

**INSTITUTO
FEDERAL**

São Paulo

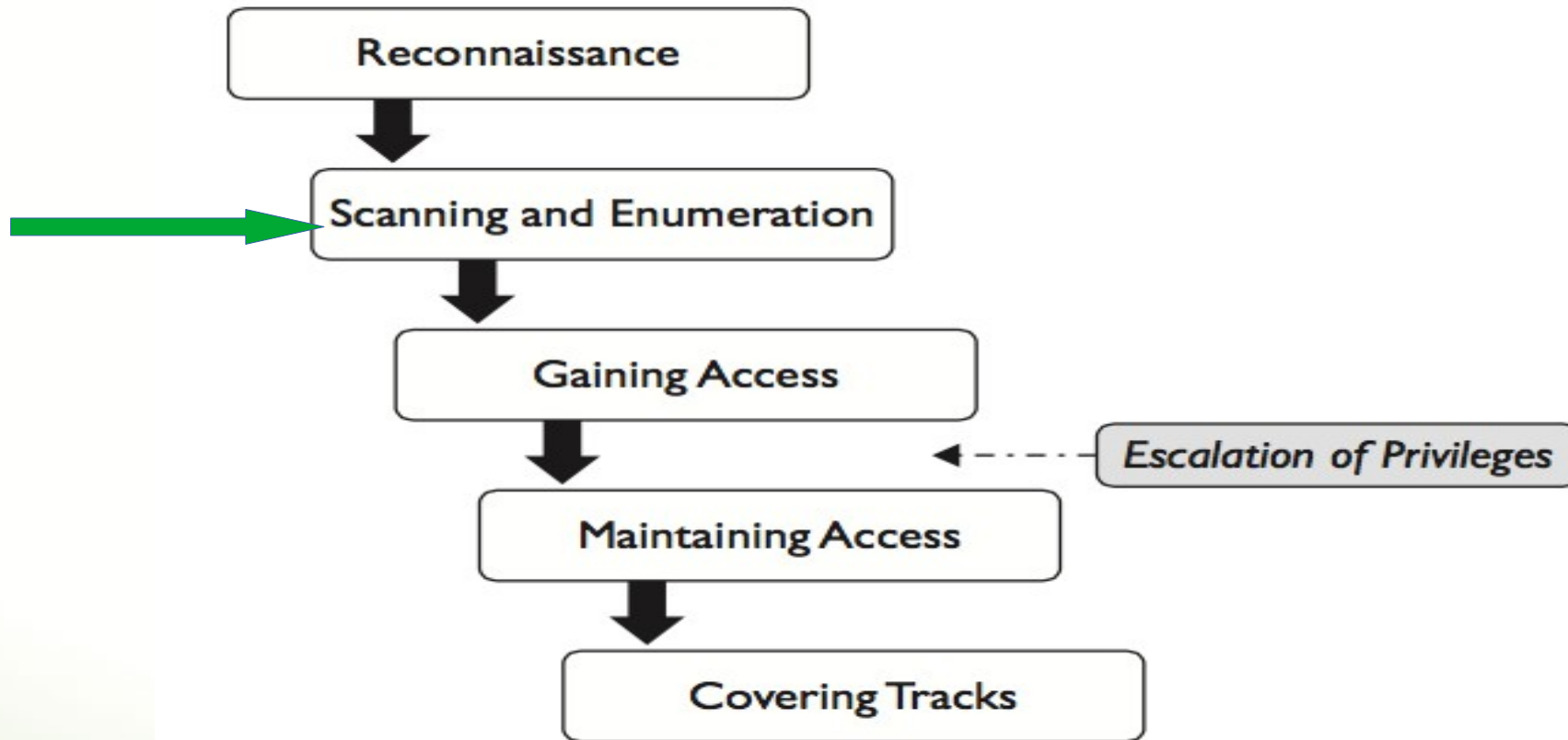
Câmpus
Barretos

Segurança da Informação

Aula 6

Prof. Lucas

Fases



Introdução

- Definição:
 - Especificar individualmente, contar ou nomear um por um.
- Analogia: Conversar com um vizinho na porta!
- Nesta fase move-se de um estado passivo para um ativo
- Após a descoberta das portas abertas, é necessário conhecer se existe compartilhamentos abertos ou informações sobre contas

Técnicas de enumeração - Banner grabbing

- Enumeração visa estimar o que está rodando em uma máquina
- Um dos métodos mais fáceis de enumeração
- Basicamente é enviado uma mensagem para uma porta aberta e olhar a resposta padrão (banner) que será retornado
- Exemplo:
 - telnet <ip_address> 80
 - telnet <ip_address> 25 / 587 (servidor de e-mail)
 - Netcat: (ferramenta poderosa de scan)
 - nc <ip_address> <porta>

Técnicas de Sniffing - Introdução

- Definição:
 - É a arte de capturar pacotes a medida que passam pelo meio físico ou wireless, objetivando capturar informações importantes
 - Alguns protocolos enviam passwords em texto puro!
 -
- 3 princípios básicos
 - Qual estado sua nic (*network interface card*) está;
 - Qual meio físico você tem acesso;
 - Qual ferramenta será executada

Introdução

- Caso sua nic esteja em uma rede cabeada (ethernet), a medida que os bits chegam, é observado o endereço MAC de destino
- Caso este endereço seja o seu, broadcast ou multicast (que você faz parte), a nic irá pegar o frame e passar para o SO processar o restante do dado

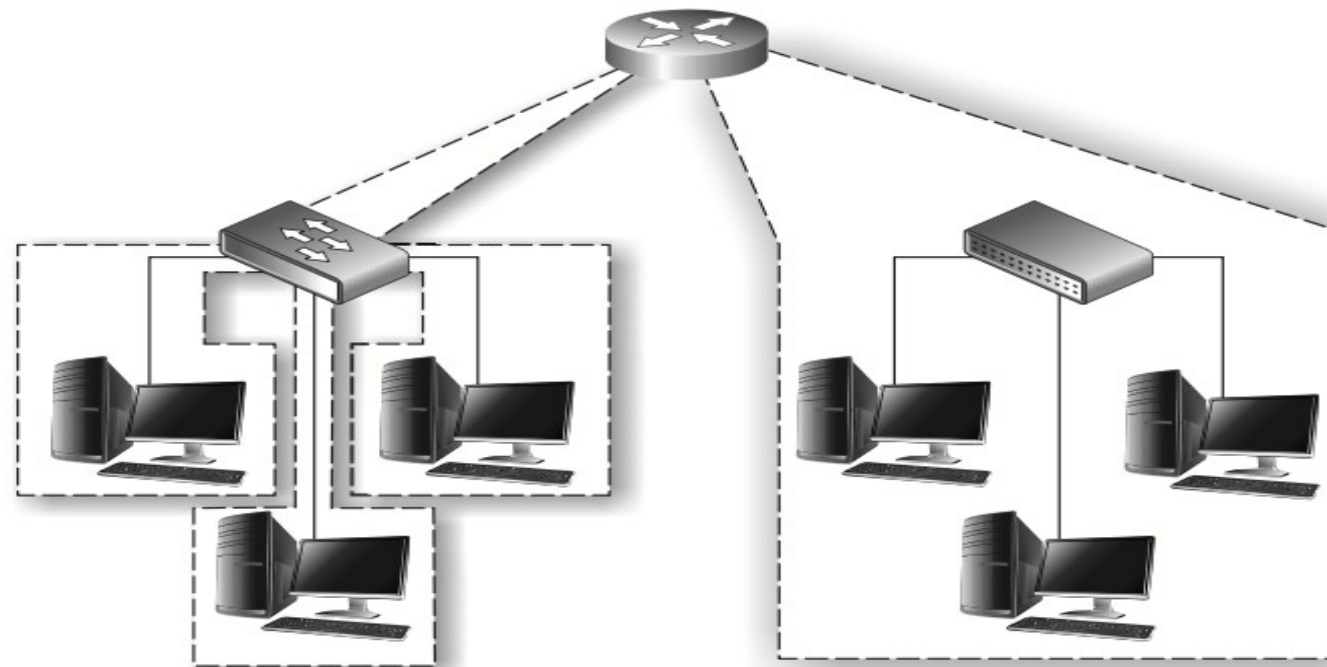
Introdução

- Em situações normais, você só terá acesso aos frames que são endereçados a você.
- Para reverter isto, é utilizado um sniffer que torna sua nic em modo promíscuo (ou modo monitor em redes wireless)
- Isto significa que, independente do endereço de destino, se o frame está passando pelo meio físico, o sniffer solicita a nic para pegar o frame
- No windows, o driver WinPcap é um exemplo de sniffer (libpcap no linux)

Introdução

- Qual meio físico você tem acesso

Se o switch possui para cada interface um domínio de colisão e o mesmo irá endereçar para um único endereço mac, qual a importância do sniffer neste tipo de situação?



A switch splits the collision domain: 4 domains.
An attacker on A can only see traffic intended for A.

Shared media using a hub: 1 collision domain
An attacker on A can see all traffic for B and C.

Protocolos

- SMTP
- TFTP
- SNMP
- POP3
- HTTP

- arp (camada 3)

Protocolos

- Arp (*address resolution protocol*) é o responsável por verificar na sub-rede quem possui o endereço físico relacionado ao IP
- 3 primeiros bytes do endereço físico – mac (24 bits) identificam a organização e o restante do endereço é controlado pela organização para que não exista 2 endereços iguais

Protocolos

- Quando um pacote não é endereçado para sua rede local, o mesmo é encaminhado para o gateway (que também possui um mac)
- O protocolo arp mantém uma tabela em cache dos endereços dos hosts em que houve uma comunicação



Exemplo

- Pingue uma máquina em sua rede
- Digite o comando `arp -a`
- Digite o comando `netsh interface ip delete arpcache`

ARP

- Como usar tal tipo de informação?
- Um host em sua rede irá construir os frames e enviá-los baseando-se na tabela arp
- E se alterarmos o gateway default de toda a rede para a nossa máquina?

Sniffing ativo e passivo

- Sniffing passivo: ativar sem nenhuma outra interação ou ação. Funciona apenas se sua nic fizer parte do mesmo domínio de colisão (hub)
- Sniffing ativo: Requer um trabalho adicional de sua parte. Você deve fazer parte do mesmo domínio de colisão. Em geral, ataca-se o switch.

Sniffing ativo e passivo

- Técnicas de sniffing ativo:
- span port **ou** port mirroring
- Mac Flooding
- Mac spoofing
- Arp poisoning
- Port security

Arp poisoning

- Processo de atacar o cache de uma máquina alterando os registros da tabela arp (broadcast)
- Switches modernos e ferramentas de monitoração conseguem identificar este tipo de ataque
- Alguns administradores travam o mac do gateway (arp -s) para ficarem permanentemente nos hosts
- Ferramentas:
 - Ethercap
 - Cain and abel
 - WINARPAtdacker
 - Ufasoft
 - dnsiff

Arp poisoning

Tabela arp da vítima

Mac do gateway: 00-10-f3-32-fc-6a

```
C:\Users\Administrador>arp -a

Interface: 172.18.0.2 --- 0x10
Endereço IP      Endereço físico      Tipo
172.18.0.3        00-40-a7-1b-91-9f    dinâmico
172.18.0.15       00-40-a7-1b-93-16    dinâmico
172.18.0.24       ce-3d-01-71-ef-46    dinâmico
172.18.0.25       62-bc-ed-8c-13-ac    dinâmico
172.18.0.30       00-10-f3-32-fc-6a    dinâmico
172.18.0.31       ff-ff-ff-ff-ff-ff    estático
224.0.0.22        01-00-5e-00-00-16    estático
224.0.0.252       01-00-5e-00-00-fc    estático
239.255.255.250   01-00-5e-7f-ff-fa    estático
255.255.255.255   ff-ff-ff-ff-ff-ff    estático

Interface: 192.168.56.1 --- 0x11
Endereço IP      Endereço físico      Tipo
192.168.56.255   ff-ff-ff-ff-ff-ff    estático
224.0.0.22        01-00-5e-00-00-16    estático
224.0.0.252       01-00-5e-00-00-fc    estático
239.255.255.250   01-00-5e-7f-ff-fa    estático

C:\Users\Administrador>arp -a
```

Arp poisoning

Após o ataque

Mac do gateway alterado para: 00-40-a7-1b-91-9f

```
Administrator: Prompt de Comando
239.255.255.250      01-00-5e-7f-ff-fa      estático
C:\Users\Administrador>arp -a
Interface: 172.18.0.2 --- 0x10
Endereço IP      Endereço físico      Tipo
172.18.0.3        00-40-a7-1b-91-9f    dinâmico
172.18.0.15       00-40-a7-1b-93-16    dinâmico
172.18.0.24       ce-3d-01-71-ef-46    dinâmico
172.18.0.25       62-bc-ed-8c-13-ac    dinâmico
172.18.0.30       00-40-a7-1b-91-9f    dinâmico
172.18.0.31       ff-ff-ff-ff-ff-ff    estático
224.0.0.22        01-00-5e-00-00-16    estático
224.0.0.252       01-00-5e-00-00-fc    estático
239.255.255.250   01-00-5e-7f-ff-fa    estático
255.255.255.255   ff-ff-ff-ff-ff-ff    estático
Interface: 192.168.56.1 --- 0x11
Endereço IP      Endereço físico      Tipo
192.168.56.255    ff-ff-ff-ff-ff-ff    estático
224.0.0.22        01-00-5e-00-00-16    estático
224.0.0.252       01-00-5e-00-00-fc    estático
239.255.255.250   01-00-5e-7f-ff-fa    estático
C:\Users\Administrador>
```

Arp poisoning

Mac do atacante: 00-40-a7-1b-91-9f

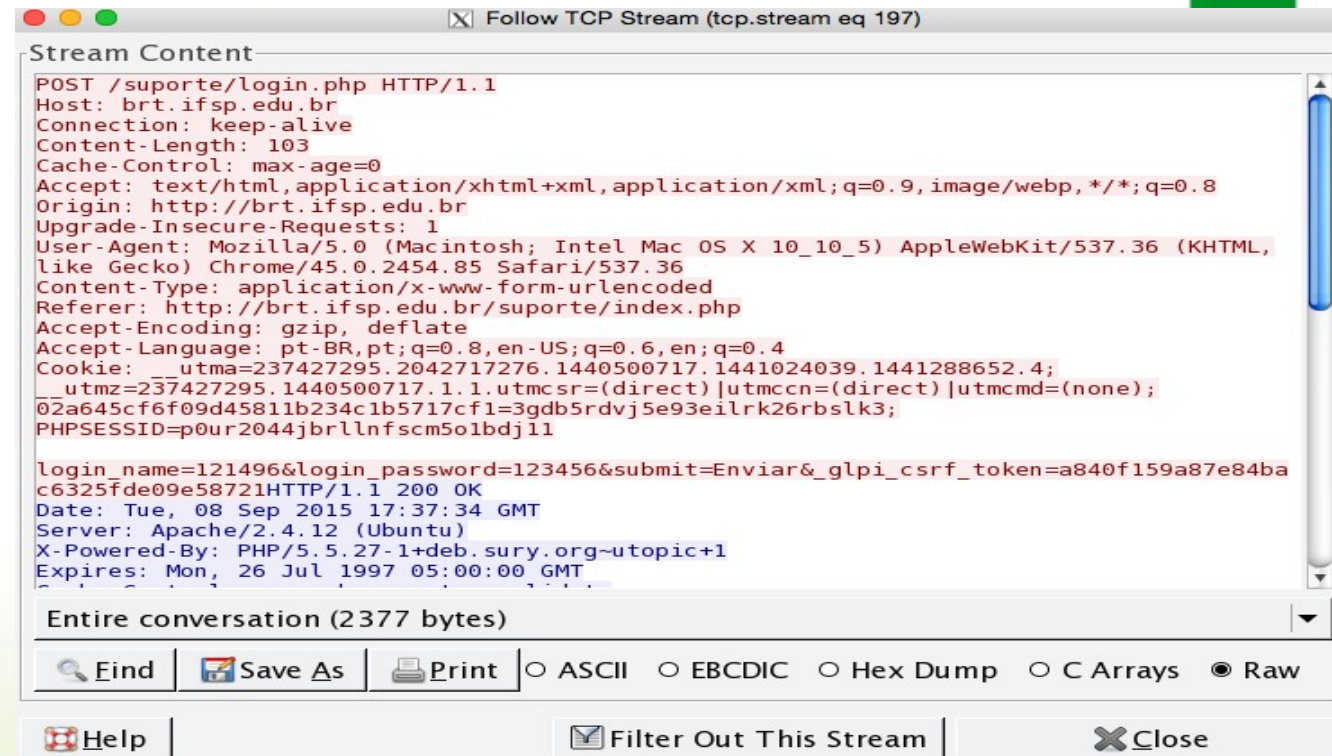
```
Administrador: C:\Windows\system32\cmd.exe

Sufixo DNS específico de conexão. . . . . : brt.ifsp.local
Descrição . . . . . : NIC Gigabit Ethernet PCI-E Realtek
Família RTL8168C(P)/8111C(P) (NDIS 6.20)
Endereço Físico . . . . . : 00-40-A7-1B-91-9F
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . : Sim
Endereço IPv6 de link local . . . . . : fe80::898f:10cb:1e96:e0ef%16(Preferencial)
Endereço IPv4. . . . . : 172.18.0.3(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.224
Concessão Obtida. . . . . : terça-feira, 8 de setembro de 2015 19:20:51
Concessão Expira. . . . . : quarta-feira, 9 de setembro de 2015 07:20:51
Gateway Padrão. . . . . : 172.18.0.30
Servidor DHCP . . . . . : 172.18.0.24
ID de DHCPv6 . . . . . : 352338087
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-1A-5F-3D-C7-44-87-FC-31-D2-A6
Servidores DNS. . . . . : 172.18.0.25
                          192.168.200.3
NetBIOS em Tcpip. . . . . : Habilitado

Adaptador Ethernet VirtualBox Host-Only Network:
```

Exercício

- Faça o ataque de arp poisoning em uma máquina
- Verifique se o mac do gateway foi alterado
- Tente capturar uma senha em um acesso http ou telnet.



Follow TCP Stream (tcp.stream eq 197)

Stream Content

```
POST /suporte/login.php HTTP/1.1
Host: brt.ifsp.edu.br
Connection: keep-alive
Content-Length: 103
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://brt.ifsp.edu.br
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.85 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://brt.ifsp.edu.br/suporte/index.php
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: __utma=237427295.2042717276.1440500717.1441024039.1441288652.4; __utms=237427295.1440500717.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); 02a645cf6f09d45811b234c1b5717cfl=3gdb5rdvj5e93eilrk26rbslk3; PHPSESSID=p0ur2044jbrllnfscm5o1bdjl1

login_name=121496&login_password=123456&submit=Enviar&glpi_csrf_token=a840f159a87e84bac6325fde09e58721HTTP/1.1 200 OK
Date: Tue, 08 Sep 2015 17:37:34 GMT
Server: Apache/2.4.12 (Ubuntu)
X-Powered-By: PHP/5.5.27-1+deb.sury.org~utopic+1
Expires: Mon, 26 Jul 1997 05:00:00 GMT
```

Entire conversation (2377 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

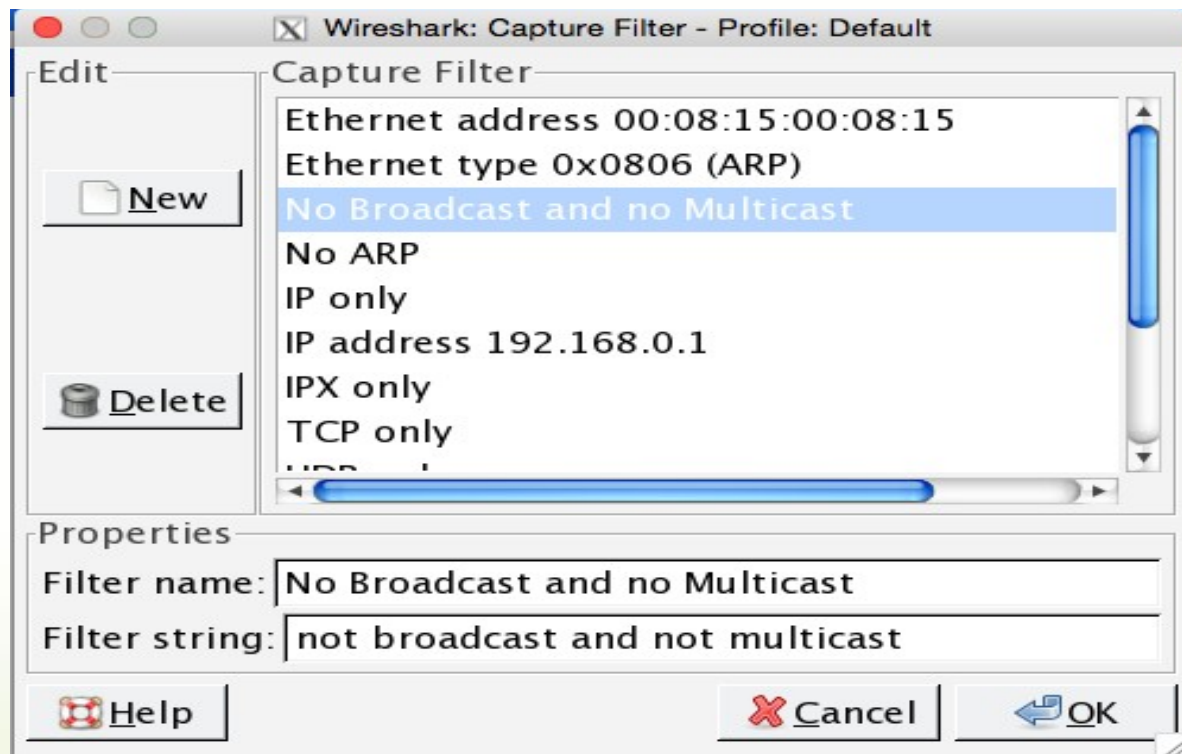
Help Filter Out This Stream Close

Dicas Wireshark

- Filtros:
 - ip.src == 192.168.1.100
 - ip.addr == 192.168.1.150
 - host 192.168.1.102
 - net 192.168.1.0/24
 - port 80
 - tcp.flags == 0x2
 - tcp.flags == 0x16
 - tcp.flags == 0x18
- Obs.: FIN = 1; SYN = 2; RST = 4; PSH = 8; ACK = 16; URG = 32

Wireshark

- Follow TCP Stream



Ferramentas de sniffing

- Wireshark
- Ettercap
- EtterPeek
- Snort
- Tcpdump
- Windump
- WinSniffer

Exercícios

- Responder o questionário disponível no moodle