais da área: o **Kali Linux**. Essa distribuição voltada para testes de penetração e análise de segurança me mostrou um novo mundo de possibilidades, onde poderia aprender e experimentar com ferramentas reais usadas no mercado.

Figura 2_img_mundo_hacker

O que é o kali-linux?

O Kali Linux é uma distribuição Linux concebida para análise forense digital e testes de intrusão. É mantido e financiado pela Offensive Security. O software baseia-se no ramo Debian Testing: a maioria dos pacotes que o Kali utiliza são importados dos repositórios Debian.

O kali é uma ferramenta muito usada no ramo da cyber segurança, serve tanto para um ataque ofensivo, quanto para defesa. E ele é bem conhecido pelo fato de portar diversas ferramentes num único lugar (sofware), como o NMAP, METAEXPLOIT, HYDRA, e muito mais.

A Diversidade

Logo a seguir de descobrir essa ferramenta (Kali-linux), parti para a instalação. Mas me surpreendi com algo interessante.

O sistema kali linux, não era uma aplicação, mas sim um sistema operacional, como:

Figura 5_img_windows11

Figura 3_img_macos

Figura 4_img_android

È um sistema linux, especializada em cyber segurança;

Figura 7_img_linux

==

Figura 6_img_kali

Depois da pequena descoberta, comecei a me perguntar se seria possivel dois sistemas operacionais num único computador. A resposta é sim. Ao fazer uma breve pesquisa descobri que:

Existem 2 jeitos…

Ventoy

O Ventoy é um utilitário gratuito e de código aberto utilizado para criar dispositivos de armazenamento de multimédia USB de arranque com ficheiros como . iso, . wim, . img, . vhd e . efi. Assim que o Ventoy estiver instalado numa unidade USB, não há necessidade de reformatar a unidade USB para adicionar novos ficheiros de instalação. Pronto

Em outras palavras, e de forma rezumida, numa pendrive, o usuario pode armazenar varios arquivos ISO (sistemas operacionais), como kali, windows, e outros. E na inicialização do computador (como a pendrive no computador), posso escolher que sistema usar. Foi minha primeira tentativa

Fazendo o passo a passo…

Instalei o ventoy

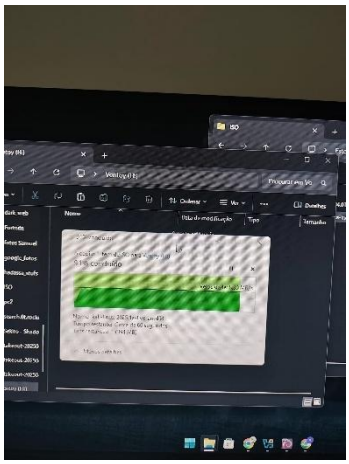


Figura 8_img_instalação_ventoy

Entrei no arquivo principal “Ventoy2Disk”

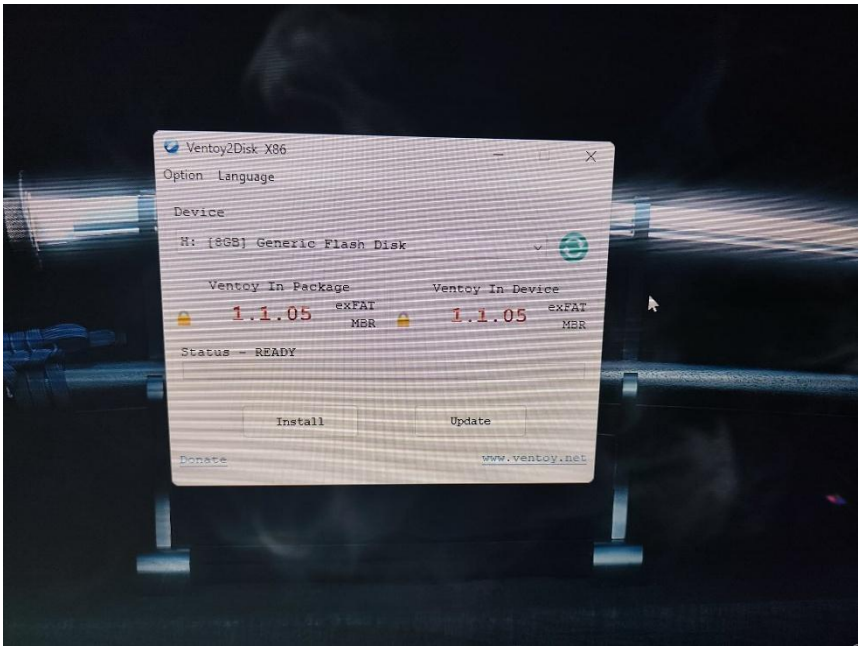


Figura 9_img_ventoy_arquivos

Preparei a ISO que usaria

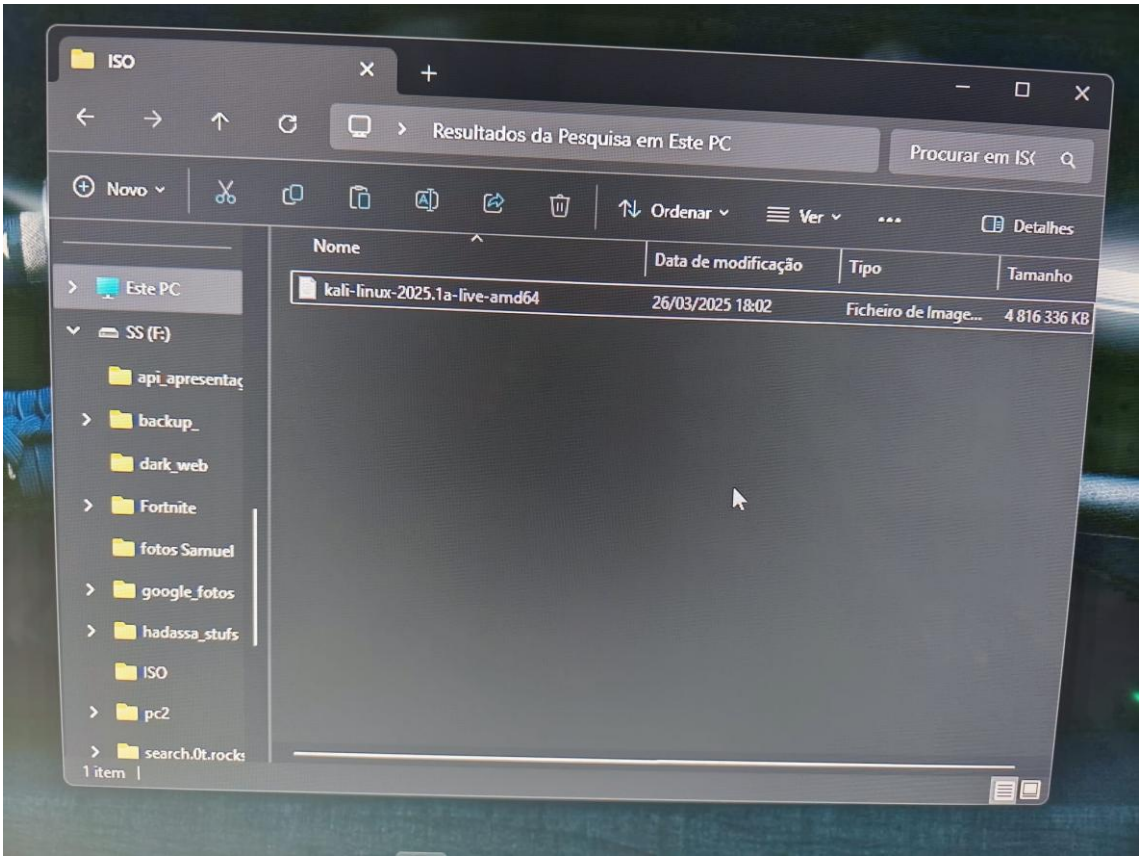


Figura 10_img_ios

Depois de seguir esses 3 passos, bastou instalar o ventoy na pendrive escolhida, arrastar o ISO para dentro da pendrive e pronto. Criei uma pendrive BOOTABLE.

Figura 11_img_pendrive_bootable

Depois do processo de instalamento e alocamento, infelizmente acabou sendo em vão. Mas porque?

- O que aconteceria se eu perdesse a pendrive?
- A incompatibilidades com certos sistemas operacionais
- A sua segurança ou integridade

Apesar de não ter gostado no geral, não descartei o ventoy, apenas o deixei de lado e fui procurar outras alternativas. No fundo, eu queria algo mais eficiente.

Continuei em busca.

A busca

Depois de um belo tempo de pesquisa, “achei o que estava buscando, sem saber o que estava buscando”.

Virtual machines

máquina virtual é a virtualização ou emulação de um sistema informático. As máquinas virtuais baseiam-se em arquiteturas de computadores e fornecem a funcionalidade de um computador físico. As suas implementações podem envolver hardware especializado, software ou uma combinação dos dois.

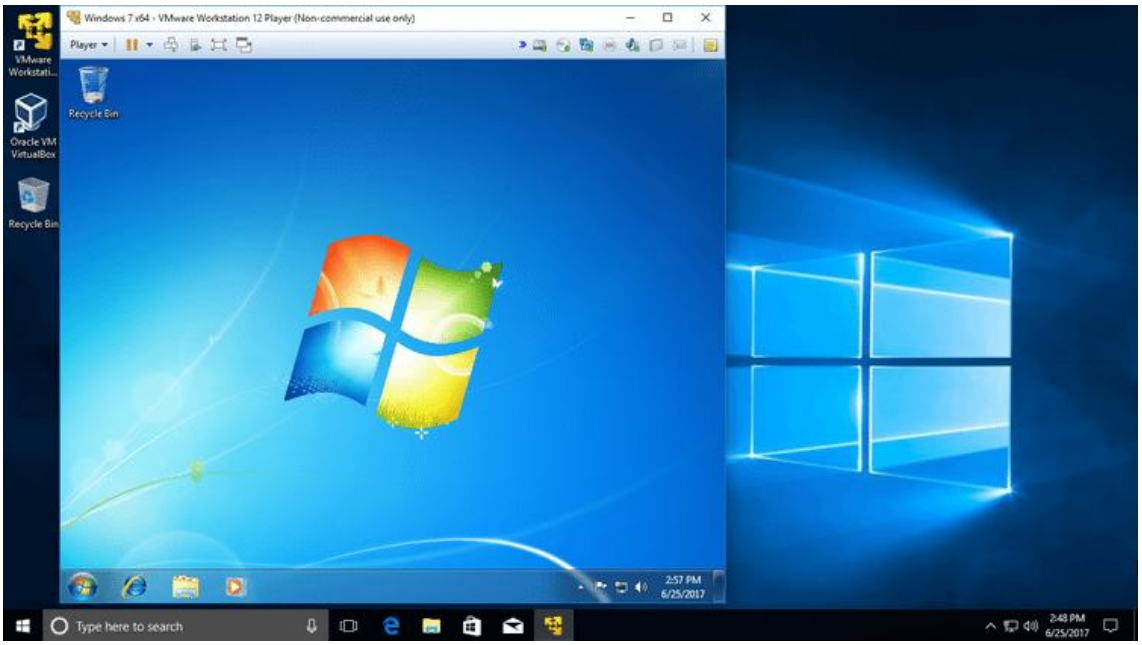


Figura 12_img_virtual_machine

Nota: Uma maquina virtual, além de portar IOSs totalmentes dirferentes, é perfeita para quem quer testar aplicações e outras coisas que precisem de teste.

De forma bem simples, a maquina virtual é como colocar uma caixa dentro de outra caixa;

Figura 13_img_box

Dentro do windows (Caixa maior), criamos um abiente completamente isolado (caixa menor), onde colocamos nosso novo sistema operacional.

Decidido a usar esse tipo de sistema, fui a diante.

Escolha da Virtual Machine

Existem varios tipos de ambientes virtuais que podemos usar, como :

- VMware Workstation
- QEMU
- VirtualBox
- ...

Instalação

Escolhi o VirtualBox. Pois além de ser a mesma da imagem acima, foi o que eu me familiarizei melhor.

A instalação foi algo bem simples, bastou acessar o sites oficial deles:

Site: https://www.virtualbox.org/

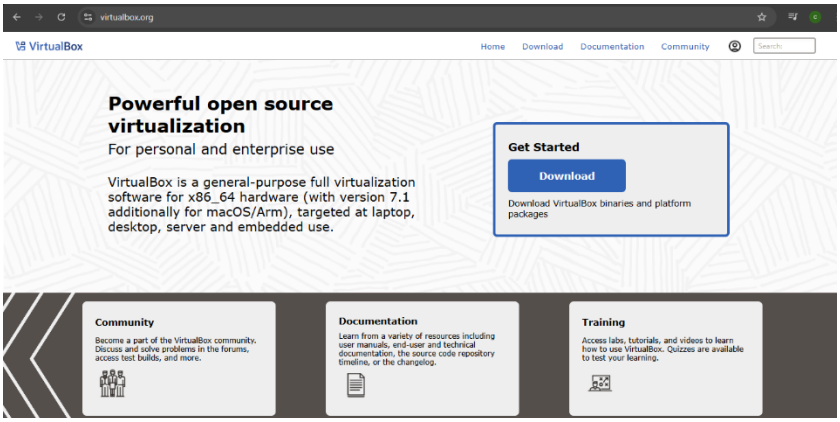


Figura 14_img_virtualbox

Depois do download, temos que instalar uma nova ISO especializada para esse tipo de ambiente. Ao acessar o site oficial do kali-linux (a ISO que queremos), e escolher a opção “Virtual Machine”

Site: https://www.kali.org/

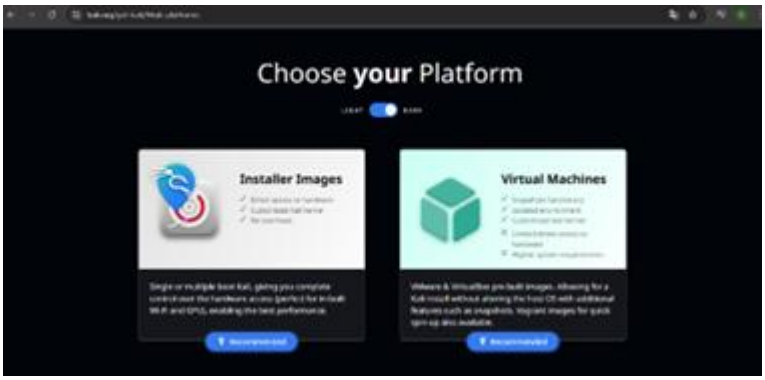


Figura 15_img_kali.org

Finalização da instalação

Finalizando ambas…

Bastei abrir o Virtual box:

Figura 16_img_abrir_virtualbox

Clicar no “Adicionar”, aparecerá a opção kali-linux

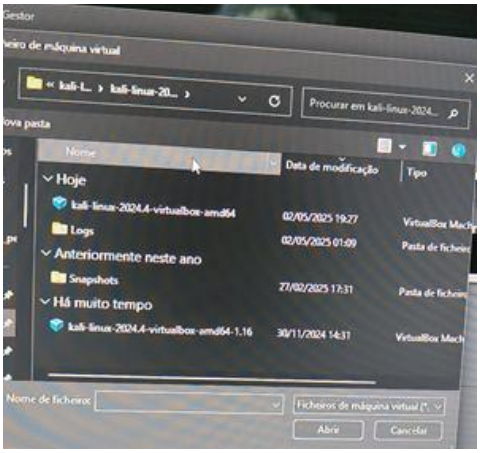


Figura 17_img_adicionar_kali

E pronto. Temos o sistema kali-linux rodando no nosso computador.

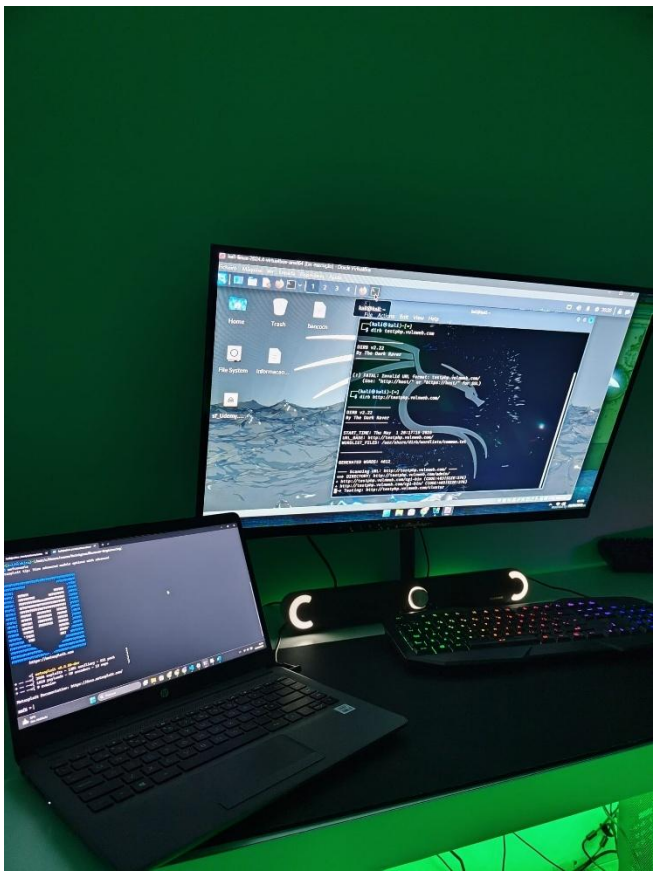


Figura 18_img_kali_pronto

Início da Prática

A partir desse dia que tudo realmente começou. Apesar de não ter muitos conhecimentos das ferramentas do kali-linux, fui fazendo testes e experimentando funcionalidades;

Figura 19_img_kali_desktop

Não estava satisfeito, ao mecher numa ferramenta perigosa como essa, temos que saber o que estamos fazendo. E eu não sabia.

Mas estava disposto a aprender;

Figura 20_img_video_aula

Dopois dessa breve introdução, pude me localizar, saber o que eu exatamente o que eu queria fazer, e como fazer.

Comecei a estudar primeiro a teoria, descobri que tem diversos níveis de Pentest.

Pentest

Pentest (teste de penetração) é uma simulação controlada de ataque a sistemas, redes ou aplicativos, feita para identificar e corrigir vulnerabilidades de segurança.

Tipos de pentest

- BlackBox: O blackbox, é um teste de penetração onde não se tem nunhuma informação sobre o alvo.
- BrayBox: O Gray já quando temos alugmas informações do alvo, como o nome, ou o tipo empresa
- WhiteBox: Já o WhiteBox, é qundo já temos total informação do alvo. Resumindo, é como um teste de pentest na nossa propria empresa.

Fases de Pentest

Para um teste de pentest mais eficiente, temos que seguir uma serie de passos. È como fazer um bolo, fazendo o passo a passo para chegar ao resultado que queremos.

Etapa 1 – Definição do escopo

A definição do escopo é o planeamento. O que queremos fazer? Qual informação queremos buscar ou obter? Qual o nosso objetivo?

Voltado ao exemplo do bolo… O etapa definição do esocopo, é como escolher o tipo de bolo queremos fazer, a sua cor, o sabor, e etc.

Figura 21_img_planeamento

Etapa 2 – Coleta de informação

A coleta de informação, como já diz o nome, é coletar informação do nosso alvo, como:

- Nome;
- Empresa ();
- Funcionarios;
- Sistemas operacional da empresa;
- Outros…

Quanto mais conhecimento do alvo tiver, mais facil o pentest

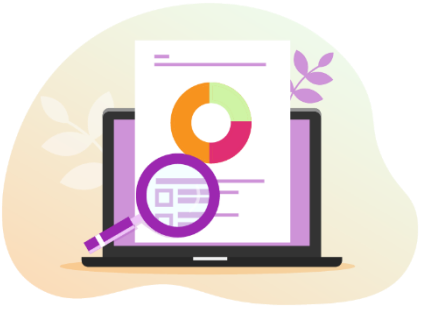


Figura 22_img_conhecer

Etapa 3 – Analise de vulnerabilidade

Numa empresa, á sempre uma vulnerabilidade, porque apesar de tudo somos humanos, e humanos cometem erros. Numa empresa, podem existir varios tipos de vulnerabilidade;

- Clicar em links maliciosos
- Compartilhamento indevido de dados
- Deixar computadores desbloqueados (Muito usual)
- Instalar softwares não autorizados
- Outros….

Cada erro ou falha desse gênero, pode ser usado como uma forma de invadir e acessar os dados da empresa

Figura 23_img_busca

Etapa 4 –Exploração

Depois de todas essas falhas, o hacker acessa (invade) o computador da empresa alvo. È onde entra a etapa exploração, depois de ter acesso, dependendo do nosso objetivo, vagar entre os ficheiros.

Figura 24_img_explorar

Etapa 5 – Pós exploração

Nessa fase final, é onde fazemos a conclusão do nosso trabalho, guardar as informações, as vulnerabilidades e dependendo do nosso objetivo, ou sair sem nenhum rastro, ou implantar um MALWERE.

Figura 25_img_após_expl

Ultima etapa – Relatório

Ao concluir todas as etapas, fazemos um relatório de todas as falhas de sgurança que encontramos para reportar a empresa. Sendo preciso e direto.

Depois de todas essas estapas, esqueci de mencionar algo muito importante e confundido por muitos HACKING/PENTEST.

Essas duas palavras são funcões parecidas, mas não iguais. Um hacker explora vulnerabilidades ilegalmente para seu proprio ganho, ao contrario de um penterter. Um pentester é alguem contratado por empresas para propositalmente achar vulnerabilidades em seus sistemas, para poder corrigir-los

Introdução ao Ethical Hacking

Depois de muita teoria, comecei a colocar tudo em prática. Iniciei por algo simples, mas fundamentar para um pentest;

Portas

As portas são como portas de entrada e saida para a comunicação entre computadores em uma rede. Cada serviço usa uma porta específica para e comunicar. Como;

- Porta 22 - normalmente usada para o SSH (Acesso remoto suguro)
- Porta 80 - normalmente usada para o HTTP (Navegação em sites sem criptografia) “Usaremos muito no futuro”
- Porta 443 - Usada pelo HTTPS (Navegação em sites com criptografia)
- Porta 8080 – Usada como alternativa ao HTTP, muito utilizada em teste ou servidores locais

Voltando

Ao voltar no kali-linux, clicando no canto superior direito, nos diparamos com diversas ferramentas que podemos usar para o pentest(nmap, hydra, aircrack...). Um dos motivos de ser uma ferramenta muito usada entre os profissionais, ou hacker.

Dentro do kali, abri o terminal;

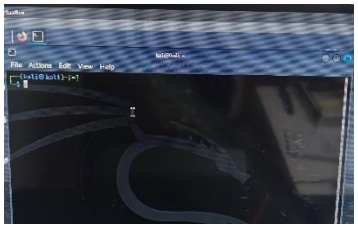


Figura 26_img_dentro_kali

E vamos usar nossa primeira ferramenta; NMAP

Mais cedo, fiz uma pequena explicação de o que são portas e dei alguns exemplos delas. A ferramenta NMAP, serve para fazer um escaneamento de portas e descobrir quais estão abertas e fechadas. Aqui um exemplo num site;

Nmap bancocn.com

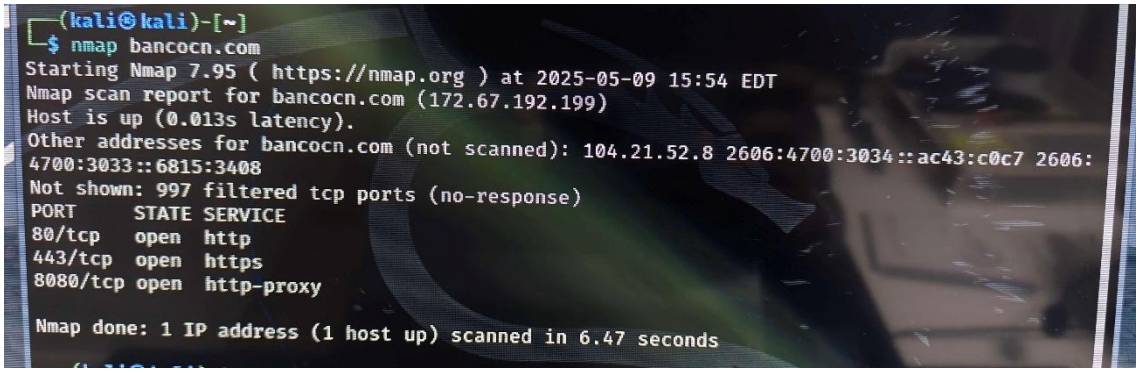


Figura 27_img_nmap

Como é visto, é bem simples usar o NMAP, bastou inserir o dominio do site.

O resultado foi algo bem interessante, mostrou as portas desse site;

- A porta 80;
- A porta 443;
- A porta 8080;

Tudo bem, mas qual a importancia de saber que portas estão abertas?

Simples, atravez dessas portas abertas que descobrimos vulnerabilidades ou até conseguimos entrar.

Repositórios escondidos

Repositórios escondidos em sites são diretórios ou arquivos não referenciados diretamente na navegação do site, mas que ainda estão acessíveis se alguém souber o caminho. Podem conter backups, códigos-fonte, arquivos de configuração ou dados sensíveis. Eles representam um risco de segurança, pois podem expor informações críticas a invasores caso não estejam devidamente protegidos. E isso é bem comum na criação de sites…

Nós conseguimos achar esse diretórios usando a ferramenta DIRB. Ele na verdade é bem facil de usar, basta:

Dirb http:://www.bancocn.com/

```
┌──(kali㉿akira)-[~]
└─$ dirb http://www.bancocn.com/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed May 28 23:26:21 2025
URL_BASE: http://www.bancocn.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://www.bancocn.com/ ----
==> DIRECTORY: http://www.bancocn.com/admin/
==> DIRECTORY: http://www.bancocn.com/assets/
==> DIRECTORY: http://www.bancocn.com/classes/
==> DIRECTORY: http://www.bancocn.com/css/
+ http://www.bancocn.com/film (CODE:521|SIZE:15)
+ http://www.bancocn.com/films (CODE:521|SIZE:15)
+ http://www.bancocn.com/filter (CODE:521|SIZE:15)
+ http://www.bancocn.com/finance (CODE:521|SIZE:15)
+ http://www.bancocn.com/financial (CODE:521|SIZE:15)
+ http://www.bancocn.com/find (CODE:521|SIZE:15)
+ http://www.bancocn.com/finger (CODE:521|SIZE:15)
+ http://www.bancocn.com/finishorder (CODE:521|SIZE:15)
+ http://www.bancocn.com/firefox (CODE:521|SIZE:15)
+ http://www.bancocn.com/firewall (CODE:521|SIZE:15)
+ http://www.bancocn.com/firewalls (CODE:521|SIZE:15)
+ http://www.bancocn.com/firmconnect (CODE:521|SIZE:15)
+ http://www.bancocn.com/firms (CODE:521|SIZE:15)
+ http://www.bancocn.com/firmware (CODE:521|SIZE:15)
```

Figura 28_img_dirb

Como podem ver, achamos incontaveis repositorios do bancocn. Mas o mais iportante, encontramos o http://www.bancocn.com/admin/ que no leva direto a essa pagina “admin”.

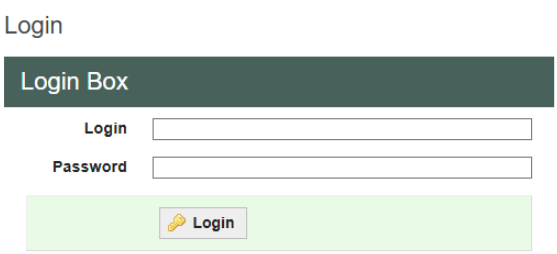


Figura 29_repoditorio_admin

SQL-Injection

De foma bem resumida, o SQL-INJECTION é quando um **hacker ou pentester insere comandos maliciosos no campo de login, busca ou URL** para **enganar o banco de dados**. Vai ser o conteudo que irei mostrar na prática presencialmente.

Para o SQl-injections, irei usar o sqlmap

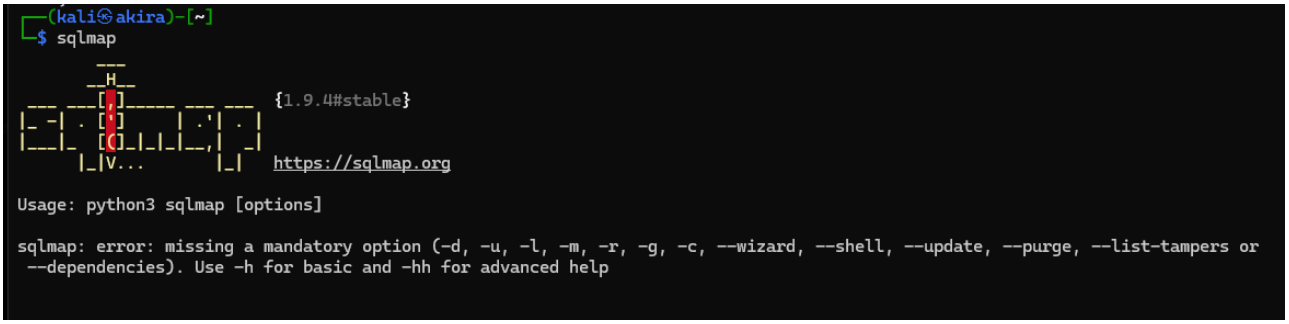


Figura 30_img_sqlmap

Essa Ferramente é poderosa quando se sabe usar…. Indo direto ao ponto, vou pegar um site (que sei que é vulneravel a esse tipo de ataque):

Site:http://testphp.vulnweb.com/listproducts.php?cat=1

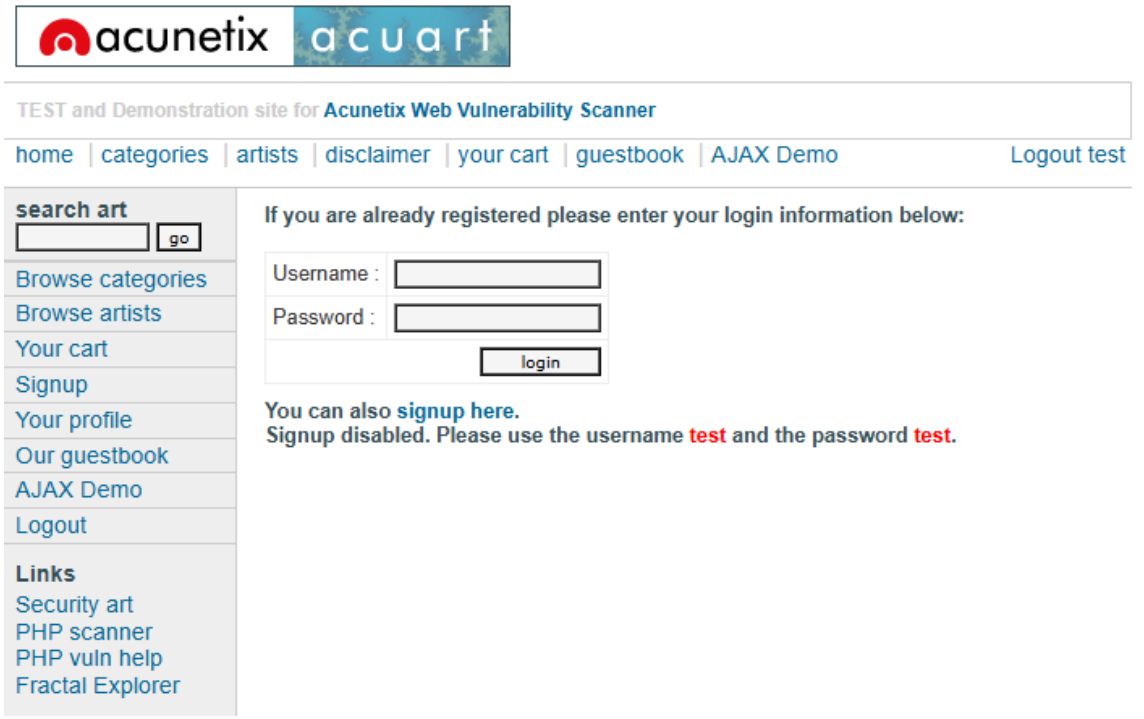


Figura 31_img_site_vulneravel

Observação: O link principal do site é http://testphp.vulnweb.com/, mas vamos escolher o anterior pelo fato da "tal vulnerabilidade". Não é sempre, mas pode indicar vulnearibulidade quando o site termina com "cat=1", isso nos diz com quase toda a certeza que existem outros dominios (...2, ...3, ...4...)

O primeiro.... DBS

Figura 32_img_sqlmap_dbs

Esse comando executa um teste de injeção SQL automatizado no parâmetro cat da URL fornecida, usando a ferramenta **sqlmap**. O objetivo é verificar se o site é vulnerável e listar os **bancos de dados** existentes no servidor, caso a falha seja explorável.

Nos dando o resultado....

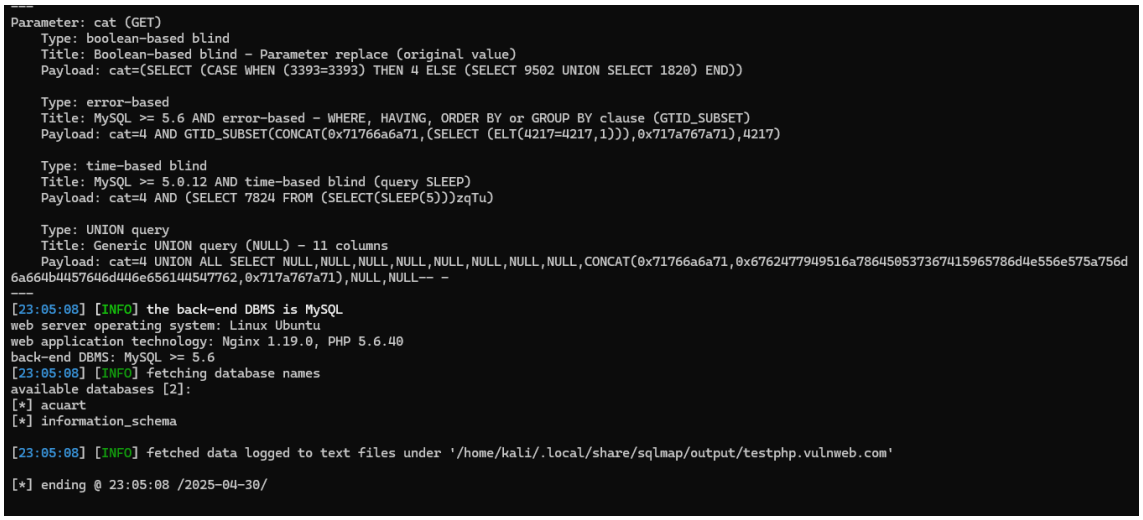


Figura 33_img_sqlmap_dbs_resultado

A ferramenta detectou que o banco de dados usado é MySQL (versão 5.6 ou superior), em um servidor **Linux Ubuntu** com aplicação escrita em PHP 5.6.40 e usando **Nginx 1.19.0** como servidor web.

Ela conseguiu explorar a falha e listar dois bancos de dados disponíveis:

- acuart
- information_schema (padrão do MySQL)

Os dados coletados foram salvos em um diretório local para análise posterior.

Agora que já temos essas infomações.... TABLES

Figura 34_img_sqlmap_tables

foi utilizado para listar as tabelas do banco de dados acuart previamente identificado como vulnerável. A ferramenta executou a injeção SQL e retornou todas as tabelas existentes nesse banco, revelando a **estrutura interna** da base de dados.

Mostrando:

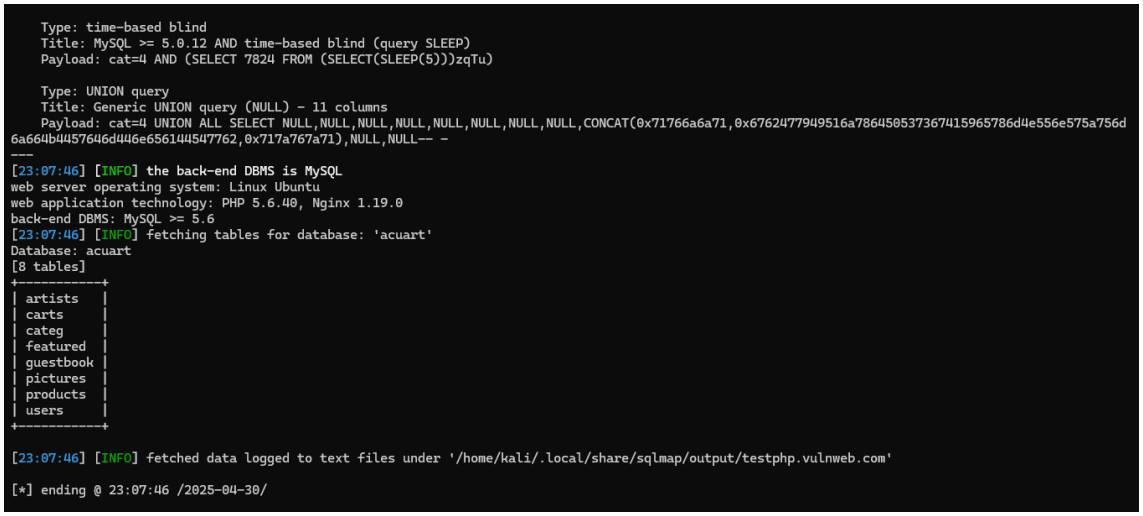


Figura 35_img_sqlmap_tables_resultado

A partir daqui, essas informações já são muito importantes:

+----------+

| artists |

| carts |

| categ |

| featured |

| guestbook |

| pictures |

| products |

| users |

+----------+

Agora, é como se eu já tivesse invadido um prédio, bastando apenas escolher os “comodos”

Seguinte:

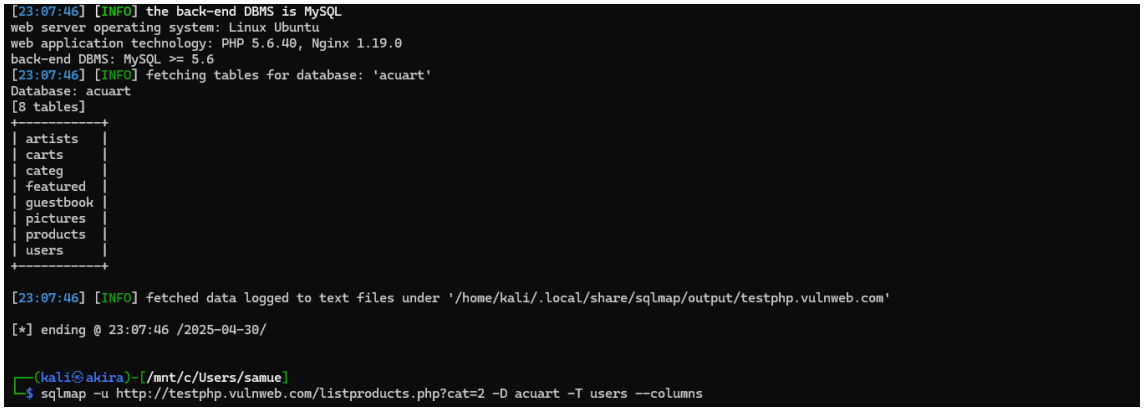


Figura 36_img_sqlmap_columns

Foi usado para **listar as colunas** da tabela users dentro do banco de dados acuart. Com isso, foi possível descobrir os **nomes dos campos** da tabela, como por exemplo username e password, o que indica onde estão armazenadas informações sensíveis de usuários.

Resultado:

Figura 37_img_sqlmap_columns_resultado

Como mostra, temos varios dados da base de dados a nossa disposizao do “alvo”. Agora vamos tentar ler exatamente os dado…

Semifinal:

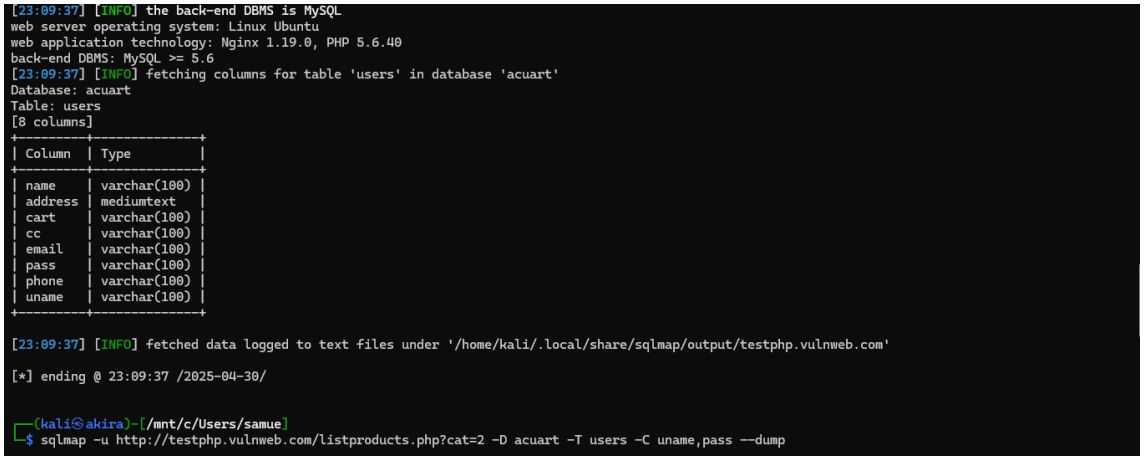


Figura 38_img_sqlmap_dump

foi utilizado para **extrair dados** (dump) das colunas uname (nome de usuário) e pass (senha) da tabela users, no banco de dados acuart.

Esse processo revelou os **usuários e suas senhas armazenadas** no sistema, demonstrando que a aplicação web é vulnerável a **SQL Injection**, permitindo o acesso não autorizado a informações confidenciais.

Vamos ver se conseguimos os dados?

Figura 39_img_sqlmap_dump_resultado

Aí esta, depois de todo esse processo, ele esta nos dizendo que…

O uname = test

A pass = test

Vamos ver se os dados são esses:

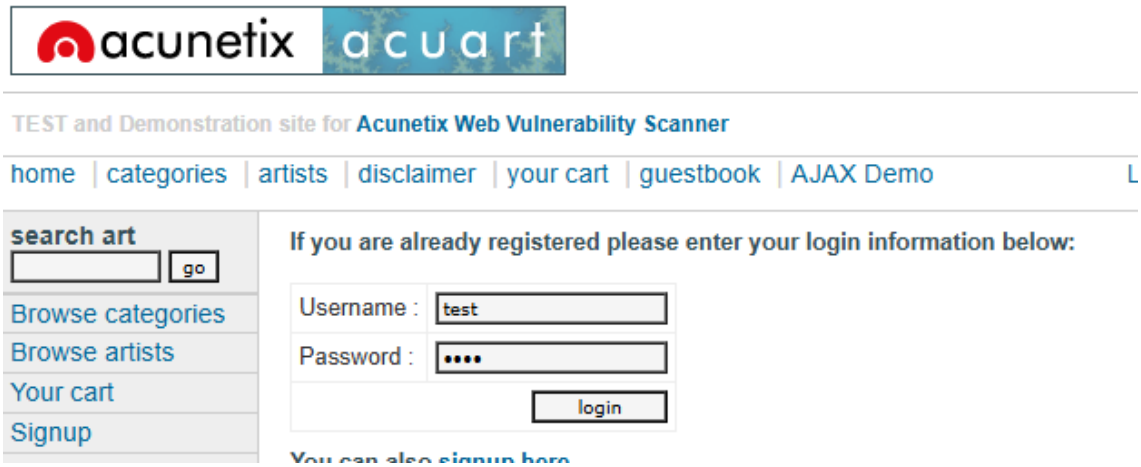


Figura 40_img_sqlmap_inserindo_dados

...

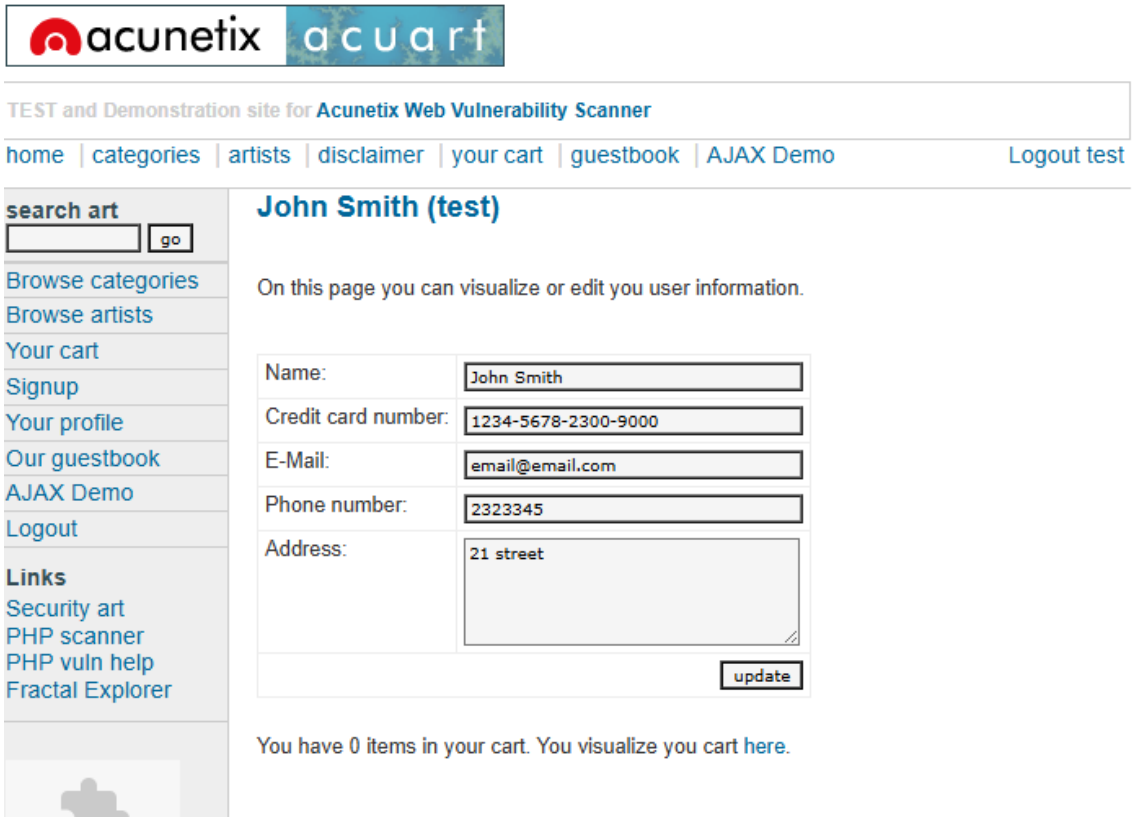


Figura 41_img_sqlmap_dados_sucesso

Exatamente.

Realizei um teste de **SQL Injection** com a ferramenta **sqlmap** na URL http://testphp.vulnweb.com/listproducts.php?cat=1. Através de uma sequência de

comandos, foi possível identificar que o sistema utiliza o **MySQL** como banco de dados e está vulnerável a injeções SQL.

Descobri dois bancos de dados disponíveis: acuart e information_schema. No banco acuart, a tabela users continha as colunas uname e pass, que foram extraídas com sucesso.

Resultado final:

- **Usuário:** test
- **Senha:** test

Essa atividade demonstrou na prática como uma aplicação mal protegida pode expor informações sensíveis por meio de falhas de segurança no tratamento de entradas do usuário.

Engenharia Social: O Poder da Manipulação

Como quse em toda a profissão, quantoo mais voce estuda, mais novas vão surgindo. Ao decorrer dos meus estudos, descobri algo interessante sobre a area do pentest, que é o ataque de Egenharia Social.

A **engenharia social** é uma técnica usada por cibercriminosos para **manipular pessoas** a fim de obter informações confidenciais, acesso não autorizado a sistemas ou realizar ações que comprometam a segurança de uma organização ou indivíduo.

Diferente de ataques puramente técnicos, a engenharia social **explora o fator humano**, confiando em **engano, persuasão e manipulação psicológica**. Os atacantes geralmente se passam por pessoas confiáveis, como técnicos de TI, colegas de trabalho ou representantes de empresas, para convencer a vítima a revelar senhas, clicar em links maliciosos ou instalar programas infectados.

De forma que voce entenda melhor, olhe esse exemplo:

Figura 42_img_netflix_email

Esse é um exemplo clássico de engenharia social. Um hacker pode criar e-mails muito parecidos com esses, chamados de **e-mails de phishing**, que parecem ser enviados por empresas confiáveis ou contatos conhecidos. O objetivo é enganar a vítima para que ela:

- Clique em links maliciosos,

- Baixe arquivos infectados,
- Ou forneça informações pessoais, como senhas e dados bancários.

Esses e-mails geralmente usam técnicas como urgência ("sua conta será bloqueada") ou ofertas tentadoras para aumentar a chance da vítima agir sem pensar.

Por isso, é fundamental estar atento e sempre verificar a autenticidade das mensagens recebidas, especialmente quando pedem informações sensíveis ou ações inesperadas. A conscientização e o treinamento são as melhores defesas contra ataques de engenharia social.

Mas isso é crime?

Sem sombra de dúvidas, sim — realizar ataques de engenharia social para obter informações sem autorização é crime previsto em diversas legislações, como a Lei Carolina Dieckmann no Brasil, que trata de crimes cibernéticos. A prática pode resultar em processos judiciais, multas e até prisão.

A única exceção é quando esse tipo de ação é feita dentro de um **pentest** (teste de invasão) autorizado, onde o objetivo é identificar vulnerabilidades de segurança para corrigir falhas antes que criminosos reais as explorem. Nesse caso, o pentester atua com permissão explícita da organização, respeitando os limites acordados e a ética profissional.

Portanto, o uso dessas técnicas deve ser sempre responsável, legal e ético, visando melhorar a segurança, e nunca para prejudicar ou invadir sistemas indevidamente.

Exemplo Prático

O **Zphisher** é uma ferramenta de código aberto usada para realizar simulações de *phishing* — uma técnica onde páginas falsas imitam sites legítimos, como redes sociais, e-mails ou plataformas bancárias, com o objetivo de enganar a vítima e capturar informações sensíveis, como senhas e nomes de usuário.

No contexto de um **pentest autorizado**, o Zphisher pode ser utilizado para demonstrar como usuários desatentos podem ser enganados por páginas falsas, ajudando empresas e instituições a perceberem a importância da educação em segurança digital.

Figura 43_img_zphisher

Como podemos ver, essa ferramenta já nos oferece várias opções de páginas falsas, como Facebook, Instagram, Netflix, Discord, entre outras. Cada uma dessas páginas é cuidadosamente clonada para se parecer com o site oficial, com o objetivo de enganar a vítima e induzi-la a inserir informações pessoais, como login e senha.

Essas opções tornam o ataque mais direcionado, pois o atacante pode escolher o serviço mais utilizado pela vítima, aumentando assim a chance de sucesso no golpe — o que destaca a importância da conscientização e da verificação do endereço (URL) de sites antes de inserir qualquer dado sensível.

Que tal usarmos a netflix?

Bastou escolher o numero da nossa, e escolher o “localhost” (Isso significa que o site será acessível apenas no computado)

Figura 44_img_zphisger_exe

Ao seguir com o ataque, copiamos um e-mail oficial e substituímos o link original pelo link gerado pela ferramenta (o link aparece em forma de número ou como "localhost", pois está sendo executado localmente, apenas no nosso computador).

Se estivéssemos usando um serviço como o Ngrok, o link seria público, e qualquer pessoa com acesso à internet poderia acessá-lo. Essa técnica é comum em ataques de *phishing*, onde o atacante tenta enganar a vítima com uma página falsa que imita um site legítimo. Ao clicar e inserir dados nessa página, a vítima entrega suas informações ao atacante.

O resultado ficaria assim:

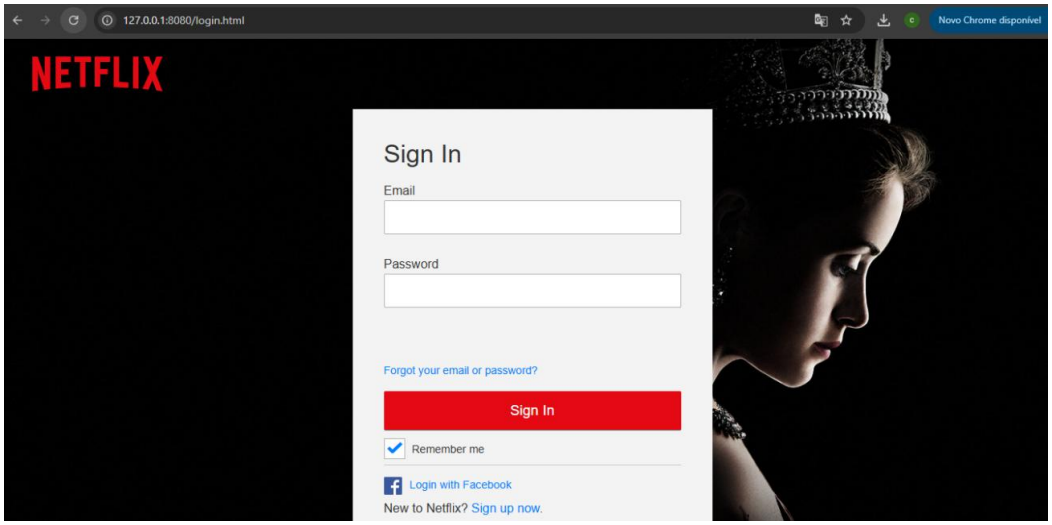


Figura 45_img_netflix_falso

Se você clicasse no link e fosse direcionado para essa página, suspeitaria que se trata de uma fraude?

A verdade é que, muitas vezes, essas páginas falsas são visualmente idênticas às originais. Por isso, um usuário desatento dificilmente perceberia a diferença. Esse é o principal perigo da engenharia social combinada com phishing: ela explora a confiança e a desatenção das vítimas, não falhas técnicas.

É por isso que campanhas de conscientização e treinamentos de segurança são tão importantes dentro de empresas e organizações. Ensinar os usuários a reconhecer sinais sutis de fraude — como erros de digitação na URL, ausência de certificado de segurança (HTTPS), ou o remetente de um e-mail suspeito — pode evitar sérios danos.

E se voce caiu na fraude e colocou suas credenciais, olha o que aparece para o invasor:

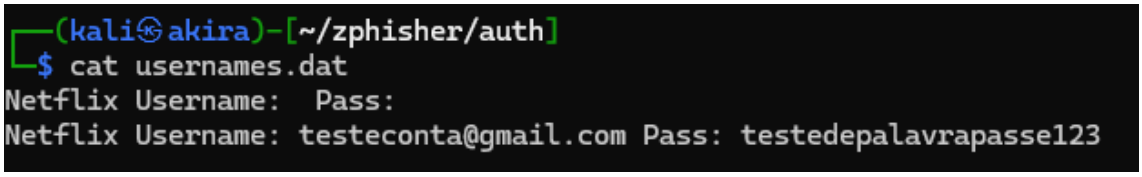


Figura 46_img_zphisher_dados

Alé de mostrar os cadastros, mostra os IPs também:

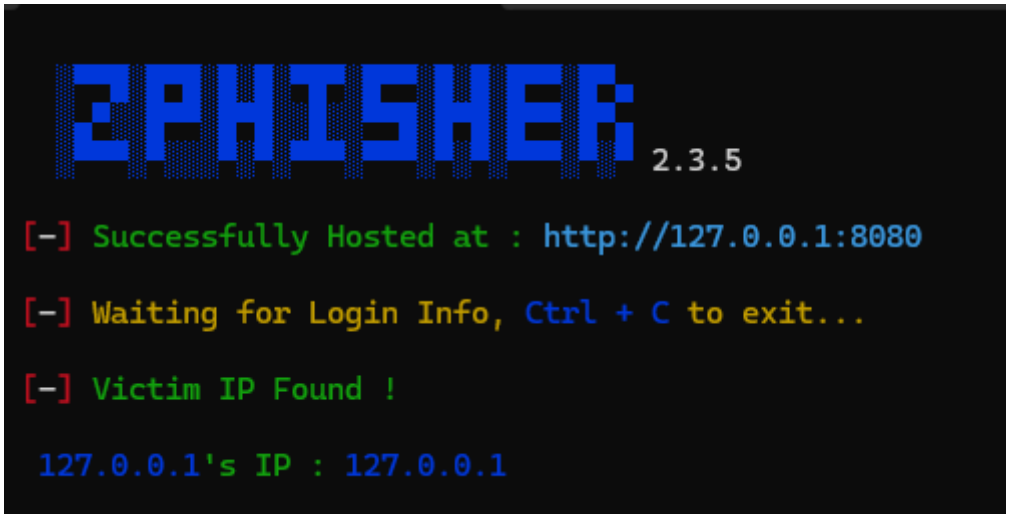


Figura 47_img_zphisher_ips

Tomo cuidados com os sites que voce entra.

Teste de Invasão

(Pentest) em um Ambiente com Windows 7

Após explorar ataques baseados em engenharia social, agora focaremos em um exemplo prático de **teste de penetração em uma máquina com o sistema operacional Windows 7**.

O objetivo desse pentest é simular um ataque real controlado para identificar vulnerabilidades que ainda existem nesse sistema, que hoje já é considerado obsoleto e sem suporte oficial da Microsoft. Isso significa que o Windows 7 **não recebe mais atualizações de segurança**, tornando-o um alvo comum em redes corporativas que ainda utilizam versões antigas do sistema.

Ferramentas Utilizadas

Para esse teste, utilizei:

- **Kali Linux** como sistema atacante (em uma máquina virtual)
- **Windows 7 SP1** como alvo (também em máquina virtual)
- **Ferramentas do Kali** como:
    - **nmap** – para identificar portas e serviços ativos
    - **msfconsole / Metasploit** – para explorar vulnerabilidades
    - **exploit/windows/smb/ms17_010_eternalblue** – um exploit conhecido para o Windows 7

Antes de continuarmos com o passo a passo, vou explicar em geral as ferramentas que usei, e o porque ter escolhido o windows7.

Por que escolhi o Windows 7?

O Windows 7 foi um dos sistemas operacionais mais utilizados no mundo por muitos anos. No entanto, desde janeiro de 2020, a Microsoft encerrou oficialmente o suporte a essa versão, o que significa que **não são mais fornecidas atualizações de segurança**, deixando-o vulnerável a diversos tipos de ataques.

Mesmo após o fim do suporte, muitas empresas, instituições públicas e usuários domésticos ainda utilizam o Windows 7 por questões de compatibilidade ou falta de atualização de infraestrutura. Isso faz com que ele seja um **alvo atrativo e realista** para testes de segurança e demonstrações educacionais.

Para este pentest, irei utilizar o exploit **EternalBlue (MS17-010)**, que se tornou amplamente conhecido após ser utilizado em ataques reais, como o ransomware WannaCry. Essa vulnerabilidade afeta o serviço **SMBv1** do Windows e permite a execução remota de código sem necessidade de autenticação. O EternalBlue é uma escolha ideal nesse cenário, pois **explora uma falha crítica que nunca foi corrigida em sistemas que permaneceram sem atualizações**, como o Windows 7. Isso torna a exploração **viável, prática e didática**, especialmente em ambientes de laboratório.

Figura 48_img_win7

Metasploit Framework

O Metasploit é uma das ferramentas mais poderosas e versáteis para pentest. Ele permite identificar vulnerabilidades, executar exploits e manter o acesso ao sistema comprometido. Para este relatório, utilizei o módulo de exploração conhecido como **MS17-010 EternalBlue**, uma vulnerabilidade crítica no protocolo SMB do Windows.

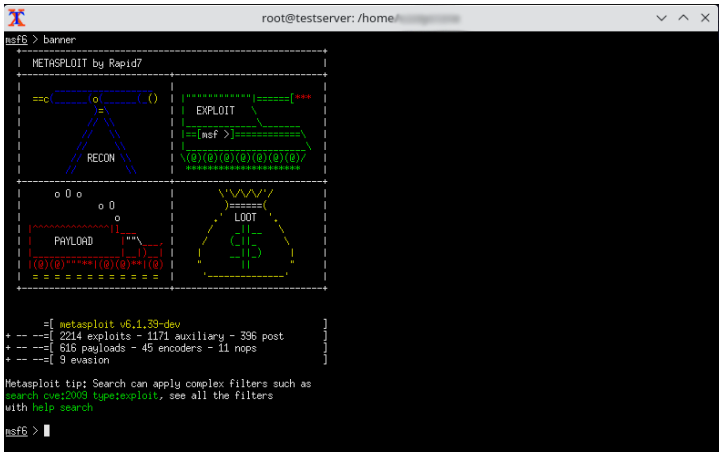


Figura 49_img_metasploit_kali

Figura 50_img_metasploit

Penetração

Para o começo da penetração, precisei procurar bastante pela internet **ISOs antigas do Windows 7** para utilizar em minha máquina virtual no VirtualBox. Muitas das opções disponíveis atualmente vêm com bloqueios, versões modificadas ou exigem chaves de ativação.

Após diversas tentativas, encontrei um site bastante interessante e confiável: https://archive.org. Esse site funciona como um **arquivo digital público**, onde é possível encontrar versões antigas de sistemas operacionais, softwares e outros conteúdos históricos. Através dele, consegui baixar uma ISO original do Windows 7, essencial para montar um ambiente de teste realista.

O processo de instalação do win7 (window 7), foi igual a instalaçao do kali.

Figura 51_img_win7_kali

Como mostrado na imagem, estou utilizando o VirtualBox para simular um ambiente de teste, onde tenho duas máquinas virtuais configuradas: à direita, o Windows 7 (vítima), e à esquerda, o Kali Linux (atacante).

Para construir um cenário realista, criei falsas pastas para simular informaçoes pessoais, como alguns contactos, e-mails e senhas .Vamos supor que realizei com sucesso um **ataque de engenharia social** contra a máquina com Windows 7, e como resultado, obtive o endereço IP da vítima:

IP da vítima: 192.168.100.5

Esse endereço será utilizado nos próximos passos para explorar vulnerabilidades conhecidas e demonstrar um exemplo prático de teste de penetração.

Penetracão – Passo1

Ajustei o endereço IP da minha máquina Kali Linux para estar na mesma sub-rede da vítima, atribuindo o IP **192.168.100.10**. Isso garante que ambas as máquinas possam se comunicar na mesma rede virtual.

Para verificar a conectividade entre elas, utilizei o comando:

ping 192.168.100.5

Esse teste confirma se a máquina atacante consegue alcançar a vítima pela rede, passo essencial antes de prosseguir com qualquer tentativa de exploração.

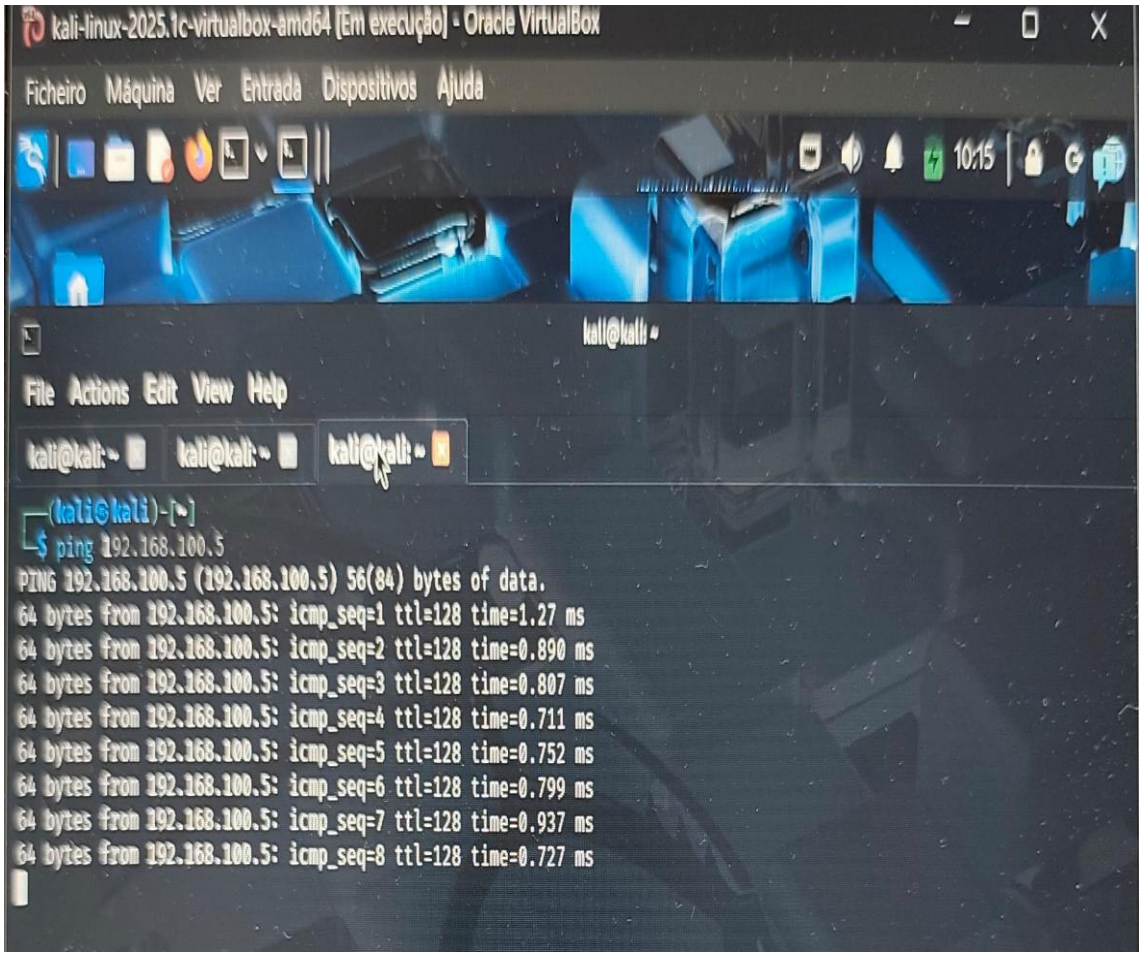


Figura 52_img_ping

Penetração – Passo2

Agora que a comunicação com o IP da máquina-alvo foi estabelecida com sucesso, o próximo passo é realizar um escaneamento de portas utilizando o Nmap. Vamos ver quais serviços estão em execução na máquina da vítima, além de possíveis vulnerabilidades exploráveis.

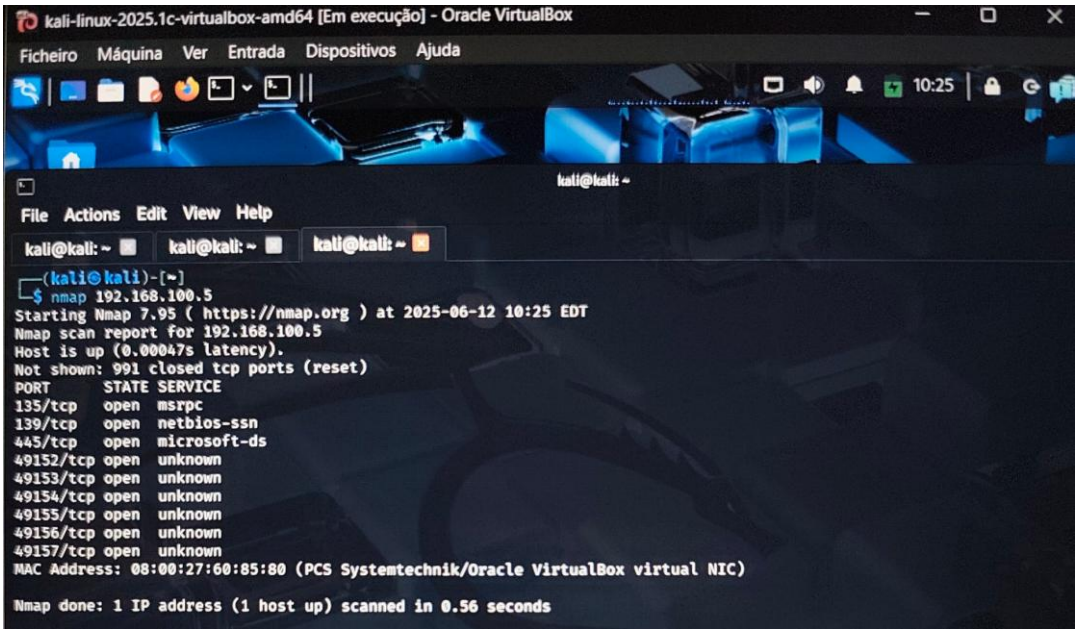


Figura 53_img_nmap_alvo

Penetração – Passo3

Como podemos observar no **passo 2**, o **Nmap** identificou diversas portas abertas na máquina-alvo. No entanto, uma porta em especial chama a atenção: a **porta 445 (microsoft-ds)**.

Essa porta é utilizada para o protocolo **SMB (Server Message Block)**, que permite o compartilhamento de arquivos e impressoras em redes Windows. É justamente **essa porta que nos interessa**, pois foi nela que foi encontrada uma das vulnerabilidades mais críticas da história: o **EternalBlue**.

Como mencionado anteriormente, a **falha explorada pelo EternalBlue** afeta o serviço SMB, permitindo que um atacante remoto execute código malicioso na máquina

vulnerável **sem autenticação**. Com isso, podemos avançar para a próxima etapa, onde exploraremos essa brecha utilizando uma ferramenta adequada, como o **Metasploit**.

Vamos começar por abrir o metasploit bastando apenas digitar no prompt msfconsole:

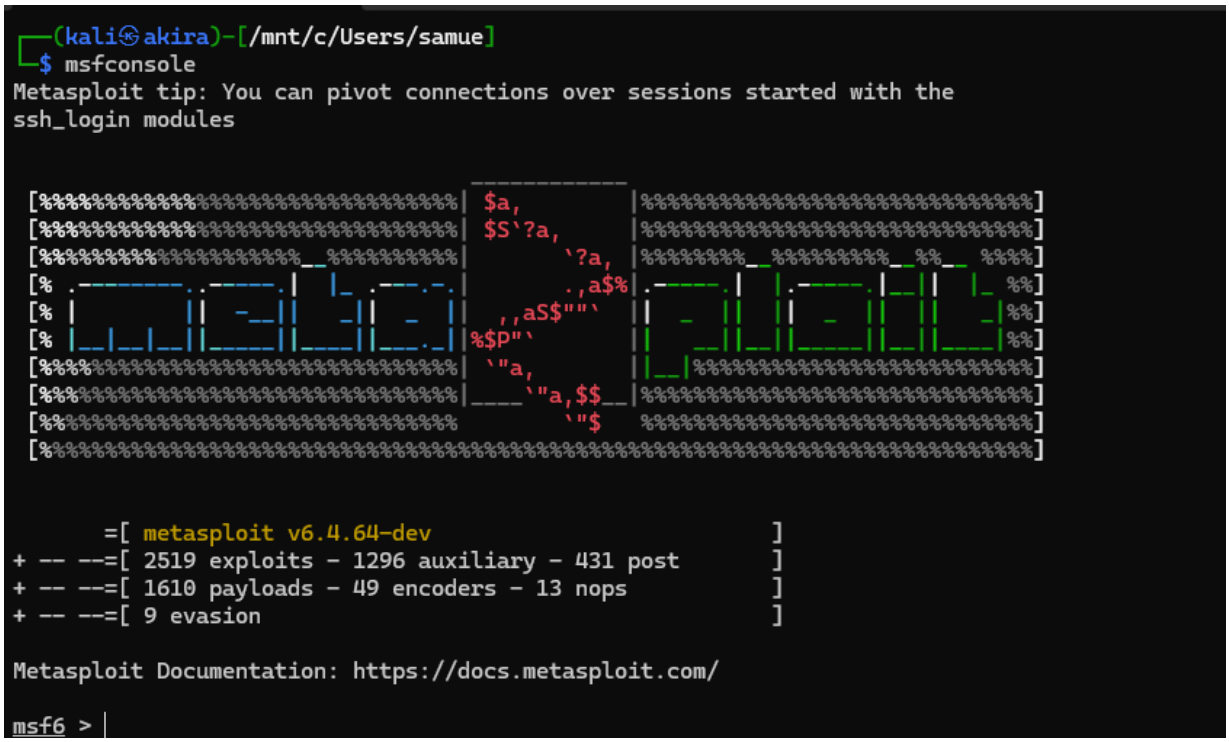
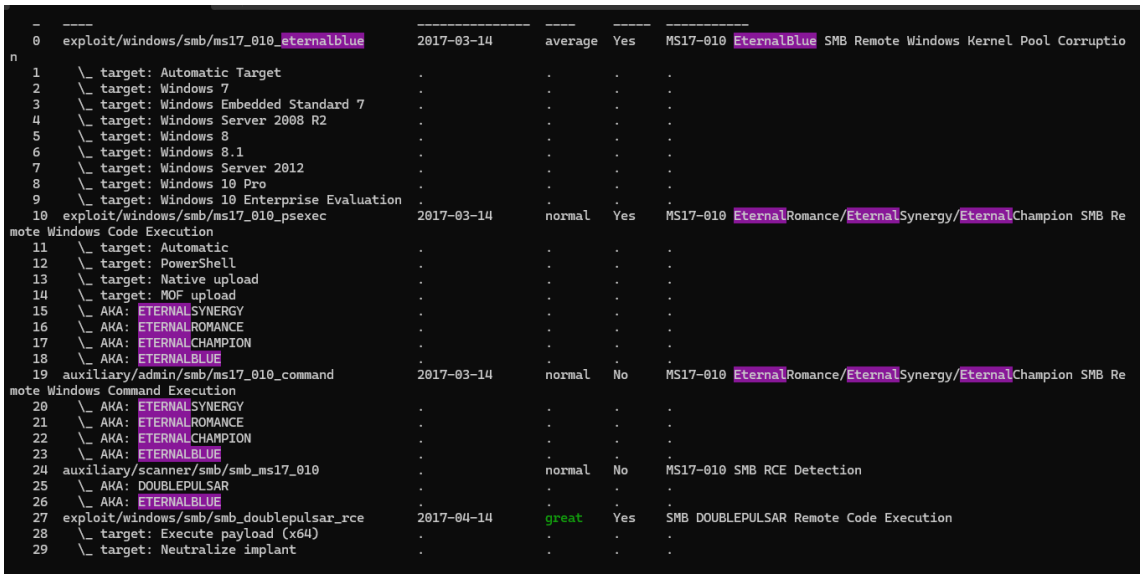


Figura 54_img_msfconsole

O **Metasploit Framework** é uma das ferramentas mais poderosas no campo do pentest, pois possui uma vasta base de dados com **centenas de módulos** prontos para explorar vulnerabilidades conhecidas.

Para facilitar nossa busca e evitar perder tempo navegando manualmente entre os módulos, podemos utilizar o comando de busca direto no console do Metasploit (msf6). No nosso caso, como queremos explorar a falha **EternalBlue**, basta digitar:

-- search eternal blue



#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	_ target: Automatic Target	.	.	.	.
2	_ target: Windows 7	.	.	.	.
3	_ target: Windows Embedded Standard 7	.	.	.	.
4	_ target: Windows Server 2008 R2	.	.	.	.
5	_ target: Windows 8	.	.	.	.
6	_ target: Windows 8.1	.	.	.	.
7	_ target: Windows Server 2012	.	.	.	.
8	_ target: Windows 10 Pro	.	.	.	.
9	_ target: Windows 10 Enterprise Evaluation	.	.	.	.
10	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11	_ target: Automatic	.	.	.	.
12	_ target: PowerShell	.	.	.	.
13	_ target: Native upload	.	.	.	.
14	_ target: MOF upload	.	.	.	.
15	_ AKA: ETERNALSYNERGY	.	.	.	.
16	_ AKA: ETERNALROMANCE	.	.	.	.
17	_ AKA: ETERNALCHAMPION	.	.	.	.
18	_ AKA: ETERNALBLUE	.	.	.	.
19	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20	_ AKA: ETERNALSYNERGY	.	.	.	.
21	_ AKA: ETERNALROMANCE	.	.	.	.
22	_ AKA: ETERNALCHAMPION	.	.	.	.
23	_ AKA: ETERNALBLUE	.	.	.	.
24	auxiliary/scanner/smb/smb_ms17_010	.	normal	No	MS17-010 SMB RCE Detection
25	_ AKA: DOUBLEPULSAR	.	.	.	.
26	_ AKA: ETERNALBLUE	.	.	.	.
27	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution
28	_ target: Execute payload (x64)	.	.	.	.
29	_ target: Neutralize implant	.	.	.	.

Figura 55_img_metasploit_modulos

Somente com esse comando de busca, o Metasploit já nos retornou **vários módulos relacionados ao EternalBlue**, cada um com suas variações e finalidades específicas.

Para este teste, **utilizaremos o primeiro da lista**, que é um dos mais clássicos e amplamente utilizados em ambientes de laboratório:

exploit/windows/smb/ms17_010_eternalblue

Este módulo é direcionado à vulnerabilidade **MS17-010**, descoberta em sistemas Windows, especificamente em implementações do protocolo SMBv1. A falha permite que um atacante remoto execute código arbitrário no sistema vulnerável — **sem necessidade de autenticação**.

Para carregarmos o módulo no Metasploit, utilizamos o comando:

use exploit/windows/smb/ms17_010_eternalblue

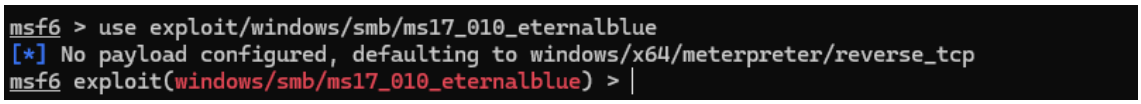


Figura 56_img_modulo_eternalblue

Ao retornar o nome do módulo em vermelho, o Metasploit indica que ele foi carregado com sucesso. Isso significa que **já estamos dentro do módulo selecionado**, prontos para configurar os parâmetros necessários e executar o exploit.

A partir deste ponto, o processo se torna ainda mais interessante. Com o módulo carregado com sucesso, podemos visualizar as opções disponíveis para configuração,

como o alvo o e o endereço IP da vítima.

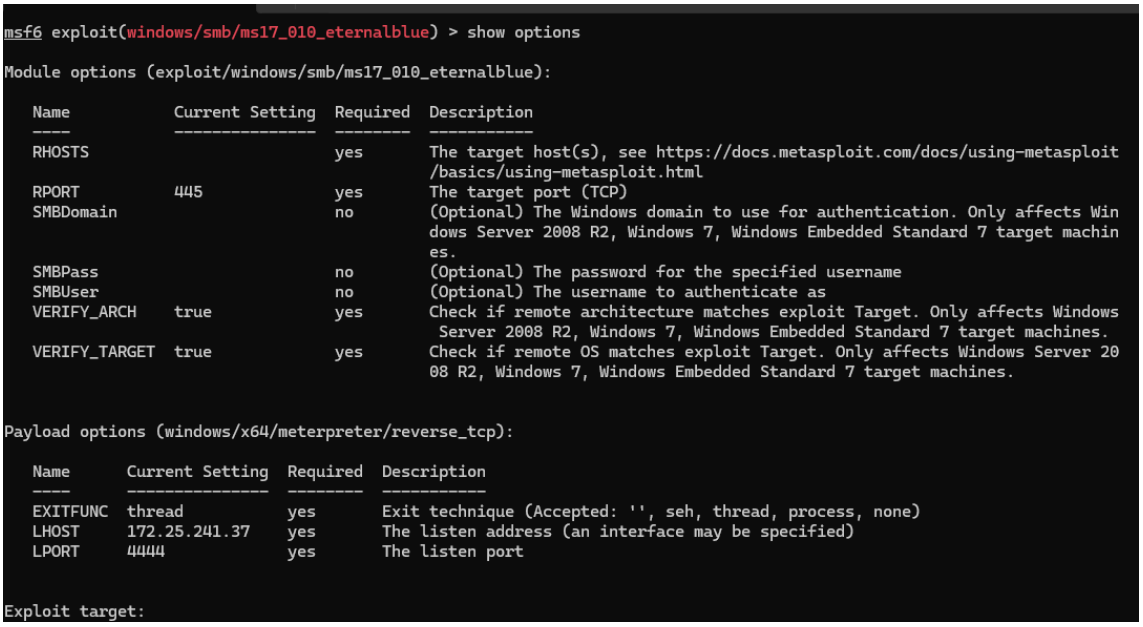


Figura 57_img_metasploit_opções_dados

Explicando de forma simples:

Nome	Descrição
RHOSTS	IP da vítima (máquina Windows 7). Ex: 192.168.100.5
RPORT	Porta do serviço vulnerável (padrão é 445, usada pelo SMB).
SMBDomain	Domínio Windows (opcional). Não é necessário em máquinas locais.
SMBPass	Senha de autenticação SMB (opcional, normalmente não usado aqui).
SMBUser	Usuário SMB (também opcional).
VERIFY_ARCH	Verifica se a arquitetura (x64) da máquina alvo é compatível.
VERIFY_TARGET	Verifica se o sistema operacional da vítima é compatível (Windows 7, Server 2008 R2 etc).

Nome	Descrição
EXITFUNC	Técnica de encerramento após execução (padrão: thread, segura para a maioria dos casos).
LHOST	IP do atacante (Kali Linux) — ou seja, onde a vítima vai se conectar de volta. No exemplo: 172.25.241.37.
LPORT	Porta do atacante onde receberá a conexão da vítima. No exemplo: 4444.

Apesar de existirem várias opções configuráveis antes de realizar a exploração, **nem todas são obrigatórias**. No caso deste módulo específico (ms17_010_eternalblue), os parâmetros realmente essenciais são:

- **RHOSTS**: o IP da vítima (ex: 192.168.100.5);
- **LHOST**: o IP do atacante (ex: 192.168.100.10);
- **RPORT**: a porta de execução de serviço.

A porta de destino do serviço vulnerável já vem **predefinida como 445**, pois este módulo foi projetado **especificamente para explorar o protocolo SMB**, que opera justamente nessa porta. Ainda assim, se necessário, é possível alterar esse valor, desde que o serviço vulnerável esteja sendo executado em outra porta.

Sendo assim apenas nos restando preencher os requisitos usando o comando SET:

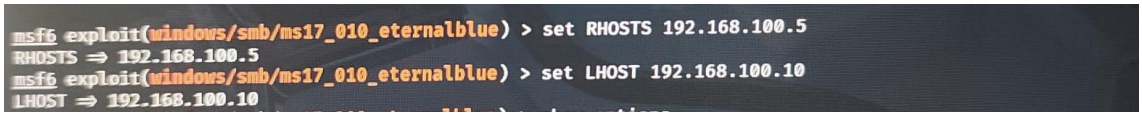


Figura 58_img_metasploit_dados_colocados

Depois de cada SET, ele confirma em baixo, depois disso, basta digitar:

- Run;
- Exploit

Para esse modulo, tanto o run quanto o exploit irão executar na mesma o modulo.

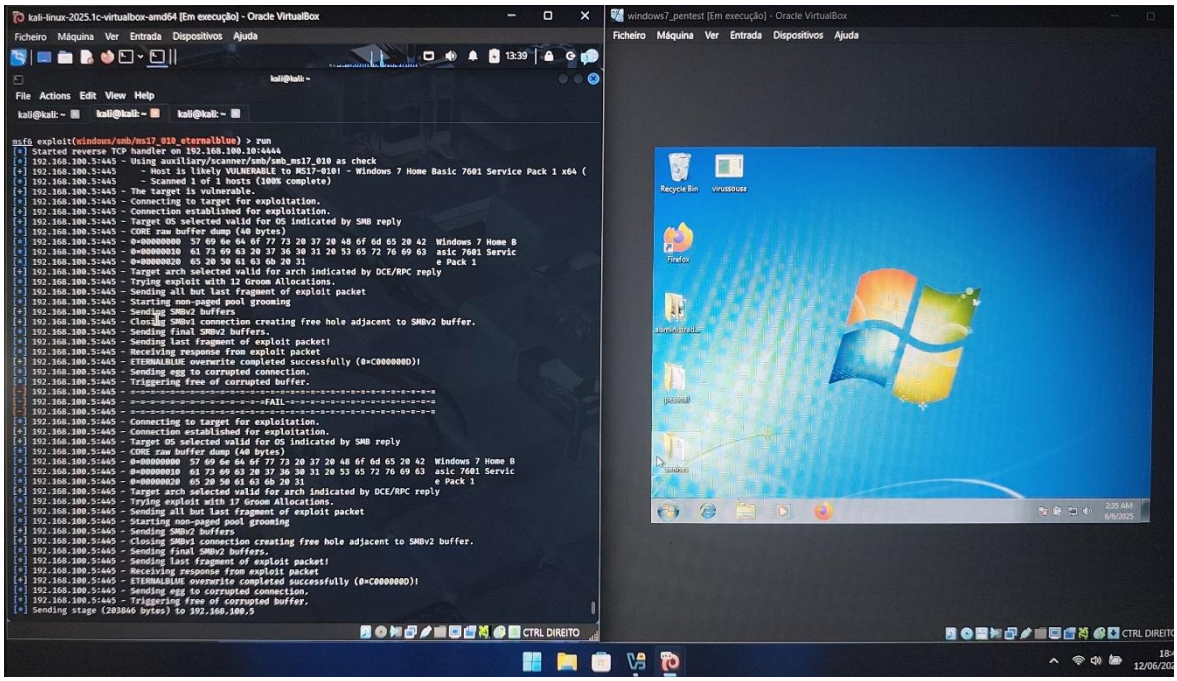


Figura 59_img_invasão_sucedida

O exploit foi bem-sucedido, como resultado, o Metasploit abriu uma **sessão Meterpreter**, confirmando que o sistema foi comprometido com sucesso.

Essa etapa simboliza a **invasão completa do sistema**, permitindo ao atacante realizar diversas ações remotas, como:

- Exploração do sistema de arquivos,
- Execução de comandos,
- Coleta de informações sensíveis.

Agora que já estamos dentro do computador da vítima, podemos começar a explorar o sistema.
Com o Meterpreter, temos acesso privilegiado e conseguimos executar diversos comandos, como listar arquivos, capturar senhas salvas, fazer capturas de tela e até mesmo ativar microfone ou webcam.
Essa etapa é essencial para entender o impacto que uma invasão pode causar, e serve como um alerta sobre a importância de manter sistemas atualizados e protegidos.

Com o meterpreter pronto…

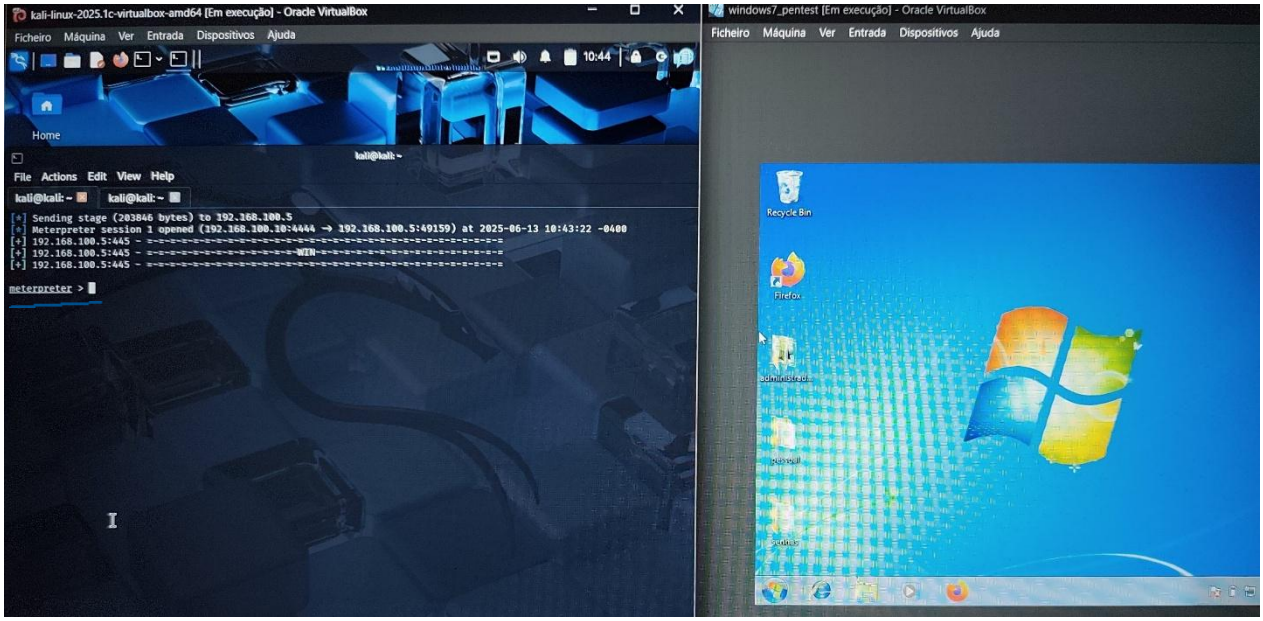


Figura 60_img_metasploit_meterpreter

Vamos digitar o comando **sysinfo**. Esse comando nos fornece informações detalhadas sobre o sistema operacional da máquina comprometida, como o nome do sistema, a versão do Windows, o nome do computador e a arquitetura (32 ou 64 bits). Esses dados são essenciais para entendermos o ambiente da vítima e, caso desejássemos continuar com outras ações, saberíamos quais ferramentas ou cargas úteis seriam compatíveis com aquele sistema.

Figura 61_img_sysinfo

Como podem ver na imagem, o comando retornou os detalhes do sistema. Esse tipo de informação pode ser extremamente útil em um teste de penetração (como é o meu caso), mas também pode ser explorado em outros tipos de ataques cibernéticos.

Para o próximo comando, vamos realizar uma ação mais direta: acessar os arquivos que estão localizados na área de trabalho (Desktop). Para isso, primeiro usamos o comando “ls”, que serve para listar os arquivos e pastas do diretório atual, permitindo que saibamos onde estamos. Em seguida, utilizamos o comando “cd” para navegar até o diretório desejado.

Com isso, conseguimos explorar os arquivos armazenados na máquina da vítima, o que pode incluir documentos importantes, senhas salvas ou outras informações sensíveis que seriam extremamente valiosas em um contexto real de ataque.

LS:

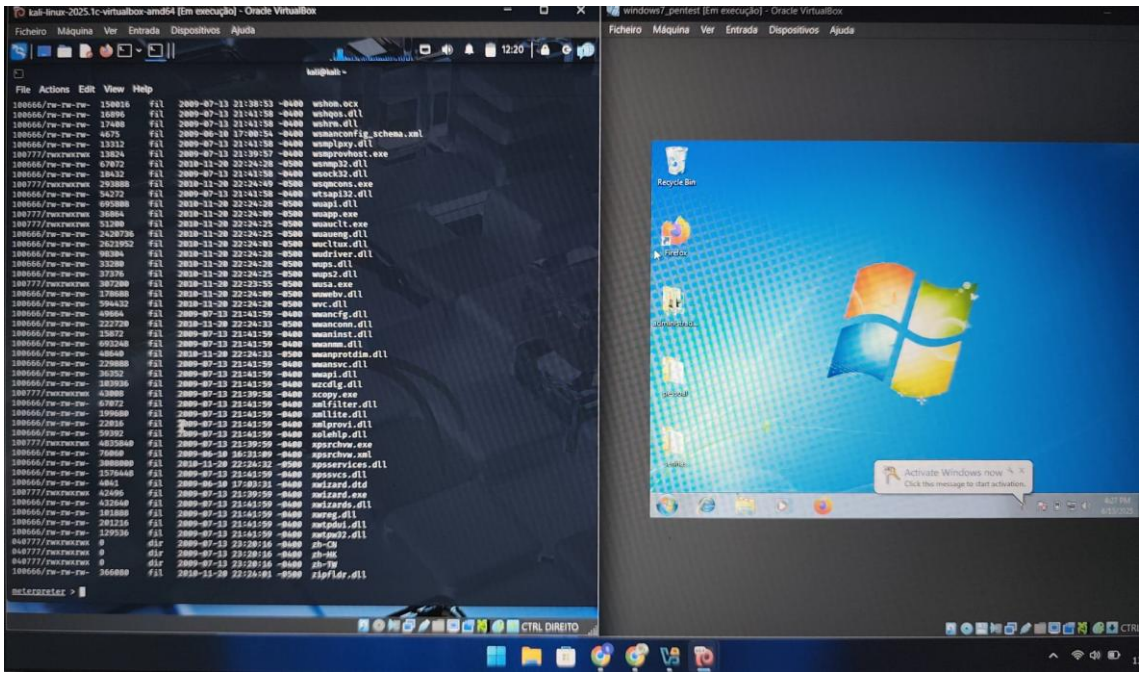


Figura 62_img_listar_arquivos

Como podem ver, o comando ls nos listou todos os arquivos e diretórios presentes no local em que estamos dentro do sistema da vítima. Essa listagem é essencial para sabermos com o que estamos lidando, pois permite identificar possíveis arquivos sensíveis, diretórios importantes e até mesmo rastros de atividades do usuário. A partir dessa visualização, podemos navegar de forma mais precisa pelo sistema, localizando dados relevantes como documentos pessoais, arquivos de senhas ou registros de e-mails.

Acessar Desktop

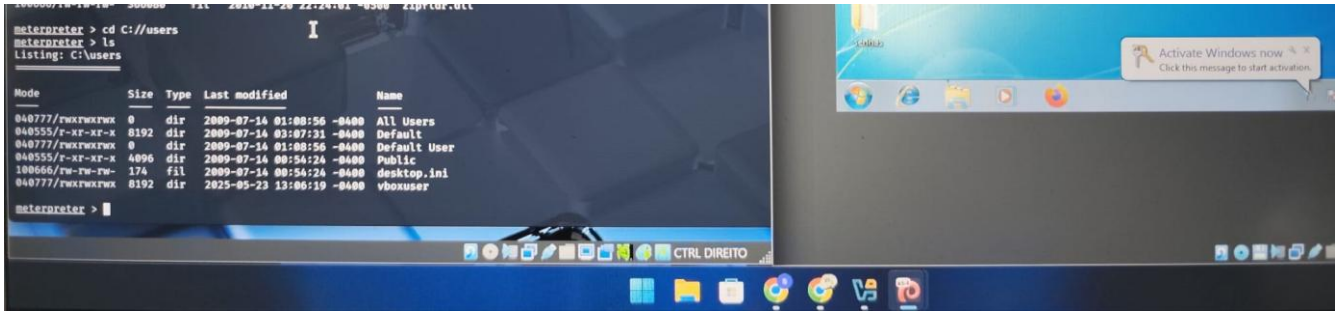


Figura 63_img_acessar_desktop

O comando a seguir foi:

“ cd C:\\Users”

Esse comando foi necessário para acessarmos a pasta onde ficam os perfis de usuários do sistema. Dentro dessa pasta, é comum encontrarmos subpastas com os nomes dos usuários registrados no Windows, e nelas estão armazenados documentos, área de trabalho (Desktop), downloads e outros arquivos pessoais. Navegar até essa localização é um passo importante para identificar informações sensíveis, como documentos confidenciais, senhas salvas ou outros dados que possam ser úteis durante um pentest.

Dando um zoom na imagem anterior, ele nos mostrou esses arquivos

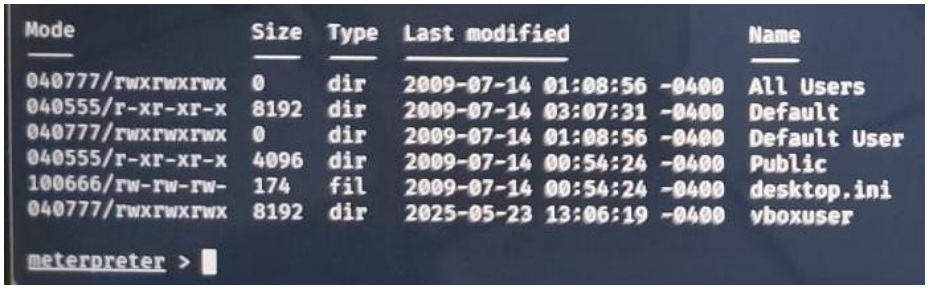


Figura 64_img_arquivos_mostrados

Nosso próximo passo é entrar no diretório **"vboxuser"**. Mas por que não explorar o **arquivo desktop.ini**, como aparece na imagem?

O arquivo desktop.ini é apenas um **arquivo de configuração do sistema**, utilizado pelo Windows para **personalizar o comportamento visual das pastas**. Ele **não contém informações sensíveis ou úteis** para um pentest ou exploração, sendo geralmente **irrelevante nesse tipo de análise**.

Por isso, decidimos entrar na pasta **"vboxuser"**, que é o nome do usuário do sistema. Nela, é mais provável encontrarmos **dados pessoais**, como documentos, imagens,

arquivos salvos, credenciais ou outras informações relevantes para o nosso cenário de teste de intrusão.O comando sendo:

“cd vboxuser” –entrar

“ls” -- para listar os arquivos e pastas do diretório atual

Figura 65_img_vboxuser

Visto na imagem, foi nos dado todos os dados do usuario do computador como documentos, dowloads, fotos, videos e etc…

Como dito antes, vamos ver as pastas do dektop usando o mesmo método:

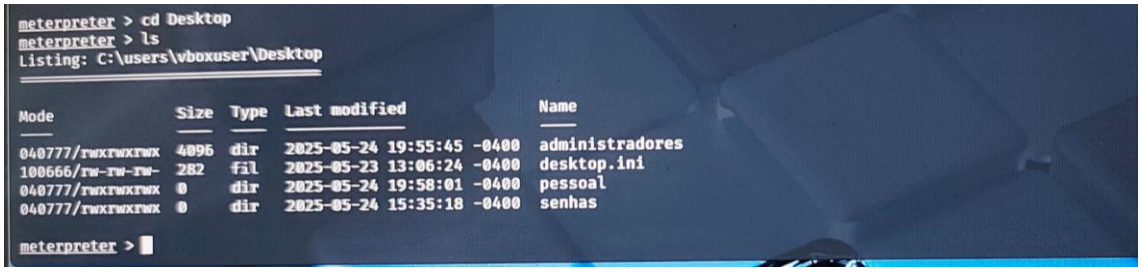


Figura 66_img_vbox_dados

Invasão feita com sucesso! Vamos conferir?

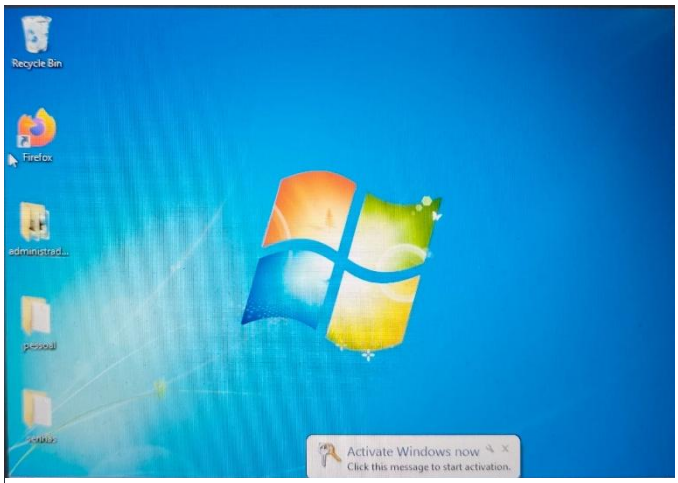


Figura 67_img_dados_conferidos

Depois de ter acceso ao computador e as pastas sensiveis, a única coisa que os resta é pegar (ler) as informaçoes.

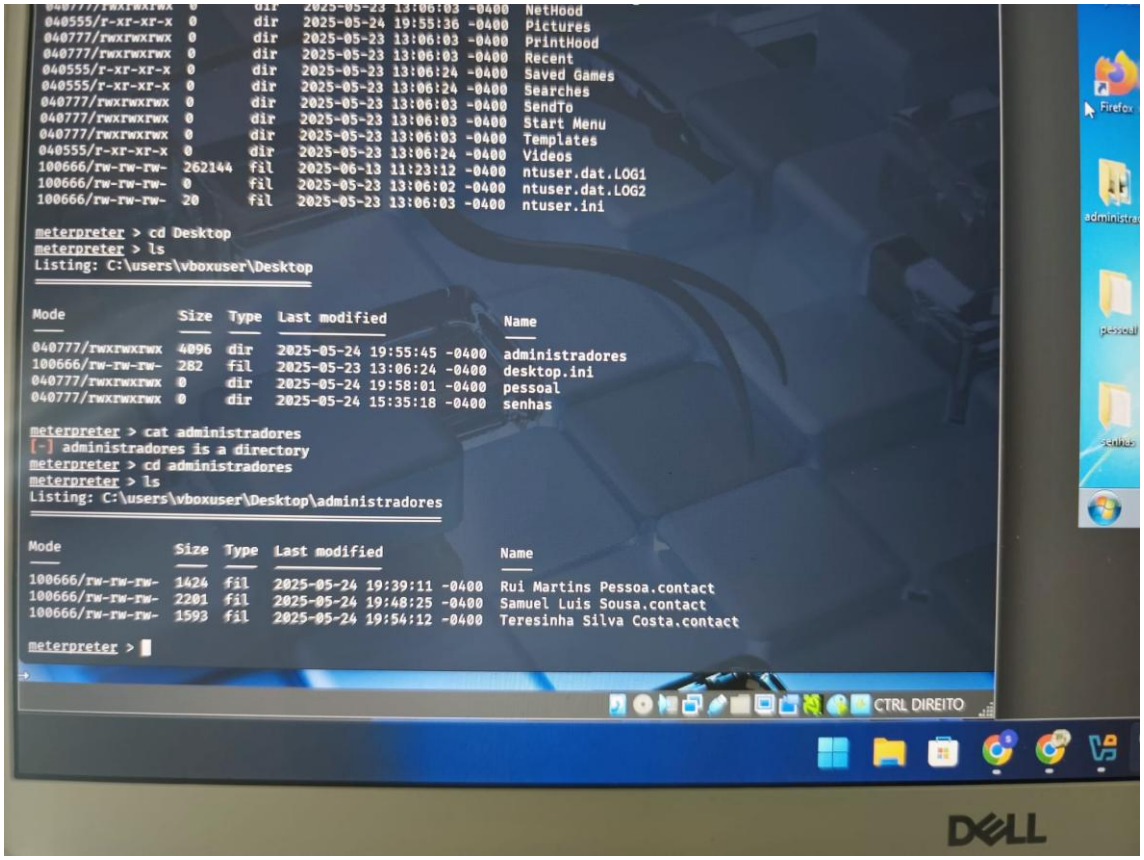


Figura 68_img_lendo_informaçoes

Depois de ter entrado na pasta “administradores”, conseguimos ver 3 contactos guardados:

- Rui Martins Pessoa
- Samuel Luis Sousa
- Teresinha Silva Costa

Se esse pentest fosse algo mais sério, esse tipo de informação seria muito perigosa, teriamos o nome de todos os administradores.

Voltando ao dektop e entrando na pasta “pessoal”...

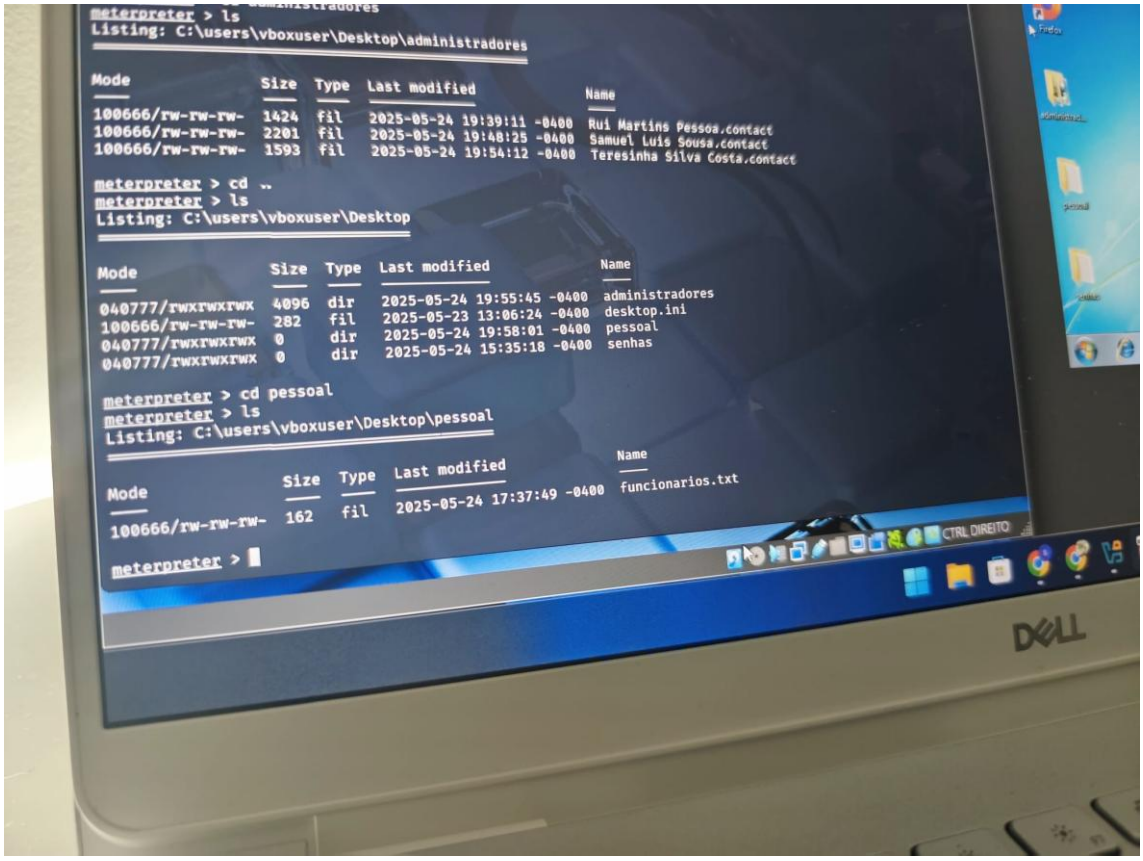


Figura 69_img_dados_funcionarios

Esta um arquivo em formato de texto (txt) de funcionarios. Usando o comando “cat”, ele nos pemite ler esses arquivos....

Figura 70_img_dados_emails

Quando executamos o comando “cat…”, ele nos deu os seguintes e-mails:

- Carlos_braga@gmail.com
- Ana123@gmail.com
- samuelsousa@gmail.com
- Felipe9999@gmail.com
- Joao_martelo@gmail.com
- Julia_santos@gmail.com

Com esta prática, concluímos a simulação de um ataque direcionado ao Windows 7, utilizando uma vulnerabilidade crítica e amplamente conhecida, o **EternalBlue**. Demonstramos como, com ferramentas adequadas e conhecimento técnico, é possível explorar falhas de segurança em sistemas desatualizados.

A atividade teve como objetivo reforçar a importância de manter os sistemas sempre atualizados, adotar boas práticas de segurança e compreender como os ataques ocorrem na prática para melhor preveni-los no mundo real.

Essa prática nos proporcionou uma visão clara das etapas de um pentest – desde a **varredura**, **identificação de vulnerabilidades**, **exploração** até o **acesso ao sistema alvo** – consolidando o aprendizado de forma prática e consciente.

Conclusão

Ao longo deste relatório, foi possível demonstrar, de forma prática e objetiva, como diversas técnicas de segurança ofensiva podem ser utilizadas tanto para identificar vulnerabilidades quanto para conscientizar sobre os riscos reais no ambiente digital.

Iniciamos com o uso da ferramenta **SQLMap**, que nos permitiu realizar ataques de **injeção SQL** e extrair credenciais diretamente de um banco de dados vulnerável. Este exemplo destacou a importância de **implementar senhas fortes** e proteger aplicações web contra falhas básicas, como validação inadequada de entradas de usuário.

Em seguida, exploramos o conceito de **engenharia social**, utilizando ferramentas como o **Zphisher** para criar páginas falsas que imitam redes sociais populares. Este exemplo evidenciou o quanto o fator humano pode ser explorado por atacantes e reforçou a necessidade de **educação digital**, tanto para usuários comuns quanto para profissionais da área, alertando para o perigo de **clicar em links suspeitos ou fornecer informações em sites não verificados**.

Com o ambiente **Kali Linux**, mostramos como uma distribuição voltada para segurança pode ser usada em simulações controladas de ataque, fornecendo um arsenal robusto de ferramentas para análise, exploração e pós-exploração. Através de um **pentest simulado em uma máquina com Windows 7**, utilizamos o exploit **EternalBlue** para demonstrar uma das vulnerabilidades mais conhecidas e impactantes da última década, reforçando como **sistemas desatualizados** se tornam **alvos fáceis para invasores**.

Além de técnicas ofensivas, o relatório teve como objetivo principal **educar, demonstrar e conscientizar**. Todas as etapas descritas foram realizadas em ambientes de teste, com fins exclusivamente didáticos, seguindo princípios éticos.

Por fim, fica evidente que **a segurança da informação vai muito além da tecnologia**: ela envolve **conhecimento, atualização constante, consciência dos riscos e boas práticas**. Espera-se que este material contribua para a formação de profissionais mais preparados, usuários mais cautelosos e sistemas mais seguros.

Problemas/soluções

Problema ao descobrir a versão correta do Kali Linux:
No início, houve dificuldade em identificar qual versão do Kali seria mais adequada para realizar os testes de pentest com estabilidade. Versões muito novas podem ter diferenças de compatibilidade com certas ferramentas, enquanto versões antigas podem estar desatualizadas.

ISO vulnerável do Windows 7:

Nem toda imagem ISO do Windows 7 vem com as vulnerabilidades necessárias para testes, como o EternalBlue. Após muita busca, com o apoio da comunidade no Reddit, encontrei uma versão funcional com SP1 no site confiável archive.org, que serviu perfeitamente para o experimento.

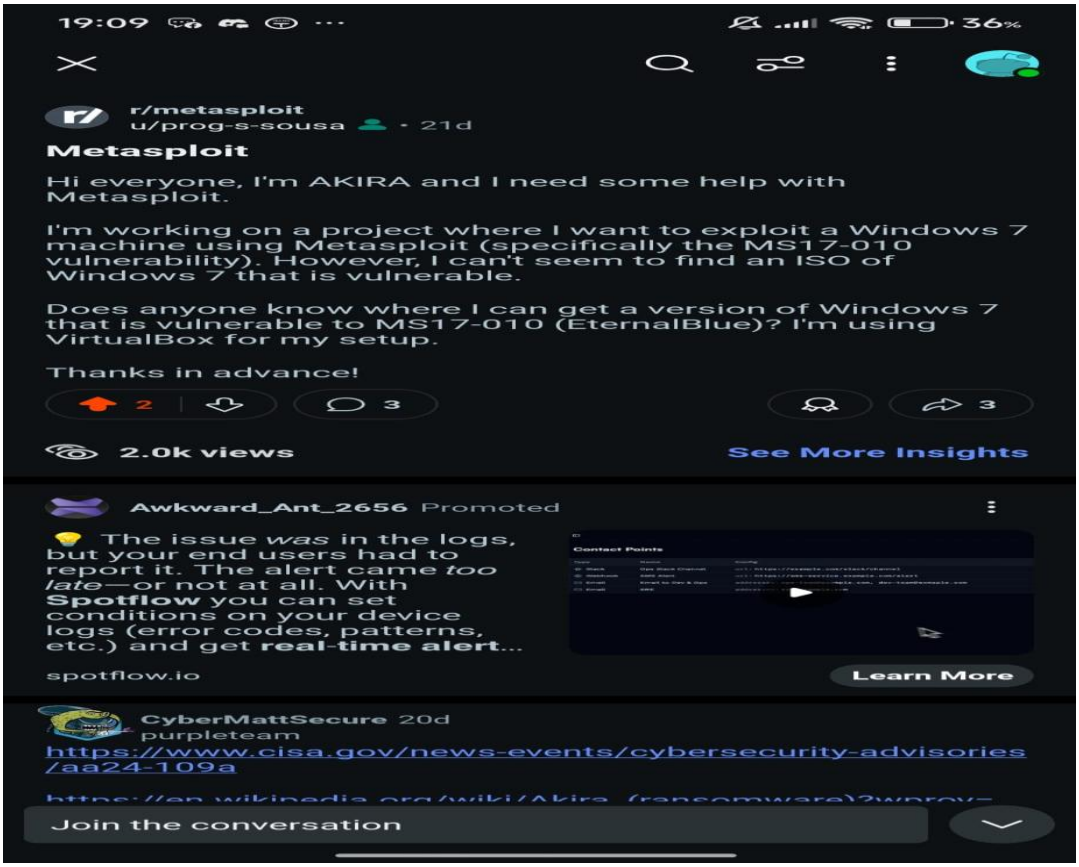
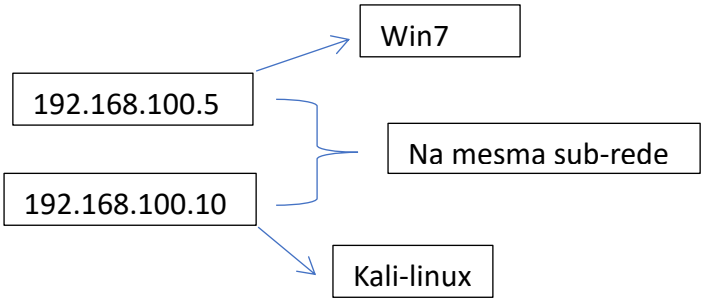


Figura 71_img_dúvida_reddit

Problemas de rede no VirtualBox:

A configuração da rede entre as máquinas virtuais (Kali e Windows 7) foi um desafio. Foi necessário ajustar o modo de rede para que ambas ficassem no mesmo ambiente virtual e pudessem se comunicar.

Máquinas não se enxergavam (Ping com erro):
Mesmo após configurar a rede, o comando ping apresentava erro, indicando que as máquinas não conseguiam se ver. O problema estava relacionado ao isolamento de rede ou às configurações de firewall do próprio Windows.



Kali Linux sem internet:
Em determinado momento, o Kali ficou sem acesso à internet, o que impediu a instalação e atualização de ferramentas necessárias. Foi preciso revisar e corrigir as configurações de rede NAT ou bridge no VirtualBox.

Problemas com a vulnerabilidade no Windows 7:
Apesar de saber que a versão era vulnerável ao EternalBlue, o ataque inicial falhou devido à presença do firewall e outros serviços de proteção ativos no Windows. Após desativar essas barreiras, a exploração pôde ser realizada com sucesso.

Referencias

- https://solyd.com.br/aluno/
- https://www.netacad.com/catalogs/learn/cybersecurity
    - Ethical Hacker
    - Introduction to Cybersecurity
- https://www.youtube.com/@brunofragax
- https://github.com/
- https://excalidraw.com/#json=UddnK4mL8SMBHxGRqOmFZ,xN4lrpvkGl-y7UTkeO5dXw