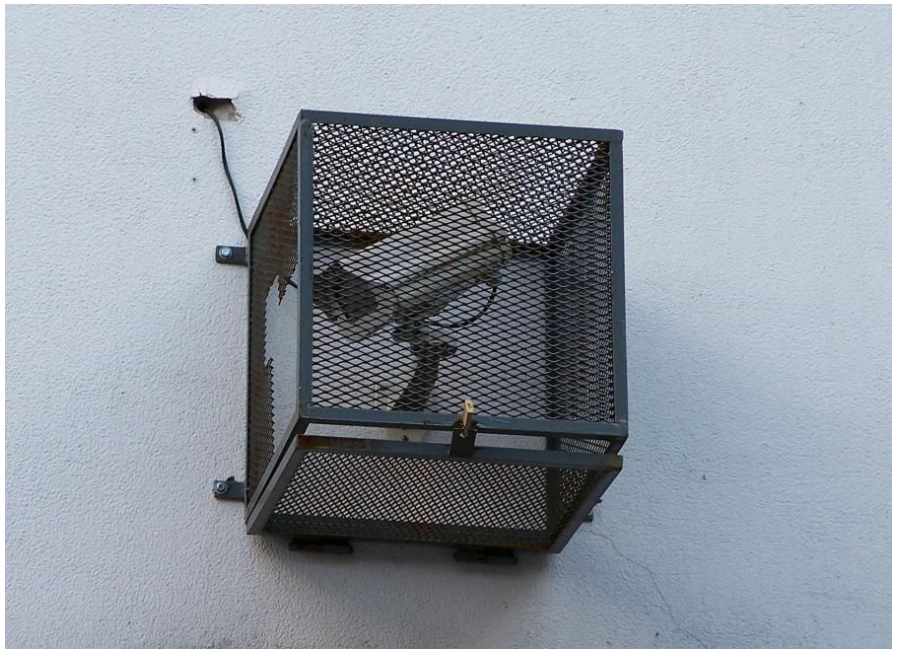
ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA



Segurança do perímetro da rede

ISEL – Instituto Superior de Engenharia de Lisboa
Rua Conselheiro Emídio Navarro, 1 | 1959-007 Lisboa

Onde estamos vulneráveis?

Remotamente

```
ncruz@deviant ~> netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp6       0      0  2001:690:2008:e1.55157 2a03:2880:f01a:1.443   ESTABLISHED
tcp4       0      0  194.210.198.132.55153  104.215.198.144.443    ESTABLISHED
tcp4       0      0  194.210.198.132.55152  162.125.32.129.443     ESTABLISHED
tcp4       0      0  194.210.198.132.53776  192.104.48.12.993      ESTABLISHED
tcp4       0      0  194.210.198.132.53775  192.104.48.12.143      ESTABLISHED
tcp46      0      0  *.60210                *.*                    LISTEN
tcp4       0      0  *.60210                *.*                    LISTEN
tcp4       0      0  127.0.0.1.631          *.*                    LISTEN
tcp6       0      0  ::1.631                *.*                    LISTEN
tcp4       0      0  10.100.254.4.50674     216.58.210.106.443     CLOSE_WAIT
tcp4       0      0  10.100.254.4.50650     216.58.208.1.443       CLOSE_WAIT
tcp4       0      0  10.100.254.4.49828     216.58.208.1.443       CLOSE_WAIT
tcp6       0      0  2001:818:dc79:20.61298 2a00:1450:4003:8.443   CLOSE_WAIT
tcp6       0      0  2001:690:2008:e1.56600 2a00:1450:4003:8.443   CLOSE_WAIT
tcp4       0      0  127.0.0.1.17603        *.*                    LISTEN
tcp4       0      0  127.0.0.1.17600        *.*                    LISTEN
tcp4       0      0  *.17500                *.*                    LISTEN
tcp6       0      0  *.17500                *.*                    LISTEN
tcp4      31      0  10.100.254.4.51388     108.160.172.236.443    CLOSE_WAIT
tcp4       0      0  194.210.194.233.49335  64.233.184.125.5222    ESTABLISHED
tcp6       0      0  2001:690:2008:e1.49214 2a00:1450:4004:8.443   ESTABLISHED
tcp6       0      0  fd5b:bbfe:3537:4.4488  *.*                    LISTEN
tcp4       0      0  127.0.0.1.4380         *.*                    LISTEN
tcp4       0      0  127.0.0.1.4370         *.*                    LISTEN
tcp4       0      0  *.88                   *.*                    LISTEN
tcp6       0      0  *.88                   *.*                    LISTEN
tcp4       0      0  *.22                   *.*                    LISTEN
tcp6       0      0  *.22                   *.*                    LISTEN
tcp4       0      0  *.5900                 *.*                    LISTEN
tcp6       0      0  *.5900                 *.*                    LISTEN
```

Onde estamos vulneráveis?

Remotamente

```
ncruz@deviant ~> netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp6       0      0  2001:690:2008:e1.55157 2a03:2880:f01a:1.443   ESTABLISHED
tcp4       0      0  194.210.198.132.55153  104.215.198.144.443    ESTABLISHED
tcp4       0      0  194.210.198.132.55152  162.125.32.129.443     ESTABLISHED
tcp4       0      0  194.210.198.132.53776  192.104.48.12.993      ESTABLISHED
tcp4       0      0  194.210.198.132.53775  192.104.48.12.143      ESTABLISHED
tcp46      0      0  *.60210                *.*                    LISTEN
tcp4       0      0  *.60210                *.*                    LISTEN
tcp4       0      0  127.0.0.1.631          *.*                    LISTEN
tcp6       0      0  ::1.631                *.*                    LISTEN
tcp4       0      0  10.100.254.4.50674     216.58.210.106.443     CLOSE_WAIT
tcp4       0      0  10.100.254.4.50650     216.58.208.1.443       CLOSE_WAIT
tcp4       0      0  10.100.254.4.49828     216.58.208.1.443       CLOSE_WAIT
tcp6       0      0  2001:818:dc79:20.61298 2a00:1450:4003:8.443   CLOSE_WAIT
tcp6       0      0  2001:690:2008:e1.56600 2a00:1450:4003:8.443   CLOSE_WAIT
tcp4       0      0  127.0.0.1.17603        *.*                    LISTEN
tcp4       0      0  127.0.0.1.17600        *.*                    LISTEN
tcp4       0      0  *.17500                *.*                    LISTEN
tcp6       0      0  *.17500                *.*                    LISTEN
tcp4      31      0  10.100.254.4.51388     108.160.172.236.443    CLOSE_WAIT
tcp4       0      0  194.210.194.233.49335  64.233.184.125.5222    ESTABLISHED
tcp6       0      0  2001:690:2008:e1.49214 2a00:1450:4004:8.443   ESTABLISHED
tcp6       0      0  fd5b:bbfe:3537:4.4488  *.*                    LISTEN
tcp4       0      0  127.0.0.1.4380         *.*                    LISTEN
tcp4       0      0  127.0.0.1.4370         *.*                    LISTEN
tcp4       0      0  *.88                   *.*                    LISTEN
tcp6       0      0  *.88                   *.*                    LISTEN
tcp4       0      0  *.22                   *.*                    LISTEN
tcp6       0      0  *.22                   *.*                    LISTEN
tcp4       0      0  *.5900                 *.*                    LISTEN
tcp6       0      0  *.5900                 *.*                    LISTEN
```

Onde estamos vulneráveis?

- Desktops a correr com um browser
- Clientes de e-mail
- *Firewalls* a analisar os pacotes
- Qualquer equipamento que processe pacotes

Serviços vulneráveis

- Devido a falta de validações de segurança
- Alavancado por:
  - Dados em formatos inesperados
    - Ataques no formato dos caracteres
    - O software não faz sanitização dos dados
  - Quantidade de dados inesperada
    - Ataques de *buffer overflow*
    - Quantidade excessiva de dados em memória
    - Falta de validação de limites
- Os serviços vulneráveis podem ser explorados de maneira a obter privilégios de administrador

Segurança de perímetro

- Privacidade
  - Esconde o tamanho da organização, sistemas e serviços
- Mitigação de riscos
  - Serviços expostos são vulneráveis a ataques
  - Permite uma primeira linha de defesa em situações de necessidade de resposta a novos ataques
- Registo
  - Mantém um registo dos acessos para permitir a auditoria aos ataques

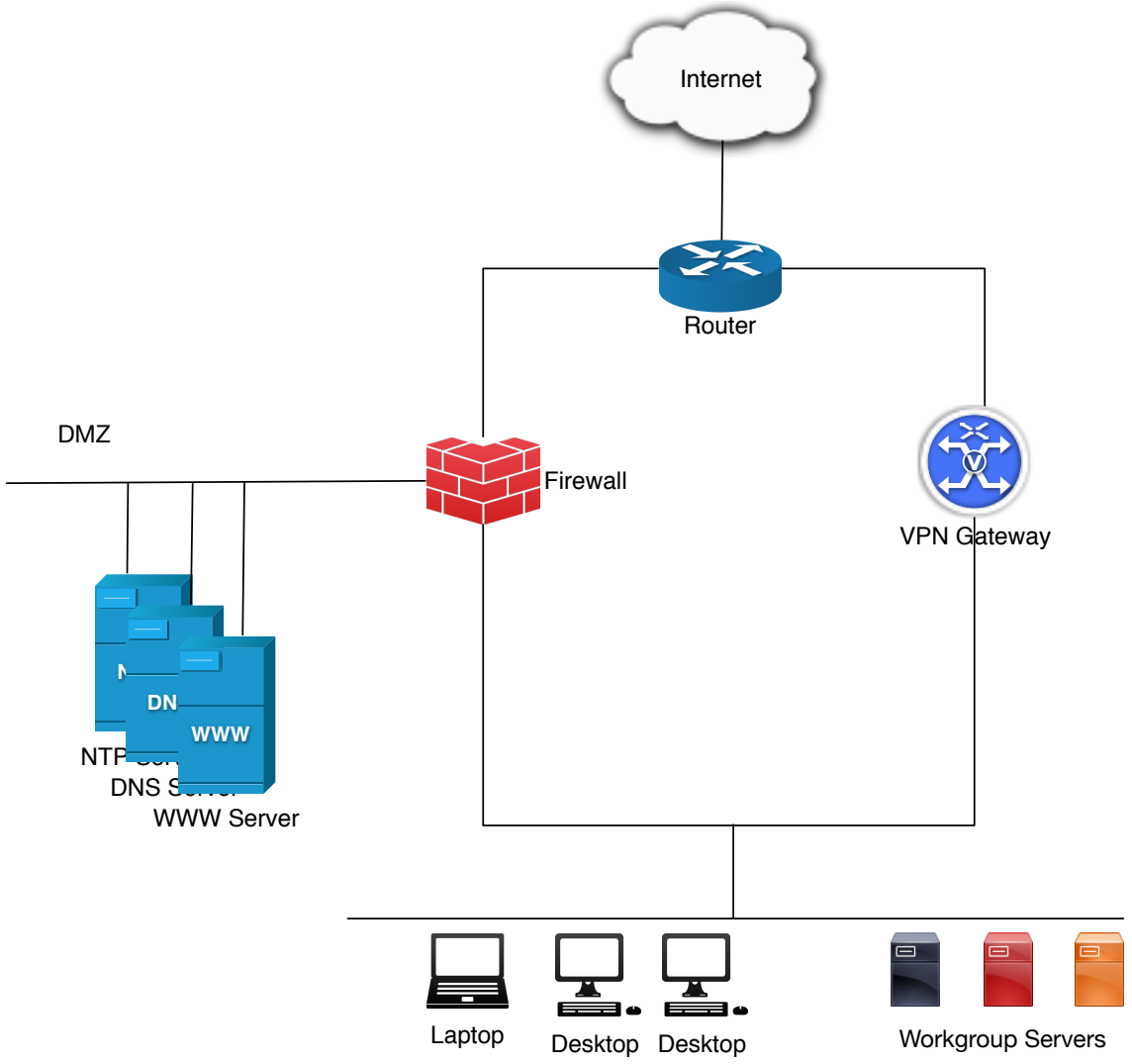
Perímetro = Uma Firewall?

- Ponto único de falha
- Utilizar implementações diferentes para objetivos diferentes
  - Filtragem de pacotes – bloqueio de redes
  - Filtragem de pacotes com estado – controlo de serviços
  - *Proxies* – controlo do conteúdo
  - Deteção de intrusões – análise dos pacotes
- Não entregar tudo a um único fabricante
- A segurança em camadas é mais difícil de ser quebrada

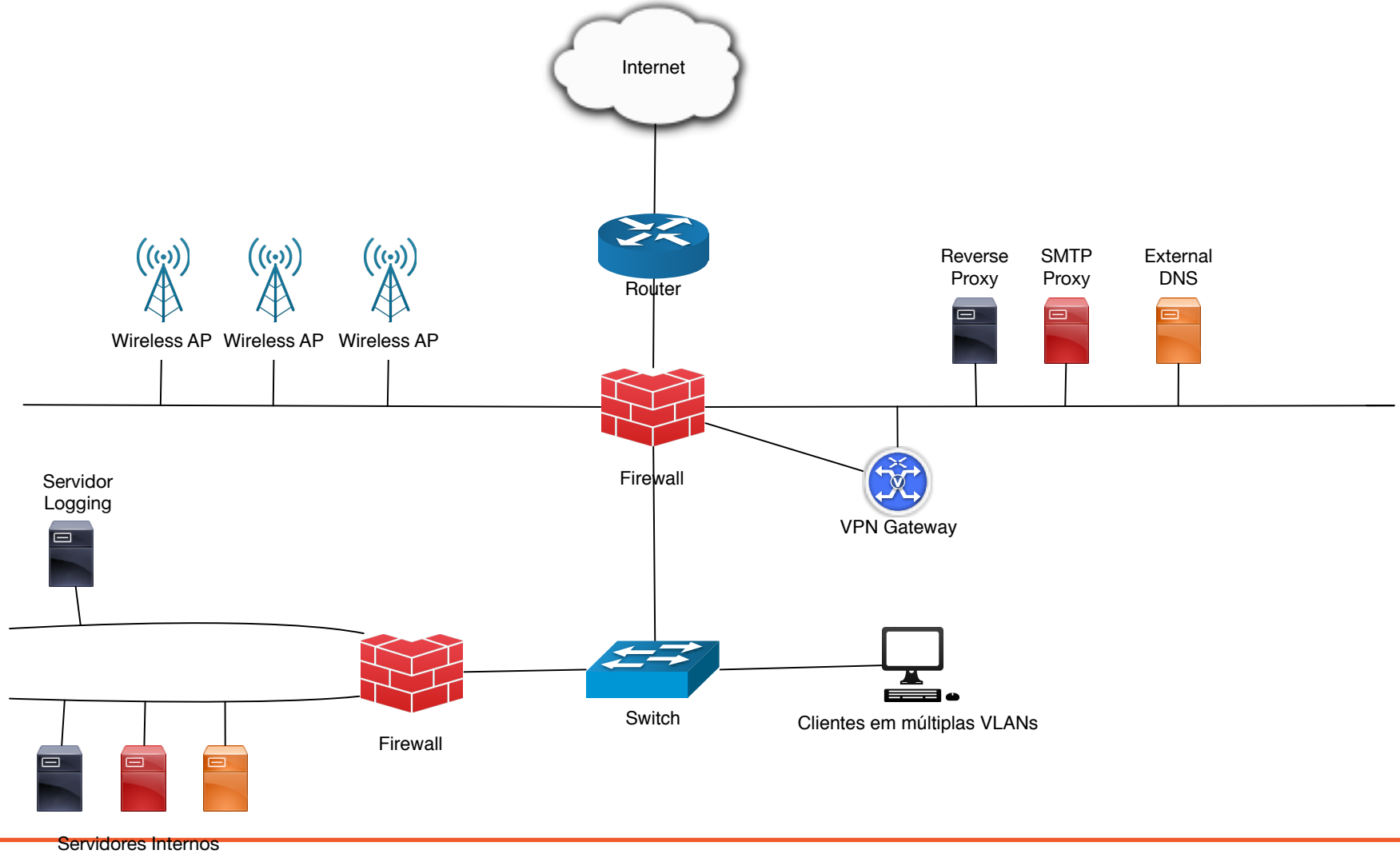
Onde está o perímetro da rede?

- Normalmente é considerado como o “fim” da rede
- Existem ligações a escritórios remotos?
  - A tentativa de acesso pode vir através destes acessos remotos
- Os colaboradores utilizam VPNs?
  - Um PC residencial está exposto à Internet
  - Pode ser usado para entrar na organização através da VPN
- Wireless?
  - As redes sem fios apresentam uma forma de entrada possível

Arquitetura de rede com suporte de VPNs



Segurança por perfis



Manutenção do perímetro

- Desenhar e configurar é a parte mais fácil
- A maior parte dos perímetros falha devido a falta de manutenção
  - Atualizações às *firewalls* e sistemas expostos
  - Auditorias regulares a regras e acessos
  - Auditorias regulares dos sistemas expostos
  - Revisão regular dos registos (*logs*)
  - Falta de alertas
- A manutenção tem de ser incluída no desenho
  - Recursos com necessidade de alertas
  - Automatização de processos
  - Reduz esforços para a manutenção

Técnicas de ataque

- Capturar tráfego (*sniffing*) num ambiente comutado (*switching*)
  - ARP *poisoning*
  - ARP *table flooding*
  - ICMP redirect
- *Port scanning* a partir de uma origem anónima
- Ataques a partir de terceiros
  - Utilizando *proxies* abertos na Internet
- Utilizar um *host* em que se confia (parceiro de negócios)
- É necessário compreender a fundo os protocolos envolvidos para conseguir manter o perímetro seguro

Decoy/Honeypot

- O perímetro de rede pode ser escondido utilizando *decoys* (iscos).
  - Escondem a *firewall*
  - Tornam mais difícil identificar serviços expostos
  - Podem fazer com que servidores ativos parecem estar desligados
  - Não previnem ataques
- A maior parte dos iscos podem ser descobertos
- Mas, a tentativa de os descobrir:
  - Força o atacante a ter mais trabalho
  - Gera mais entradas nos *logs*
  - Permite a descoberta de endereços hostis

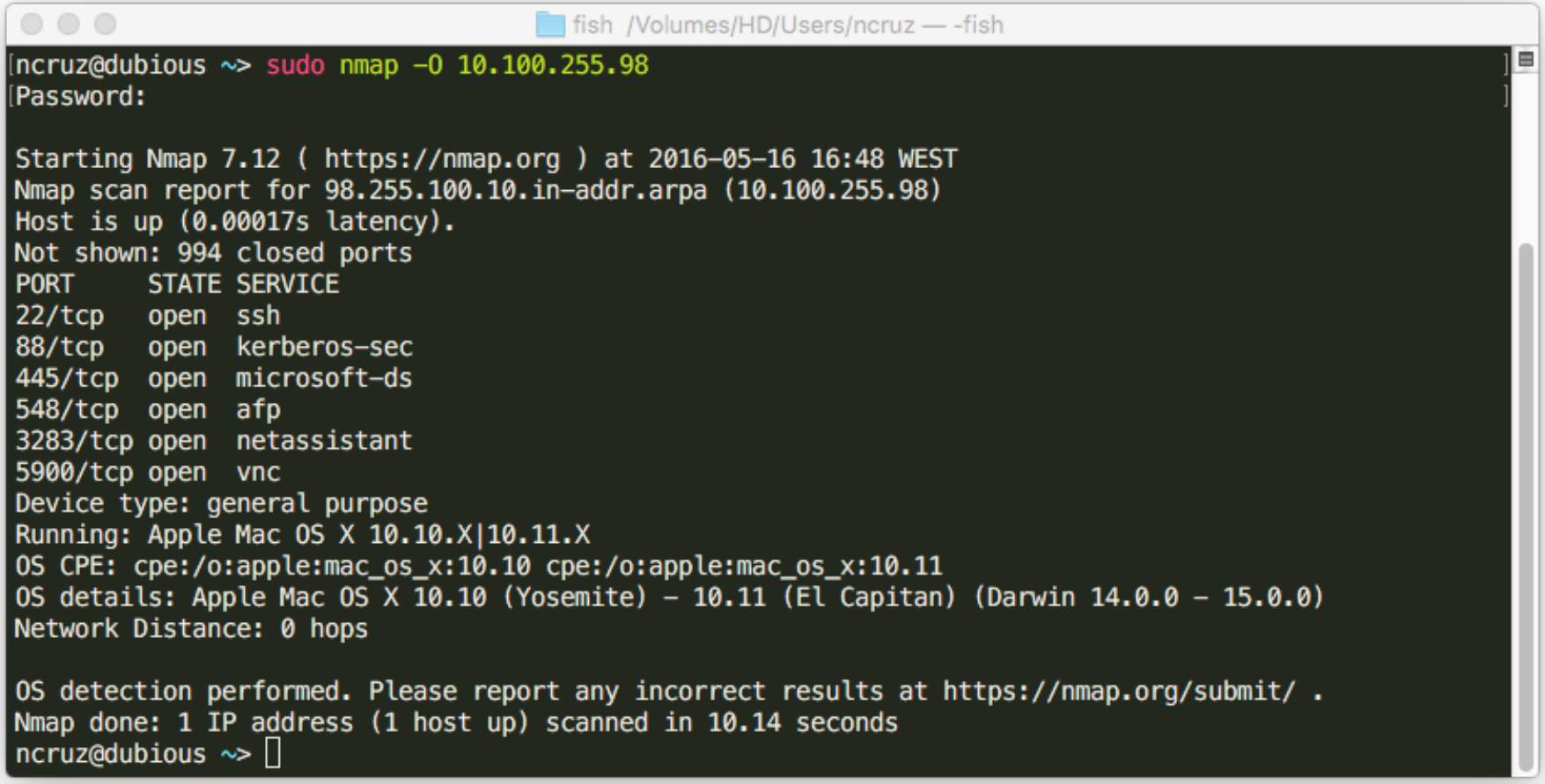
Identificação de sistemas operativos

- Através de análise do tráfego
  - TTL
  - IDENTIFICATION
  - Números de sequência TCP
- Ferramentas
  - nmap

Exploração do perímetro

- nmap
  - *Portscan*
  - Multiplas técnicas de *portscan*
  - Deteção de aplicações e sistemas operativos
  - Utilização de scripts para identificação de vulnerabilidades
- hping3
  - Permite a manipulação dos pacotes enviados com maior detalhe
  - Permite testar a performance da rede
  - Avaliar a implementação da pilha TCP/IP
  - Gerar ICMP Redirects, ou outros pacotes especializados

nmap


fish /Volumes/HD/Users/ncruz — -fish
ncruz@dubious ~> sudo nmap -O 10.100.255.98
Password:
Starting Nmap 7.12 (https://nmap.org) at 2016-05-16 16:48 WEST
Nmap scan report for 98.255.100.10.in-addr.arpa (10.100.255.98)
Host is up (0.00017s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
22/tcp open ssh
88/tcp open kerberos-sec
445/tcp open microsoft-ds
548/tcp open afp
3283/tcp open netassistant
5900/tcp open vnc
Device type: general purpose
Running: Apple Mac OS X 10.10.X|10.11.X
OS CPE: cpe:/o:apple:mac_os_x:10.10 cpe:/o:apple:mac_os_x:10.11
OS details: Apple Mac OS X 10.10 (Yosemite) - 10.11 (El Capitan) (Darwin 14.0.0 - 15.0.0)
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.14 seconds
ncruz@dubious ~>