



Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER -  
SECURITY IMPLEMENTATION

# Progresso do curso

**Módulo 6.** System Hacking

**Módulo 7.** Malware Threats






**Módulo 8.** Sniffing

**Módulo 9.** Social Engineering

**Módulo 10.** Denial-of-Service (DoS)

## Conceitos de System Hacking:

Todo criminoso comete um crime para atingir determinado objetivo. Da mesma forma, o invasor também pode ter certos objetivos por trás de realizar determinados ataques em um sistema. A tabela mostra a meta de um atacante em diferentes estágios de hackers e a técnica usada para atingir esse objetivo.

Hacking-Stage	Goal	Technique/Exploit Used
 <b>Gaining Access</b>	To collect enough information to gain access	Password eavesdropping, brute forcing
 <b>Escalating Privileges</b>	To create a privileged user account if the user level is obtained	Password cracking, known exploits
 <b>Executing Applications</b>	To create and maintain backdoor access	Trojans
 <b>Hiding Files</b>	To hide malicious files	Rootkits
 <b>Covering Tracks</b>	To hide the presence of compromise	Clearing logs

# CEHv12 (ANSI)

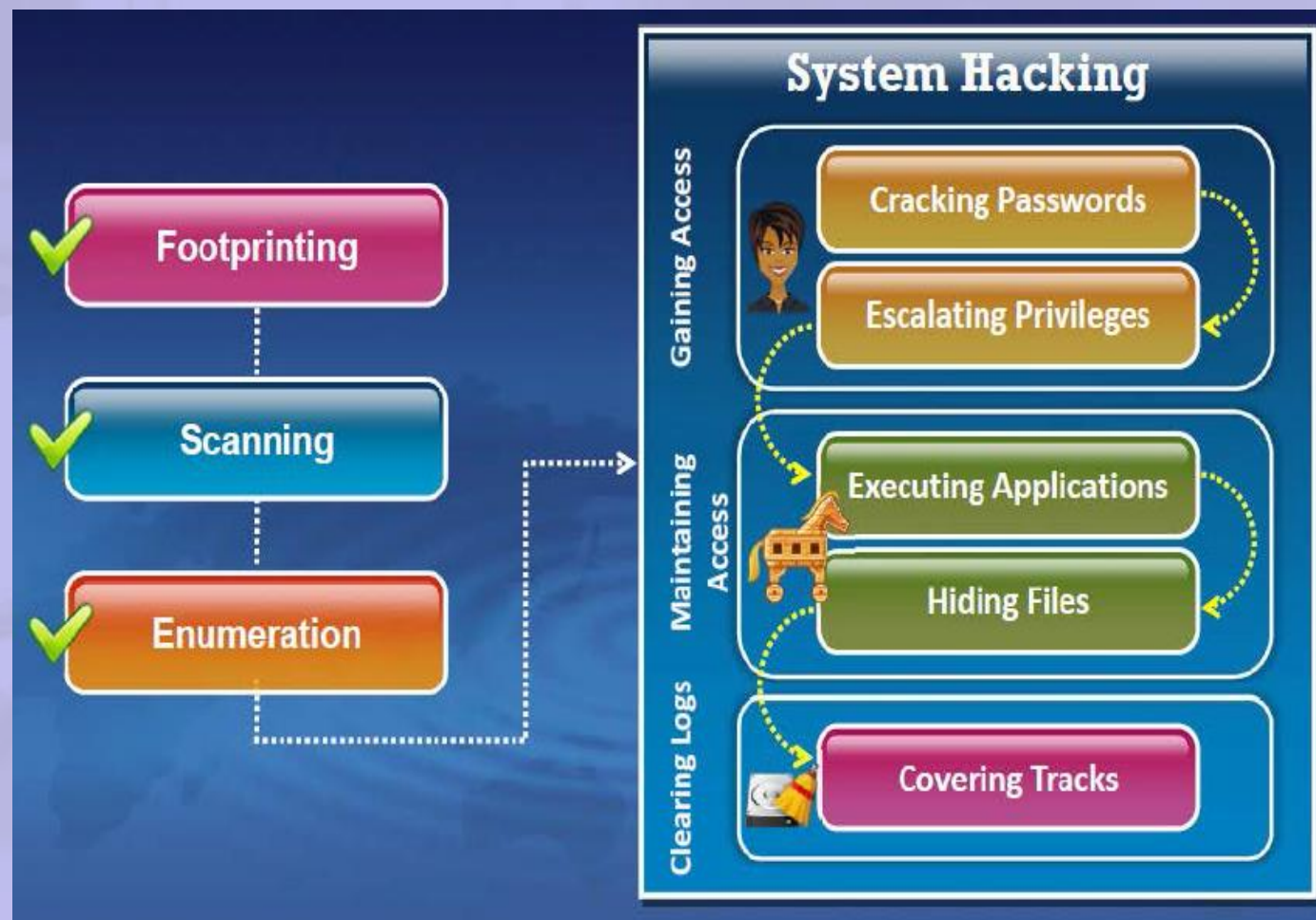
## 06.System Hacking



# Pesquisa de Vulnerabilidade

- Antes de hackear um sistema, um atacante passa pelas etapas de footprinting, scanning e técnicas de enumeração para detectar a área alvo do ataque e as vulnerabilidades. Uma vez que o atacante obtém todas as informações necessárias, ele começa a etapa de hacking.
- Semelhante ao atacante, um hacker ético também segue as mesmas etapas para testar um sistema ou rede. A fim de assegurar a eficácia do teste, o hacker ético segue a metodologia de hacking.

O diagrama a seguir descreve a metodologia de hacking seguida por hackers éticos.



# Metodologia

O System hacking não pode ser realizado em um único movimento. É realizado através de várias etapas que incluem password cracking, escalada de privilégios, execução de aplicações, esconder arquivos, cobrir rastros, e finalmente, testes de invasão.

Agora é hora de discutir estes passos, um por um cuidadosamente, para determinar como o atacante compromete o sistema. Em uma tentativa de invadir um sistema, o atacante tenta primeiro quebrar senhas.

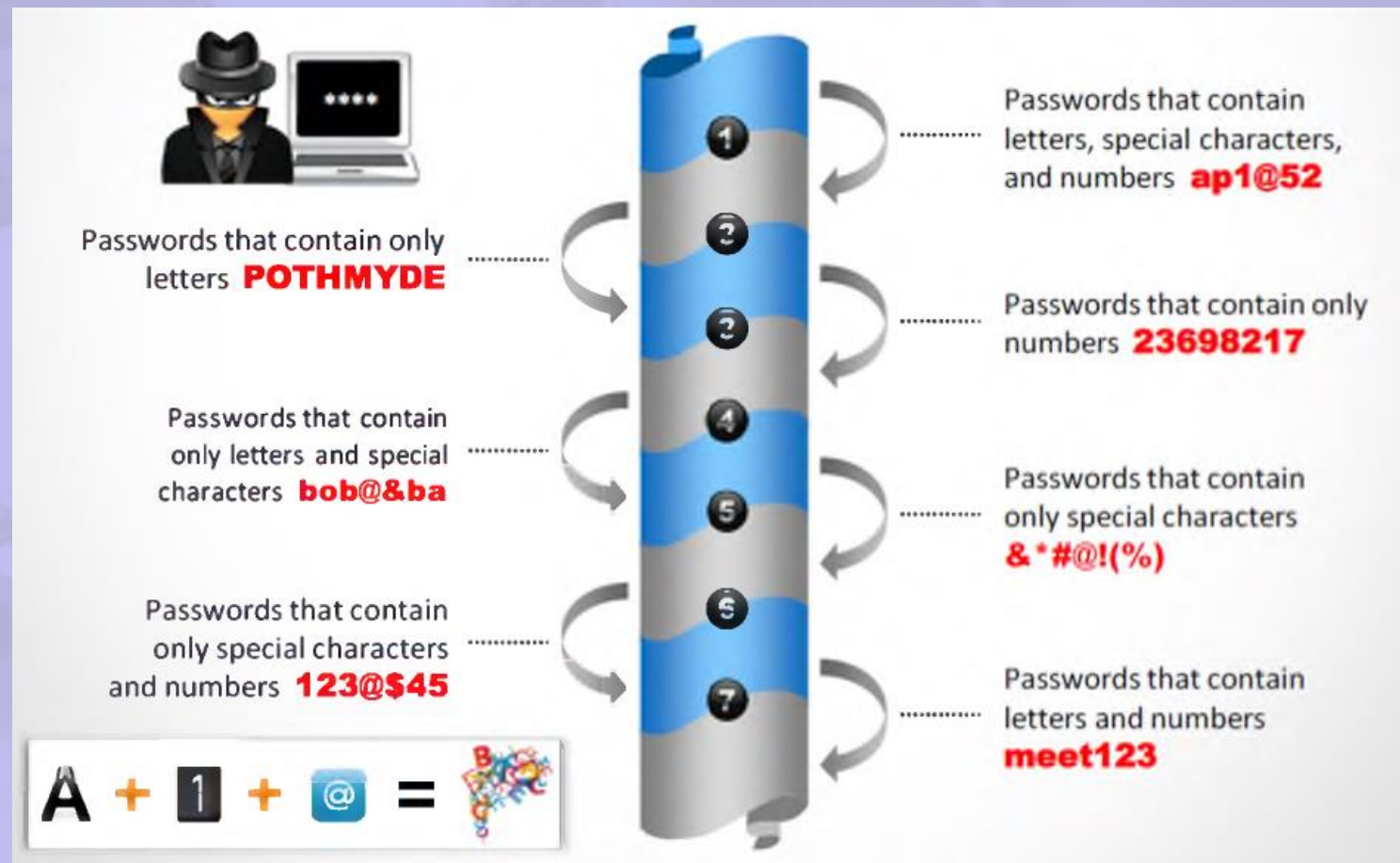
# Password Cracking

Quebra de senha é o processo de recuperação de senhas de dados que tenham sido transmitidos por um sistema de computador ou armazenados nele. O objetivo da quebra de senha pode ser a de ajudar um usuário recuperar uma senha esquecida ou perdida, como uma medida preventiva pelos administradores do sistema para verificar se há senhas facilmente dedutíveis ou também pode ser usada para obter acesso não autorizado a um sistema.

Muitas tentativas de hacking começam com tentativas de quebra de senhas. As senhas são a peça-chave da informação para acessar um sistema. Consequentemente, a maioria dos atacantes utilizam técnicas de quebra de senhas para obter acesso não autorizado ao sistema vulnerável.

# Complexidade de senha

- A complexidade de senha desempenha um papel fundamental na melhoria da segurança contra ataques. É o elemento importante que os usuários devem garantir ao criar uma senha. A senha não deve ser simples, já que senhas simples são propensas a ataques. As senhas que você escolher deve ser sempre complexa, longa e difícil de lembrar.
- A senha que você está definindo para a sua conta deve atender a definição de políticas e requisitos de complexidade. Os caracteres de senha devem ser uma combinação de caracteres alfanuméricos. Caracteres alfanuméricos consistem de letras, números, sinais de pontuação e símbolos matemáticos convencionais e outros.

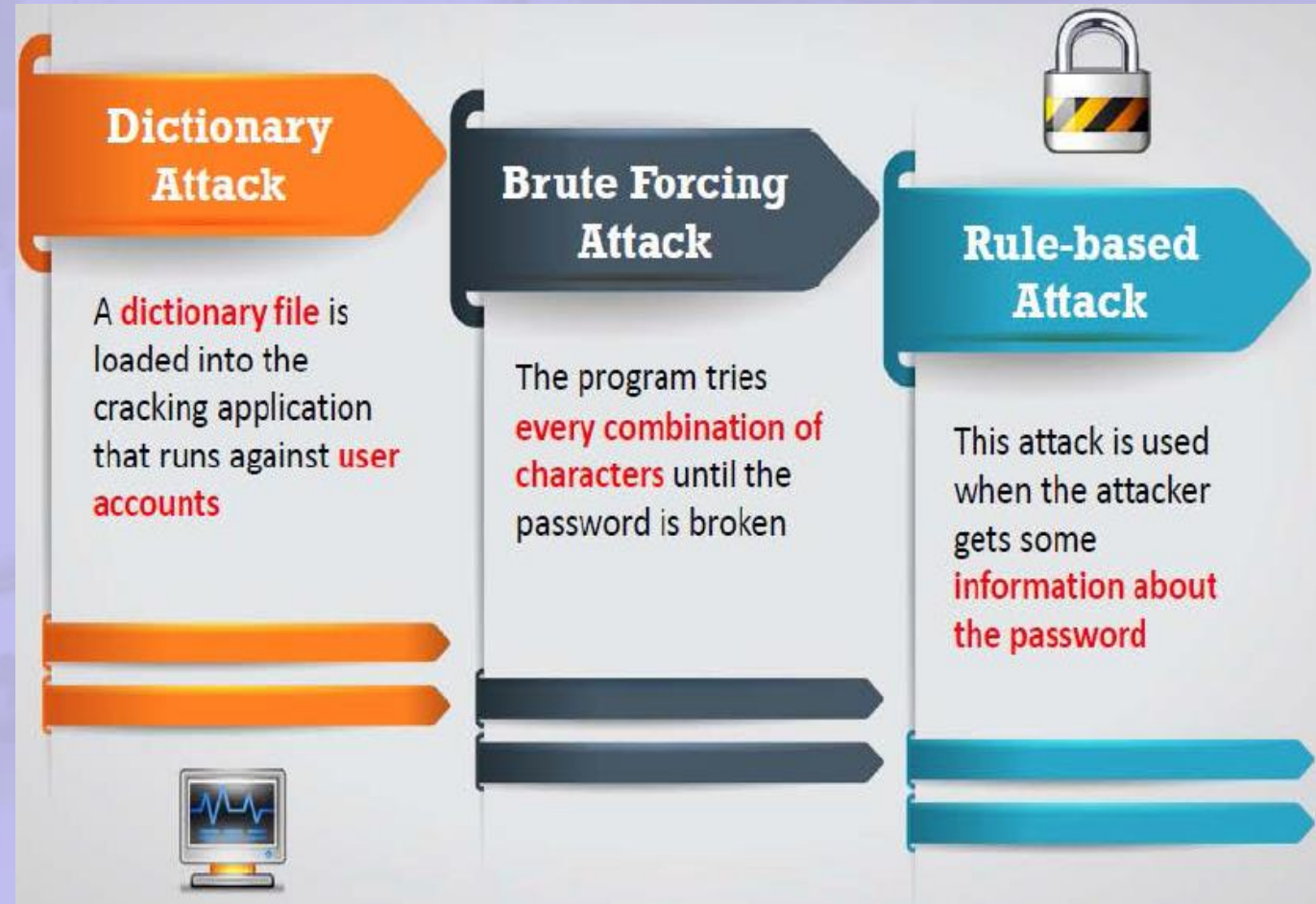




# Técnicas de cracking de senhas

---

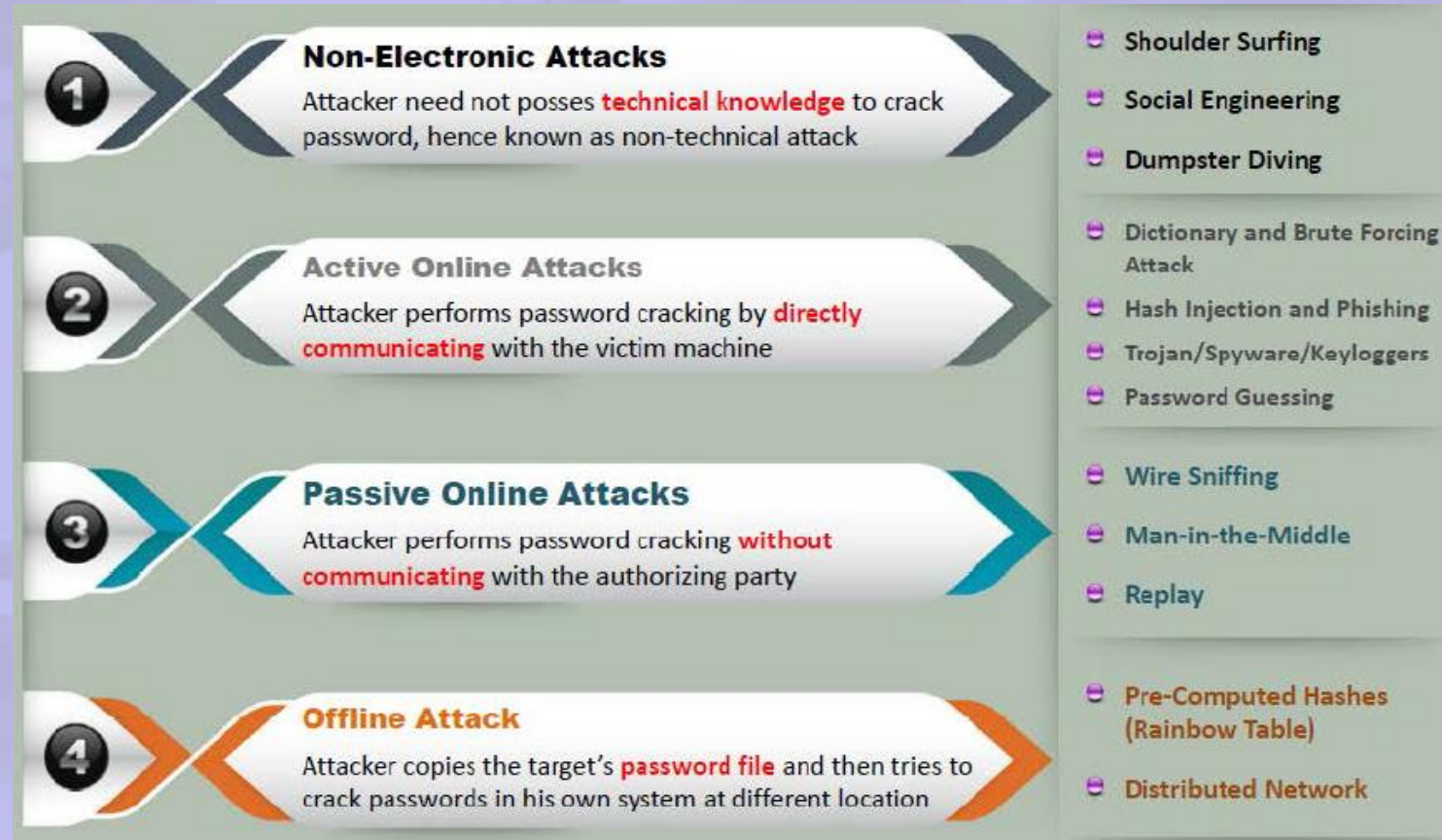
- Cracking de senhas é a técnica utilizada para descobrir senhas.
- É a maneira clássica de obter privilégios a um sistema de computador ou rede.
- A abordagem comum para rachar uma senha é tentar continuamente palpites para a senha com várias combinações até chegar a uma correta.





# Tipos de ataques

- Quebra de senha é uma das etapas cruciais de hacking do sistema.
- A quebra de senha utilizada para fins legais recupera a senha esquecida de um usuário, se for utilizada por usuários ilegítimos, pode levá-los a obter privilégios não autorizados à rede ou sistema.
- Os ataques de senha são classificados com base nas ações do atacante para quebrar uma senha. Normalmente, há quatro tipos.



# Tipos de ataques



## ATAQUES NÃO ELETRÔNICOS

Ataques não eletrônicos são conhecidos como ataques não técnicos.

Este tipo de ataque não requer qualquer conhecimento técnico sobre os métodos de comprometer outro sistema.

Existem três tipos de ataques não eletrônicos.

- Shoulder surfing
- Social engineering
- Dumpster diving

# Tipos de ataques



## Shoulder Surfing

O surfe de ombro, ou shoulder surfing em inglês, é uma técnica utilizada por pessoas mal-intencionadas para roubar informações valiosas de uma determinada pessoa ou organização.

Esta prática conhecida como visual hacking, é um ato utilizado para coletar informações por meios visuais e que não requer habilidades com computadores ou qualquer outro tipo de tecnologia.

- Escuta de conversas telefônicas.
- Ser assistido enquanto troca mensagens em redes sociais.
- Estar cercado de alguém enquanto digita no laptop.
- Ser observado enquanto utiliza o caixa eletrônico.

# Tipos de ataques



## Social Engineering

“A Engenharia Social usa a influência, a persuasão e a manipulação para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade não é. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.” – Referência: Livro A Arte de Enganar – Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação do Kevin D. Mitnick

As formas mais comuns, de um Engenheiro Social agir, são:

- Se passam por um fornecedor (empresa parceira)
- Fingem ser um empregado novo que solicita ajuda
- Fingem ser alguém com autoridade
- Fingem ser um fabricante de sistemas que ligam para oferecer um patch ou uma atualização de sistema
- Envia um vírus anexo por Correio Eletrônico (e-mail)
- Deixam um CD/Pendrive com software malicioso em algum lugar no local de trabalho
- Usam um jargão e terminologia interna para ganhar a confiança
- Surfam sobre os ombros (shoulder surfing), para obter informações
- Mergulham no lixo (dumpster diving) para obter informações que não foram devidamente destruídas corretamente



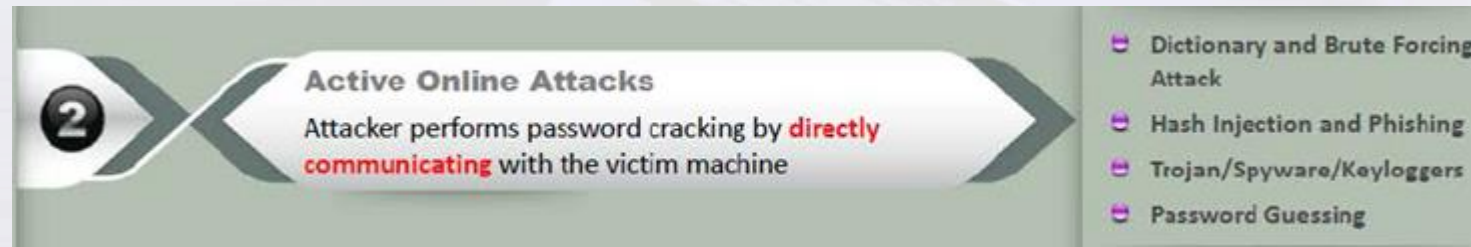
# Tipos de ataques



## Dumpster Diving

Dumpster Diving ou trashing é o termo utilizado para a ação de hackers que vasculham o lixo de empresas ou residencial do alvo para descobrir informações e invadir mais facilmente os sistemas em busca de nomes de contas, senhas, informações pessoais e confidenciais. Algumas informações importantes podem ser para o planejamento de ataques, como lista telefônica corporativa, organograma, memorandos internos, manuais de política, calendários de reuniões, inventários de hardware, entre outros. Também há as pessoas que vasculham o lixo atrás de objetos que os interessam, como jogos e aparelhos eletrônicos.

# Tipos de ataques



## ATAQUES ONLINE ATIVOS

Um ataque online ativo é a maneira mais fácil de ganhar acesso administrativo não autorizado ao sistema, neste tipo de ataque há comunicação direta entre o atacante e o alvo. Existem quatro tipos de ataques online ativos.

- Password guessing
- Trojan/spyware/keylogger
- Hash injection e Phishing
- Dicionário e força bruta

# Tipos de ataques



## Dictionary and Brute Forcing Attack

### Ataque de Dicionário

Utiliza uma lista de senhas, palavras e frases comuns para tentar adivinhar a senha

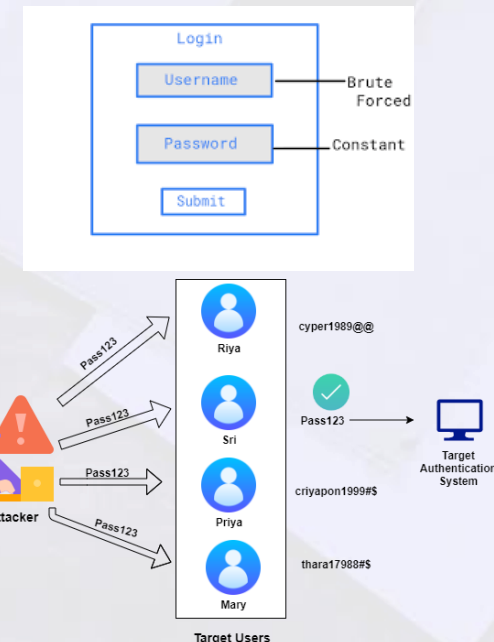
### Ataque de Força Bruta

Tenta quebrar uma senha adivinhando todas as combinações possíveis de números, letras e caracteres especiais

## Ataque de Dicionário:

```
root@JEFFLAB-DEB02:~/CrackMapExec# cme smb JEFFLAB-APP01 -u Administrator -d builtin -p ~/passwords.txt
SMB 192.168.12.240 445 JEFFLAB-APP01 [*] Windows Server 2016 Standard 14393 x64 (name:JEFFLAB-APP01)
1) (domain:builtin) (signing:False) (SMBv1:True)
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Winter2017 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:P4$$word STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Fall2017 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Spring2017 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Summer2017 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Summer2017 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Fall2015 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Spring2015 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Summer2015 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Summer2015 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Fall2014 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Spring2014 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Summer2014 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Summer2014 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Fall2016 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Spring2016 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Summer2016 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Summer2016 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:P@$$word!@# STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:password!@# STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:P@$$w0rd STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:P4$$w0rd STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:P@$$word!@# STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Password123 STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:Password!!! STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator:P@$$word!@# STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [-] builtin\Administrator: STATUS_LOGON_FAILURE
SMB 192.168.12.240 445 JEFFLAB-APP01 [+] builtin\Administrator:P@$$word (Pwn3d!)
```

## password spraying:



# Tipos de ataques



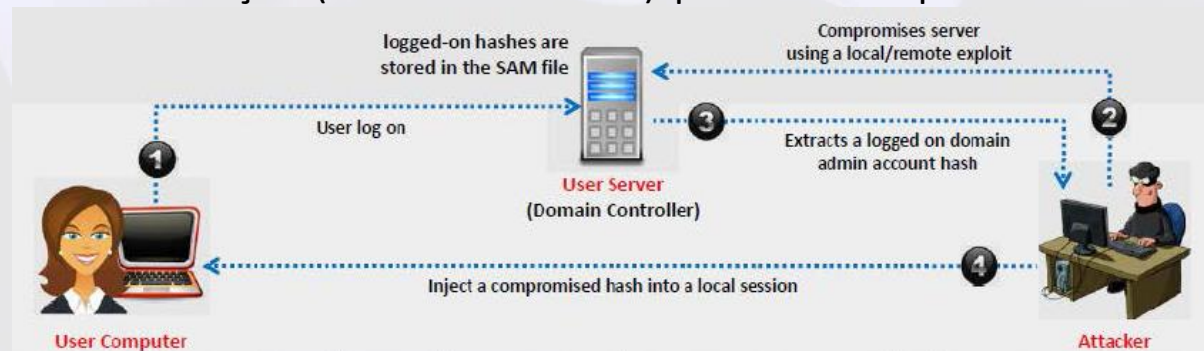
## Hash Injection and Phishing

### Hash Injection

Este é o conceito de injetar um hash comprometido em uma sessão local e, em seguida, utilizar este hash para autenticar os recursos da rede. Este método elimina a necessidade de quebra de senha em um ambiente Windows.

### Phishing

Interceptar tentativas de autenticação (hashes Net-NTLM) por meio de protocolos Multicast/Broadcast para capturar hashes de autenticação.



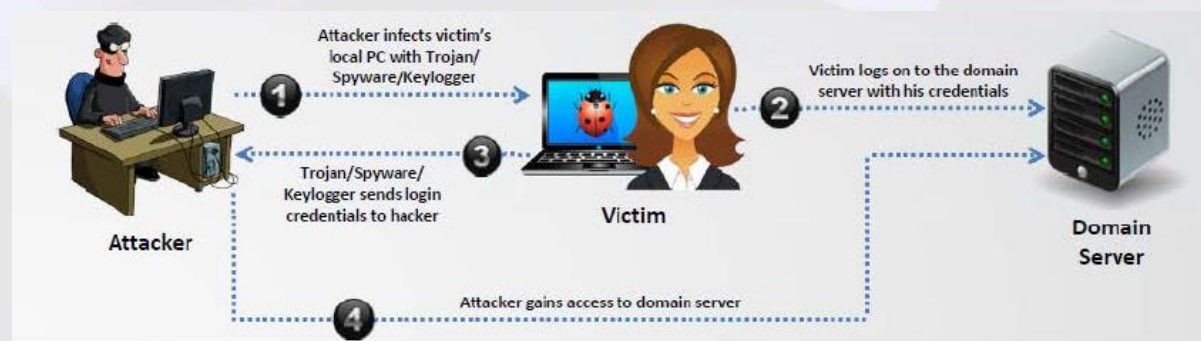


# Tipos de ataques

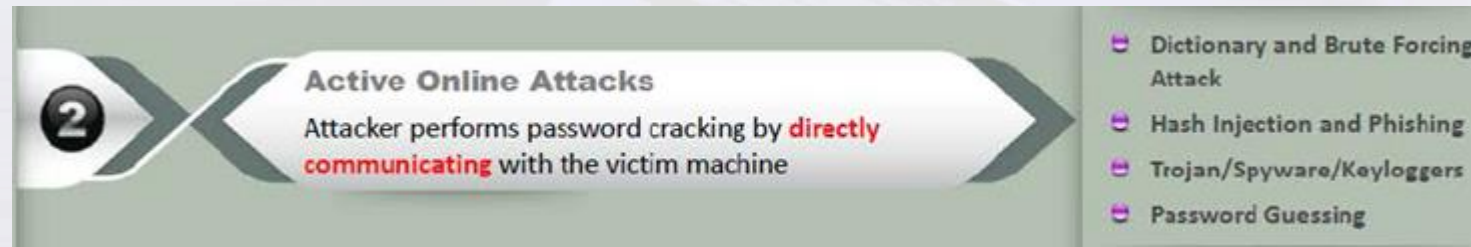


## Trojan / Spyware / Keylogger

Um cavalo de Tróia é um programa destrutivo que se passa como uma aplicação benigna. Antes da instalação ou execução, o software inicialmente parece desempenhar uma função desejável, mas na prática rouba informações ou danifica o sistema. Com um Trojan, os atacantes podem ter acesso remoto ao computador de destino. Os atacantes podem ter acesso ao computador remotamente e executar várias operações que são limitadas por privilégios do usuário no computador de destino.



# Tipos de ataques



## Password Guessing

Os adversários sem conhecimento prévio de credenciais legítimas dentro do sistema ou ambiente podem adivinhar senhas para tentar acessar as contas. Sem o conhecimento da senha de uma conta, um adversário pode optar por adivinhar sistematicamente a senha utilizando um mecanismo repetitivo ou iterativo. Um adversário pode adivinhar as credenciais de login sem conhecimento prévio das senhas do sistema ou do ambiente durante uma operação utilizando uma lista de senhas comuns. A adivinhação de senha pode ou não levar em conta as políticas do alvo sobre a complexidade da senha ou usar políticas que podem bloquear contas após várias tentativas malsucedidas.

Adivinhar senhas pode ser uma opção arriscada porque pode causar inúmeras falhas de autenticação e bloqueios de contas, dependendo das políticas de falha de login da organização.

- ❏ A default password is a password supplied by the **manufacturer** with new equipment (e.g. switches, hubs, routers) that is password protected
- ❏ Attackers use default passwords in the list of words or dictionary that they use to perform **password guessing attack**




**Online tools** to search default passwords:

- 
- <http://cirt.net>  
<http://default-password.info>  
<http://www.defaultpassword.us>  
<http://www.passwordsdatabase.com>  
<https://w3dt.net>  
<http://www.virus.org>  
<http://open-sez.me>  
<http://securityoverride.org>  
<http://www.routerpasswords.com>  
<http://www.fortypoundhead.com>

HOME
BB-WS
FORUMS
SEARCH
Articles
Code Bank
Downloads
Hacking Challenges
IRC
Contact Us

Navigation

Don't go RAW  
Always Use Protection



privateinternetaccess™  
for web browsing, email, file access, etc.

Monday 1 July 2013 - 01:19 PM

Log In

Username

Password

Log In

Not a member yet?  
Click here to register.

Forgot your password?  
Request a new one here.

DONATE

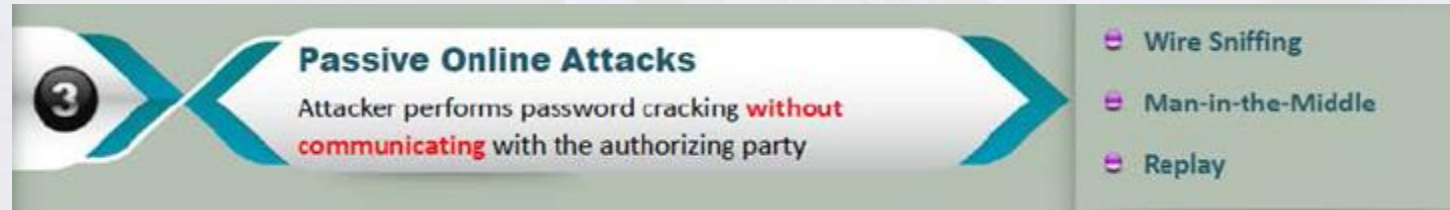
The Default Password List

This table displays a list of all default passwords.

Manufacturer	Model	Version	Username	Password
3COM		1.25	root	telnet
3COM	3C640		admin	(none)
3COM	3C640		admin	(none)
3COM	3C640		admin	(none)
3COM	3COM SuperStack 3		security	security
3COM	3COM etherHub200		tech	tech
3COM	3COM MLT 7	1.2	(none)	12345678
3COM	3COM MLT J2	2.06 (Sep 21 2005)	admin	12345678
3COM		R 2	administrator	admin
3COM		1.0	admin	admin
3COM	AirConnect Access Point	n/a	n/a	connectcom
3COM	Cell Management System	Mac2000 & NS	DDCS_APP	3com
3COM	CDMA-1X (RTEC)			
3COM	CPH90 / 4007	3	Type User: FORCE	(none)
3COM	CdTelnet		admin	admin
3COM	CdTelnet		admin	admin
3COM	CdTelnet		admin	admin
3COM	CdTelnet		admin	admin
3COM	CdTelnet	7990	admin	ynet
3COM	CdTelnet	7990	tech	(none)
3COM	CdTelnet	7990	root	(none)
3COM	CdTelnet	7990	tech	(none)

<http://securityoverride.org>

# Tipos de ataques



## ATAQUES ONLINE PASSIVOS

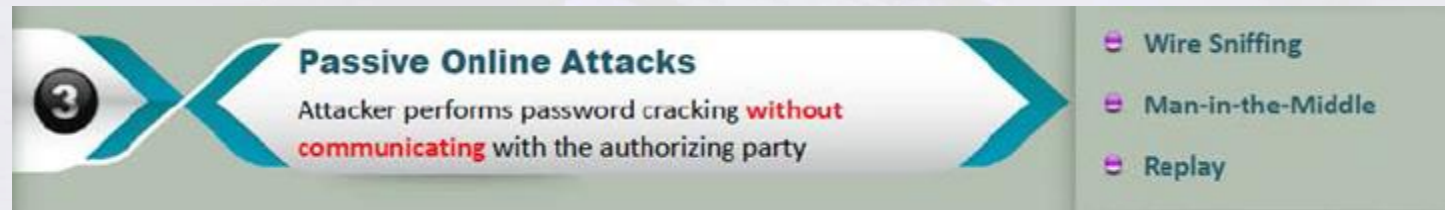
Um ataque passivo é um ataque a um sistema que não resulta em uma mudança para o sistema em si. O ataque é simplesmente monitorar o sistema ou gravar dados. Um ataque passivo em um sistema criptográfico é aquele em que o criptoanalista não pode interagir com qualquer das partes envolvidas, a tentativa de quebrar o sistema unicamente com base em dados observados.

Existem três tipos de ataques online passivos:

- Wire Sniffing
- Man-in-the-middle
- Replay



# Tipos de ataques



## Wire Sniffing

Uma ferramenta de packet sniffer é raramente utilizada para um ataque. Isto porque um sniffer pode trabalhar apenas em um domínio de colisão comum.

Domínios de colisão comuns não estão conectados por um switch. Como sniffers recolhem pacotes na camada de enlace de dados, eles podem pegar todos os pacotes na LAN da máquina que está executando o programa sniffer. Este método é relativamente difícil para perpetrar e é computacionalmente complicado.

Quaisquer dado enviado através da LAN é realmente enviado para cada máquina conectada à rede local. Se um invasor executar um sniffer em um sistema na LAN, ele pode reunir dados enviados para qualquer outro computador na rede local. A maioria das ferramentas de sniffer é idealmente adequada para farejar dados num ambiente utilizando hubs.





# Tipos de ataques



## Man-in-the-Middle e Replay

Quando duas partes estão se comunicando, o ataque man-in-middle pode ser executado. Neste caso, um terceiro intercepta a comunicação entre as duas partes, assegurando as duas partes que eles estão se comunicando uns com os outros. Para realizar este ataque, o man-in-middle executa o sniffing de ambos os lados da comunicação simultaneamente. Não é fácil de implementar tais ataques devido aos números de sequência TCP.

Em um ataque de repetição, os pacotes são capturados utilizando um sniffer. Após a informação relevante ser extraída, os pacotes são colocados de volta na rede. Este tipo de ataque pode ser utilizado para reproduzir transações bancárias ou outros tipos similares de transferência de dados na esperança de replicar ou alterar atividades, tais como depósitos ou transferências.



# Tipos de ataques



## ATAQUES OFFILE

Ataques offline ocorrem quando o intruso verifica a validade das palavras chaves. Ele observa como a senha é armazenada no sistema alvo. Se os nomes de utilizador e as senhas são armazenados em um arquivo que pode ser lido, torna-se fácil para o invasor para obter acesso ao sistema. A fim de proteger a sua lista de senhas que deve sempre ser mantida de forma ilegível, o que significa que têm de ser criptografada.

Ataques off-line são muitas vezes demorados.

Existem três tipos de ataques off-line:

- Pre-computed hashes
- Distributed network
- Rainbow

# Tipos de ataques



## Pre-Computed Hashes (Rainbow Table)

### Rainbow Table

Uma tabela de valores de hash pré-computada que contém senhas conhecidas utilizadas para quebra de senha offline

Ataques offline ocorrem quando o intruso verifica a veracidade das palavras-chave. Ele observa como a senha é armazenada. Se os nomes de utilizador e as senhas são armazenados em um arquivo que pode ser lido, torna-se fácil para o atacante ter acesso ao sistema

Precomputed Hashes	
1qazwed	4259cc34599c530b28a6a8f225d668590
hh021da	c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf	3cd696a8571a843cda453a229d741843
sodifo8sf	c744b1716cbf8d4dd0ff4ce31a177151



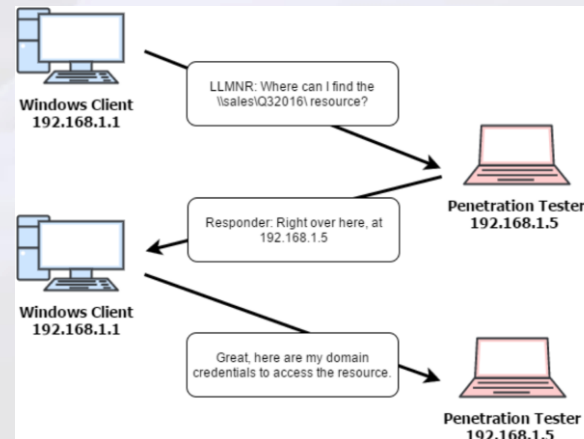
# Tipos de ataques



## Distributed Network

Quando nos conectamos a unidades compartilhadas para acessar o arquivo necessário, primeiro é verificado se há permissão para ler o arquivo.

Pela rede, a unidade compartilhada enviará a você um desafio e você calculará um novo valor utilizando sua senha com hash e o desafio e o transmitirá de volta ao servidor para autorização. Um invasor poderá realizar o ataque de quebra de senha offline se conseguir farejar a rede e obter o desafio e a resposta.

[illegible]




# Autenticação

## Autenticação Microsoft


O banco de dados SAM é o banco de dados Security Accounts Manager. Ele é usado pelo Windows para gerenciar contas de usuário e as senhas no formato hash (one-way hash). As senhas nunca são armazenadas em formato de texto simples. Elas são armazenadas no formato hash para protegê-las de ataques.

O banco de dados SAM é implementado como um arquivo de registro e o kernel do Windows obtêm e mantêm um filesystem exclusivo para bloquear o arquivo SAM. Como este arquivo é fornecido com um bloqueio de sistema de arquivos, este fornece alguma medida de segurança para o armazenamento das senhas.




### Security Accounts Manager (SAM) Database

Windows stores user passwords in SAM, or in the **Active Directory database** in domains. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM



### NTLM Authentication

- The NTLM authentication protocol types:
  - NTLM authentication protocol**
  - LM authentication protocol**
- These protocols stores user's password in the SAM database using different hashing methods



### Kerberos Authentication

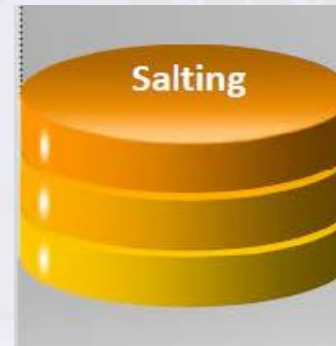
Microsoft has upgraded its **default authentication protocol** to Kerberos which provides a stronger authentication for client/server applications than NTLM

# Autenticação

## Password Salting

A salting é uma forma de tornar as senhas mais seguras através da adição de sequências aleatórias de caracteres para as senhas antes que o hash MD5 seja calculado. Isso faz com que cracking de senhas se torne mais difícil. Quanto mais longa a cadeia aleatória, mais difícil se torna para quebrar a senha.

A sequência aleatória de caracteres deve ser uma combinação de caracteres alfanuméricos. O nível de segurança ou a força de proteção de suas senhas contra vários ataques de senha depende do comprimento da cadeia de caracteres aleatórios.



```
Alice:root:b4ef21:3ba4303ce24a83fe0317608de02bf38d  
Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac  
Cecil:root:209be1:a483b303c23af34761de02be038fde08
```

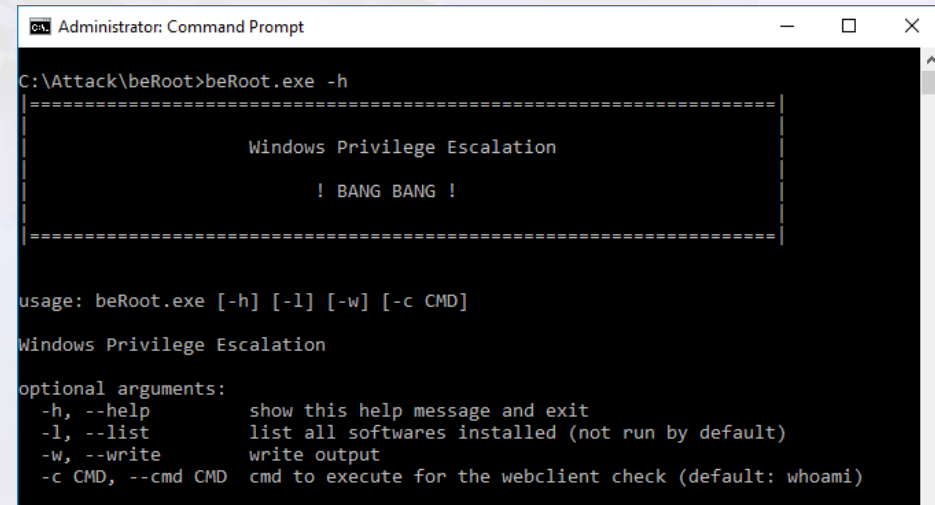
**Note:** Windows password hashes are not salted

# Autenticação

## Escalção de privilégios

Uma vez que um invasor ganha acesso a um sistema remoto com um nome de usuário e senha válido, ele vai tentar aumentar os seus privilégios escalando a conta do usuário para uma conta com maior privilégio, como a de um administrador.

Com estes privilégios o invasor pode facilmente roubar informações pessoais, apagar arquivos e pode até mesmo implantar arquivos maliciosos, ou seja, programas indesejados, como cavalos de Tróia, vírus, etc., no sistemas da vítima.



```
Administrator: Command Prompt
C:\Attack\beRoot>beRoot.exe -h
=====
                        Windows Privilege Escalation
                        ! BANG BANG !
=====

usage: beRoot.exe [-h] [-l] [-w] [-c CMD]

Windows Privilege Escalation

optional arguments:
  -h, --help            show this help message and exit
  -l, --list            list all softwares installed (not run by default)
  -w, --write           write output
  -c CMD, --cmd CMD    cmd to execute for the webclient check (default: whoami)
```

```
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL

#Permissoes do Zeze
zeze   ALL=(root) NOPASSWD: /usr/bin/find

# See sudoers(5) for more information on "#include" directives:

#include /etc/sudoers.d
root@Ubuntu:~# █
```

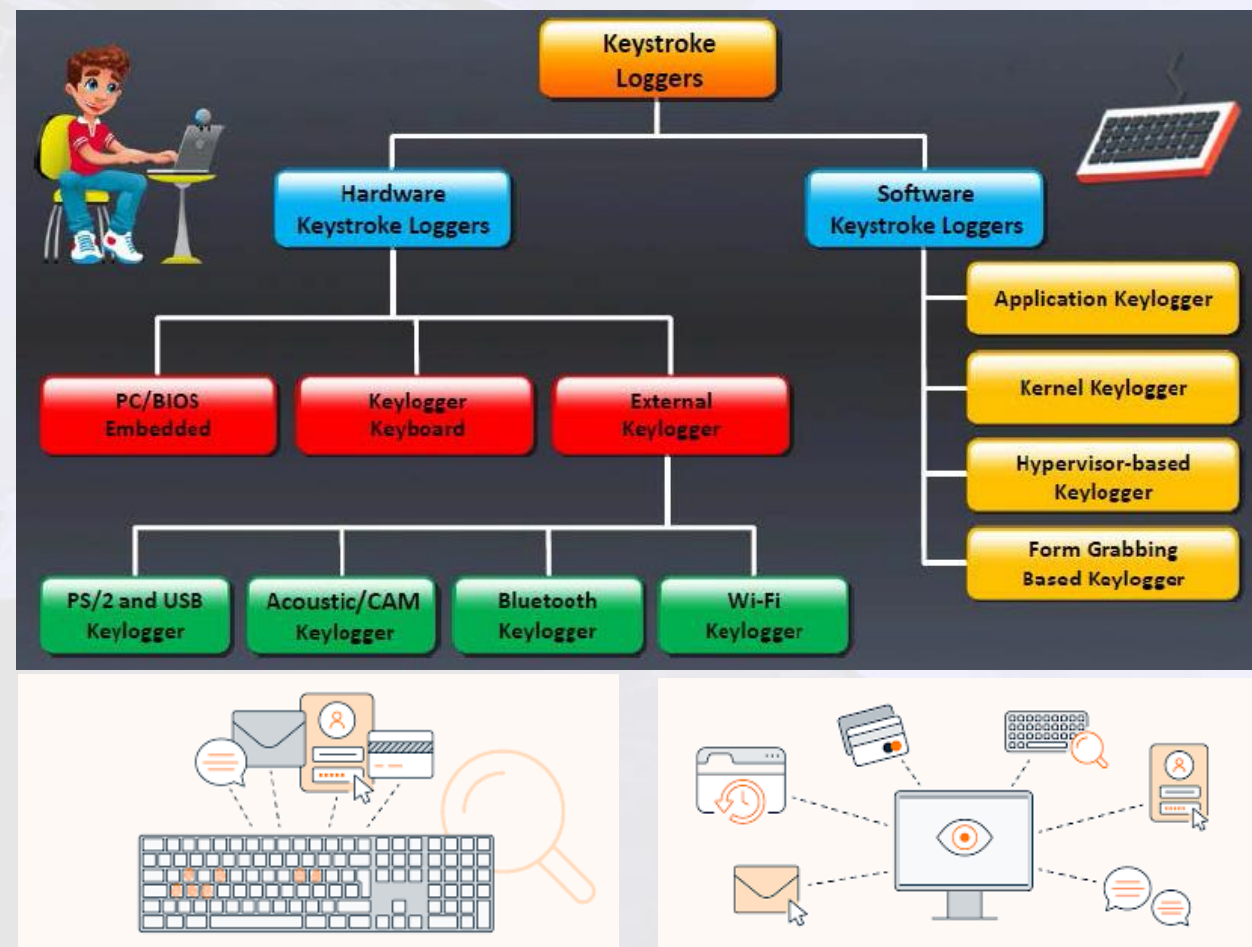


# Keylogger, Spyware e Rootkits

## Keylogger

Keyloggers, também chamados de keystroke logging, são programas de software ou dispositivos de hardware que registram as teclas pressionadas no teclado do computador de um usuário. Você pode ver todas as teclas que são digitadas em qualquer momento, em seu sistema, instalando este dispositivo de hardware ou programa.

Ele registra quase todas as teclas que são digitadas por um usuário e salva a informação gravada em um arquivo de texto. As pessoas não sabem que suas atividades estão sendo monitoradas. É utilizado principalmente para fins positivos, como em escritórios e ambientes industriais para monitorar as atividades do computador dos empregados e em ambientes domésticos onde os pais querem monitorar o que seus filhos estão fazendo na internet.



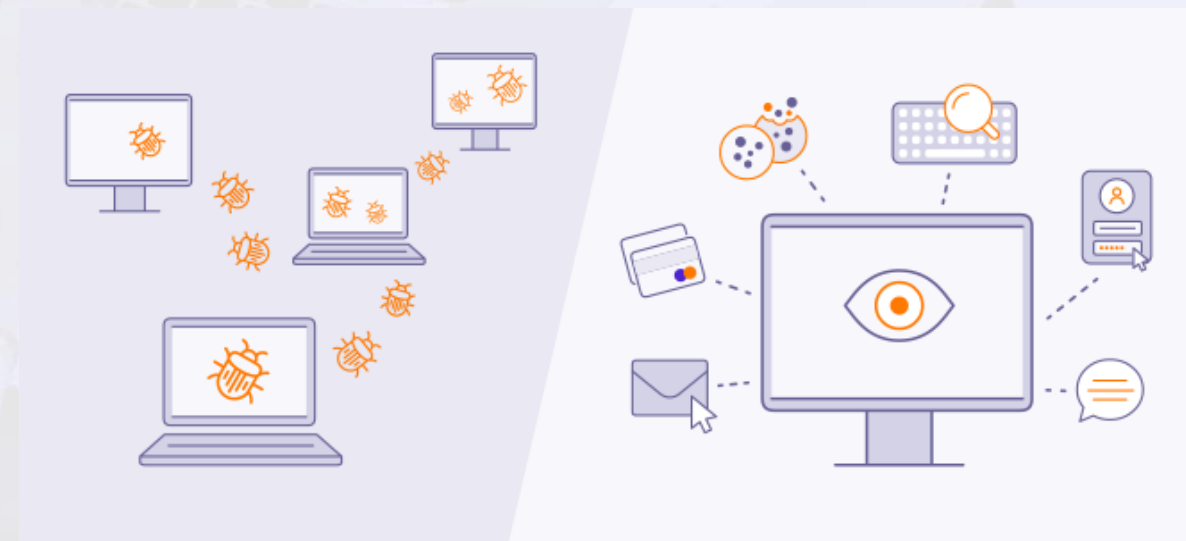


# Keylogger, Spyware e Rootkits

## Spyware

Spyware é um software de monitorização de computador, que permite gravar secretamente todas as atividades do computador de um usuário. Ele fornece automaticamente registros para você via e-mail ou FTP, incluindo todas as áreas do sistema, tais como e-mail enviado, sites visitados, todas as teclas (incluindo login/senha de ICQ, MSN, AOL, AIM e Yahoo Messenger ou Webmail), operações de arquivo e conversas de bate-papo on-line.

Ele também leva screenshots em intervalos definidos, assim como uma câmera de vigilância diretamente apontada para o monitor do computador. O Spyware é geralmente adicionado como um elemento oculto nos programas freeware ou shareware que podem ser baixadas da Internet.



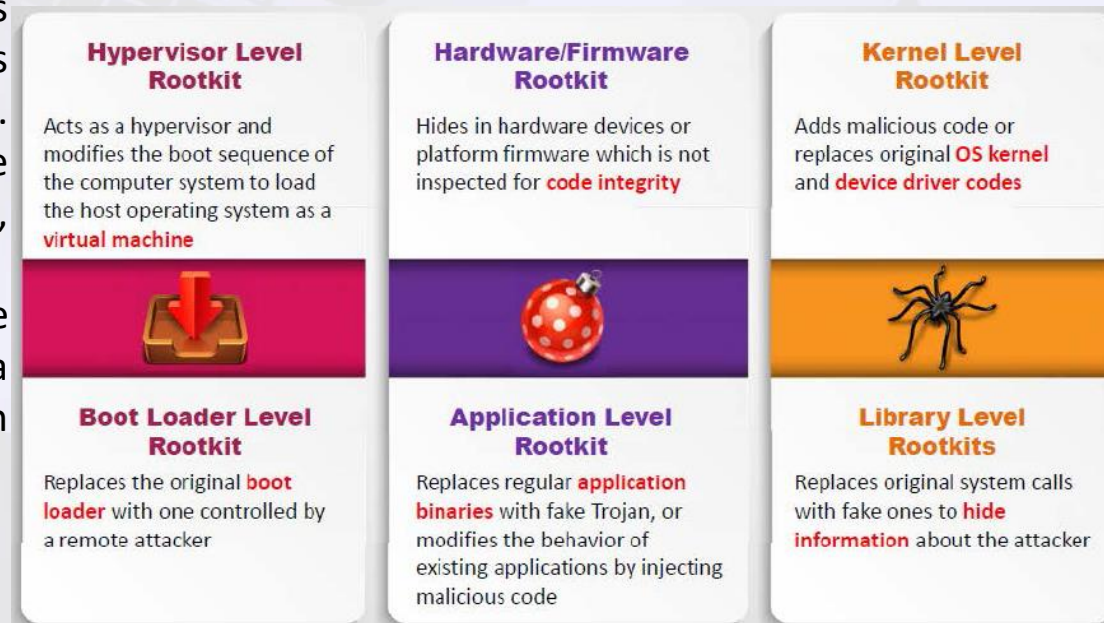
# Keylogger, Spyware e Rootkits

## Rootkits

Rootkits são programas destinados a ganhar acesso a um computador sem ser detectado. Estes são malwares que podem ser utilizados para obter acesso não autorizado a um sistema remoto e executar atividades maliciosas. O objetivo do rootkit é ganhar privilégios de root em um sistema. Ao iniciar a sessão como usuário root de um sistema, um invasor pode executar qualquer tarefa, tais como a instalação de software, excluir arquivos, etc.

Rootkits substituem certas chamadas do sistema operacional e utilitários com suas próprias versões modificadas dessas rotinas, que por sua vez minam a segurança do sistema causando funções maliciosas a serem executadas.

Um atacante implanta um rootkit das seguintes maneiras:  
Fazendo scanning em computadores vulneráveis e servidores na web.  
Envolvendo rootkit em um pacote especial como jogos por exemplo.  
Instalando rootkit em computadores públicos e computadores corporativos através de engenharia social.  
Realizando ataques Oday.



# Esteganografia

## Rootkits

Esteganografia é definida como a arte de esconder dados por trás de outros dados sem o conhecimento do inimigo.

Ele substitui bits de dados não utilizados por arquivos gráficos, de som, texto, áudio, vídeo por outros pedaços que foram obtidos sub-repticiamente. Os dados escondidos podem ser texto simples ou texto cifrado, ou podem ser uma imagem.

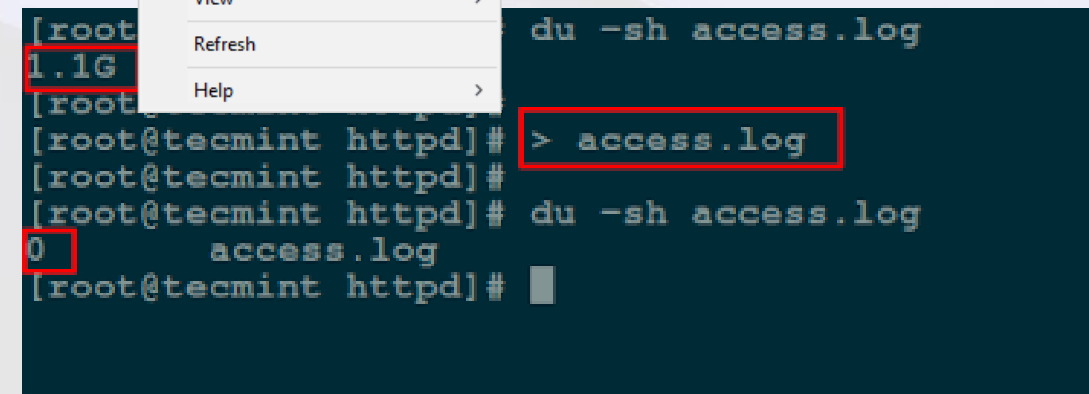
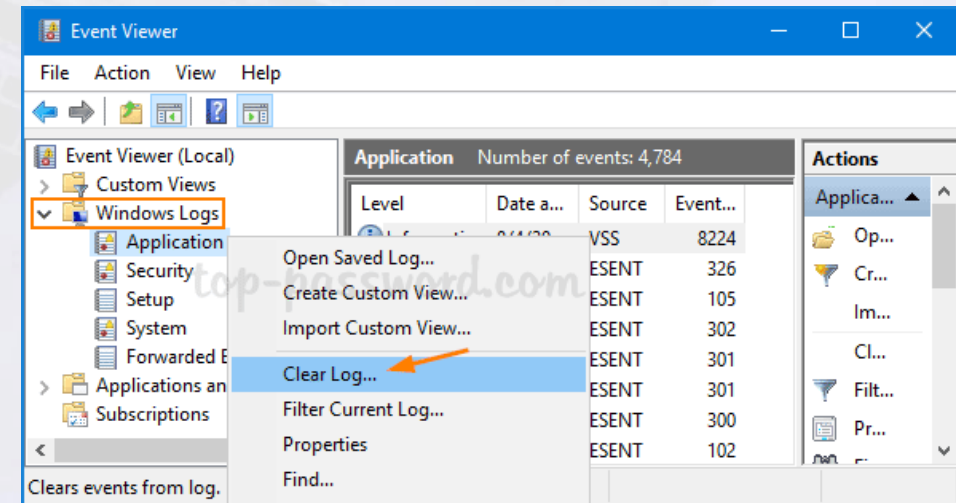


# Apagando rastros

Apagar as evidências é um requisito para qualquer invasor que gostaria de permanecer oculto. É um método para contornar o rastreo do invasor.

Apagando os logs contaminados e possíveis mensagens de erro que possam ter sido geradas pelo ataque. Ao manipular e aprimorar os logs dos eventos, o administrador do sistema pode ficar convencido que a saída do seu sistema está correta, e que nenhuma invasão ocorreu.

A primeira coisa que um administrador de sistema faz para monitorar a atividade incomum é verificar os arquivos de log do sistema, é comum que os intrusos utilizem um utilitário para modificar os registros do sistema. Em alguns casos, rootkits podem desativar e descartar todos os logs existentes. Isso ocorre se o intruso pretende usar o sistema por um longo período de tempo como base para futuros ataques.





# Pesquisa de Vulnerabilidade

- Pesquisa de vulnerabilidade é o processo de análise de protocolos, serviços e configurações para descobrir as vulnerabilidades e falhas de design que irão expor um sistema operacional e seus aplicativos à exploração, ataque ou uso indevido.

```
root@kali:~# nmap --script vuln -p139,445 192.168.0.18
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-25 20:58 CDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.18
Host is up (0.0017s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Host script results:
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|     https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|     https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_
Nmap done: 1 IP address (1 host up) scanned in 39.49 seconds
root@kali:~#
```

## Conceitos de Hacking de Sistemas:

A avaliação da vulnerabilidade desempenha um papel importante no fornecimento de segurança aos recursos e infraestrutura de qualquer organização contra várias ameaças internas e externas. Para proteger uma rede, um administrador precisa realizar o gerenciamento de patches, instalar um software antivírus adequado, verificar as configurações, resolver problemas conhecidos em aplicativos de terceiros e solucionar problemas de hardware com configurações padrão. Todas essas atividades juntas constituem uma avaliação de vulnerabilidade.



# TEORIA NA PRÁTICA

## CEHv12 (ANSI)

---

### 06.System Hacking



# Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.