SAP


PITÚ
PITÚ
Premium de Brasil
AGUARDENTE DE CANA
PITÚ
CACHAÇA


YOU SHØT THE
SHERIFF

# 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

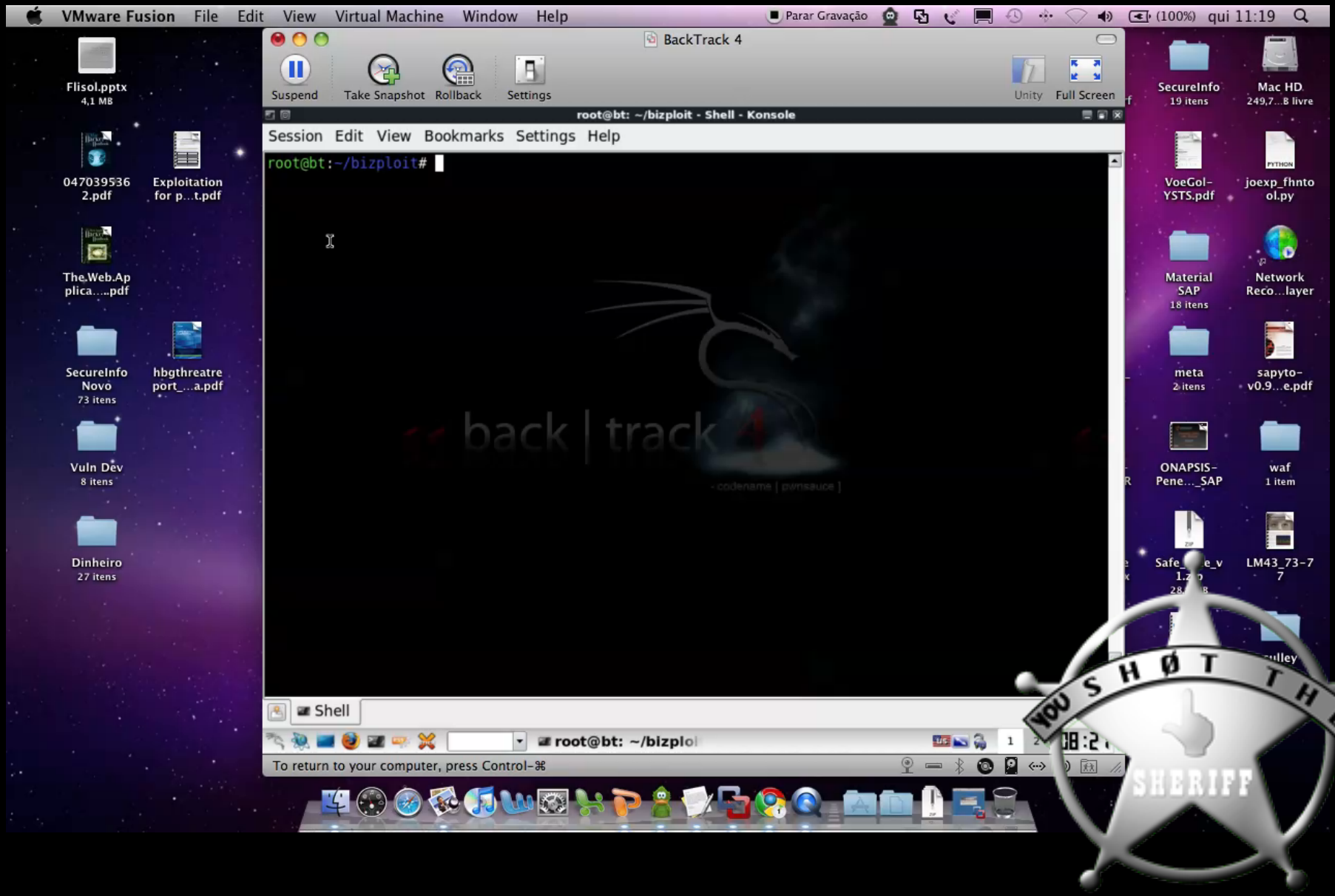
onapsis

Securing Business Essentials

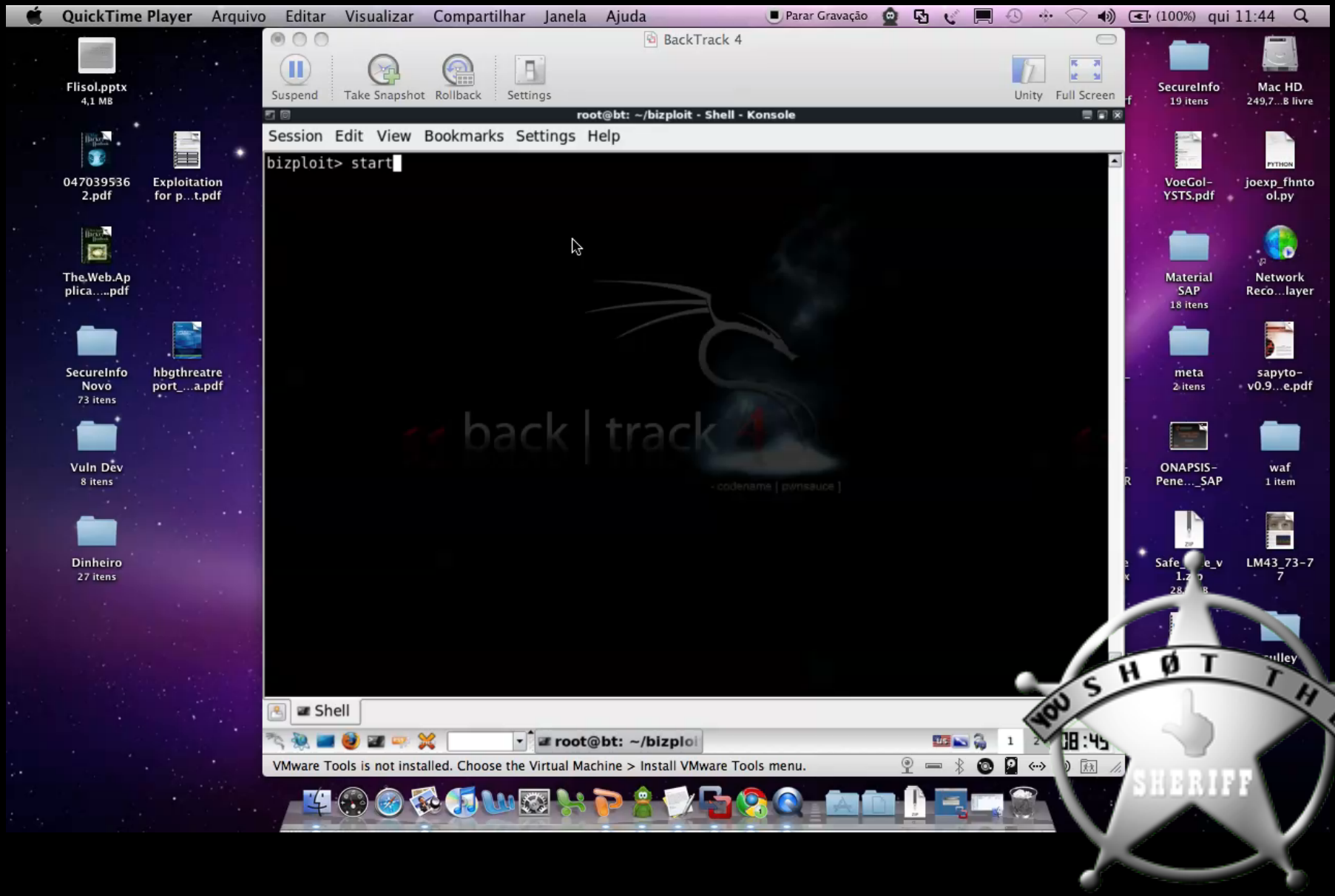
# Demo

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

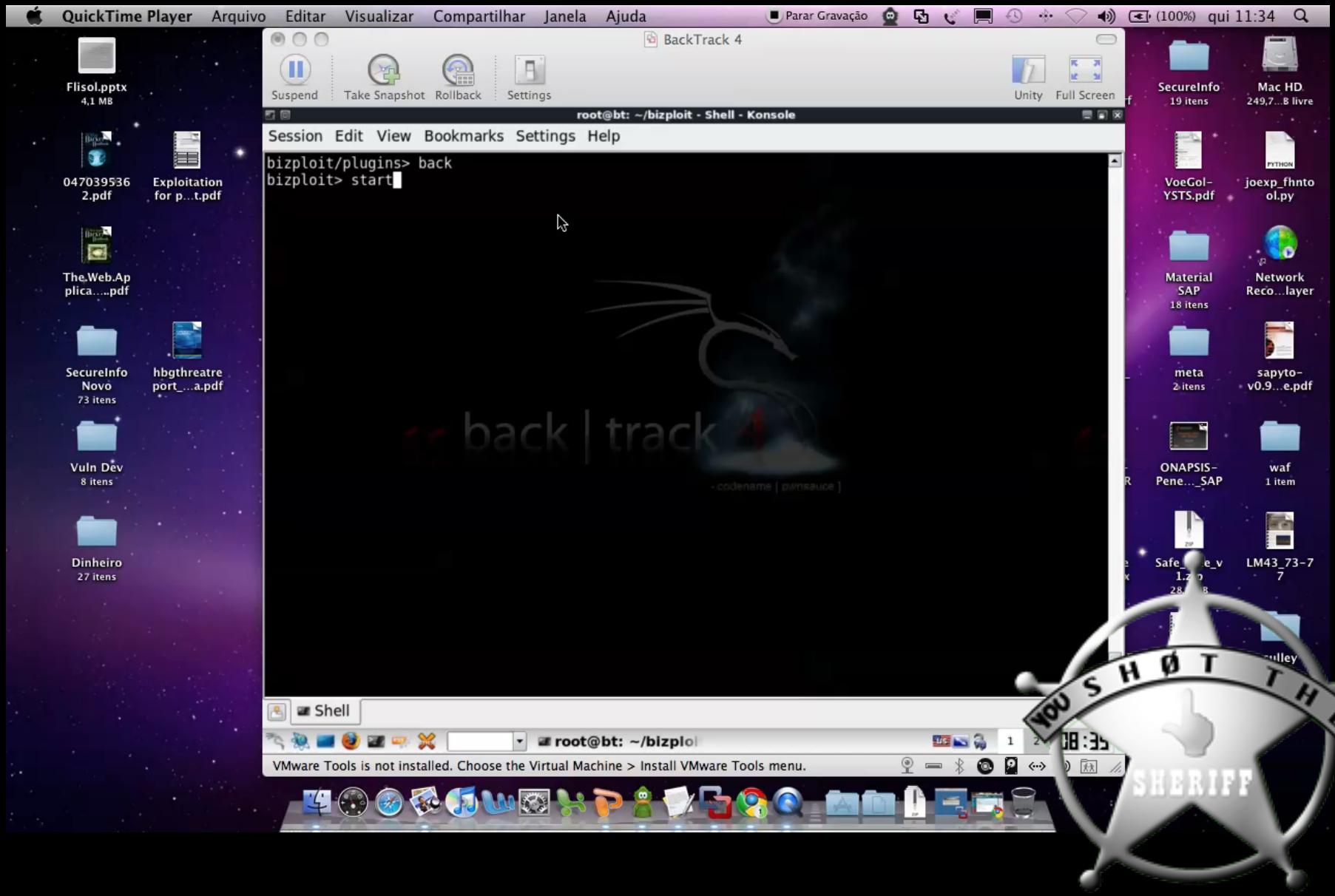
# Demo - getClients



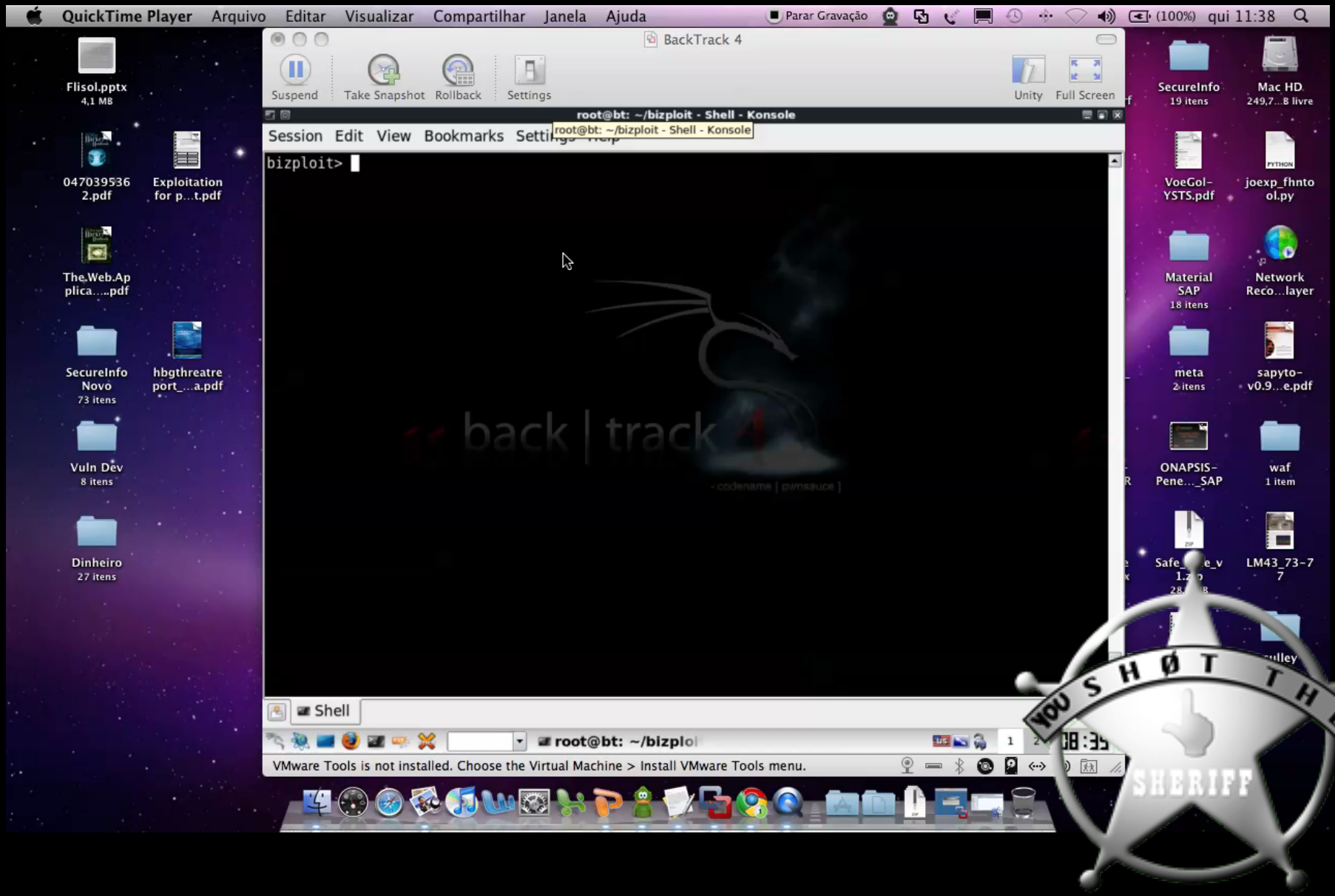
# Demo - sapinfo



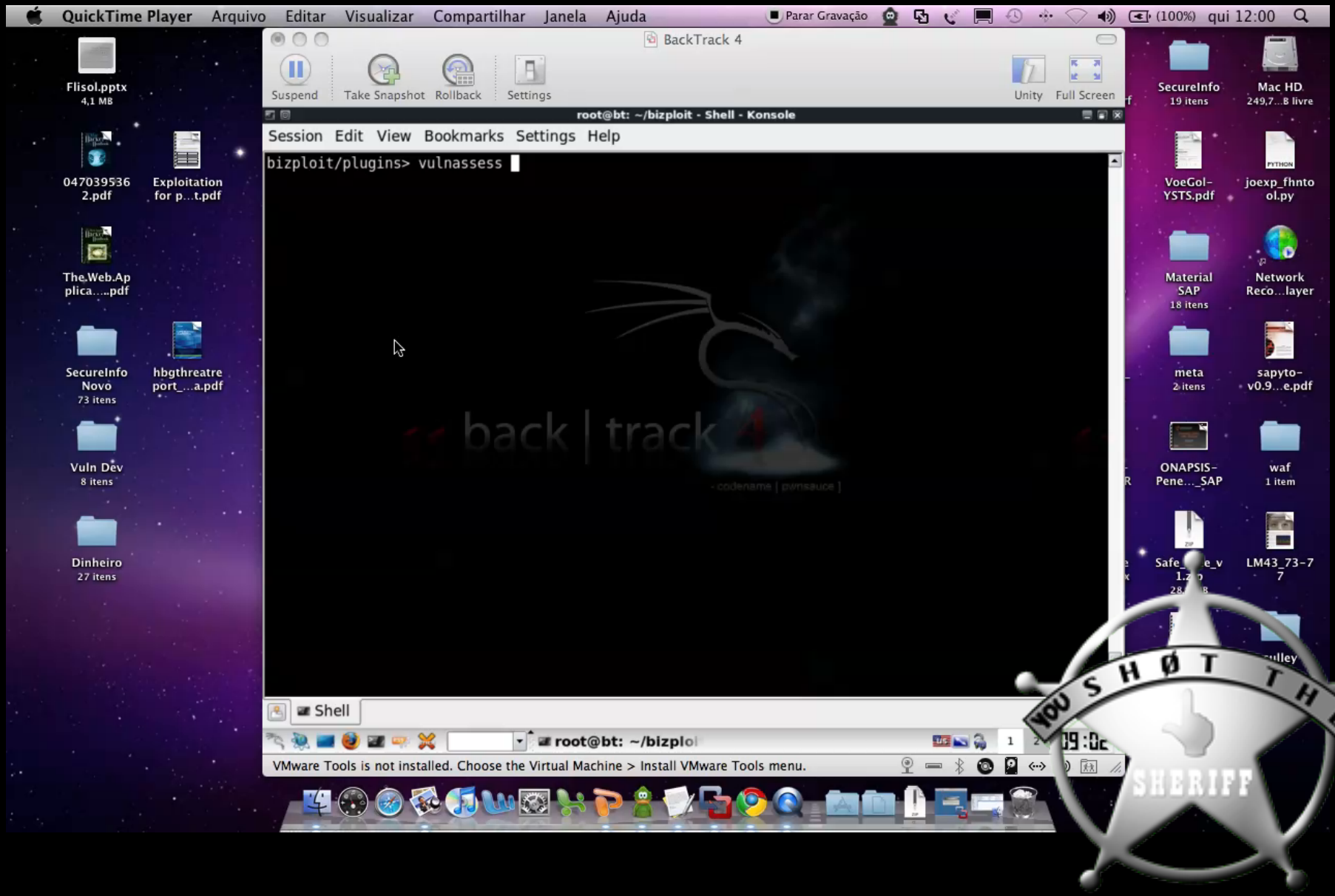
# Demo – getApplicationServers



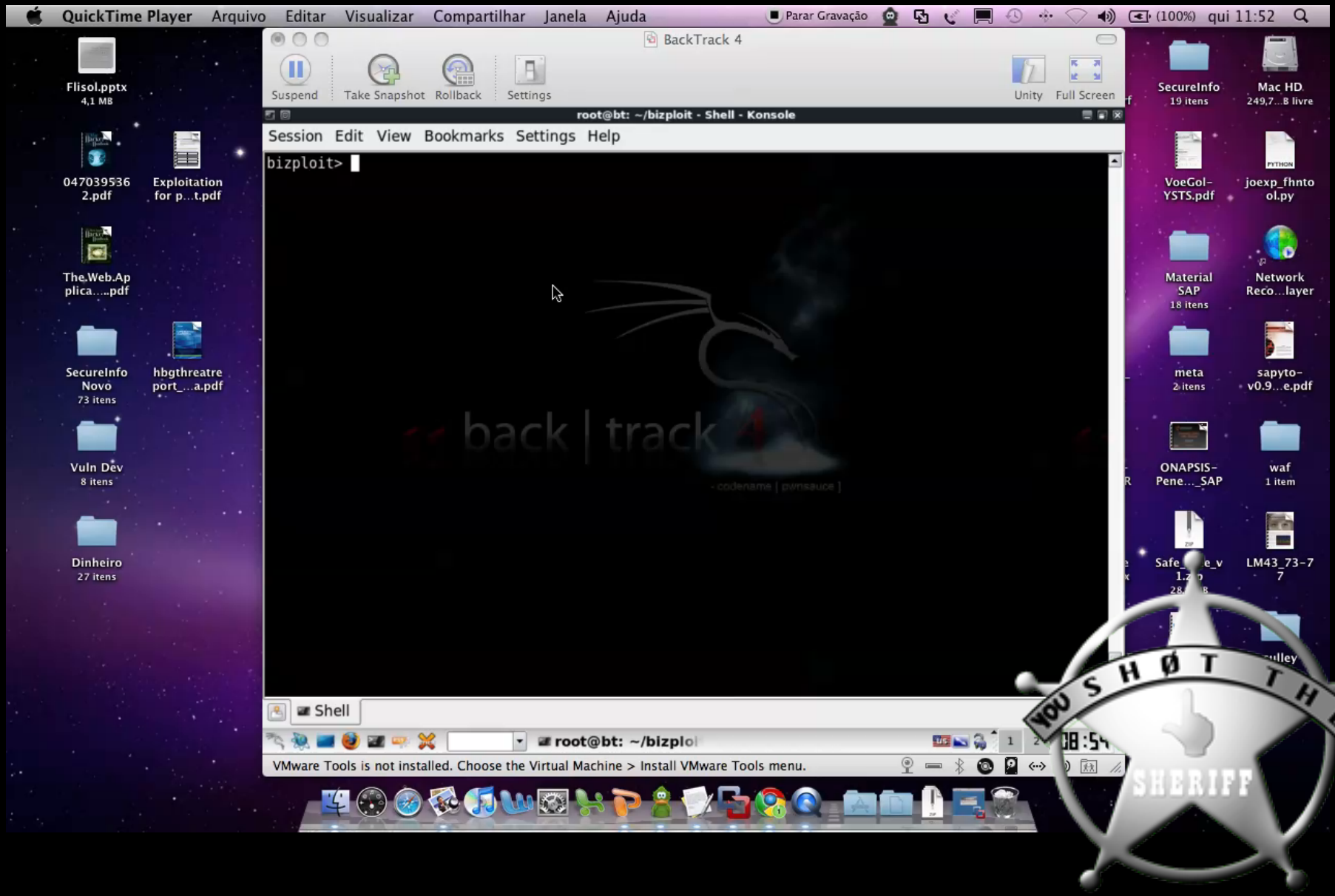
# Demo – findRegRFCServers



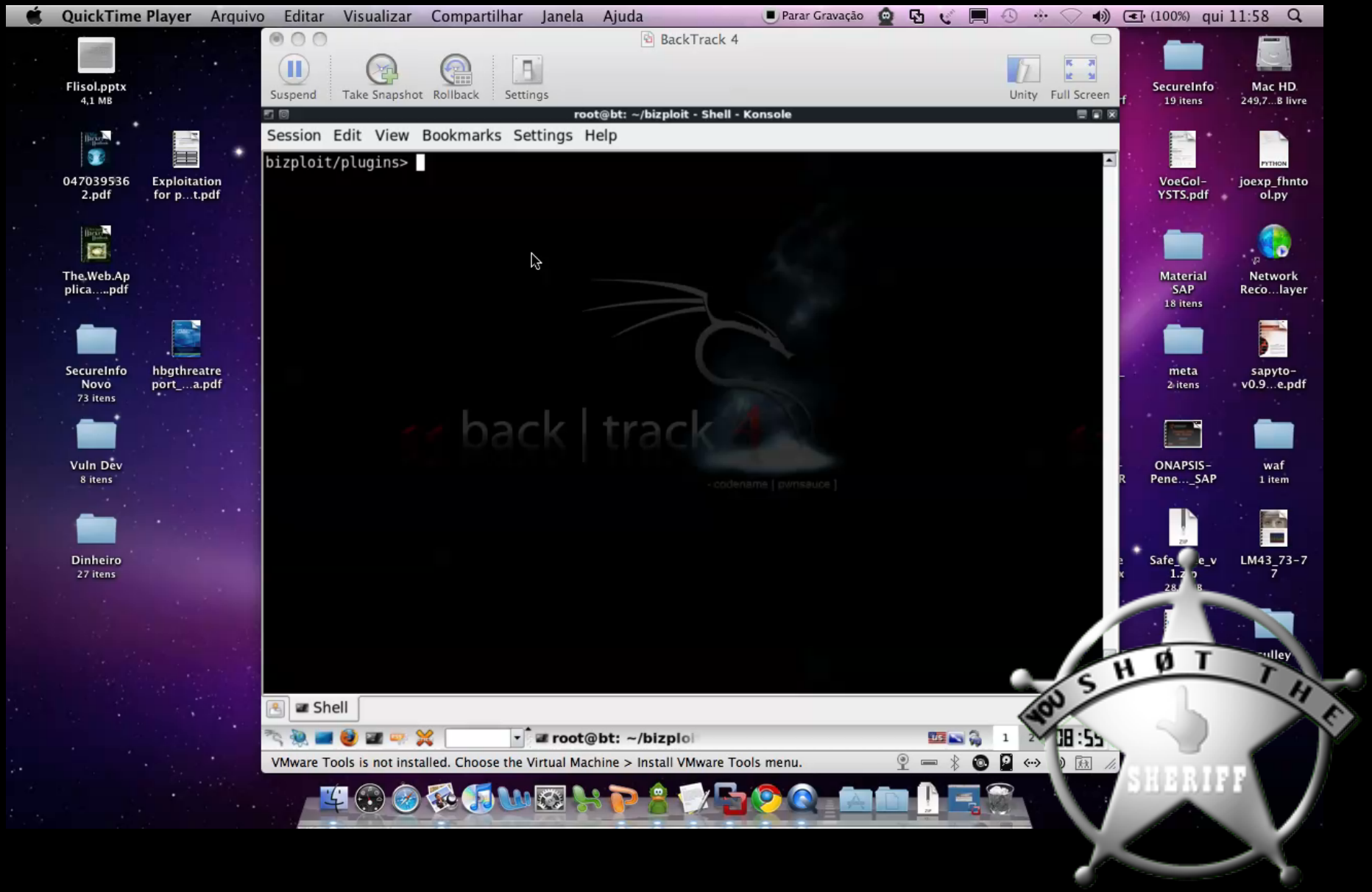
# Demo - registerExtServer



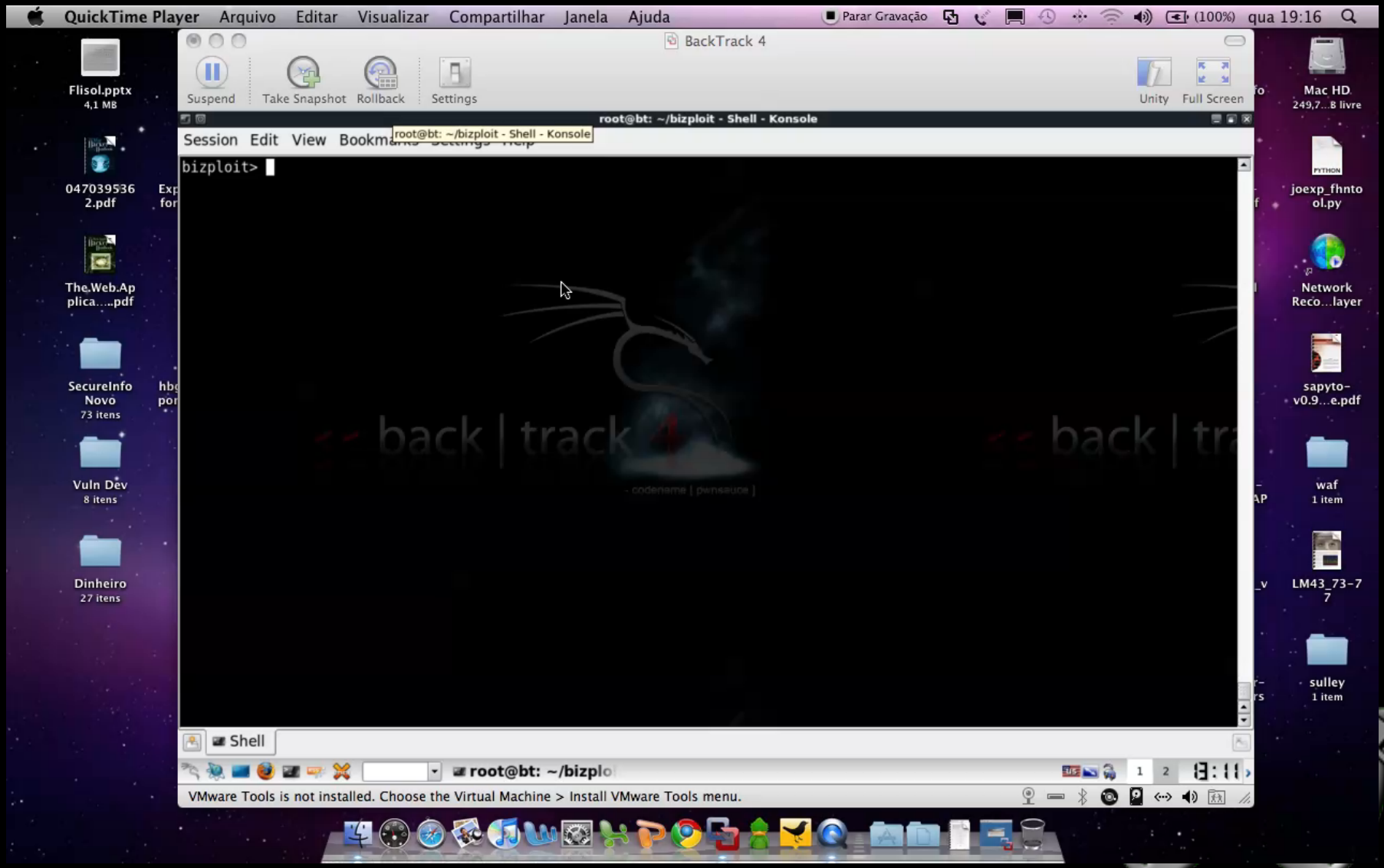
# Demo - bruteLogin



# Demo - vulnassess



# Demo – checkRFCEXEC



# Thanks

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

# Contato

espinhara.net@gmail.com

@jespinhara

# FIM!