
UNAERP
Universidade de Ribeirão Preto
Campus Ribeirão Preto · Campus Guarujá

# Segurança da Informação

Tópicos Especiais em Engenharia

# Maior Dúvida

- ✘ Achei interessante as ferramentas apresentadas. Queria saber qual a precisão dos dados exibidos nos relatórios. Pode ser que existam dados errados? Acontece com frequência ou, em geral, os dados apresentados são certeiros?
- ✘ Como proteger minha aplicação de SQL Injections?
- ✘ O ataque de redes wireless também são recorrentes em empresas de grande porte? como podem ser evitados? como funcionam pelo kali?
- ✘ Professor eu queria que você mostrasse um exemplo de relatório completo, de como são documentadas as possíveis vulnerabilidades de um site

# Maior Dúvida

- ✘ O que alguém poderia fazer se conseguisse hackear um satélite da NASA ?
- ✘ Existe alguma forma das ferramentas mostradas evitarem a utilização destes programas para o mal? Se alguém faz má utilização destes programas, e a vítima deseja processar, os donos do programa ou ferramenta podem ser considerados culpados também?

# Ethical Hacking

Ferramentas para Acesso
Evitando rastros
Relatórios


PenTest
Teste de Intrusão / Penetração

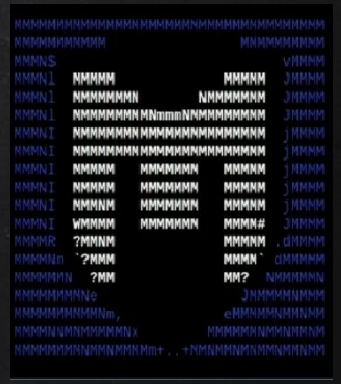
# Fases de um Pentest

- ✘ Etapa 0 : Negociação
- ✘ Etapa 1 : Levantamento de dados (FootPrinting)
- ✘ Etapa 2 : Varredura
- ✘ Etapa 3 : Ganhando Acesso
- ✘ Etapa 4 : Mantendo Acesso
- ✘ Etapa 5 : Limpando Rastros
- ✘ Etapa 6 : Escrita de Relatórios

# Hashcat

- ✘ Multi-Thread
- ✘ Multi-OS
  - GNU/Linux, Windows e OS X
- ✘ Multi-Algoritmo
  - MD4, MD5, SHA1, DCC, NTLM, MySQL
- ✘ Ambiente distribuído
- ✘ Múltiplas wordlists inclusive especificando mais de um diretório contendo wordlists
- ✘ Número de threads configurável

# Metasploit



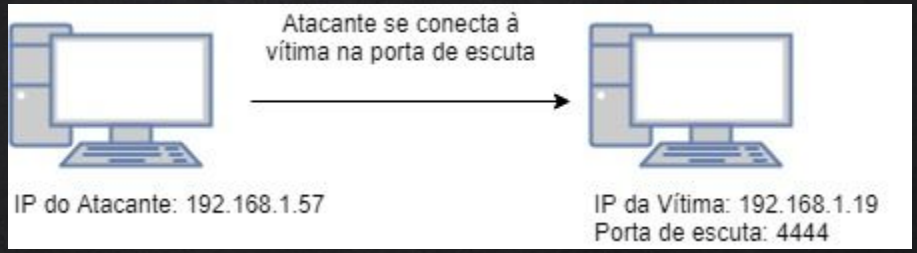
- ✘ Framework open source
- ✘ Ruby, organizado por módulos
- ✘ Módulos possuem programas (exploits) que executam códigos maliciosos (payloads)
- ✘ Necessita do postgresql: service postgresql start
- ✘ Iniciar metasploit: service metasploit start
- ✘ Abrir metasploit: msfconsole

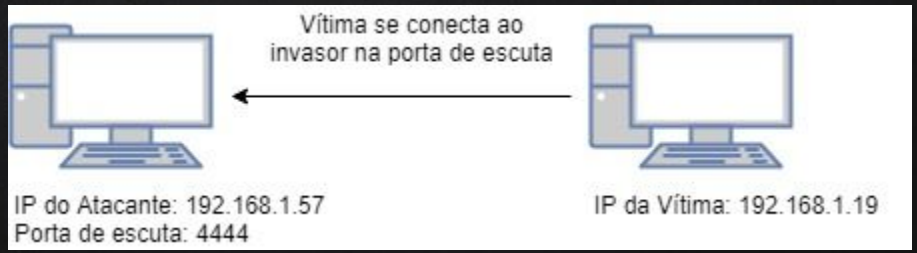
# Beef XSS

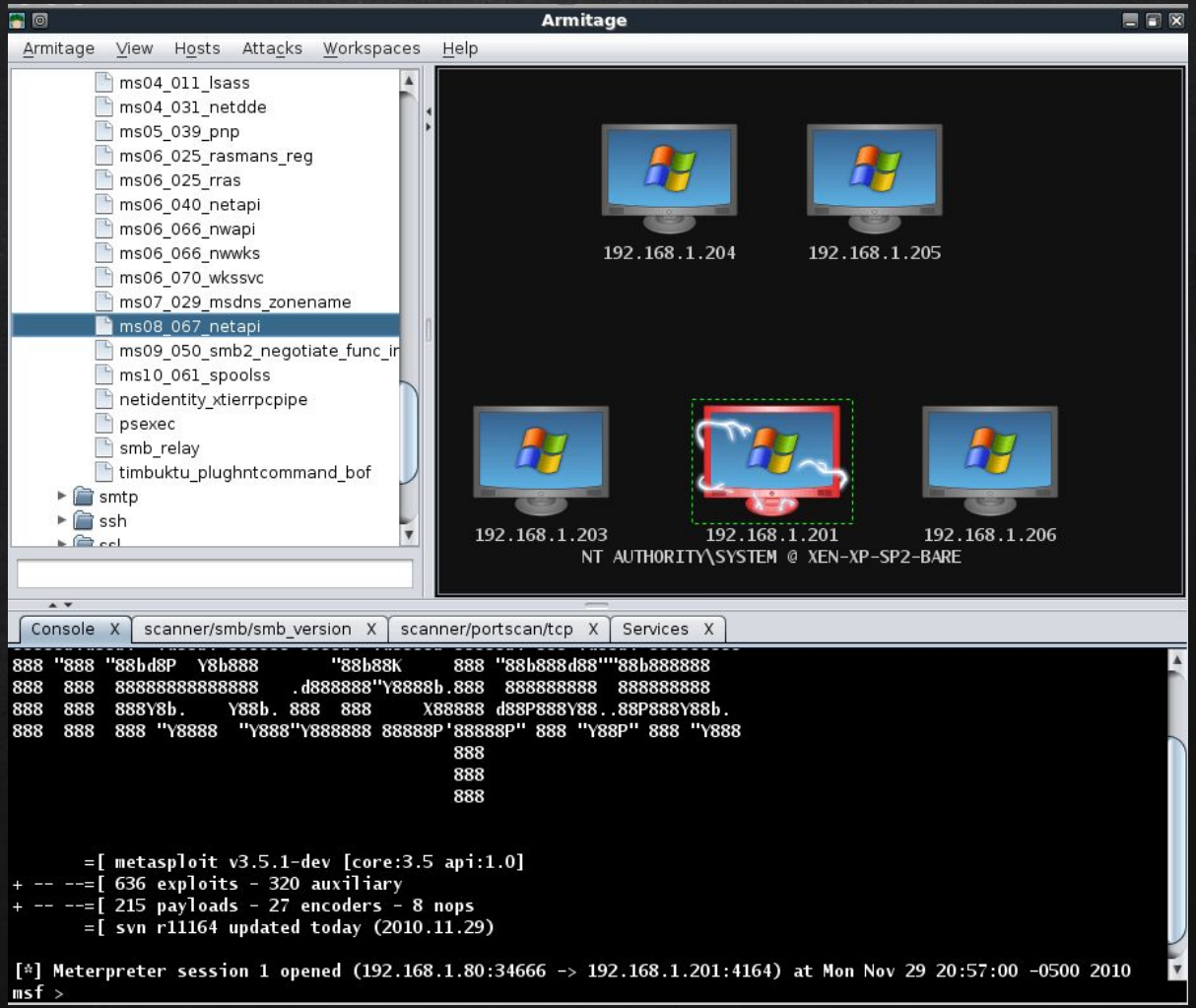

- ✘ Framework para exploits em browsers
- ✘ Ruby on Rails
- ✘ Integrado com Metasploit

# Shell Reverso

- ✘ Armitage
- ✘ http://www.fastandeasyhacking.com/



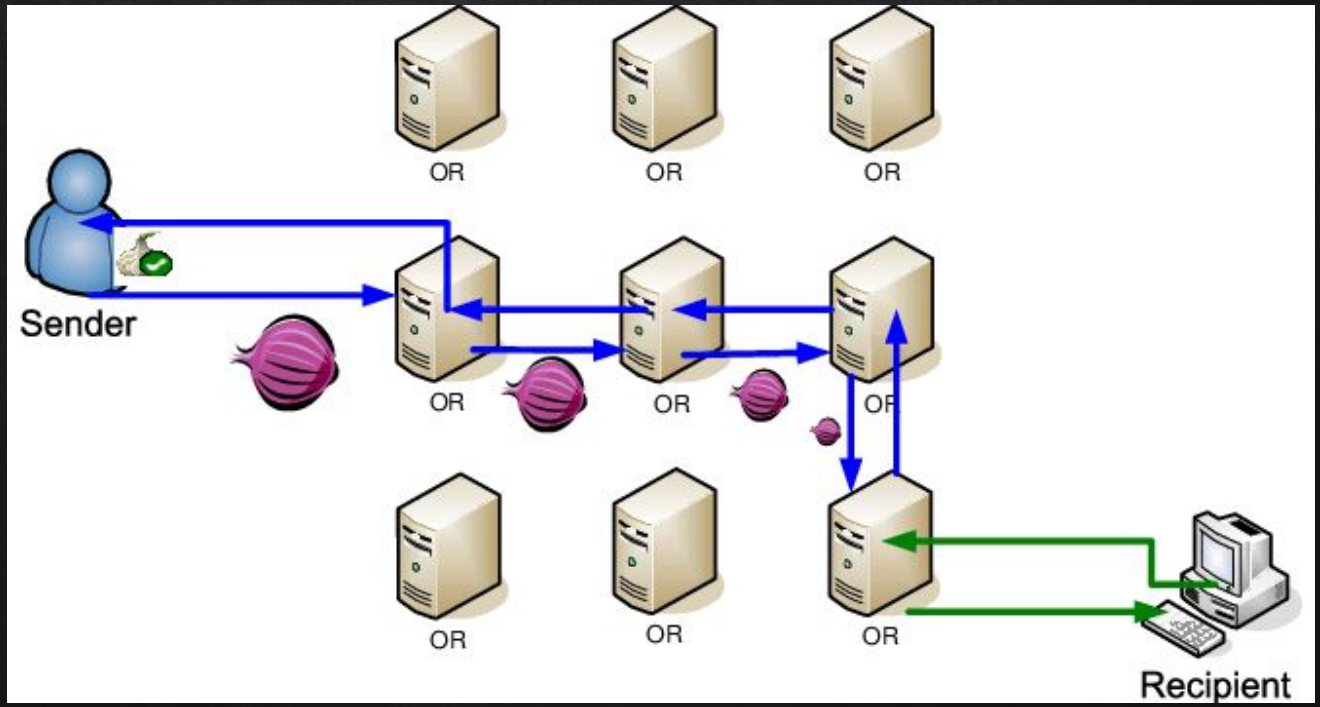




Armitage
Armitage View Hosts Attacks Workspaces Help
ms04_011_lsass
ms04_031_netdde
ms05_039_pnp
ms06_025_rasmans_reg
ms06_025_rras
ms06_040_netapi
ms06_066_nwapi
ms06_066_nwwks
ms06_070_wkssvc
ms07_029_msdns_zonename
ms08_067_netapi
ms09_050_smb2_negotiate_func_ir
ms10_061_spoolss
netidentity_xtierrpcpipe
psexec
smb_relay
timbuktu_plughntcommand_bof
smtp
ssh
192.168.1.204
192.168.1.205
192.168.1.203
192.168.1.201
192.168.1.206
NT AUTHORITY\SYSTEM @ XEN-XP-SP2-BARE
Console X
scanner/smb/smb_version X
scanner/portscan/tcp X
Services X
888 "888 "88bd8P Y8b888 "88b88K 888 "88b888d88""88b888888
888 888 88888888888888 .d888888"Y8888b.888 888888888 888888888
888 888 888Y8b. Y88b. 888 888 X88888 d88P888Y88..88P888Y88b.
888 888 888 "Y8888 "Y888"Y888888 88888P'88888P" 888 "Y88P" 888 "Y888
888
888
888
=[ metasploit v3.5.1-dev [core:3.5 api:1.0]
+ -- --=[ 636 exploits - 320 auxiliary
+ -- --=[ 215 payloads - 27 encoders - 8 nops
=[ svn r11164 updated today (2010.11.29)
[*] Meterpreter session 1 opened (192.168.1.80:34666 -> 192.168.1.201:4164) at Mon Nov 29 20:57:00 -0500 2010
msf >

# Limpando Rastros

- ✘ Tor
  - The Onion Router
  - https://metrics.torproject.org/
- ✘ Proxy Chains

# ToR



# Proxy Chains

- ✘ Pacote que possibilidade fazer o roteamento das requisições das suas aplicações através de proxys colocados em uma lista.
- ✘ Comando proxychains antes do comando
- ✘ Necessita sudo

# Relatório

- ✘ Modelo gerado pela Offensive Security
- ✘ https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

# DÚVIDAS?

- ✘ Não esqueça de enviar sua maior dúvida pelo link que está no ClassRoom.
- ✘ Críticas/Sugestões: ezarpelao@unaerp.br

# Credits

Special thanks to all the people who made and released these awesome resources for free:

- ✘ Presentation template by SlidesCarnival
- ✘ Photographs by Unsplash