Módulo 2 - Aulas 3 e 4

Tarefas

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

- Atividade 2.6: passo 8.
- Atividade 2.7: passo 5.
- Atividade 2.8: passo 7.
- Atividade 2.9: passo 4.
- Atividade 2.10: passo 7.

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 2.6: [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 2.6 – Explorando o controle técnico de criptografia de dados com Ccrypt no Kali Linux

Nesta atividade, vamos explorar a ferramenta CCrypt e fazer a demonstração do seu uso no Kali Linux. O CCrypt implementará a cifração e decifração de dados como exemplo de controle técnico de dados. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

1. No navegador do seu computador (não na VM do nosso laboratório), acesse o seguinte site e estude o potencial da ferramenta Ccrypt:

```
https://ccrypt.sourceforge.net/
```

2. Inicialize nosso Kali Linux via RDP ao IP Kali: 192.168.98.40, com usuário “aluno” e senha “rnpesr”. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

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

3. Acesse a pasta Documentos e crie um arquivo de texto com uma mensagem:

```
┌──(root㉿kali)-[~]
└─# cd /home/aluno/Documentos/

┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ls

┌──(root㉿kali)-[/home/aluno/Documentos]
└─# nano mensagem.txt
```

4. Insira o seguinte texto:

```
Hackers do bem!
```

5. Em seguida, aperte “Ctrl + x”, “s” para salvar e “Enter” para confirmar. Neste momento, acabamos de criar o arquivo “mensagem.txt”. Liste os arquivos na pasta para verificar que o arquivo foi criado:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ls
mensagem.txt
```

6. Veja as opções de execução do ccrypt:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ccrypt -h
ccrypt 1.11. Secure encryption and decryption of files and streams.

Usage: ccrypt [mode] [options] [file...]
       ccencrypt [options] [file...]
       ccdecrypt [options] [file...]
       ccat [options] file...

Modes:
    -e, --encrypt         encrypt
    -d, --decrypt         decrypt
    -c, --cat             cat; decrypt files to stdout
    -x, --keychange       change key
    -u, --unixcrypt       decrypt old unix crypt files

Options:
    -h, --help            print this help message and exit
    -V, --version         print version info and exit
    -L, --license         print license info and exit
    -v, --verbose         print progress information to stderr
    -q, --quiet           run quietly; suppress warnings
    -f, --force           overwrite existing files without asking
    -m, --mismatch        allow decryption with non-matching key
    -E, --envvar var      read keyword from environment variable
(unsafe)
    -K, --key key         give keyword on command line (unsafe)
    -k, --keyfile file    read keyword(s) as first line(s) from file
    -P, --prompt prompt   use this prompt instead of default
    -S, --suffix .suf     use suffix .suf instead of default .cpt
    -s, --strictsuffix    refuse to encrypt files which already have
suffix
    -F, --envvar2 var     as -E for second keyword (for keychange mode)
    -H, --key2 key        as -K for second keyword (for keychange mode)
    -Q, --prompt2 prompt  as -P for second keyword (for keychange mode)
    -t, --timid           prompt twice for encryption keys (default)
    -b, --brave           prompt only once for encryption keys
    -y, --keyref file     encryption key must match this encrypted file
    -r, --recursive       recurse through directories
    -R, --rec-symlinks    follow symbolic links as subdirectories
    -l, --symlinks        dereference symbolic links
    -T, --tmpfiles        use temporary files instead of overwriting
(unsafe)
    --                    end of options, filenames follow
```

7. Apliquemos o controle de acesso com criptografia em cima do arquivo “mensagem.txt” com o ccrypt uma senha qualquer (sugestão de senha: abcd1234):

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ccrypt -e mensagem.txt
Enter encryption key:
Enter encryption key: (repeat)
```

Os parâmetros desse comando são:

- ccrypt: Este é o comando principal para usar o programa ccrypt.
- -e: Este é o parâmetro que indica que você está realizando a operação de criptografia (encryption). Quando você usa "-e", está instruindo o ccrypt a criptografar o arquivo especificado.
- mensagem.txt: Este é o argumento que fornece o nome do arquivo que você deseja criptografar. Neste caso, o arquivo alvo é chamado "mensagem.txt".

8. Veja no que se converteu o arquivo "mensagem.txt" e observe que seu conteúdo será algo similar ao apresentado abaixo (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ls
mensagem.txt.cpt

┌──(root㉿kali)-[/home/aluno/Documentos]
└─# cat mensagem.txt.cpt
Z�w�.����K��^�������>�I6E9Y�i��8Z;mU\�;X�
```

Veja que o arquivo está cifrado.

9. Decifre a mensagem com a senha inserida anteriormente:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ccrypt -d mensagem.txt.cpt
Enter decryption key:
```

Os parâmetros desse comando são:

- ccrypt: Este é o comando principal para usar o programa ccrypt.
- -d: Este é o parâmetro que indica que você está realizando a operação de descriptografia (decryption). Quando você usa "-d", está instruindo o ccrypt a descriptografar o arquivo especificado.
- mensagem.txt.cpt: Este é o argumento que fornece o nome do arquivo que você deseja descriptografar. Neste caso, o arquivo alvo é chamado "mensagem.txt.cpt". Geralmente, os arquivos criptografados pelo ccrypt têm a extensão ".cpt" adicionada ao nome original.

10. Verifique que o arquivo original foi recuperado e veja seu conteúdo:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ls
mensagem.txt

┌──(root㉿kali)-[/home/aluno/Documentos]
└─# cat mensagem.txt
Hackers do bem!
```

11. Apague o arquivo “mensagem.txt” e na sequência feche o Terminal:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# rm mensagem.txt

┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ls
```

Parabéns! Você aprendeu a aplicar o controle técnico de criptografia com a ferramenta Ccrypt!

Atividade 2.7 – Explorando os eventos de sistema com o Logcheck no Linux

Nesta atividade, vamos explorar a ferramenta Logcheck para analisar os principais eventos de sistema do Kali Linux como controle detectivo. O Logcheck é uma ferramenta para análise de logs em sistemas Linux, projetada para identificar e relatar padrões incomuns ou potencialmente preocupantes nas mensagens de log do sistema. Ao automatizar a análise de logs, o Logcheck permite que os administradores de sistema identifiquem rapidamente eventos relevantes, como tentativas de acesso não autorizado, falhas de autenticação ou outros comportamentos anômalos. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

A ferramenta possui três modos de filtragem:

- Servidor: nível padrão contendo diferentes daemons.
- Paranóico: máquinas de alta segurança funcionam como serviço neste nível também é prolixo.
- Estação de trabalho: Nível para máquinas protegidas, filtragem de mensagens.

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 o usuário “aluno” (insira a senha “rnpesr” caso o Terminal a solicite). No seu caso a saída pode ser maior caso você tenha reiniciado a VM Kali Linux:

```
┌──(aluno㉿kali)-[~]
└─$ sudo -u logcheck logcheck -o -t
This email is sent by logcheck. If you no longer wish to receive
such mail, you can either uninstall the logcheck package or modify
its configuration file (/etc/logcheck/logcheck.conf).

Security Events for sudo
=-=-=-=-=-=-=-=-=-=-=-=-=-
2024-02-08T18:04:35.855136-03:00 ip-192-168-98-40 sudo: pam_unix(sudo-
i:session): session closed for user root
fev 08 18:04:35 kali sudo[5209]: pam_unix(sudo-i:session): session
closed for user root

System Events
=-=-=-=-=-=-=
2024-02-08T18:02:53.499503-03:00 ip-192-168-98-40 dhclient[495]: XMT:
Solicit on eth0, interval 108860ms.
2024-02-08T18:04:42.410794-03:00 ip-192-168-98-40 dhclient[495]: XMT:
Solicit on eth0, interval 125740ms.
2024-02-08T18:04:50.231955-03:00 ip-192-168-98-40 xrdp-chansrv[1991]:
[ERROR] clipboard_event_selection_request: unknown target text/
plain;charset=utf-8
2024-02-08T18:04:50.239116-03:00 ip-192-168-98-40 xrdp-chansrv[1991]:
[ERROR] clipboard_event_selection_request: unknown target text/
plain;charset=utf-8
fev 08 18:02:53 kali dhclient[495]: XMT: Solicit on eth0, interval
108860ms.
fev 08 18:04:42 kali dhclient[495]: XMT: Solicit on eth0, interval
125740ms.
fev 08 18:04:50 kali xrdp-chansrv[1991]: [ERROR]
clipboard_event_selection_request: unknown target text/
plain;charset=utf-8
fev 08 18:04:50 kali xrdp-chansrv[1991]: [ERROR]
clipboard_event_selection_request: unknown target text/
plain;charset=utf-8
```

Os parâmetros do comando são:

- -u logcheck: Este parâmetro especifica o usuário sob o qual o comando será executado. Portanto, o comando logcheck -o -t será executado com os privilégios do usuário logcheck.
- logcheck: Este é o comando principal que está sendo executado. O logcheck é uma ferramenta utilizada para analisar e relatar mensagens de log do sistema.

- -o: Este parâmetro indica que o logcheck deve operar no modo "online". Ele analisará e relatará mensagens de log à medida que são geradas, em vez de processar logs antigos.
- -t: Este parâmetro especifica que o logcheck deve exibir os relatórios em um formato de texto simples.

2. O log apresenta uma série de eventos do sistema capturados pelos logs do kernel. Veja os eventos mais relevantes (podem variar um pouco no seu ambiente): **Security Events for sudo**:

- **2024-02-08T18:04:35.855136-03:00 ip-192-168-98-40 sudo: pam_unix(sudo-i:session)**: session closed for user root: Esta mensagem indica que a sessão sudo para o usuário root foi encerrada. A data e hora da ocorrência são: 8 de fevereiro de 2024 às 18:04:35, horário local. O serviço ip-192-168-98-40 relatou o evento. É um evento relacionado à segurança, indicando o encerramento de uma sessão sudo.

System Events:

- **2024-02-08T18:02:53.499503-03:00 ip-192-168-98-40 dhclient[495]: XMT: Solicit on eth0, interval 108860ms.**: Este log é gerado pelo dhclient (cliente DHCP) tentando obter um endereço IP para a interface de rede eth0. A data e hora da ocorrência são: 8 de fevereiro de 2024 às 18:02:53, horário local. O serviço ip-192-168-98-40 relatou o evento. É um evento relacionado ao sistema, indicando uma solicitação DHCP para a interface eth0.
- **2024-02-08T18:04:50.231955-03:00 ip-192-168-98-40 xrdp-chansrv[1991]: [ERROR] clipboard_event_selection_request: unknown target text/plain;charset=utf-8**: Este log é gerado pelo serviço xrdp-chansrv (Servidor de Canal do XRDP) e indica um erro relacionado a uma solicitação de evento de área de transferência com um destino desconhecido. A data e hora da ocorrência são: 8 de fevereiro de 2024 às 18:04:50, horário local. O serviço ip-192-168-98-40 relatou o evento. É um evento de erro relacionado ao sistema, indicando uma falha ao processar uma solicitação de evento de área de transferência.

- **2024-02-08T18:06:48.170853-03:00 ip-192-168-98-40 dhclient[495]: XMT: Solicit on eth0, interval 114710ms.**: Este log é semelhante ao primeiro log do dhclient, indicando outra tentativa de solicitar um endereço IP para a interface de rede eth0. A data e hora da ocorrência são: 8 de fevereiro de 2024 às 18:06:48, horário local. O serviço ip-192-168-98-40 relatou o evento. É um evento relacionado ao sistema, indicando outra tentativa de solicitar um endereço IP DHCP para a interface eth0.

3. Vamos agora dar uma olhada no arquivo de configuração logcheck.conf de logcheck localizado no diretório / etc / logcheck. Entre no modo super usuário e abra o arquivo de configuração:

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

┌──(root㉿kali)-[~]
└─# nano /etc/logcheck/logcheck.conf
```

4. Com o arquivo de configuração aberto, altere o REPORTLEVEL para “workstation”. Opcionalmente, insira seu e-mail para que possa receber os relatórios e logs no E-mail (se estiver usando um usuário do sistema, ele deve ter um alias válido para o logcheck e o remetente / mailer - mail, sendmail, sSMTP, Postfix- deve ser instalado) e como anexo:

```
REPORTLEVEL="workstation"

# Controls the address mail goes to:
# *NOTE* the script does not set a default value for this variable!
# Should be set to an offsite "emailaddress@some.domain.tld"

SENDMAILTO="umemail@gmail.com"

# Send the results as attachment or not.
# 0=not as attachment; 1=as attachment; 2=as gzip attachment
# Default is 0

MAILASATTACH=1
```

Em seguida, aperte “Ctrl + X”, “S” para salvar e “Enter” para confirmar.

5. Execute novamente o passo 1 e veja a nova saída (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO! Somente as 20 primeiras linhas**):

```
┌──(root㉿kali)-[~]
└─# exit

┌──(aluno㉿kali)-[~]
└─$ sudo -u logcheck logcheck -o -t
This email is sent by logcheck. If you no longer wish to receive
such mail, you can either uninstall the logcheck package or modify
its configuration file (/etc/logcheck/logcheck.conf).

Security Events for sudo
=-=-=-=-=-=-=-=-=-=-=-=-
2024-02-08T18:04:35.855136-03:00 ip-192-168-98-40 sudo: pam_unix(sudo-
i:session): session closed for user root
2024-02-08T18:12:31.367745-03:00 ip-192-168-98-40 sudo: pam_unix(sudo-
i:session): session opened for user root(uid=0) by (uid=1001)
2024-02-08T18:16:03.554902-03:00 ip-192-168-98-40 sudo: pam_unix(sudo-
i:session): session closed for user root
fev 08 18:12:31 kali sudo[8454]: pam_unix(sudo-i:session): session
opened for user root(uid=0) by (uid=1001)
fev 08 18:16:03 kali sudo[8454]: pam_unix(sudo-i:session): session
closed for user root

System Events
=-=-=-=-=-=-
2024-02-08T18:02:53.499503-03:00 ip-192-168-98-40 dhclient[495]: XMT:
Solicit on eth0, interval 108860ms.
2024-02-08T18:04:42.410794-03:00 ip-192-168-98-40 dhclient[495]: XMT:
Solicit on eth0, interval 125740ms.
2024-02-08T18:04:50.231955-03:00 ip-192-168-98-40 xrdp-chansrv[1991]:
[ERROR] clipboard_event_selection_request: unknown target text/
plain;charset=utf-8
2024-02-08T18:04:50.239116-03:00 ip-192-168-98-40 xrdp-chansrv[1991]:
[ERROR] clipboard_event_selection_request: unknown target text/
plain;charset=utf-8
2024-02-08T18:06:48.170853-03:00 ip-192-168-98-40 dhclient[495]: XMT:
Solicit on eth0, interval 114710ms.
2024-02-08T18:08:42.922879-03:00 ip-192-168-98-40 dhclient[495]: XMT:
Solicit on eth0, interval 112740ms.
2024-02-08T18:10:35.763167-03:00 ip-192-168-98-40 dhclient[495]: XMT:
Solicit on eth0, interval 129930ms.
2024-02-08T18:12:45.793377-03:00 ip-192-168-98-40 dhclient[495]: XMT:
Solicit on eth0, interval 129080ms.
2024-02-08T18:13:47.104704-03:00 ip-192-168-98-40 xrdp-chansrv[1991]:
[ERROR] clipboard_event_selection_request: unknown target text/
plain;charset=utf-8
2024-02-08T18:13:47.111981-03:00 ip-192-168-98-40 xrdp-chansrv[1991]:
[ERROR] clipboard_event_selection_request: unknown target text/
plain;charset=utf-8
```

```
plain;charset=utf-8
2024-02-08T18:14:54.973652-03:00 ip-192-168-98-40 dhclient[495]: XMT:
Solicit on eth0, interval 114690ms.
fev 08 18:08:42 kali dhclient[495]: XMT: Solicit on eth0, interval
112740ms.
fev 08 18:10:35 kali dhclient[495]: XMT: Solicit on eth0, interval
129930ms.
fev 08 18:12:45 kali dhclient[495]: XMT: Solicit on eth0, interval
129080ms.
fev 08 18:13:47 kali xrdp-chansrv[1991]: [ERROR]
clipboard_event_selection_request: unknown target text/
plain;charset=utf-8
fev 08 18:13:47 kali xrdp-chansrv[1991]: [ERROR]
clipboard_event_selection_request: unknown target text/
plain;charset=utf-8
fev 08 18:14:54 kali dhclient[495]: XMT: Solicit on eth0, interval
114690ms.
```

Os logs novos explicam o seguinte: **Security Events**:

- **2024-02-08T18:12:31.367745-03:00 ip-192-168-98-40 sudo: pam_unix(sudo-i:session): session opened for user root(uid=0) by (uid=1001)**: Esta mensagem indica que uma nova sessão sudo foi aberta para o usuário root. A data e hora da ocorrência são: 8 de fevereiro de 2024 às 18:12:31, horário local. O serviço ip-192-168-98-40 relatou o evento. É um evento relacionado à segurança, indicando a abertura de uma sessão sudo para o usuário root.
- **2024-02-08T18:16:03.554902-03:00 ip-192-168-98-40 sudo: pam_unix(sudo-i:session): session closed for user root**: Esta mensagem indica que a sessão sudo para o usuário root foi encerrada. A data e hora da ocorrência são: 8 de fevereiro de 2024 às 18:16:03, horário local. O serviço ip-192-168-98-40 relatou o evento. É um evento relacionado à segurança, indicando o encerramento de uma sessão sudo para o usuário root.

System Events

- **2024-02-08T18:08:42.922879-03:00 ip-192-168-98-40 dhclient[495]: XMT: Solicit on eth0, interval 112740ms.**: Esta mensagem indica uma nova tentativa do cliente DHCP (dhclient) de solicitar um endereço IP para a interface de rede eth0. A data e hora da ocorrência são: 8 de fevereiro de 2024 às 18:08:42, horário local. O serviço ip-192-168-98-40 relatou o evento. É um evento relacionado ao sistema, indicando uma solicitação DHCP para a interface eth0.

- **2024-02-08T18:13:47.104704-03:00 ip-192-168-98-40 xrdp-chansrv[1991]: [ERROR] clipboard_event_selection_request: unknown target text/plain;charset=utf-8**: Esta mensagem é semelhante às anteriores, indicando um erro relacionado a uma solicitação de evento de área de transferência com um destino desconhecido. A data e hora da ocorrência são: 8 de fevereiro de 2024 às 18:13:47, horário local. O serviço ip-192-168-98-40 relatou o evento. É um evento de erro relacionado ao sistema, indicando uma falha ao processar uma solicitação de evento de área de transferência.

6. Feche o Terminal.

Parabéns! Agora você conhece como implantar controles detectivos analisando os logs do Kali Linux.

Atividade 2.8 – Explorando o navegador Tor no Kali Linux

Nesta atividade, vamos explorar o navegador Tor Browser e fazer a configuração para navegar na DeepWeb no Kali Linux. O Tor Browser permitirá que naveguemos na DeepWeb e veremos como o IP é emascarado quando usamos o Tor Browser para navegar na DeepoWeb. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

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

1. Na barra de navegação inferior, abra o Terminal e execute o seguinte comando para abrir o navegador Tor que está previamente configurado:

```
┌──(aluno㉿kali)-[~]
└─$ torbrowser-launcher
Lançador do Navegador Tor
By Micah Lee & Tor Project, licensed under MIT
versão 0.3.7
https://gitlab.torproject.org/tpo/applications/torbrowser-launcher/
Criando o diretório inicial do GnuPG /home/aluno/.local/share/
torbrowser/gnupg_homedir
Downloading Tor Browser for the first time.
Baixando https://aus1.torproject.org/torbrowser/update_3/release/
Linux_x86_64-gcc3/x/ALL
MESA: error: ZINK: failed to choose pdev
glx: failed to create drisw screen
Versão mais recente: 13.5.6
Baixando https://dist.torproject.org/torbrowser/13.5.6/tor-browser-
linux-x86_64-13.5.6.tar.xz.asc
Baixando https://dist.torproject.org/torbrowser/13.5.6/tor-browser-
linux-x86_64-13.5.6.tar.xz
Verificando Assinatura
Downloading latest Tor Browser signing key...
Key imported successfully
Extraindo tor-browser-linux-x86_64-13.5.6.tar.xz
Rodando /home/aluno/.local/share/torbrowser/tbb/x86_64/tor-browser/
start-tor-browser.desktop
Launching './Browser/start-tor-browser --detach'...
```

2. Veja que o navegador Tor foi aberto. Clique no botão roxo “Conectar”.
3. Veja que a mensagem “Estabelecendo uma Conexão” é mostrada. Isso significa que o navegador está estabelecendo conexão com a rede Tor.
4. Provavelmente a mensagem de falha na conexão deve aparecer. Nesse caso, clique em “Try a bridge”.
5. No navegador Tor, acesse o site (clique em “Sim” para a sugestão de obter a versão em inglês):

```
https://duckduckgo.com/
```

6. Veja que o site DuckDuckGo foi aberto! Agora, abra uma nova aba e acesse o site (clique em “AGREE” na mensagem “We value your privacy”):

```
https://whatismyipaddress.com/
```

7. Anote o IP e a localização apresentada. Ao elaborar este conteúdo, os dados foram (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
IPv6: ? 2a0b:f4c0:16c:16::1

IPv4: ? 185.220.100.240

Your location may be exposed!
Hide My IP Address Now

Show Complete IP Details

My IP Information:

ISP: Stiftung Erneuerbare Freiheit

Services: Tor Exit Node

City: Frankfurt am Main

Region: Hessen

Country: Germany
```

8. Para confirmar que o navegador Tor realmente está na rede Tor, abra o Mozilla Firefox (em “Aplicativos” → “Navegador Web”) e acesse novamente o site do passo 6. No caso deste exemplo, os dados foram:

```
IPv4: 107.22.123.86

IPv6: Not detected

Your location may be exposed!
Hide My IP Address Now

Show Complete IP Details

My IP Information:

ISP: Amazon.com Inc.

City: Ashburn

Region: Virginia

Country: United States
```

9. Veja que a localização do IP apresentada pelo navegador Tor é diferente da mostrada pelo Firefox, que está saindo pelo ISP da Amazon. Isso significa que o navegador Tor está de fato navegando pela rede Tor e o navegador Firefox ESR está navegando normalmente (fora da rede Tor).
10. Não feche o navegador Firefox nem o Tor porque serão usados na próxima atividade.

Parabéns! Agora você está conectado à rede Tor e pronto para navegar na DeepWeb.

Atividade 2.9 – Navegando na DeepWeb pelo navegador Tor no Kali Linux

Nesta atividade, vamos dar continuidade à atividade anterior. Agora, com o navegador Tor configurado, vamos navegar na DeepWeb. Todo material apresentado aqui deve ser usado somente para fins acadêmicos. Tome cuidado e não navegue sem pesquisar a fonte do link para não acessar conteúdo relacionado a crimes cibernéticos.

É importante ressaltar que embora a navegação na rede Tor possa oferecer anonimato e privacidade online, seu uso para atividades criminosas é estritamente proibido e pode resultar em sérias consequências legais. Ao utilizar a rede Tor, os usuários devem estar cientes de que certas atividades, como acesso ilegal a sistemas, distribuição de material ilegal, acesso a pornografia infantil, fraude, violação de direitos autorais e outras atividades criminosas, são estritamente proibidas e sujeitas a penalidades legais severas. Além disso, governos e autoridades de aplicação da lei em muitos países monitoram de perto o uso da rede Tor para detectar e punir atividades ilegais.

Vamos dar continuidade à Atividade 2.8.

1. No navegador Firefox e acesse o site:

```
https://thehiddenwiki.org
```

2. Veja que foi aberto um site que contém endereços de sites da DeepWeb. Os sites da DeepWeb têm a característica de finalizar com a extensão ".onion".
3. Como teste, abra uma nova aba no navegador Tor e acesse o site (demora um par de minutos):

```
http://6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldeommfxjz3wkhalzgjqxzqd.onion
```

4. Veja que o site foi aberto com a mensagem (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
The Hidden Wiki

The Original Hidden Wiki - Only @
6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldeommfxjz3wkhalzgjqxzqd.onion

Update 07.2020: The old short v2 .onion hidden service links will no
longer work after october 2021. We will list only v3 .onion's in the
future.
```

5. Abra outras abas no navegador Tor e acesse outros sites sugeridos (Dark Web) na página aberta do passo 4. Entre eles:

```
http://n6qisfgjauj365pxccpr5vizmtb5iavqaug7m7e4ewkxuygk5iim6yyd.onion

http://prjd5pmbug2cnfs67s3y65ods27vamswdaw2lnwf45ys3pjl55h2gwqd.onion

http://xf2gry25d3tyxkiu2xlvczd3q7jl6yyhtpodevjugnxia2u665asozad.onion

http://stormwayszuh4juycoy4kwoww5gvcu2c4tdtpkup667pdwe4qenzwayd.onion
```

6. Pode ser que alguns links não estejam funcionando (todos funcionaram no momento da elaboração e revisão deste curso). Isso pode acontecer porque provavelmente estão fora do ar devido a ordens judiciais de alguns países ou ataques cibernéticos.
7. Continue explorando com responsabilidade a DeepWeb.
8. Feche todas as janelas dos navegadores Tor e Firefox ESR, assim como o Terminal. Parabéns! Agora você sabe como navegar na DeepWeb.

Atividade 2.10 – Explorando as Políticas Locais e de Conta das Configurações de Segurança no Windows Server 2022

Nesta atividade, vamos explorar a Política de Segurança como Controle Gerencial no Windows Server 2022. Exploraremos o comando Secpol e o conteúdo da Política de Segurança. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

Vamos começar inicializando o Windows Server 2022 (servidor) via RDP ao IP: 192.168.98.20, com usuário “administrator” e senha “RnpEsr123@” (use a senha “RnpEsr123@2” caso o SO peça para atualizar a senha). Aceite a mensagem de certificado e clique em “Yes” na mensagem “Do you want to allow your PC to be discoverable ....”.

1. Na barra de tarefas, clique em “Type here to search” e escreva:

```
secpol
```

2. Clique no botão “Local Security Policy” e veja a janela aberta.

3. Expanda “Account Policies” e clique em “Password Policy”. Veja as principais funcionalidades:

- Enforce password history (Aplicar histórico de senhas): Especifica o número de senhas anteriores que o sistema deve lembrar. Isso impede que os usuários reutilizem senhas antigas.
- Maximum password age (Idade máxima da senha): Define o período após o qual uma senha expira e o usuário é solicitado a alterá-la.
- Minimum password age (Idade mínima da senha): Determina o tempo mínimo que uma senha deve ser mantida antes de ser alterada.
- Minimum password length (Comprimento mínimo da senha): Especifica o número mínimo de caracteres que uma senha deve ter.
- Password must meet complexity requirements (A senha deve atender a requisitos de complexidade): Exige que as senhas atendam a critérios específicos de complexidade, como incluir caracteres em maiúsculas, minúsculas, números e caracteres especiais.

4. Clique em “Account Lockout Policy”. Veja as principais funcionalidades:

- Account lockout duration (Duração do bloqueio de conta): Define o tempo que uma conta permanece bloqueada após exceder o número máximo de tentativas de login permitidas.
- Account lockout threshold (Limiar de bloqueio de conta): Especifica o número de tentativas de login falhadas antes de uma conta ser bloqueada.
- Reset account lockout counter after (Redefinir contador de bloqueio de conta após): Define o tempo necessário para que o contador de tentativas de login falhadas seja redefinido.

5. Expanda “Local Policies” e clique em “Audit Policy”. Veja as principais funcionalidades:

- Audit account logon events (Auditar eventos de logon de conta): Permite auditar tentativas de logon em uma conta.
- Audit account management (Auditar gerenciamento de contas): Permite auditar eventos relacionados à criação, modificação e exclusão de contas de usuário e grupo.

- Audit directory service access (Auditar acesso ao serviço de diretório): Permite auditar eventos relacionados ao acesso a objetos de diretório no Active Directory.
- Audit logon events (Auditar eventos de logon): Permite auditar tentativas de logon no sistema.
- Audit object access (Auditar acesso a objetos): Permite auditar eventos relacionados ao acesso a objetos, como arquivos, pastas e chaves de registro.
- Audit policy change (Auditar alterações de política): Permite auditar eventos relacionados a alterações na política de auditoria.
- Audit privilege use (Auditar uso de privilégios): Permite auditar eventos relacionados ao uso de privilégios elevados.
- Audit process tracking (Auditar rastreamento de processos): Permite auditar eventos relacionados à criação e término de processos.
- Audit system events (Auditar eventos do sistema): Permite auditar eventos do sistema, como reinicializações e desligamentos.

6. Clique em “User Rights Assignment”: Permite a configuração de direitos específicos concedidos a usuários ou grupos em relação a determinadas operações no sistema.
7. Clique em “Security Options” (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

- Accounts: Administrator account status (Contas: Status da conta do administrador): Permite ativar ou desativar a conta de administrador.
- Accounts: Guest account status (Contas: Status da conta de convidado): Permite ativar ou desativar a conta de convidado.
- Devices: Allow undock without having to log on (Dispositivos: Permitir desacoplar sem precisar fazer login): Permite ou impede que um laptop seja desacoplado sem a necessidade de login.
- Domain member: Digitally encrypt or sign secure channel data (Membro do domínio: Criptografar digitalmente ou assinar dados de canal seguro): Configura a criptografia ou assinatura digital de dados de canal seguro.
- Domain member: Disable machine account password changes (Membro do domínio: Desativar alterações de senha da conta de máquina): Impede alterações automáticas de senha da conta de máquina.

- Interactive logon: Do not display last user name (Logon interativo: Não exibir último nome de usuário): Impede a exibição do último nome de usuário na tela de logon.
- Interactive logon: Do not require CTRL+ALT+DEL (Logon interativo: Não exigir CTRL+ALT+DEL): Permite ou impede a necessidade de pressionar CTRL+ALT+DEL para fazer login.

8. Feche todas as janelas.

Parabéns! Agora você conhece os recursos presentes nas Políticas locais e de contas do Windows Server 2022.