Módulo 1 - Aulas 3 e 4

Tarefas

No final deste módulo você deve submeter em um ÚNICO arquivo PDF os seguintes prints:

- Atividade 1.6: passo 11
- Atividade 1.7: passo 4.
- Atividade 1.8: passo 10.
- Atividade 1.9: passo 9.
- Atividade 1.10: passo 8.

Regras para a elaboração do documento:

1. Antes de cada Print, adicione obrigatoriamente uma frase explicativa que sinalize do que se trata o print. A inserção de prints sem a devida frase explicativa será considerada como tentativa de atrapalhar a correção do instrutor e será penalizada a critério do instrutor. Exemplo:

Print da atividade 1.6: [Imagem com o Print]

2. Os Prints devem ser tirados da TELA CHEIA. Quando tirados da VM da AWS, devem ser capturados **obrigatoriamente** da tela cheia clicando no botão “Screenshot” → “Take screenshot” da barra de ferramentas do Hypervisor da AWS.
3. Insira **somente a quantidade de Prints solicitados por atividade** usando exclusivamente 1 página por print. **A página do documento onde você vai inserir o Print deve estar com a orientação no modo PAISAGEM** ´para termos melhor aproveitamento do espaço. Ou seja, seu documento deverá ter a mesma quantidade de páginas que a quantidade do total de Prints! A inserção de prints desnecessários será considerada como tentativa de atrapalhar a correção do instrutor e será penalizada com nota 0.

4. Apresente Prints legíveis e com tamanho correto para fácil leitura. O envio de prints com letras minúsculas poderá ser considerado como tentativa de atrapalhar a correção do instrutor e será penalizada a critério do instrutor.

Atividade 1.6 – Conhecendo a ferramenta de Phishing ShellPhish no Kali Linux

Nesta atividade, vamos explorar a ferramenta de ShellPhish para simular ataques de phishing no Kali Linux.

Vamos começar inicializando nosso Kali Linux via RDP ao IP Kali: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.

1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

```
┌──(aluno㉿kali)-[~]
└─$ sudo -i
[sudo] senha para aluno:
```

2. Acesse a pasta da aplicação:

```
┌──(root㉿kali)-[~]
└─# cd /curso/ShellPhish

┌──(root㉿kali)-[/curso/ShellPhish]
└─# ls
capture.png  README.md          screenshot.png  sites
LICENSE      screenshot_fb.png  shellphish.sh   update.sh
```

3. Execute o Shellphish para inicializar a ferramenta:

```
┌──(root㉿kali)-[/curso/ShellPhish]
└─# bash shellphish.sh
```

4. Com a ferramenta aberta, vamos criar um link local para que a vítima acesse um site falso do Facebook. Selecione a opção 1:

```
      __  _               _  _            _                 _
     / / | | v2.5-MOD  | || | ______  | |     _       | |
    / /  | |           | || |(_____ \ | |    (_)      | |
    \ \  | |___   ____ | || | _____) )| |___  _   ___ | |___
     \ \ | |_  | / _  )| || ||  ____/ | |_  || | /___)| |_  |
 _____) )| | | |( (/ / | || || |      | | | || ||___ || | | |
(______/ |_| |_| \____)|_||_||_|      |_| |_||_|(___/ |_| |_|

      .:.:. Phishing Tool Moded by @AbirHasan2005 .:.:.

 :: Disclaimer: Developers assume no liability and are not    ::
 :: responsible for any misuse or damage caused by ShellPhish ::

.:. Choose any social site which you want to hack .:.

[01] Facebook     [11] Twitch       [21] DeviantArt
[02] Instagram    [12] Pinterest    [22] Badoo
[03] Google       [13] Snapchat     [23] Origin
[04] Microsoft    [14] Linkedin     [24] CryptoCoin
[05] Netflix      [15] Ebay         [25] Yahoo
[06] PayPal       [16] Dropbox      [26] Wordpress
[07] Steam        [17] Protonmail   [27] Yandex
[08] Twitter      [18] Spotify      [28] StackoverFlow
[09] PlayStation  [19] Reddit       [29] VK
[10] GitHub       [20] Adobe

[ST] Termux Setup [SL] Linux Setup  [EX] Exit

[~] Select an option: 1
```

5. Selecione a opção de abrir a página tradicional de login do Facebook:

```
[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page

[~] Select an option: 1
```

6. Selecione a opção de usar o localhost como meio de exibição web:

```
[01] LocalHost
[02] Ngrok.io
[03] Serveo.net
[04] Localhost.run

[~] Select a Port Forwarding option: 1
```

7. Selecione a porta 5050:

```
[~] Select a Port (Default: 5555 ): 5050

[~] Initializing ... (localhost:5050)

[~] Successfully Hosted at: http://localhost:5050


[~] Waiting for Login Info, Press Ctrl + C to exit ...
```

8. Tudo pronto! Em “Aplicativos” → “Navegador Web”, abra o navegador Firefox ESR e insira o endereço (certifique-se que copiou o campo “http://” como parte do link):

```
http://localhost:5050
```

9. Na página fake de Facebook, insira as credenciais “teste_usuario” e “teste_senha” e clique em “Log In” (clique em “Don´t save” para não salvar a senha).
10. Veja que a autenticação falha e você é encaminhado para o domínio correto do Facebook, na página de encontrar sua conta. Feche o Firefox ESR.
11. Volte o Terminal e veja que as credenciais foram capturadas (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
[*] Victim IP Found!

[~] Victim IP: 127.0.0.1

[~] Saved: sites/facebook/victim_ip.txt

[*] Login info Found!

[~] Account: teste_usuario
[~] Password:  teste_senha

[~] Saved: sites/facebook/login_info.txt

[~] Waiting for Next Login Info, Press Ctrl + C to exit ...
```

12. Aperte “Ctrl + C” para sair. Feche o Terminal.

Parabéns! Você conhece o princípio básico de um ataque Phishing que captura credenciais do Facebook.

Atividade 1.7 – Explorando a Ferramenta WHOIS no Kali Linux

Nesta atividade, vamos explorar a ferramenta WHOIS, nativa do Kali Linux. A ferramenta WHOIS é um serviço de pesquisa de informações relacionadas a registros de domínios na Internet. Ele fornece detalhes sobre a propriedade, administração e informações de contato associadas a um domínio específico, incluindo o nome e informações de contato do registrante, data de registro, servidores de nomes associados e informações de registro. O WHOIS é amplamente utilizado para verificar a disponibilidade de domínios, identificar proprietários de sites e investigar questões relacionadas à segurança cibernética.

Vamos começar inicializando nosso Kali Linux via RDP ao IP Kali: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.

1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

```
┌──(aluno㉿kali)-[~]
└─$ sudo -i
[sudo] senha para aluno:
```

2. Exploremos nosso primeiro alvo com a ferramenta WHOIS:

```
┌──(root㉿kali)-[~]
└─# whois esr.rnp.br

% Copyright (c) Nic.br - Use of this data is governed by the Use and
% Privacy Policy at https://registro.br/upp . Distribution,
% commercialization, reproduction, and use for advertising or similar
% purposes are expressly prohibited.
% 2025-09-04T21:29:43-03:00 - 54.227.80.239

domain:      rnp.br
owner:       Rede Nacional de Ensino e Pesquisa
owner-c:     RCO217
tech-c:      RCO217
nserver:     nscl1.rnp.br 162.159.8.154 2400:cb00:2049:1::a29f:89a
nsstat:      20250903 AA
nslastaa:    20250903
nserver:     nscl2.rnp.br 162.159.9.208 2400:cb00:2049:1::a29f:9d0
nsstat:      20250903 AA
nslastaa:    20250903
nserver:     nscl3.rnp.br 162.159.10.128 2400:cb00:2049:1::a29f:a80
nsstat:      20250903 AA
nslastaa:    20250903
nserver:     nscl4.rnp.br 162.159.11.186 2400:cb00:2049:1::a29f:bba
nsstat:      20250903 AA
nslastaa:    20250903
dsrecord:    2371 ECDSA-SHA-256
E22F8BE0F554F9285C4760CC398C47D4BE37C94C4A62DB6A9F1E726FEB2D0694
dsstatus:    20250903 DSOK
dslastok:    20250903
created:     before 19950101
changed:     20201126
status:      published

nic-hdl-br:  RCO217
person:      RNP - Centro de Engenharia e Operações
created:     20060406
changed:     20240919

% Security and mail abuse issues should also be addressed to cert.br,
% respectivelly to cert@cert.br and mail-abuse@cert.br
%
% whois.registro.br only accepts exact match queries for domains,
% registrants, contacts, tickets, providers, IPs, and ASNs.
```

O comando mostrado acima conta com os seguintes parâmetros:

- **domain: rnp.br**: Indica o nome do domínio registrado no sistema do Registro.br. Neste caso, trata-se do domínio rnp.br, pertencente à Rede Nacional de Ensino e Pesquisa (RNP), instituição responsável pela rede acadêmica e de pesquisa no Brasil.
- **owner: Rede Nacional de Ensino e Pesquisa**: Mostra o proprietário do domínio. No caso, a Rede Nacional de Ensino e Pesquisa é a entidade responsável pelo domínio rnp.br.
- **owner-c: RCO217**: Este é o handle ou código do proprietário no banco de dados de registro de domínios. Serve como identificador único da entidade proprietária (neste caso, "RCO217").
- **tech-c: RCO217**: Representa o código ou handle da pessoa ou equipe técnica responsável pela administração e configuração técnica do domínio. Neste caso, o código técnico é o mesmo do proprietário.
- **nserver: nscl1.rnp.br 162.159.8.154 2400:cb00:2049:1::a29f:89a**: Informa o servidor de nomes (DNS) principal associado ao domínio, que é nscl1.rnp.br. Os endereços IPs vinculados a esse servidor de nomes são 162.159.8.154 (IPv4) e 2400:cb00:2049:1::a29f:89a (IPv6). Este servidor DNS é responsável por resolver o domínio para seus respectivos endereços IP.

3. Veja as informações de uma prefeitura de um município:

```
┌──(root㉿kali)-[~]
└─# whois guanambi.ba.gov.br

% Copyright (c) Nic.br - Use of this data is governed by the Use and
% Privacy Policy at https://registro.br/upp . Distribution,
% commercialization, reproduction, and use for advertising or similar
% purposes are expressly prohibited.
% 2025-09-04T21:35:30-03:00 - 54.227.80.239

domain:      ba.gov.br
owner:       Cia. de Processamento de Dados do Estado da Bahia
owner-c:     CPDBA1
tech-c:      CPDBA1
nserver:     cpu0034.ba.gov.br 200.187.60.34
nsstat:      20250904 AA
nslastaa:    20250904
nserver:     cpu0020.prodeb.gov.br
nsstat:      20250904 AA
nslastaa:    20250904
nserver:     ns1.pop-ba.rnp.br
nsstat:      20250904 AA
nslastaa:    20250904
nserver:     ns2.pop-ba.rnp.br
nsstat:      20250904 AA
nslastaa:    20250904
dsrecord:    50863 ECDSA-SHA-256
C2E73306203E5B21A7B6D859927971CA94D3E7CA23F31577154D0080DAA9D7E1
dsstatus:    20250904 DSOK
dslastok:    20250904
created:     19951227 #4932
changed:     20250416
status:      published

nic-hdl-br:  CPDBA1
person:      Cia de Processamendo de Dados da Bahia
created:     20170815
changed:     20240308

% Security and mail abuse issues should also be addressed to cert.br,
% respectivelly to cert@cert.br and mail-abuse@cert.br
%
% whois.registro.br only accepts exact match queries for domains,
% registrants, contacts, tickets, providers, IPs, and ASNs.
```

O comando mostrado acima conta com os seguintes parâmetros:

- **domain: ba.gov.br**: Indica o nome do domínio consultado, que é ba.gov.br, utilizado pelo governo do estado da Bahia, Brasil.
- **owner: Cia. de Processamento de Dados do Estado da Bahia**: Mostra o proprietário do domínio. Neste caso, é a Cia. de Processamento de Dados do Estado da Bahia (PRODEB), responsável pela administração de dados e sistemas para o governo estadual.
- **owner-c: CPDBA1**: Este é o handle ou código único no banco de dados de registro, que identifica o proprietário do domínio (neste caso, "CPDBA1").
- **tech-c: CPDBA1**: Representa o código ou handle da pessoa ou entidade técnica responsável pelas configurações e suporte do domínio, que também é a Cia. de Processamento de Dados da Bahia ("CPDBA1").
- **nserver: cpu0034.ba.gov.br 200.187.60.34**: Informa um dos servidores de nomes (DNS) associados ao domínio, que é cpu0034.ba.gov.br. O endereço IP desse servidor DNS é 200.187.60.34, responsável por resolver as requisições de DNS para esse domínio.

4. Finalmente, exploremos o domínio de outro município (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO! MAXIMIZE O TERMINAL E CAPTURE A MAIOR QUANTIDADE POSSÍVEL DE INFORMAÇÕES**):

```
┌──(root㉿kali)-[~]
└─# whois itapaje.ce.gov.br

% Copyright (c) Nic.br - Use of this data is governed by the Use and
% Privacy Policy at https://registro.br/upp . Distribution,
% commercialization, reproduction, and use for advertising or similar
% purposes are expressly prohibited.
% 2025-09-04T21:37:08-03:00 - 54.227.80.239

domain:      ce.gov.br
owner:       EMPRESA DE TECNOLOGIA DA INFORMACAO DO CEARA-ETICE
owner-c:     RAOLI10
tech-c:      VLS171
nserver:     intsrv007.etice.ce.gov.br 189.90.164.21
2801:80:60:dc:cea4:a:164:21
nsstat:      20250903 AA
nslastaa:    20250903
nserver:     intsrv008.etice.ce.gov.br 189.90.164.31
2801:80:60:dc:cea4:a:164:31
nsstat:      20250903 AA
nslastaa:    20250903
nserver:     intsrv009.etice.ce.gov.br 138.118.143.178
nsstat:      20250903 TIMEOUT
nslastaa:    20230428
created:     19960527 #8516
changed:     20191025
status:      published

nic-hdl-br:  RAOLI10
person:      Raimundo Osman Lima
created:     20070509
changed:     20240202

nic-hdl-br:  VLS171
person:      Vera Lucia Carneiro de Sousa
created:     20041230
changed:     20221220

% Security and mail abuse issues should also be addressed to cert.br,
% respectivelly to cert@cert.br and mail-abuse@cert.br
%
% whois.registro.br only accepts exact match queries for domains,
% registrants, contacts, tickets, providers, IPs, and ASNs.
```

O comando mostrado acima conta com os seguintes parâmetros:

- **domain: ce.gov.br**: Esta linha mostra o nome do domínio consultado, que é ce.gov.br, utilizado pelo governo do estado do Ceará, Brasil.
- **owner: EMPRESA DE TECNOLOGIA DA INFORMACAO DO CEARA-ETICE**: Informa o proprietário do domínio, que é a Empresa de Tecnologia da Informação do Ceará (ETICE), a instituição responsável pela gestão de TI no estado do Ceará.
- **owner-c: RAOLI10**: Este é o handle (código único) que identifica o proprietário do domínio no banco de dados de registro. Neste caso, "RAOLI10" refere-se à pessoa ou entidade associada ao proprietário.
- **tech-c: VLS171**: Representa o código ou handle da pessoa ou equipe técnica responsável pela administração técnica do domínio. O handle aqui, "VLS171", refere-se à técnica responsável.
- **nserver: intsrv007.etice.ce.gov.br 189.90.164.21 2801:80:60:dc:cea4🅰️164:21**: Informa um dos servidores de nomes (DNS) associados ao domínio, que é intsrv007.etice.ce.gov.br. O endereço IP desse servidor é 189.90.164.21 (IPv4) e 2801:80:60:dc:cea4🅰️164:21 (IPv6). Esse servidor DNS é um dos responsáveis pela resolução de nomes para o domínio ce.gov.br.

5. Feche o Terminal.

Parabéns! Agora você conhece o tipo de informações públicas que um domínio de site pode oferecer!

Atividade 1.8 – Explorando a Ferramenta de Engenharia Social Maltego no Kali Linux

Nesta atividade, vamos usar o software Maltego, nativa do Kali Linux, para explorar as ferramentas de OSINT disponíveis.

1. Do seu computador pessoal ou celular (não da máquina virtual), acesse o site do Maltego e crie uma conta grátis com seus dados:

```
https://www.maltego.com/maltego-id-registration/
```

2. Agora, entre na VM do nosso cursp e inicie nosso Kali Linux via RDP ao IP Kali: 192.168.98.40, com usuário “aluno” e senha “rnpesr”. Em seguida, abra o Terminal e execute o seguinte comando com o usuário “aluno”:

```
┌──(aluno㉿kali)-[~]
└─$ maltego
```

3. Agora, o programa Maltego será aberto! Na janela “Welcome to Maltego”, seleciona a opção “MALTEGO ID” e clica em “Next”.
4. No seguinte passo, seleciona “Online Activation (Default)” e clica em “Next”.
5. Na janela “Configure Maltego”, selecione “Accept” e clique em “Next”.
6. Agora, clique em “Browser Login”, espere que o Firefox seja aberto e insira as credenciais (e-mail e senha) criadas no passo 1 e clique em “SIGN IN TO MALTEGO”. Você verá a mensagem “Authentication Complete” no Firefox.
7. Volte ao Maltego, veja a mensagem “Have fun using Maltego” e clique em “Next” 4 vezes até chegar ao passo “7. Data Sources T&Cs” apresentado na coluna da esquerda.
8. Marque a caixa “*By checking the box, I declare that...*” e clique em “Next” 5 vezes até chegar ao passo “12. Ready”. Clique em “Finish” para completar a configuração do Maltego. O Maltego abrirá! Clique na caixa “Don´t show this again” e em “OK” na janela “Low Memory Allocation Detected”.
9. Na mensagem amarela “Maltego Product Tour”, selecione “Don´t ask again” e clique em “Not now” → “Close”.
10. Explore a aba “Transforms” → “Maltego Data Hub” e visualize as aplicações disponíveis de OSINT no Maltego (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**).
11. Feche o software Maltego, feche o Firefox e feche o Terminal.

Parabéns! Agora você está pronto para usar a ferramenta Maltego!

Atividade 1.9 – Reconhecimento passivo OSINT com Maltego no Kali Linux

Nesta atividade, vamos usar o software Maltego para executar reconhecimento passivo OSINT a partir de páginas Web de instituições.

Vamos começar inicializando nosso Kali Linux via RDP ao IP Kali: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.

1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

```
┌──(aluno㉿kali)-[~]
└─$ maltego
```

2. Com o “Maltego” aberto, aguarde 1 minuto para que carregue totalmente e clique em “New”.
3. Na barra de navegação da esquerda, em “Entity Palette”, procure a opção “Website” no grupo “Infrastructure” e arraste esse botão para o painel em branco da direita.
4. Mude o site “www.maltego.com” para “ufc.br” (site da Universidade Federal do Ceará). Na janela “Trust Certificate?”, clique em “Cancel”.
5. Clique com o botão direito no símbolo verde WWW do site “ufc.br”, selecione “+ All Transforms” → “[Utilities] To Domains [withnin Properties]”. Será aberto o domínio da UFC.
6. Agora, vamos encontrar os nomes DNS associados. Clique com o botão direito no símbolo verde WWW do site “ufc.br”, selecione “[Utilities] To DNSNames [withnin Properties]”.
7. Em seguida, vamos encontrar pessoas vinculadas ao site. Clique com o botão direito no símbolo do site (bola azul) “ufc.br” e selecione “[Utilities] To Person [PGP]”. Veja que muitos nomes foram apresentados.
8. Na sequência, vamos encontrar e-mails institucionais vinculados ao site. Clique com o botão direito no símbolo do site (bola azul) “ufc.br”, selecione “[Utilities] To Email Addresses [PGP]”. Veja que muitos e-mails institucionais de pessoas foram apresentados.
9. Agora, vamos encontrar qual servidor de e-mail institucional usa a instituição. Clique com o botão direito no símbolo do site (bola azul) “ufc.br”, selecione “[Utilities] To DNS Name – MX (mail server)”. Veja que os servidores apresentados são Google (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**).
10. Feche o Maltego e selecione a opção “Discard All”. Feche o Terminal.

Parabéns! Agora você sabe os princípios do uso do Maltego para reconhecimento de informações públicas.

Atividade 1.10 – Conhecendo Ataques Contra Aprendizagem de Máquinas (Adversarial Machine Learning)

Nesta atividade, vamos usar o software “adversarial.js” para executar, visualizar e entender ataques de Adversarial Machine Learning. Neste site é possível escolher uma imagem que será corretamente decodificada por um sistema de aprendizagem de máquinas. Em seguida, a imagem corretamente decodificada sofre alterações imperceptíveis para o olho humano, mas acaba sendo decodificada erroneamente pelo sistema de aprendizagem de máquinas após essas alterações. Dessa maneira, o sistema de aprendizagem de máquinas consegue ser enganado e o ataque Adversarial Machine Learning é executado com sucesso.

Use seu computador!

1. Adversarial Machine Learning refere-se a uma área de pesquisa que explora as vulnerabilidades e desafios associados à segurança de modelos de aprendizado de máquina. Nesse contexto, adversarial refere-se a entidades maliciosas que buscam explorar as fraquezas dos modelos, introduzindo entradas manipuladas de forma a enganar ou comprometer o desempenho do sistema. Essas manipulações podem envolver pequenas perturbações nos dados de entrada, projetadas de maneira inteligente para induzir erros nos modelos, resultando em classificações incorretas. Os ataques adversariais podem ser direcionados a diversos tipos de modelos de aprendizado de máquina, como redes neurais, SVMs e modelos de regressão, e podem ter implicações significativas em domínios críticos, como segurança, saúde e finanças. A pesquisa em Adversarial Machine Learning busca desenvolver técnicas robustas para mitigar essas ameaças e fortalecer a segurança dos modelos em ambientes do mundo real.
2. Abra o navegador da sua preferência e insira o endereço:

```
https://kennysong.github.io/adversarial.js/
```

3. Selecione o modelo “GTSRB (street sign recognition)” para visualizar a imagem (STOP) que será lida pelo sistema de aprendizagem de máquinas.

4. Na coluna “Original Image”, clique em “RUN NEURAL NETWORK”.
5. Abaixo, veja que a imagem é corretamente decodificada e a predição é correta.
6. Na coluna “Adversarial Image”, clique no botão azul “GENERATE” para visualizar a imagem com alterações que será lida pelo sistema de aprendizagem de máquinas novamente (demora alguns segundos).
7. Veja que outra imagem muito parecida a “Original Image” é apresentada.
8. Na coluna “Adversarial Image”, clique em “RUN NEURAL NETWORK” e veja que a predição da imagem lida resulta em erro! Ou seja, o sistema de Inteligência Artificial foi enganado, resultado no ataque Adversarial Machine Learning! (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**).
9. Feche seu navegador.

Parabéns! Agora você entende como funciona o ataque Adversarial Machine Learning!