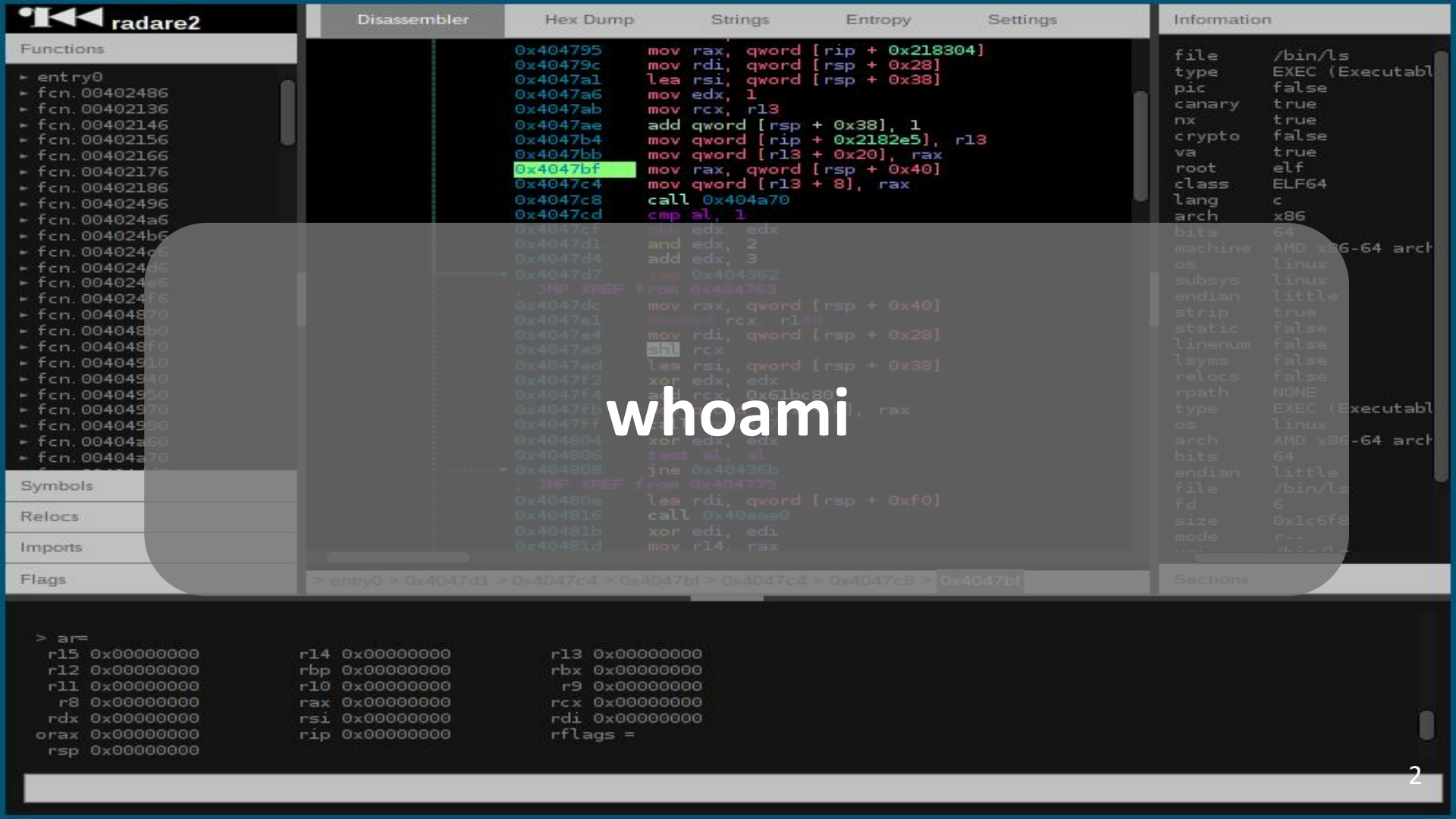
Curso de Férias - Dia 1

Estevam Arantes


radare2
Disassembler
Hex Dump
Strings
Entropy
Settings
Information
Functions
Symbols
Relocs
Imports
Flags
Sections
whoami

Objetivos do curso

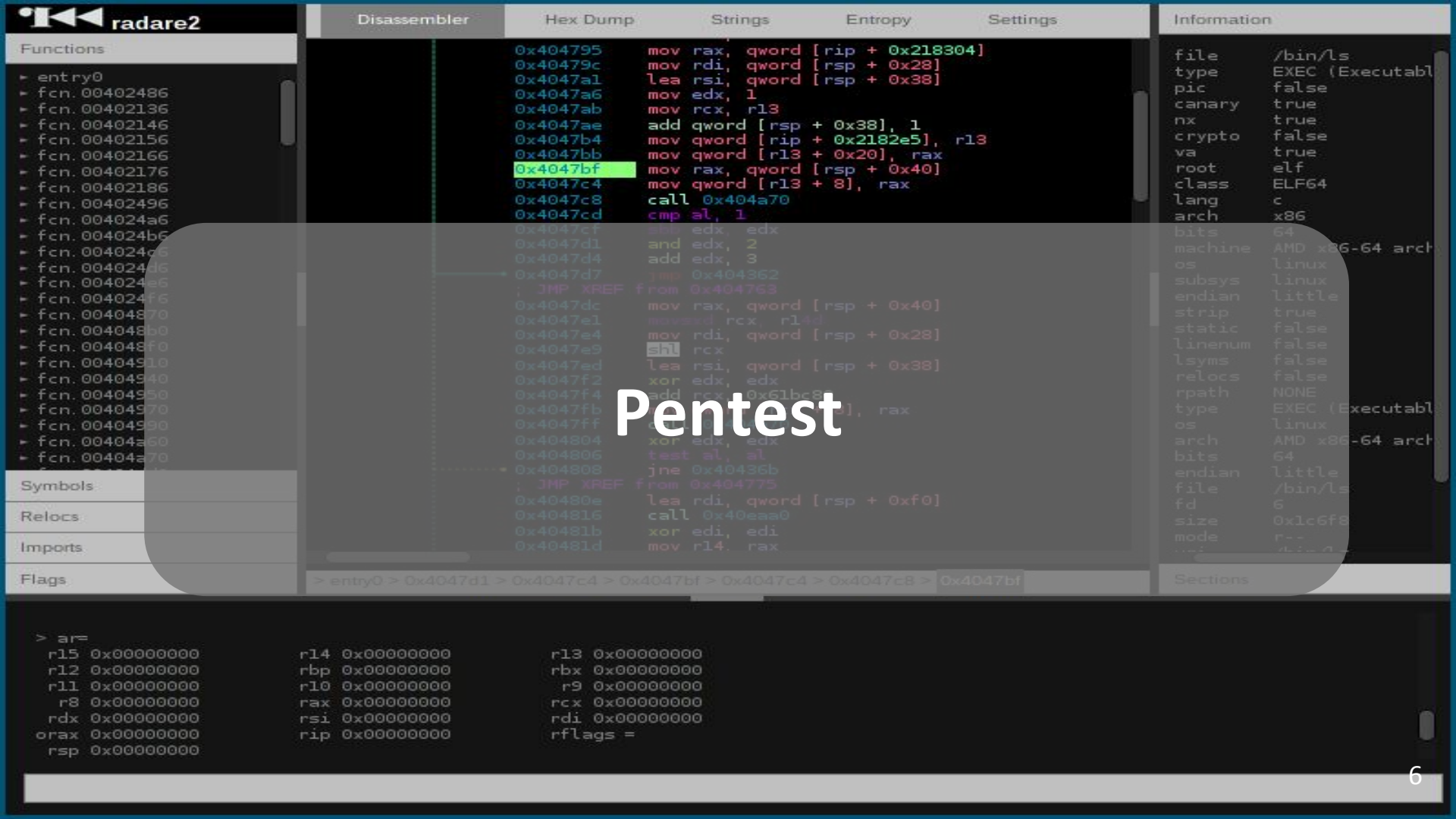
- Aprendizado teórico com prática;
- Aprender a aprender;
- Visão geral sobre vários assuntos (outros além do Ping!
- Passar dicas e experiências.

Programação (sujeita a alterações)

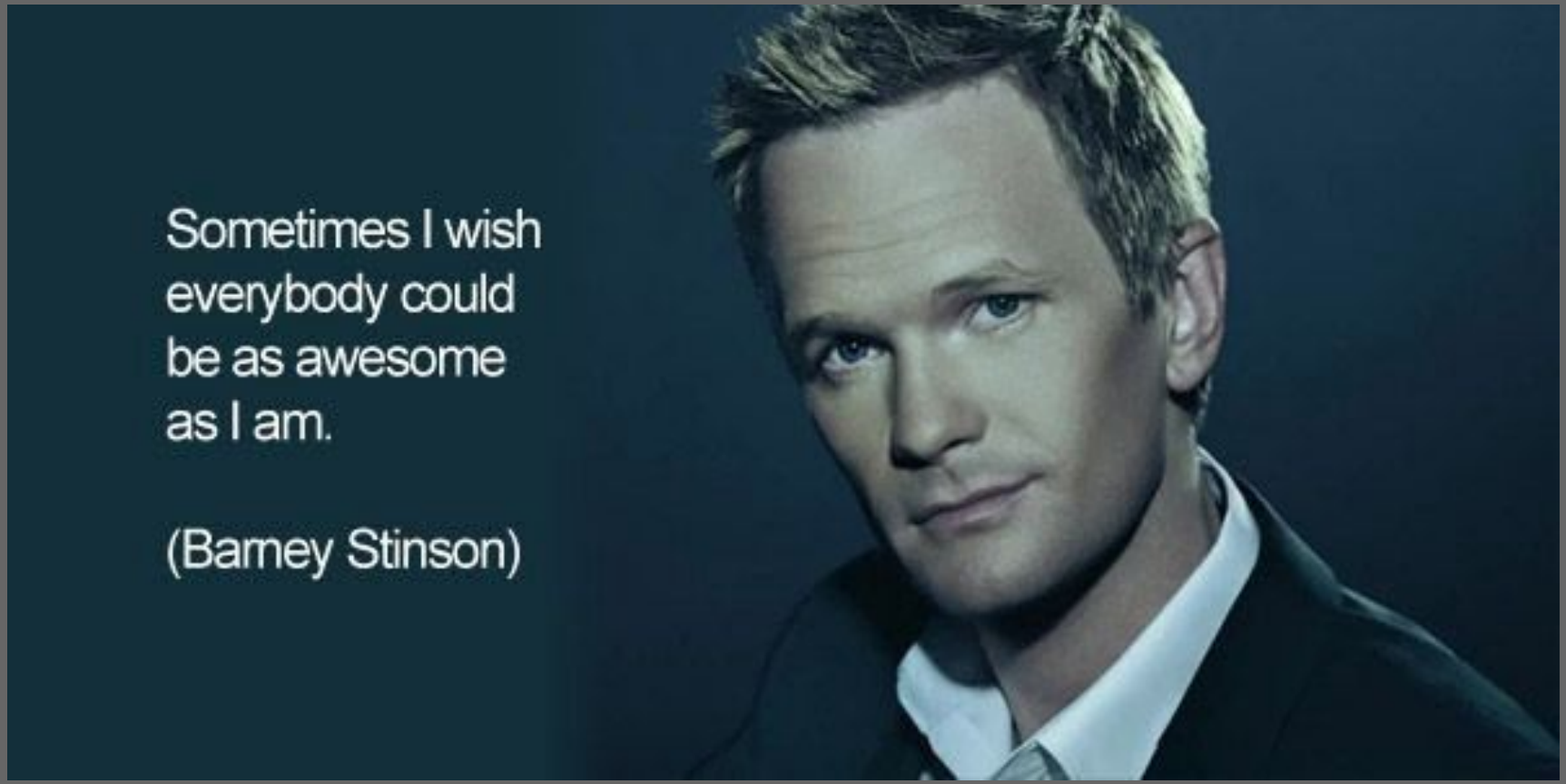
- Dia 1 (manhã) - Eventos e certificações na área de segurança, pentesting e suas fases, vulnerabilidades famosas + metasploit, reconhecimento e scanners, servidores, proxies, VPNs e instruções sobre a parte prática;
- Dia 1 (tarde) - Desafios de revisão e nivelamento, introdução à VPN do Ganesh, desafios de recon e vulnerabilidades famosas;
- Dia 2 (manhã) - Vulnerabilidades WEB seguindo OWASP Top 10 - SQL Injection, XSS, XXE, Broken Auth, etc. e ferramentas relacionadas;
- Dia 2 (tarde) - Juiceshop, Webgoat e outros - Prática de WEB;

Programação (sujeita a alterações)

- Dia 3 (manhã) - Ataques diversos: Shell Reversa, File Upload Bypass, Bruteforcing e hashing, proxychain, ataques em redes locais e metasploit em mais detalhes.
- Dia 3 (tarde) - Exercícios e desafios dos tópicos da manhã (entre outros :D)
- Dia 4 (manhã) - Livre
- Dia 4 (tarde) - Escalação de privilégios, OSINT, firewalls, phishing, computação forense e esteganografia.
- Dia 5 (manhã) - Engenharia Reversa em ELF e em APKs.
- Dia 5 (tarde) - Prática de engenharia reversa (possivelmente com malwares reais :D)


radare2
Disassembler
Hex Dump
Strings
Entropy
Settings
Information
Functions
Symbols
Relocs
Imports
Flags
Sections
0x404795 mov rax, qword [rip + 0x218304]
0x40479c mov rdi, qword [rsp + 0x28]
0x4047a1 lea rsi, qword [rsp + 0x38]
0x4047a6 mov edx, 1
0x4047ab mov rcx, r13
0x4047ae add qword [rsp + 0x38], 1
0x4047b4 mov qword [rip + 0x2182e5], r13
0x4047bb mov qword [r13 + 0x20], rax
0x4047bf mov rax, qword [rsp + 0x40]
0x4047c4 mov qword [r13 + 8], rax
0x4047c8 call 0x404a70
0x4047cd cmp al, 1
file /bin/ls
type EXEC (Executabl
pic false
canary true
nx true
crypto false
va true
root elf
class ELF64
lang c
arch x86
bits 64
machine AMD x86-64 arch
os linux
subsys linux
endian little
strip true
static false
linenum false
lsyms false
relocs false
rpath NONE
type EXEC (Executabl
os linux
arch AMD x86-64 arch
bits 64
endian little
file /bin/ls
fd 6
size 0x1c6f8
mode r--
Pentest
> ar=
r15 0x00000000
r14 0x00000000
r13 0x00000000
r12 0x00000000
rbp 0x00000000
rbx 0x00000000
r11 0x00000000
r10 0x00000000
r9 0x00000000
r8 0x00000000
rax 0x00000000
rcx 0x00000000
rdx 0x00000000
rsi 0x00000000
rdi 0x00000000
orax 0x00000000
rip 0x00000000
rflags =
rsp 0x00000000

Motivação


Sometimes I wish
everybody could
be as awesome
as I am.
(Barney Stinson)

Motivação II

- Trabalho desafiador
- Divertido

Mercado de Trabalho

- Global
- Oportunidades Home Office
- Linkedin é o seu amigo (Ganesh)
- Não faça besteira!
  - Background check
- Mercado baseado em reputação

Certificações

Certificações

- Não garantem o seu emprego!
- Ajuda? Sim!
- CEH - Fuja! Run to the hills!!!
- Offensive Security
  - OSCP
  - OSWP
  - OSCE
  - OSEE
  - OSWE

Certificações e Cursos (Pagos)

- SANS
  - GIAC *
- Cursos
  - Offensive Security
  - SANS
  - Treinamentos em conferências (vide H2HC)

Certificações e Eventos

- Eventos
  - Brasil
    - H2HC
    - Roadsec
    - Bsides
    - YSTS
    - Etc.
- Exterior
  - Defcon (USA)
  - CCC (GER)
  - Blackhat (USA, EU)
  - EkoParty (ARG)
  - Infiltrate (USA)

Conformidade

- PCI - PCI Security Standards Council
  - https://pt.pcisecuritystandards.org/minisite/env2/
- Importância
  - PCI

O que é Penetration Test?

- Aka Pentest
- Tradução literal: “Teste de Penetração”
- Processo de identificar e explorar vulnerabilidades em sistemas, redes, hardware, etc.
- Diversos métodos: lógicos, físicos, engenharia social, místicos
- Única forma de mensurar o risco real de uma vulnerabilidade

Tipos de Pentest

- Blind/Black box
- Gray box
- Non blind/White box
- Externo
- Interno
- Wireless
- Físico
- Engenharia social
- Client-side
- Aplicação, etc.

Pentest x Análise de Vulnerabilidade

- Confusão!
- Pentest não é análise de vulnerabilidades.
- Análise de vulnerabilidades não é pentest.

Pentest x Análise de Vulnerabilidade

- Análise de Vulnerabilidades
  - Não ocorre a exploração de vulnerabilidade
  - Alta ocorrência de falsos positivos
- Pentest
  - Exploração das vulnerabilidades
  - Não existe falso positivo
  - Risco Real

Devo realizar um pentest?

- Sim!
- Quem deve realizar um pentest?
  - Todo mundo! :D
- Porquê?
  - Simulação real de ataque
  - Avaliação das suas soluções de defesa (firewall, ids, ips, av)

Benefícios

- Rápida avaliação da situação real da segurança da empresa.
  - Eficaz
- Ajuda na tomada de decisões (investimentos, alocação de recursos)
- Recomendações direcionadas a sanar um problema.

Pentester

- Pessoa que faz o teste
- Pentester != Pesquisador
- Brasil
  - Consultor de Segurança
  - Analista de Segurança
  - Analista de Suporte
  - Analista de RH, Analista de Software (oh wait)
- Empresas especializadas
  - Consultores especializados

Pentester - Conhecimento necessário

- Depende!
- Network
  - Redes
  - Protocolos
  - A lot of stuff!
- Application
  - Programação
  - Protocolos
  - A lot of stuff!

Pentester - Conhecimento necessário II

- Diferenciais
- Foco
- Idiomas estrangeiros (Inglês principalmente!)

Fases de um pentest

- Definição de alvo
- Enumerar e identificar ativos
- Identificar as vulnerabilidades
- Explorar as vulnerabilidades
- Atividades pós exploratórias
- Coleta de evidências
- Escrita do relatório

Fases de um pentest

- Definição de alvo
- Enumerar e identificar ativos
- Identificar as vulnerabilidades
- Explorar as vulnerabilidades
- Atividades pós exploratórias
- Coleta de evidências
- Escrita do relatório

Fases de um pentest

- Definição de alvo
- Enumerar e identificar ativos
- Identificar as vulnerabilidades
- Explorar as vulnerabilidades
- Atividades pós exploratórias
- Coleta de evidências
- Escrita do relatório

Demos!

Shellshock - () { :;}; echo

BACKGROUND

What is Shellshock?

Shellshock is a vulnerability, security bug, in Bash.

Bash (Bourne-again shell)

An open-source command interpreter, a program that allows a user or program to issue commands via a terminal to the operating system to execute other programs.

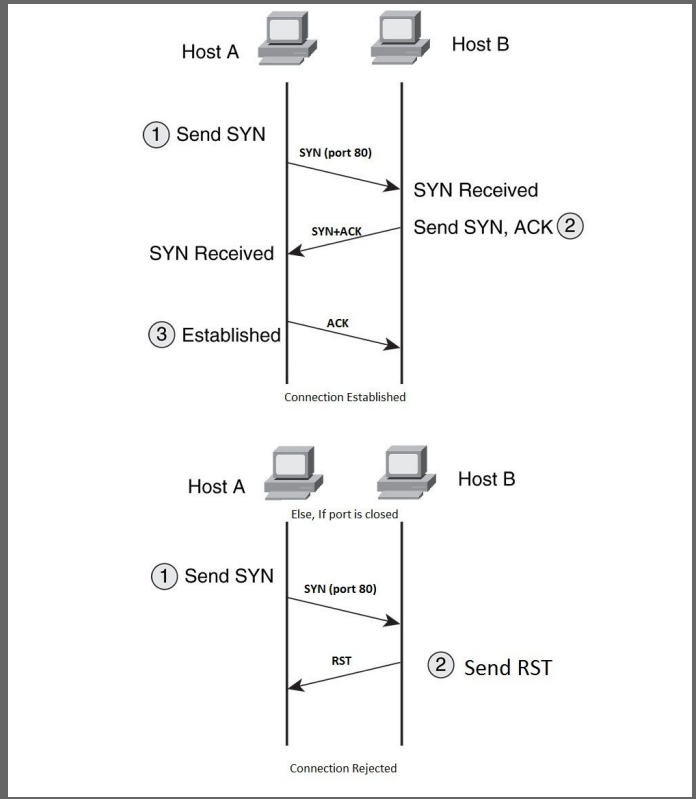
Widely available and the default shell on most Linux distributions, Mac OSX, even Windows (Cygwin) and some embedded systems.

HEARTBLEED

```
00e0: 3B 71 3D 30 2E 38 0D 0A 41 63 63 65 70 74 2D 4C  ;q=0.8..Accept-L
00f0: 61 6E 67 75 61 67 65 3A 20 65 6E 2D 55 53 2C 65  anguage: en-US,e
0100: 6E 3B 71 3D 30 2E 35 0D 0A 41 63 63 65 70 74 2D  n;q=0.5..Accept-
0110: 45 6E 63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20  Encoding: gzip,
0120: 64 65 66 6C 61 74 65 2C 20 62 72 0D 0A 52 65 66  deflate, br..Ref
0130: 65 72 65 72 3A 20 68 74 74 70 73 3A 2F 2F 31 39  erer: https://19
0140: 32 2E 31 36 38 2E 31 2E 31 30 35 3A 38 34 34 33  2.168.1.105:8443
0150: 2F 62 57 41 50 50 2F 6C 6F 67 69 6E 2E 70 68 70  /bWAPP/login.php
0160: 0D 0A 44 4E 54 3A 20 31 0D 0A 43 6F 6E 6E 65 63  ..DNT: 1..Connec
0170: 74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 76 65  tion: keep-alive
0180: 0D 0A 43 6F 6F 6B 69 65 3A 20 73 65 63 75 72 69  ..Cookie: securi
0190: 74 79 5F 6C 65 76 65 6C 3D 30 3B 20 50 48 50 53  ty_level=0; PHPS
01a0: 45 53 53 49 44 3D 63 63 33 63 65 34 64 37 63 30  ESSID=cc3ce4d7c0
01b0: 37 38 36 33 39 30 37 63 66 32 35 35 32 65 61 34  7863907cf2552ea4
01c0: 38 33 39 31 38 30 0D 0A 55 70 67 72 61 64 65 2D  839180..Upgrade-
01d0: 49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74  Insecure-Request
01e0: 73 3A 20 31 0D 0A 0D 0A 2D 9D DA A0 6A 88 FE 12  s: 1....-...j...
01f0: FA FD 11 00 E6 16 B4 0B 63 37 62 33 65 39 31 36  ........c7b3e916
0200: 65 32 64 39 39 37 66 30 37 66 37 0D 0A 55 70 67  e2d997f07f7..Upg
0210: 72 61 64 65 2D 49 6E 73 65 63 75 72 65 2D 52 65  rade-Insecure-Re
0220: 71 75 65 73 74 73 3A 20 31 0D 0A 0D 0A 6C 6F 67  quests: 1....log
0230: 69 6E 3D 62 65 65 26 70 61 73 73 77 6F 72 64 3D  in=bee&password=
0240: 62 75 67 26 73 65 63 75 72 69 74 79 5F 6C 65 76  bug&security_lev
0250: 65 6C 3D 30 26 66 6F 72 6D 3D 73 75 62 6D 69 74  el=0&form=submit
0260: 68 71 88 28 1A 02 C4 BD 0A E3 CA 24 47 63 B8 EB  hq.(.......$Gc..
0270: 02 C0 39 C0 37 C0 36 00 8A C0 35 00 18 00 51 00  ..9.7.6...5...Q.
0280: 4C C0 46 C0 31 00 00 00 B5 C0 2A C0 11 00 AD 00  L.F.1.....*.....
0290: 2D C0 27 00 A2 00 73 00 79 C0 24 00 64 C0 22 C0  -.'...s.y.$.d.".
02a0: 1F 00 7C C0 5C C0 1B 00 60 C0 1A CC AA C0 12 C0  ..|.\...`.......
02b0: 29 C0 10 C0 0F C0 69 C0 0B C0 03 00 97 00 C5 C0  ).....i.........
02c0: 53 00 C2 00 BE 00 04 C0 5D 00 8D C0 30 C0 3E 00  S.......]...0.>.
02d0: AF 00 9E 00 A9 00 5A 00 A3 00 A1 00 A0 00 AA C0  ......Z.........
02e0: 01 00 96 00 94 00 03 00 3F 00 93 00 17 00 91 00  ........?.......
```

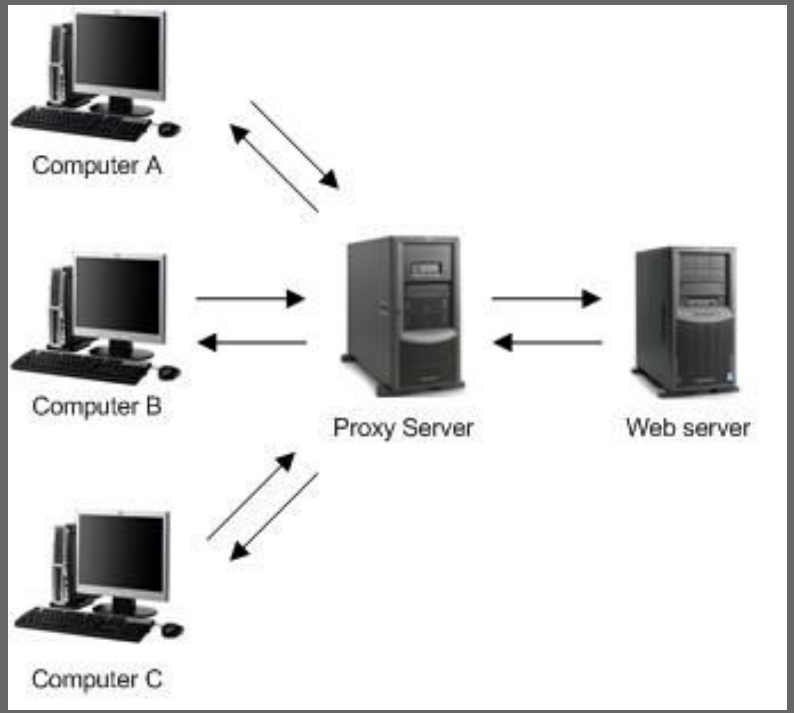
Scanners!

- Scan de portas, serviços e vulnerabilidades
  - Nmap (TCP ou UDP)
  - Reconnoitre
- Vulnerabilidades em frameworks
  - Wpscan
- Subdomínios e diretórios



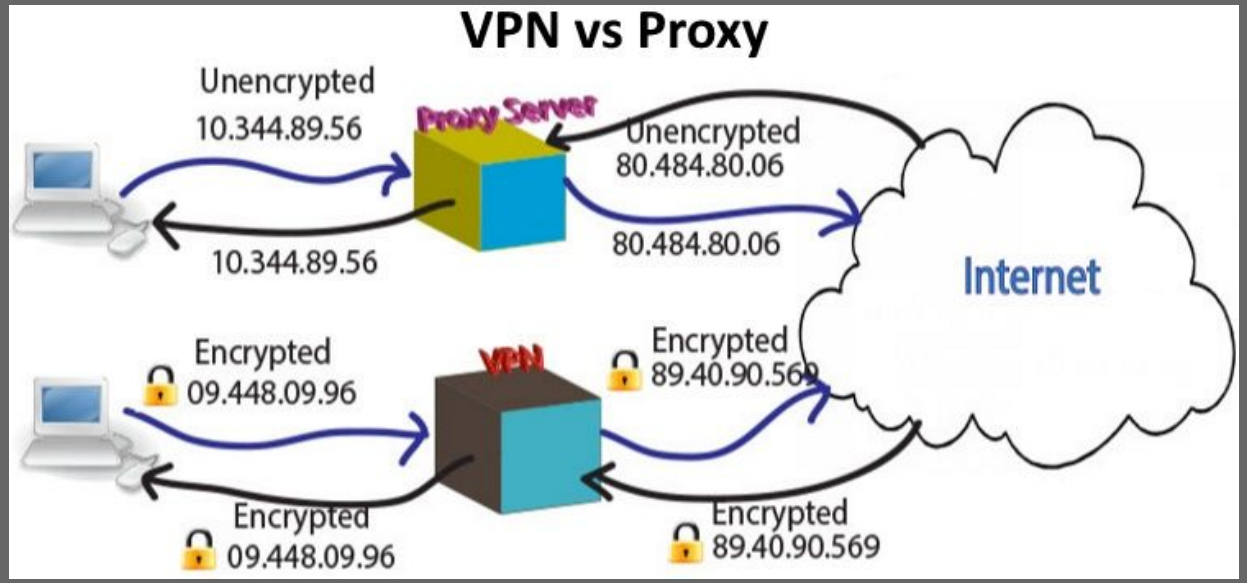
Proxies!

- Interceptando/Redirecionando e Controlando Informações
  - Burpsuite + FoxyProxy - Aprendendo a configurar o firefox!
  - Zed Attack Proxy



VPN - Virtual Private Network

- Interceptando e Redirecionando Informações
  - Openvpn e nossas máquinas vulneráveis



Links úteis

- Heartbleed - Computerphile
- RFC HeartBeat
- Shellshock CVE
- Metasploit

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br