



SAP and Caipirinha with Pitú

Joaquim Espinhara

You Sh0t the Sheriff 4

São Paulo



Sobre

\$./whoami

[+] Pesquisador Independente

[+] H2HC6, YSTS 4

[+] Só isso!



Agenda

- Introdução
- Motivação
- Objetivos
- Pentest SAP
 - sapyto (old)
 - bizploit (Rulez)
 - Demo (bizploit)
- Conclusão
- Thanks



Introdução

- SAP?
- SAP System ID (SID)
- Clientes (000,001,066)
- Remote Function Call (RFC)



Remote Function Call (RFC)

- O que é?
- Histórico
- Segurança
 - Sniffing -> Texto Claro -> SNC (Secure Network Communications)
 - Senha ofuscada (XOR) -> getPassword



Motivação

- Projetos longos e complexos
- Cliente
- SAP Partner
- Segurança == Atraso
- Fatos
 - FBI/CSI Computer Crime & Security Survey 2008
 - USD 463,100
 - ONAPSIS
 - 95% suscetível a fraude



Objetivo



Pentest - SAP

- SAP Security
 - User/Pass , Profiles
- Segregation of Duties (SoD)
- SAP (coração da empresa)
- Frameworks
 - sapyto (old)
 - bizploit



sapyto (old)



sapyto

- targets
- connectors
 - SAPRFC
 - SAPRFC_EXT
 - SAPGATEWAY
 - SAPROUTER



sapyto - Plugins

- discovery
 - Ping
 - findRegRFCServers
 - getApplicationServers
 - getClients
 - saprouterSpy
- Audit
 - bruteLogin
 - checkGwMon
 - checkRFCEXEC
 - checkRFCPrivs
 - ConnectExtRFC
 - getDocu
 - oraAuth
 - registerExtServer
 - sapinfo



sapyto – Plugins (Cont)

- exploit
 - callback
 - eviltwin
 - gwmon
 - oraEscalation
 - oraShell
 - rfcShell
 - rfcexec
 - stick



bizploit



onapsis
Securing Business Essentials



<http://www.onapsis.com/bizploit>



bizploit - Demo



onapsis
Securing Business Essentials

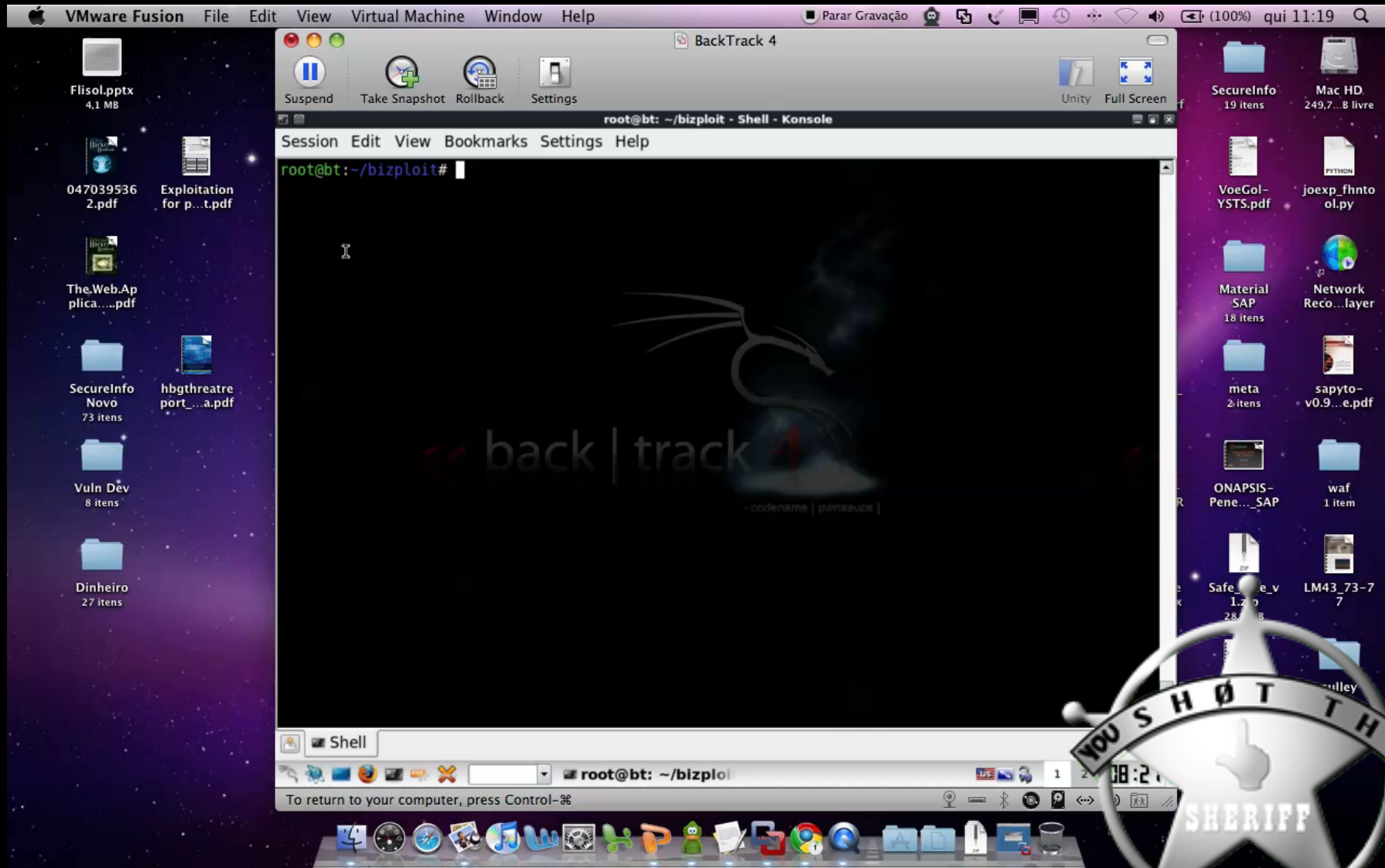


Demo

- getClients
- sapinfo
- getApplicationServers
- findRegRFCServers
- registerExtServer
- bruteLogin
- vulnassess



Demo - getClients



Demo - sapinfo

The image shows a Mac OS desktop environment with a purple and black starry background. A central window titled "BackTrack 4" is open, displaying a terminal window. The terminal prompt is "root@bt: ~/bizploit - Shell - Konsole". The terminal content shows the command "bizploit> start" being entered. The terminal background features a dragon logo and the text "back | track" and "-codename | pensauce |". The desktop contains various files and folders, including "Flisol.pptx", "047039536 2.pdf", "Exploitation for p...t.pdf", "The.Web.Ap plica....pdf", "SecureInfo Novo 73 itens", "hbgthreatre port....a.pdf", "Vuln Dev 8 itens", "Dinheiro 27 itens", "SecureInfo 19 itens", "Mac HD 249,7...8 livre", "VoeGol-YSTS.pdf", "joexp_fhnto ol.py", "Material SAP 18 itens", "Network Reco...layer", "meta 2 itens", "sapyto-v0.9...e.pdf", "ONAPISIS-Pene...SAP", "waf 1 item", "Safe...e_v 1.2... 28...8", and "LM43_73-7 7". The top of the screen shows the menu bar with "QuickTime Player" and other applications. The bottom of the screen shows the dock with various application icons. A watermark logo in the bottom right corner reads "YOU SHOT THE SHERIFF".

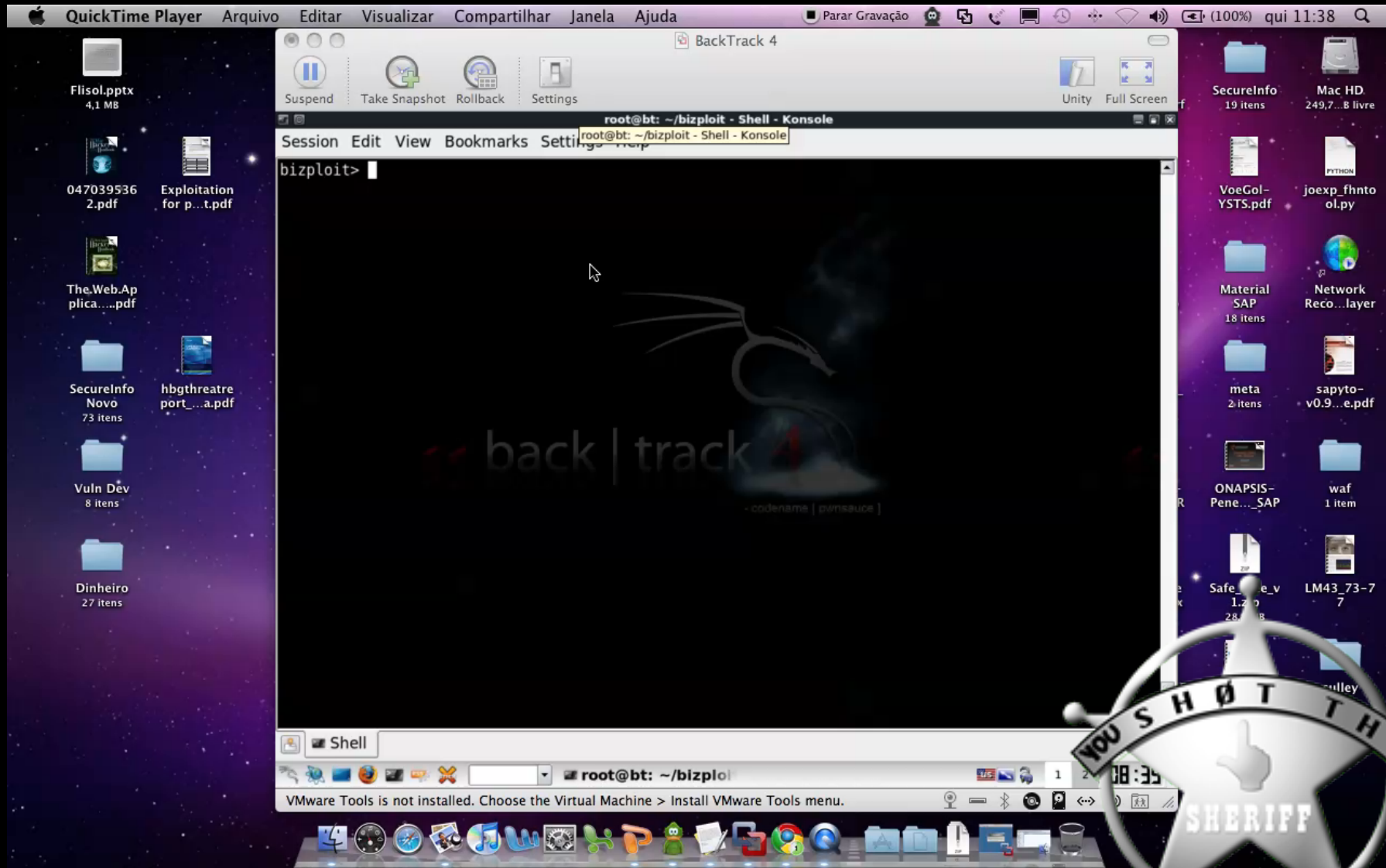
Demo – getApplicationServers

The screenshot shows a Mac desktop environment. A QuickTime Player window is open, displaying a terminal window titled "BackTrack 4". The terminal prompt is "root@bt: ~/bizploit - Shell - Konsole". The terminal content shows the following commands and output:

```
Session Edit View Bookmarks Settings Help
bizploit/plugins> back
bizploit> start
```

The terminal window also displays the BackTrack logo and the text "back | track" and "-codename | pensauce |". The desktop background is a purple space-themed wallpaper. Various folders and files are visible on the desktop, including "Flisol.pptx", "047039536 2.pdf", "Exploitation for p...t.pdf", "The.Web.Ap plica....pdf", "SecureInfo Novo 73 itens", "Vuln Dev 8 itens", "Dinheiro 27 itens", "SecureInfo 19 itens", "Mac HD 249,7...8 livre", "VoeGol-YSTS.pdf", "joexp_fhnto ol.py", "Material SAP 18 itens", "Network Reco...layer", "meta 2 itens", "sapyto-v0.9...e.pdf", "ONAPSI-Pene...SAP", "waf 1 item", "Safe...e_v 1.2... 28...8", and "LM43_73-7". The system menu bar at the top shows the time as "qui 11:34". The dock at the bottom contains various application icons. A watermark logo is visible in the bottom right corner, featuring a star with the text "YOU SHOT THE SHERIFF".

Demo – findRegRFCServers



Demo - registerExtServer

QuickTime Player Arquivo Editar Visualizar Compartilhar Janela Ajuda Parar Gravação (100%) qui 12:00

BackTrack 4

root@bt: ~/bizexploit - Shell - Konsole

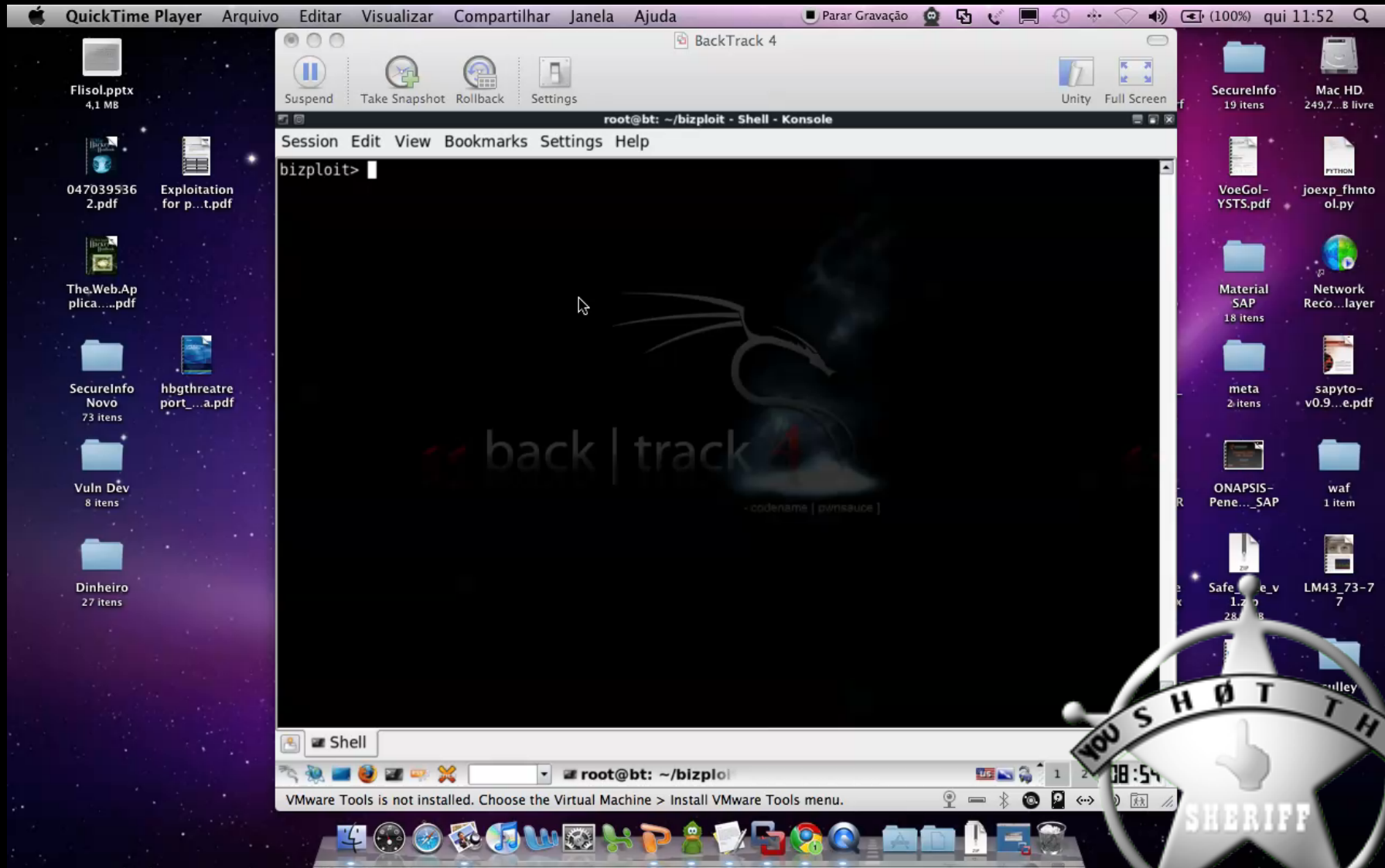
```
Session Edit View Bookmarks Settings Help
bizexploit/plugins> vulnassess
```

back | track

VMware Tools is not installed. Choose the Virtual Machine > Install VMware Tools menu.

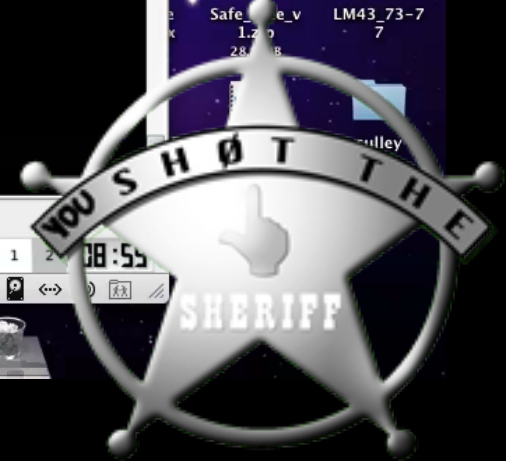
YOU SHOT THE SHERIFF

Demo - bruteLogin

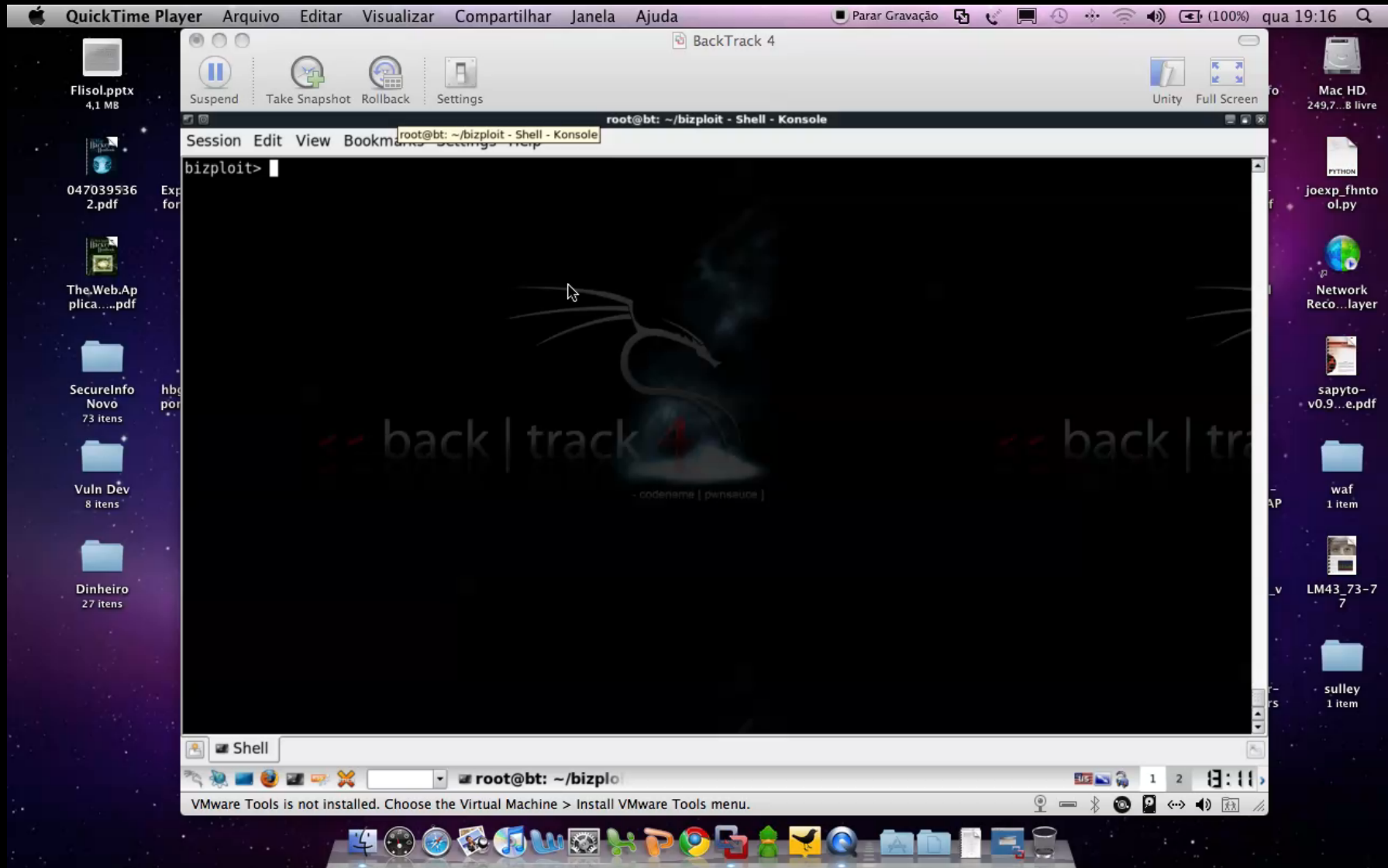


Demo - vulnassess

The screenshot shows a Mac desktop environment with a purple and black starry background. A window titled "BackTrack 4" is open, displaying a terminal window. The terminal prompt is "bizsploit/plugins>". The desktop contains several folders and files, including "Flisol.pptx", "047039536 2.pdf", "Exploitation for p...t.pdf", "The.Web.Appl...pdf", "SecureInfo Novo 73 itens", "hbqthreatre port...a.pdf", "Vuln Dev 8 itens", and "Dinheiro 27 itens". A watermark in the bottom right corner reads "YOU SHOT THE SHERIFF".



Demo – checkRFCEXEC



Thanks

- Mariano Nuñez Di Croce (ONAPSIS)
- SecureInfo
- YSTS



Contato



espinhara.net@gmail.com



@jespinhara

FIM!

