INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Tato inovace předmětu Analýza dat je spolufinancována Evropským sociálním fondem a Státním rozpočtem ČR, projekt č. CZ.1.07/2.2.00/28.0014, "Interdisciplinární vzdělávání v ICT s jazykovou kompetencí".

Analýza paketů - metody a nástroje

Analýza dat

Bc. Filip Pávek

Ústav informatiky
Filozoficko-přírodovědecká fakulta
Slezská univerzita v Opavě

filippavek@gmail.com

2012

Obsah prezentace

Co nového se naučíme?

- Odpovíme na otázky: Co je analýza paketů? Kdy můžeme analýzu paketů použít? Jak analýzu paketů provádět?
- Než můžeme začít něco analyzovat a dělat závěry, musíme nejdříve nějaký tok dat zachytit - prozkoumáme tedy metody zachycení toku dat v síťi (přes rozbočovač, přepínač (SPAN, RSPAN)).
- U SPAN a RSPAN si ukážeme konfigurace.
- Řekneme si o nástrojích prostřednictvím kterých lze síťový traffic zachytit a interpretovat.
- Podrobně o paket snifferu Wireshark.

Obsah prezentace

Co nového se naučíme?

- Vysvětlíme si základní principy nejběžnějších síťových útoků, navrhneme vhodné zabezpečení a za použití nástroje Cain & Abel demostrujeme útok ARP Spoofing.

V průběhu cvičení budeme vše prakticky testovat na reálném síťovém zařízení a běžných příkladech z praxe.

Analýza paketů

- Mezi používané anglické ekvivalenty patří Packet (Protocol) Analysis nebo Packet Sniffing.
- Představuje zachycení a interpretaci síťového provozu.
- Odpovídá na otázky co se děje na síti.
- Př. Kdo je na síti, co dělá, jaké používá zdroje, kdo s kým komunikuje, co zatěžuje naší síť, identifikuje slabá místa sítě, pomáhá odhalit útočníky a jejich zlomyslné aktivity, ...
- V reálném síťovém provozu slouží analýza paketů především k odhalení nestadartně se chovájících aplikací (př. konflikt DHCP serveru) nebo ověření konfigurace aktivních síťových prvků. Odhalení útočníka může být jeden z výsledků.
- Abychom mohli tento typ analýzy provést musíme použít některý z nástrojů kategorie Packet Sniffer (Wireshark, TCPdump, ...).

Packet Sniffer

Před výběrem vhodného nástroje je nutné se zamyslet nad několika fakty. Co chceme s nástrojem analyzovat (podporované protokoly)? Jaké jsou naše znalosti? Cena nástroje? Podpora OS? ...

Obecná charakteristika

- Nástroj umožňuje zachytit „surový“ raw síťový provoz a následně ho interpretovat - vidíme komunikaci na úrovni paketů.
- Existují komerční i volně dostupné nástroje.
- Různě uživatelsky příjemná prostředí (GUI - Wireshark, příkazová řádka - TCPdump).
- Nástroje pracují pod OS Windows nebo Linux (nebo obojí - Wireshark).
- Běžné protokoly jako ARP, DNS, DHCP jsou v nástroji podporovány vždy u netradičních protokolů to tak být nemusí.

Co k odposlouchávání potřebujeme?

- Stanici na které budeme zachytávat síťový provoz.
- Námi zvolený packet sniffer nástroj - Wireshark.
- Může se hodit přímý Ethernet kabel a hub (viz. dále).
- NIC (Network Interface Card) s podporou promiskuitního režimu (promiscuous mode).

Chování NIC s vypnutým promiskuitním režimem

Síťový provoz, který není určen pro stanici, je na základě L2 informací v hlavičce rámce zahozen (ARP broadcast). Otázka: Na které vrstvě OSI modelu je zastaven update protokolu RIPv1 na PCs v LAN pokud není nastaven passive-interface na routeru?

Chování NIC se zapnutým promiskuitním režimem

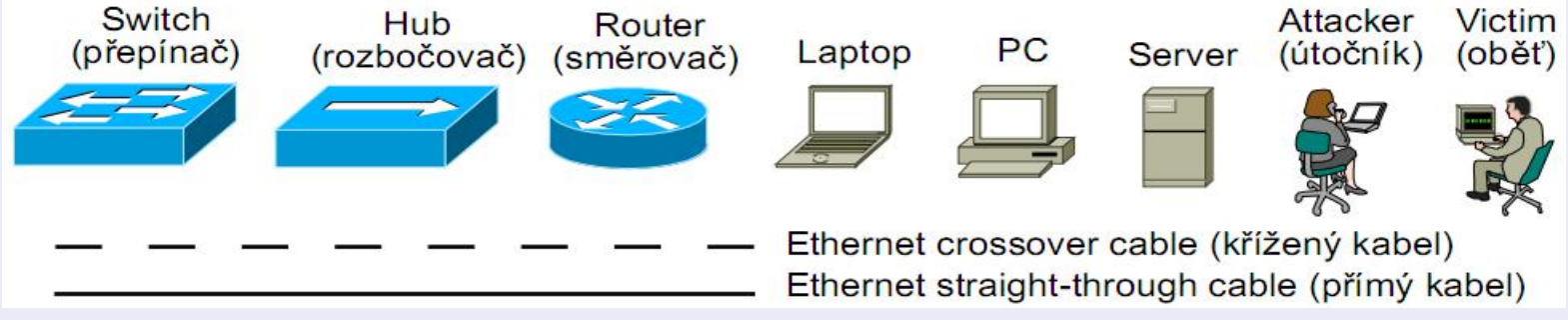
Igonoruje info v L2 hlavičce a zachytí tak veškerý síťový provoz.

Metody odposlouchávání

Rozdíly dle prostředí

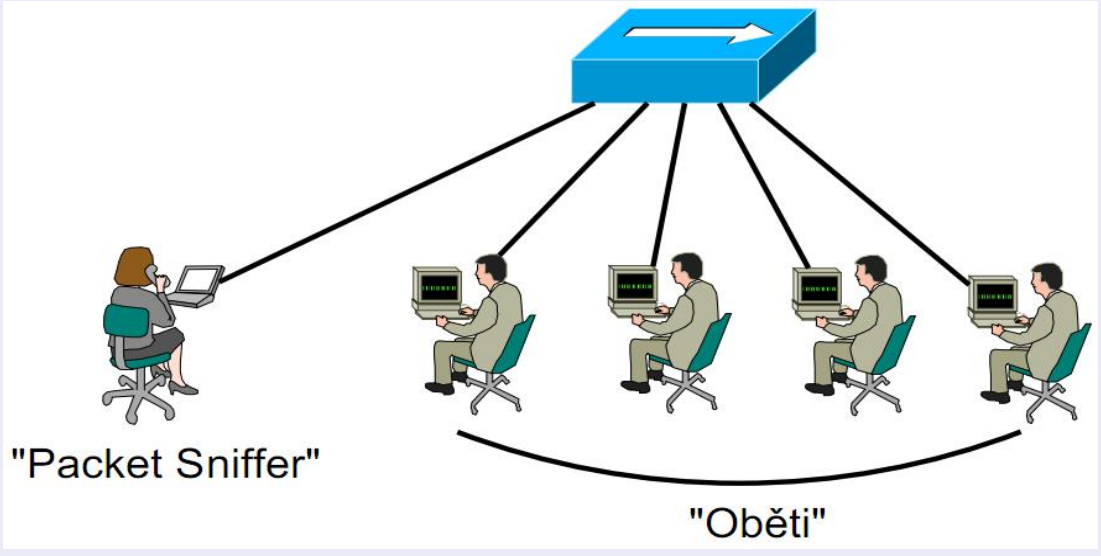
- Již jsme zopakovali chování rozbočovače a přepínače. Známe tedy jejich vnitřní pracovní logiku. Toho využijeme při naslouchouní na síti.
- Koncoví uživatelé propojeni přes rozbočovač nebo přepínač.
- Uvědomujete si již nyní zásadní rozdíl při naslouchání na zařízení hub a switch?
- Jak by jste řešili odposlouchávání na switchi (viz.dále)?

Ikony používané v diagramech



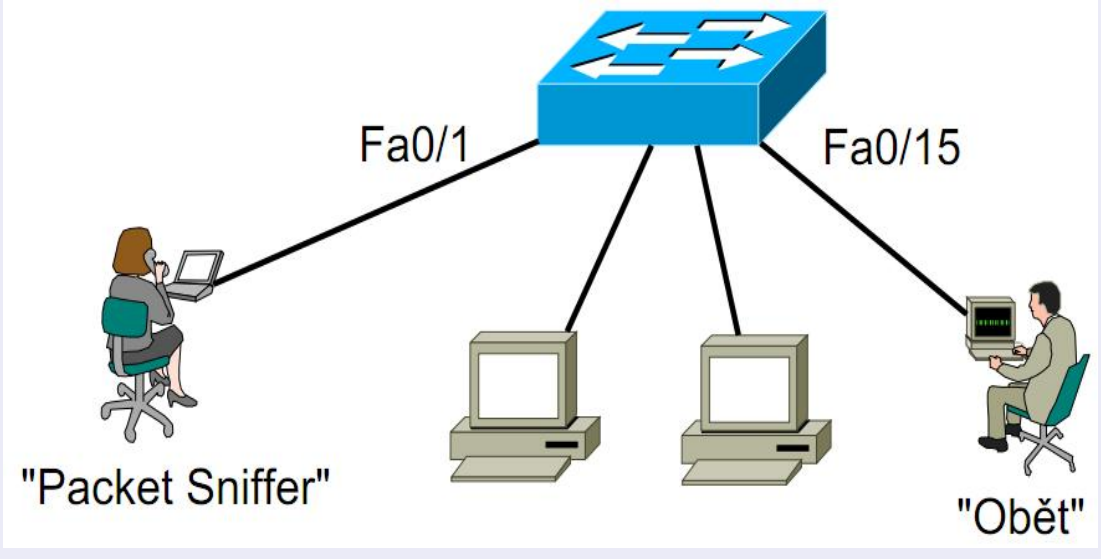
Použití rozbočovače k odposlouchávání

- Chová se jako klasický repeater - opakovač.
- Nejideálnější prostředí pro odposlouchávání (moc neuvidíte).
- Je-li našim cílem koncoví host, stačí připojit stanici do volného portu na daném rozbočovači a zapnout packet sniffer.
- Packet Sniffer představuje stanici na které zachycujeme odposlechnutý provoz (admin). Oběť - cíl odposlouchávání.



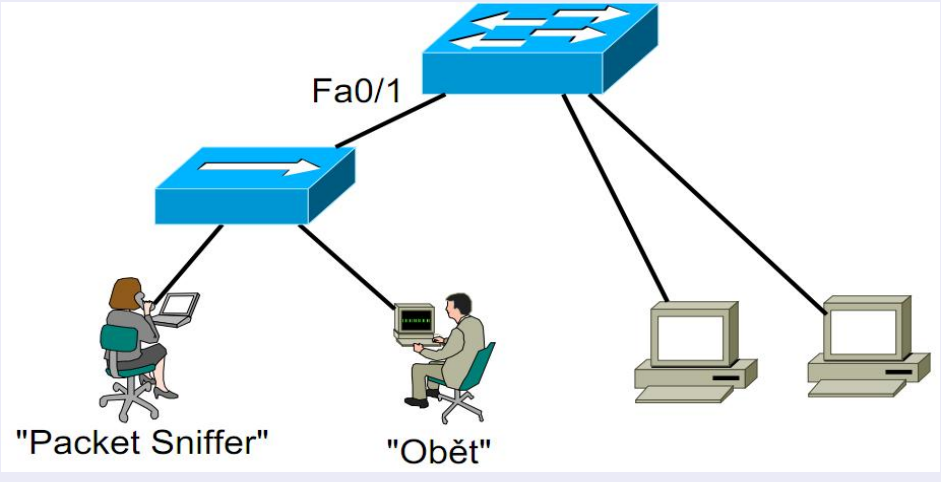
Použití přepínače k odposlouchávání

- Uživatelé jsou připojeny do sítě přes switch.
- Zopakujeme-li příklad zobrazený níže pak útočník uvidí pouze svůj síťový provoz a broadcast (Kdy to neplatí?).
- Chceme-li zjistit, co vysílá „obět“ na portu Fa0/15 je potřeba použít jiná „kouzla“ než jen vše propojit a odposlouchávat.
- Co je MAC Address Flooding? Princip a zabezpečení?



Odposlouchávání za pomoci rozbočovače v prostředí přepínačů

- Ideální v případě, kdy switch nepodporuje zcadlení portů.
- Koncového uživatele, původně připojeného do portu Fa0/15, propojíme přes rozbočovač s PC na kterém běží paket analyzátor.
- Samozřejmě musíme mít fyzický přístup k zařízením.
- Pozor na nastavenou L2 port securitu.



Kontrola konfigurace před zahájením činnosti

Výpis konfigurace portu Fa0/1 na Cisco Catalyst 2960

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky f04d.a2eb.5993
```

Výpis stavu zabezpečení na portu Fa0/1na Cisco Catalyst 2960

```
Switch#sh port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : f04d.a2eb.5993:10
Security Violation Count   : 0
```

```
Switch#sh port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : f04d.a2eb.d2a3:10
Security Violation Count   : 1
```

Zrcadlení portu - Port Mirroring

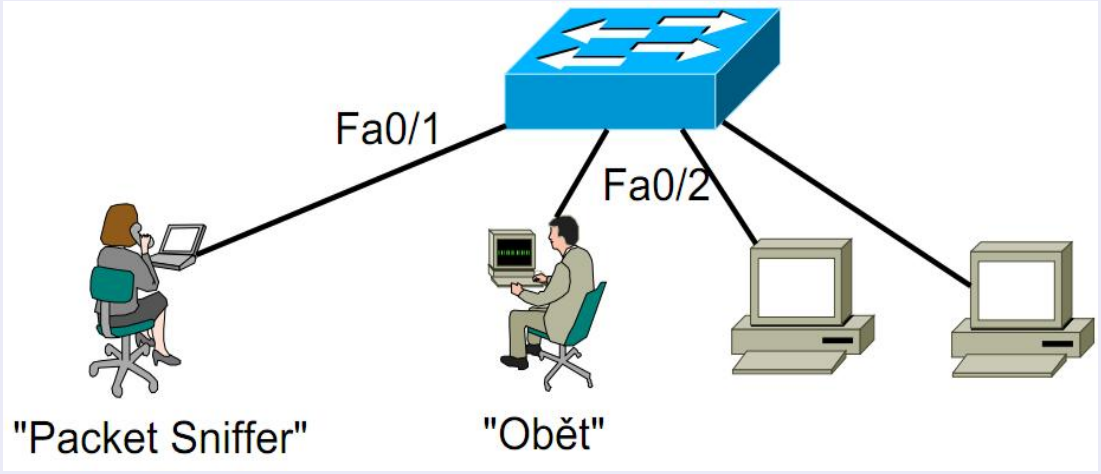
Základní charakteristika

- Jinak také Switched Port Analyzer (SPAN).
- Slouží ke kopírování síťového provozu z VLAN, portu nebo portů na vybraný port.
- Umožňuje vidět co přichází/odchází/obojí na port.
- Nutný přístup do příkazové řádky zařízení - konfigurace.
- Ověřit podporu zrcadlení na zařízení u výrobce.
- Pozor na situaci, kdy chcete zrcadlit port s velkým množstvím trafficu (trunk port). Port, kde je připojený packet sniffer nemusí stíhat „odbavovat“ všechny pakety a bude je zahazovat.
- Př. Zdroj trunk port 10Gbps skrz který jde 100 VLANs a cíl 10Mbps port.
- Velmi důležité a používané při troubleshootingu.

SPAN

Základní charakteristika

- Podmínka: zdroj (koho chceme odposlouchávat) a cíl (kam chceme traffic zrcadlit) musí být v rámci stejného zařízení.
- Na přepínači potřebujeme vždy jeden volný port pro připojení laptopu s analyzátorem.
- Zdroj, který chceme odposlouchávat je připojen do portu Fa0/2 a cíl, kam chceme zrcadlit traffic je na portu Fa0/1.



SPAN - konfigurace na Cisco Catalyst 2960

Konfigurace SPAN

- Vytvoříme jednu monitorovací session pro zdroj i cíl.

```
Switch(config)#monitor session 1 source interface fastEthernet 0/2
Switch(config)#monitor session 1 destination interface fastEthernet 0/1
```

Bližší specifikace zdroje zrcadlení v onfiguraci SPAN

```
Switch(config)#monitor session 1 source interface fastEthernet 0/1 ?
  ,      Specify another range of interfaces
  -      Specify a range of interfaces
  both   Monitor received and transmitted traffic
  rx     Monitor received traffic only
  tx     Monitor transmitted traffic only
```

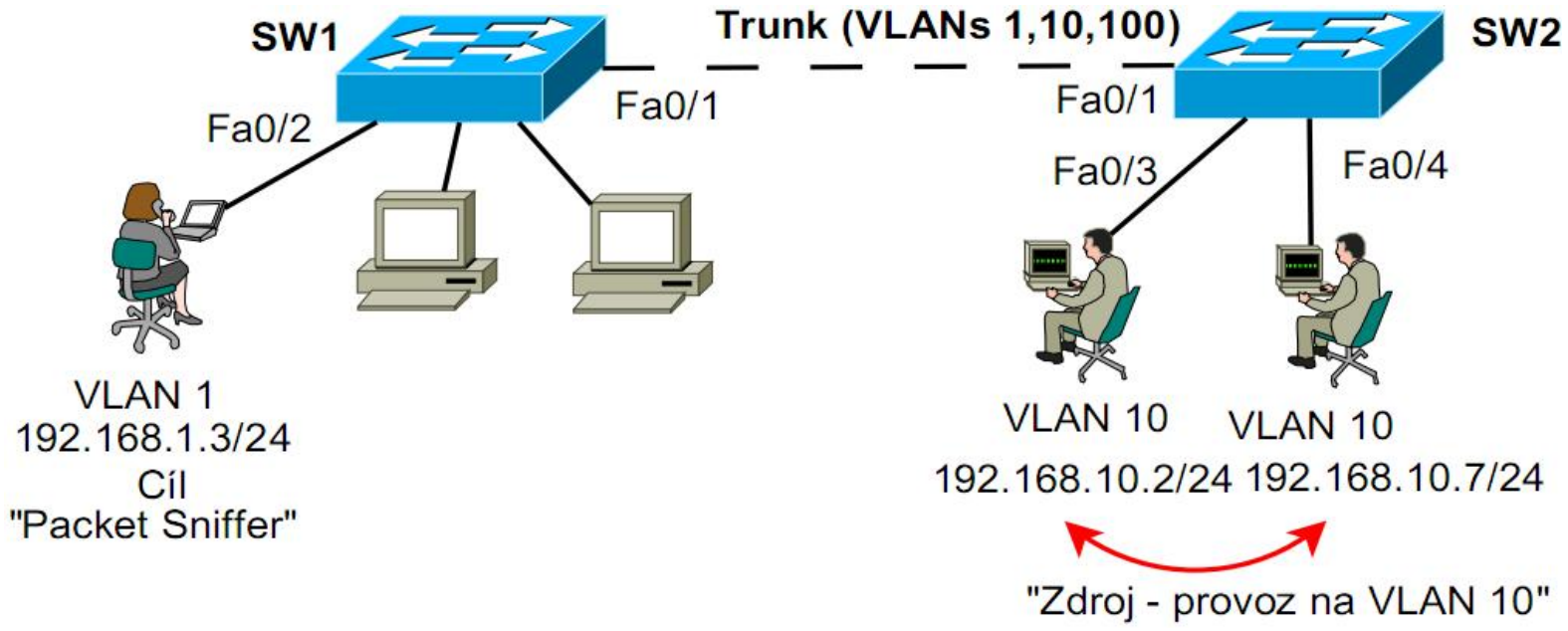
Výpis aktuální konfigurace SPAN

```
Switch#show monitor session 1
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Fa0/2
Destination Ports      : Fa0/1
    Encapsulation      : Native
          Ingress      : Disabled
```

Remote SPAN

Základní charakteristika

- Má stejné vlastnosti jako SPAN + rozšíření.
- Rozdíl: zdroj a cíl nejsou na stejném zařízení.
- Zdroj (koho monitorujeme) představují hosté na SW2 v VLAN10 a cíl (packet sniffer) je na SW1 port Fa0/2 VLAN1.



Remote SPAN - konfigurace na Cisco Catalyst 2960

remote-span VLAN

- Vyžaduje vytvořit remote-span VLAN, která bude sloužit pro přenos monitorovaného provozu.
- Remote-span VLAN musí být na všech přepínačích, přes které budeme posílat ze zdroje do cíle monitorovací traffic.
- Remote-span konfigurujeme na všech přepínačích ručně nebo na VTP serveru (pokud VTP používáme).

Vytvoření remote-span VLAN na SW1 a SW2

```
SW1(config)#vlan 100
SW1(config-vlan)#name 100
SW1(config-vlan)#remote-span
SW1(config-vlan)#exit
```

```
SW2(config)#vlan 100
SW2(config-vlan)#name 100
SW2(config-vlan)#remote-span
SW2(config-vlan)#exit
```

Remote SPAN - konfigurace na Cisco Catalyst 2960

- Při RSPAN vytváříme DVĚ monitorovací session.

Zdrojová session na SW2

- Na SW2 určíme, že chceme monitorovat celou VLAN10 a vytvoříme zdrojovou session s číslem 2. Cíl představuje VLAN 100 (remote-span). Pozor, u Cisco Catalyst 2950 je nutné za druhý příkaz přidat klíčové slovo reflector-port

```
SW2(config)#monitor session 2 source vlan 10
SW2(config)#monitor session 2 destination remote vlan 100
```

Cílová session na SW1

- Cílová session 3 si jako zdroj bere obsah remote span VLAN 100 a posílá ho na port FA0/2, kde je zapojený packet sniffer.

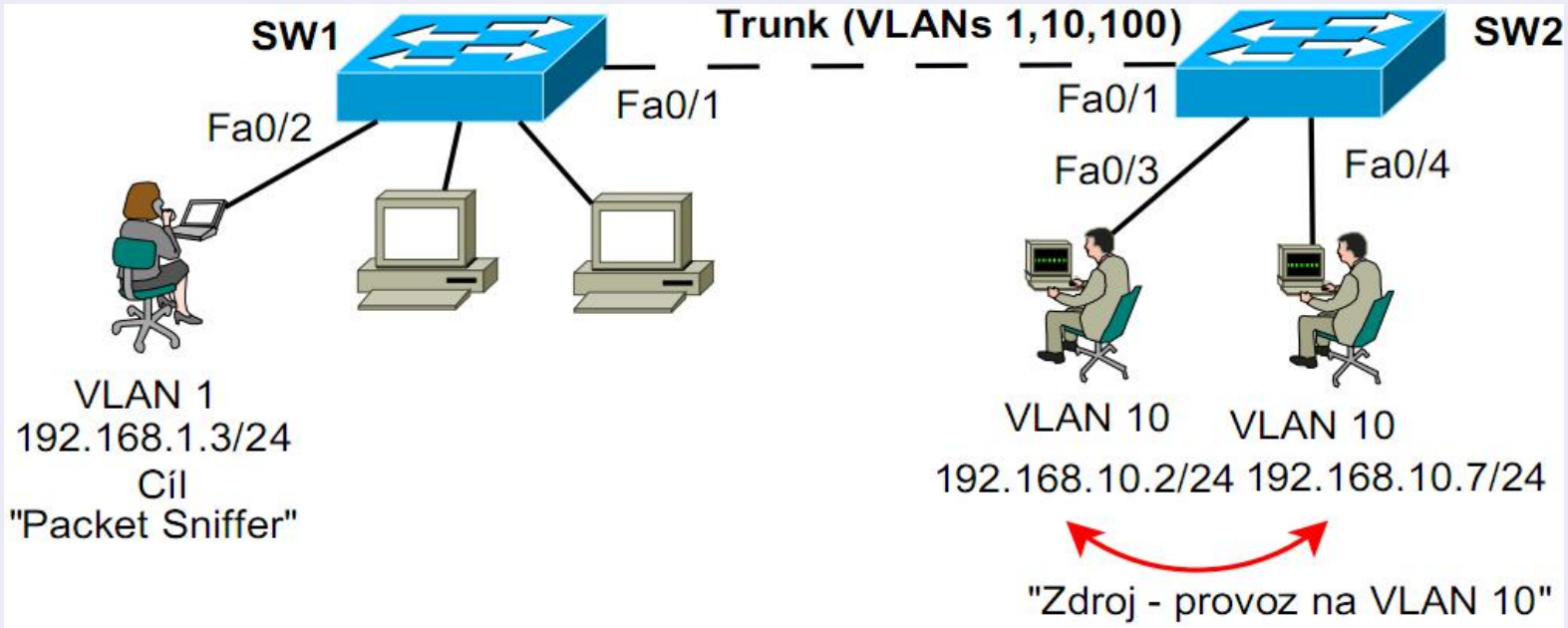
```
SW1(config)#monitor session 3 source remote vlan 100
SW1(config)#monitor session 3 destination int fast 0/2
```

Remote SPAN - ověření konfigurace

#show monitor session „číslo“

```
SW1#sh monitor session 3
Session 3
---------
Type                   : Remote Destination Session
Source RSPAN VLAN      : 100
Destination Ports      : Fa0/2
    Encapsulation      : Native
          Ingress      : Disabled
```

```
SW2#show monitor session 2
Session 2
---------
Type                   : Remote Source Session
Source VLANs           :
    Both               : 10
Dest RSPAN VLAN        : 100
```

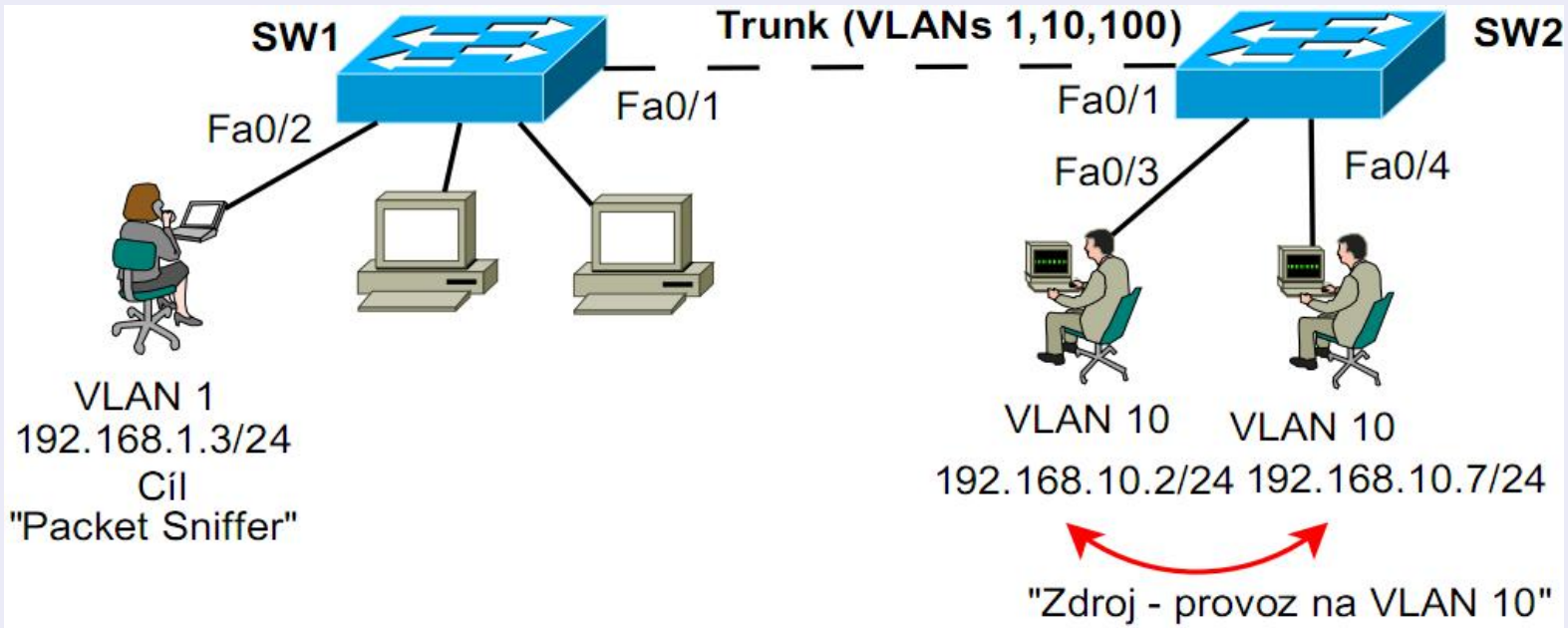


Ověření RSPAN pomocí nástroje Wireshark

Provoz VLAN10 zachycený na portu Fa0/2 přepínače SW1

No.	Time	Source	Destination	Protocol	Length	Info
13	14:31:31.694377	192.168.10.7	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=128
14	14:31:31.694392	192.168.10.7	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=128
15	14:31:32.698416	192.168.10.2	192.168.10.7	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128
16	14:31:32.698418	192.168.10.2	192.168.10.7	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128
17	14:31:32.698527	192.168.10.7	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=128
18	14:31:32.698528	192.168.10.7	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=128
19	14:31:33.712385	192.168.10.2	192.168.10.7	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128
20	14:31:33.712387	192.168.10.2	192.168.10.7	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128

Topologie sítě



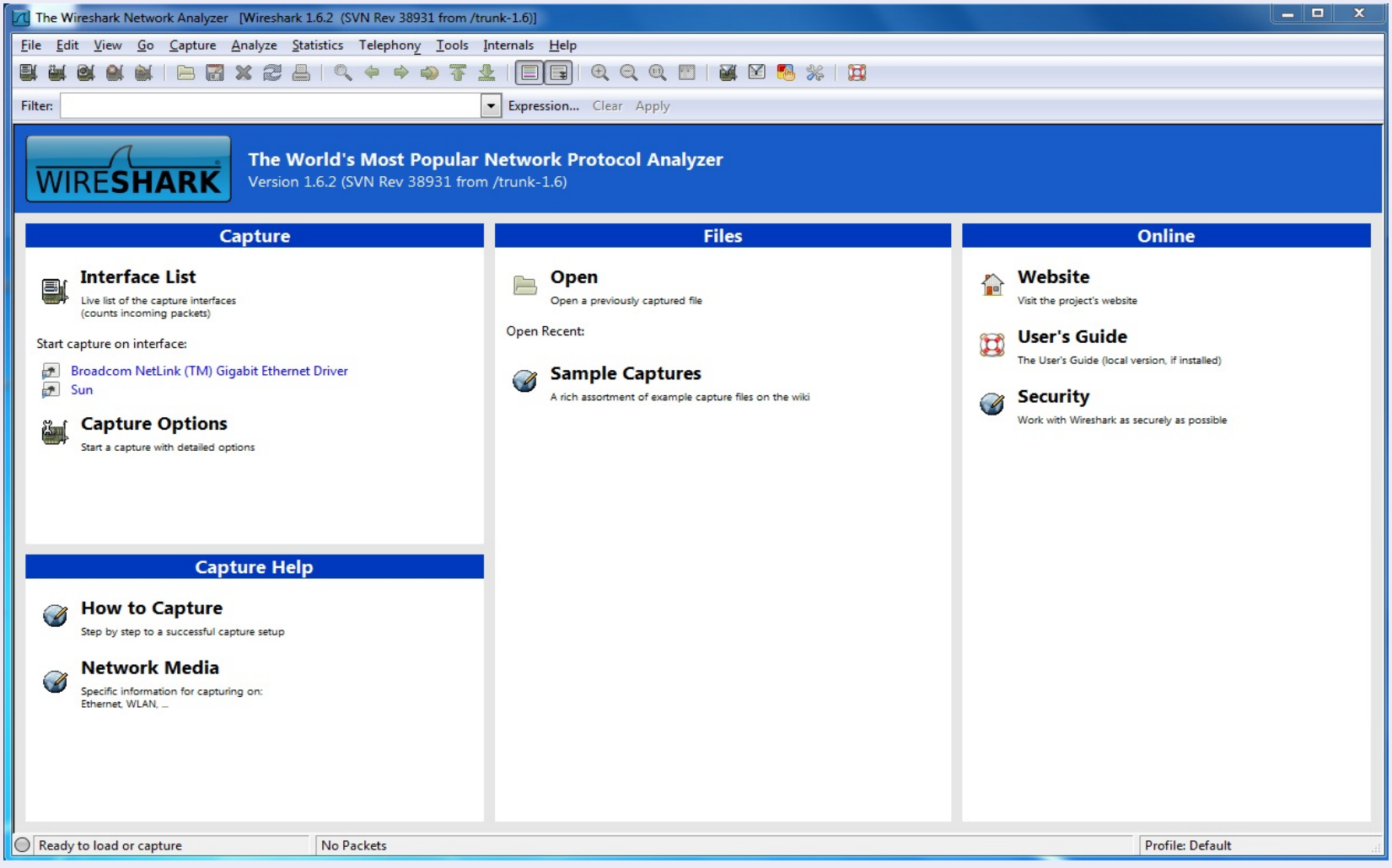
O programu Wireshark

Základní charakteristika

- 1. místo v Top Network Security Tools (http://sectools.org/),
- open-source nástroj k analýze a monitorování provozu sítě,
- nástupce nástroje Ethereal, podpora stovek protokolů,
- možný zásah do kódu, použití pro osobní i komerční účely,
- Wireshark najdete na každém Forensic Live CD,
- díky GUI velmi snadný a intuitivní na ovládání,
- ideální pokud začínáme s monitorováním a analýzou provozu,
- podporován pod OS Windows i Linux, minimální HW nároky,
- nástroj lze stáhnout na (http://www.wireshark.org/),
- triviální instalace na OS Windows (WinPcap je součástí instalačky)/OS Linux dle distribuce,
- TcpDump(http://www.tcpdump.org/) sniffer v příkazové řádce.

Poprvní spuštění nástroje Wireshark

Uvítací plocha, která nijak nevítá :-) Začínáme...

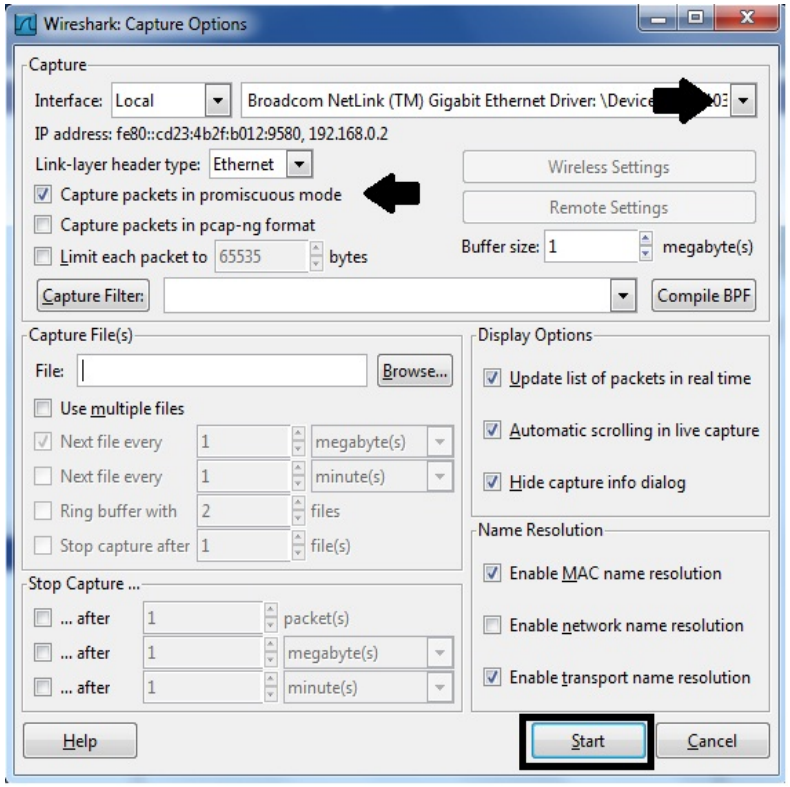


Základní nastavení

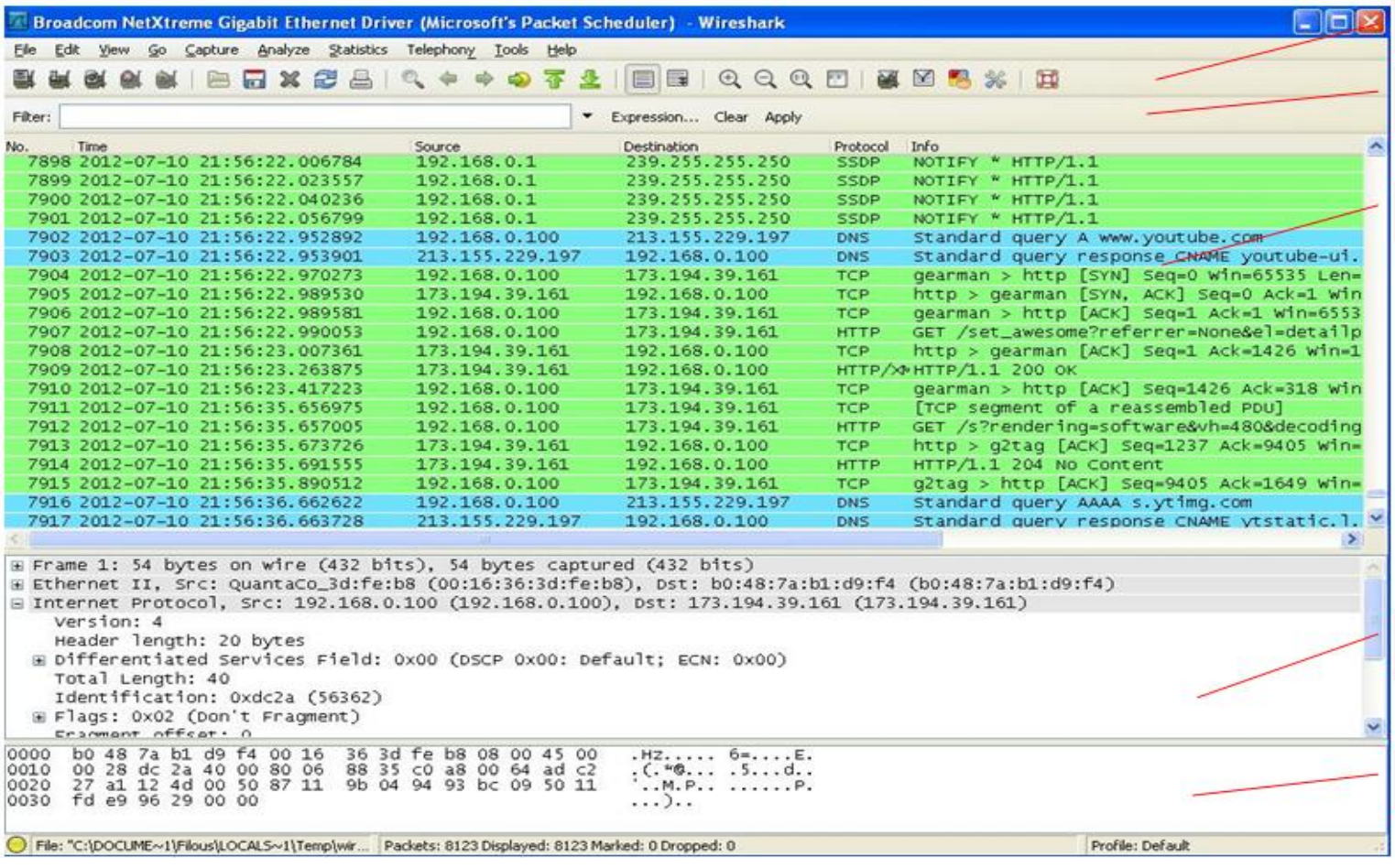
Cesta k nastavení

Vyberte v hlavním menu **Capture** → **Options..**

- Vyberte rozhraní na kterém chcete monitorovat provoz,
- promiskuitní mód aktivní,
- **Start**.
- Dále si ukážeme, kde lze změnit defaultní nastavení pokud nám nevyhovuje (např. režim nebo rozhraní).



Hlavní pracovní okno - popis a význam panelů v programu



Zachytávání ukočíme pomocí 4. ikony z leva v panelu nástrojů nebo **Capture** → **Stop**.

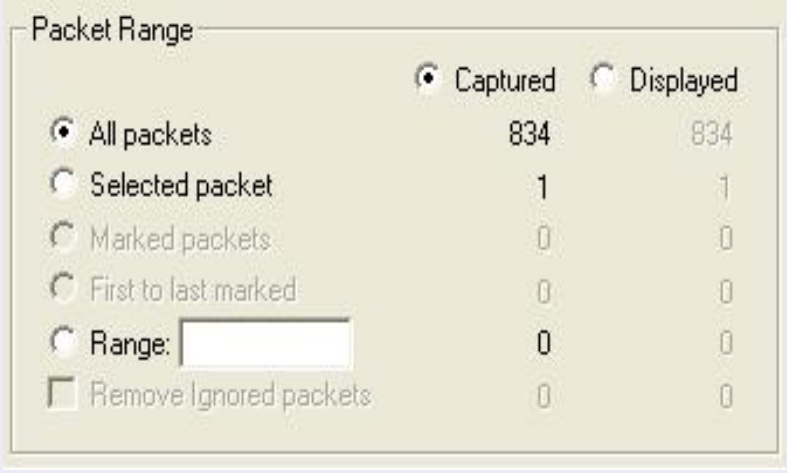
Pracujeme se zachyceným síťovým provozem

Primitivní vyhledávání

- Stačí chvíle a zachytíte tisíce i desetitisíce paketů (různé prokoly, IP, MAC adresy, velikosti, flagy, . . .).
- Klávesové zkratky :**Ctrl + F**, **Ctrl + N**, **Ctrl + B**.
- Do Filtru napište např. název protokolu (icmp).

Netradičně tradiční Uložit jako - uložte si zachycené pakety

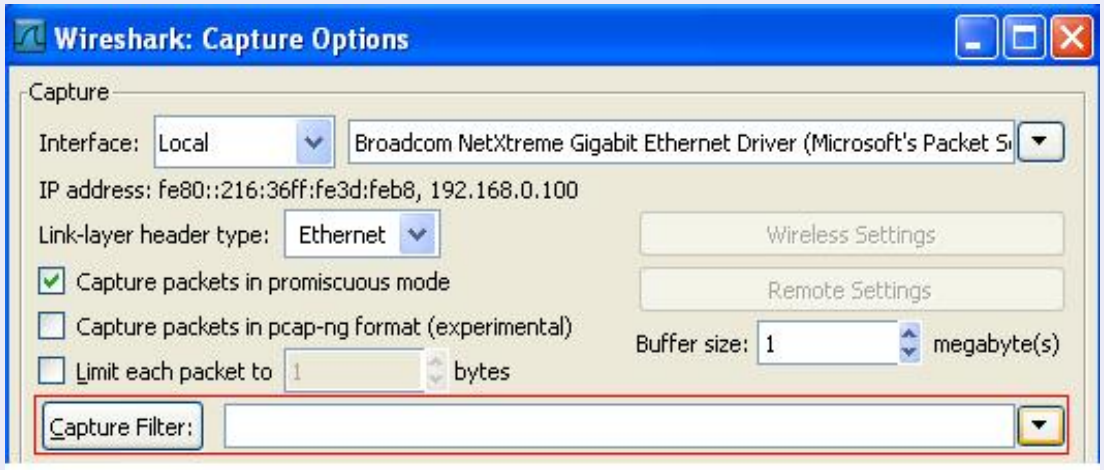
- Vyberte v hlavním menu **File** → **Save As..**



Nastavení filtru před spuštěním zachytávání

Zachytávací filtry - „Capture Filters“

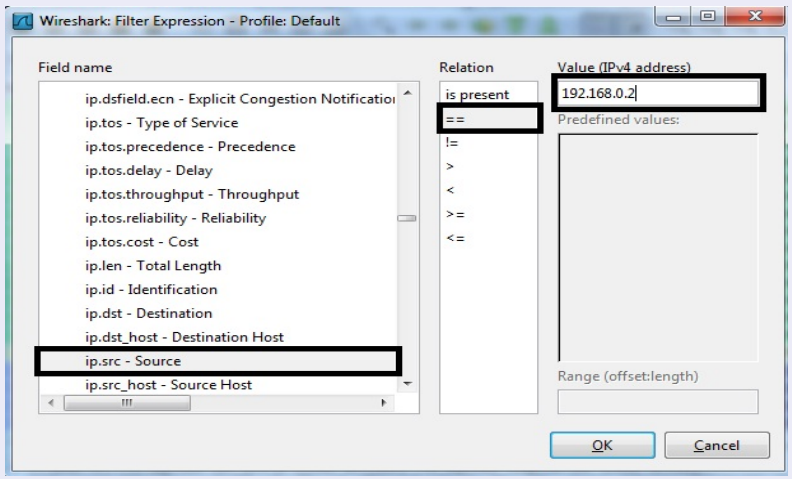
- Definujeme, co chceme či nechceme aby náš sniffer zachytil.
- K filtrování dochází již při zachytávání síťového provozu.
- Filtry vytváříme pomocí výrazů.
- V hlavním panelu :**Capture** → **Options..**
- Pokud před spuštěním zachytávání víme, že nechceme vidět protokol ARP, stačí do „Capture Filters“ napsat řetězec „!arp“.



Filtrujeme pakety až po zachycení

Zobrazovací filtry - „Display Filters“

- Aplikujeme na celou množinu již zachycených paketů - vyfiltrujeme co potřebuje (např. traffic na tcp.dstport==23) - pro návrat do celého dumpu stačí smazat filtr.
- Filtry píšeme ručně do pole pod panel nástrojů nebo použijeme „klikátko“ **Expression..** Zobrazovací filtry jsou v praxi více používany. Doporučuji psát filtry ručně.



Operátory ve filtrech

Porovnávací operátory

- Porovnávací operátory nám umožňují porovnávat hodnoty mezi sebou.
- Např. vyber všechny pakety které mají zdrojovou adresu 172.16.0.3 (ip.src==172.16.0.3).

Logické operátory

- Díky logickým operátorům můžeme vzájemně kombinovat několik filtrů.
- Např. vyber všechny pakety které mají zdrojovou adresu 172.16.0.3 a cílový port 23 (ip.src==172.16.0.3 and tcp.dstport==23).

Porovnávací a logické operátory

Porovnávací a logické operátory

Porovnávací operátory			Logické operátory	
==	eq	Rovná se	and	Obě podmínky musí platit
!=	ne	Nerovná se	or	Jedna s podmínek musí platit
<	lt	Menší než	xor	Jen jedna s podmínek platí
>	gt	Větší než	not	Žádná s podmínek neplatí
>=	ge	Větší nebo rovno		
<=	le	Menší nebo rovno		

Vytváříme vlastní filtry

Několik základních příkladů zobrazovacích filtrů

Zobrazovací filtr	Význam	Zobrazovací filtr	Význam
ip.src	Zdrojová IP adresa	arp.src.hw_mac	Zdrojová MAC v ARP
ip.dst	Cílová IP adresa	arp.dst.hw_mac	Cílová MAC v ARP
ip.addr	IP adresa	udp.srcport	Zdrojový UDP port
ipv6.src	Zdrojová IPv6 adresa	udp.dstport	Cílový UDP port
ipv6.dst	Cílová IPv6 adresa	udp.port	UDP port
ipv6.addr	IPv6 adresa	tcp.srcport	Zdrojový TCP port
eth.src	Zdrojová MAC adresa	tcp.dstport	Cílový TCP port
eth.dst	Cílová MAC adresa	tcp.port	TCP port
eth.addr	MAC adresa	vlan.id	ID VLAN

Skvělý zdroj zobrazovacích filtrů pro Wireshark

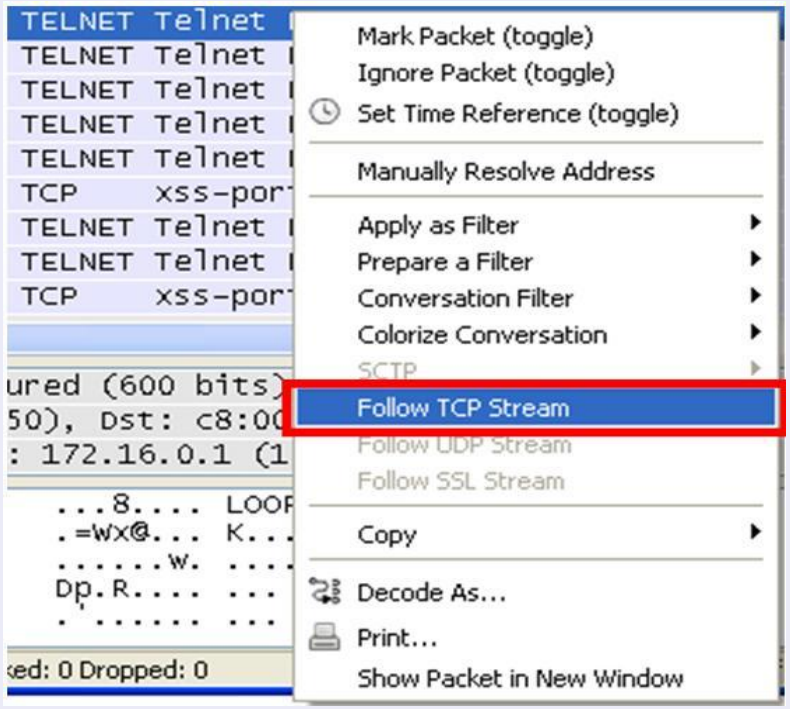
http://media.packetlife.net/media/library/13/Wireshark_Display_Filters.pdf

Cvičení

Stáhněte si z Moodlu připravený dump pro Wireshark, na kterém si vyzkoušíme několik filtrů.

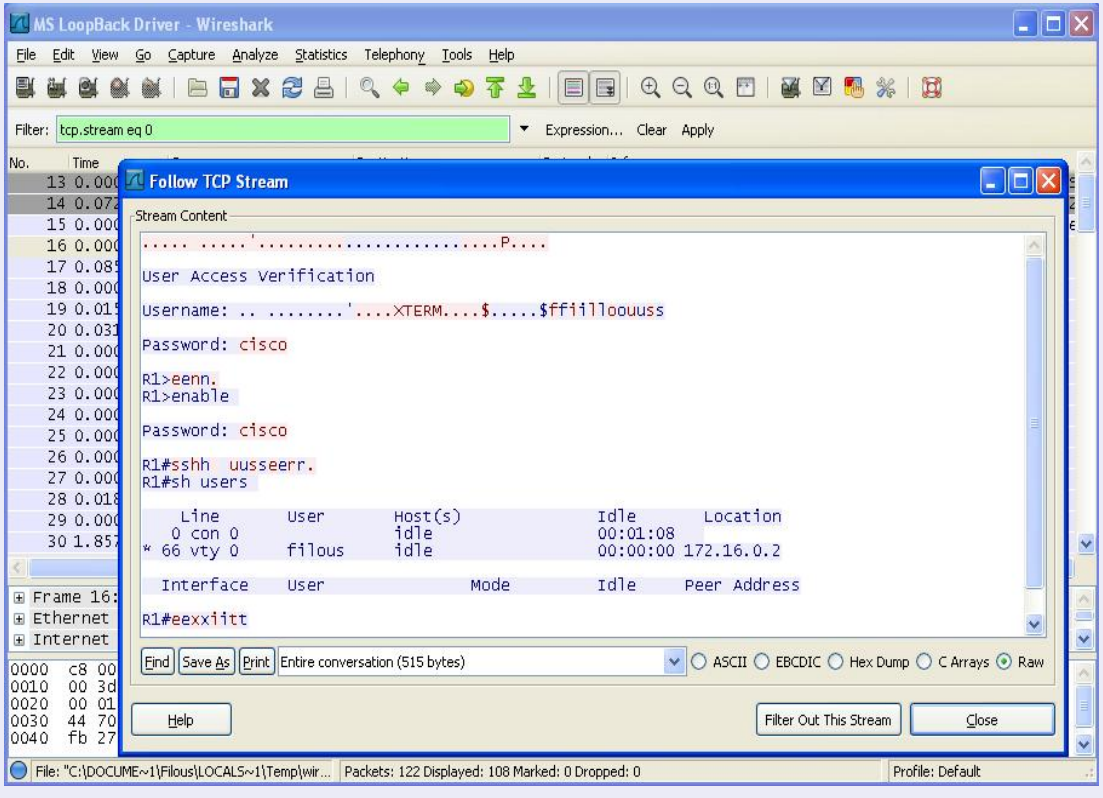
Někdy pohled na packety nestačí

- Umožňuje nám vidět zachycené packety, jak je vidí uživatel obsluhující aplikaci.
- Klikněte pravým tlačítkem myši na packet v hlavním panelu → **Follow TCP Stream**.



Spojte packety do streamu

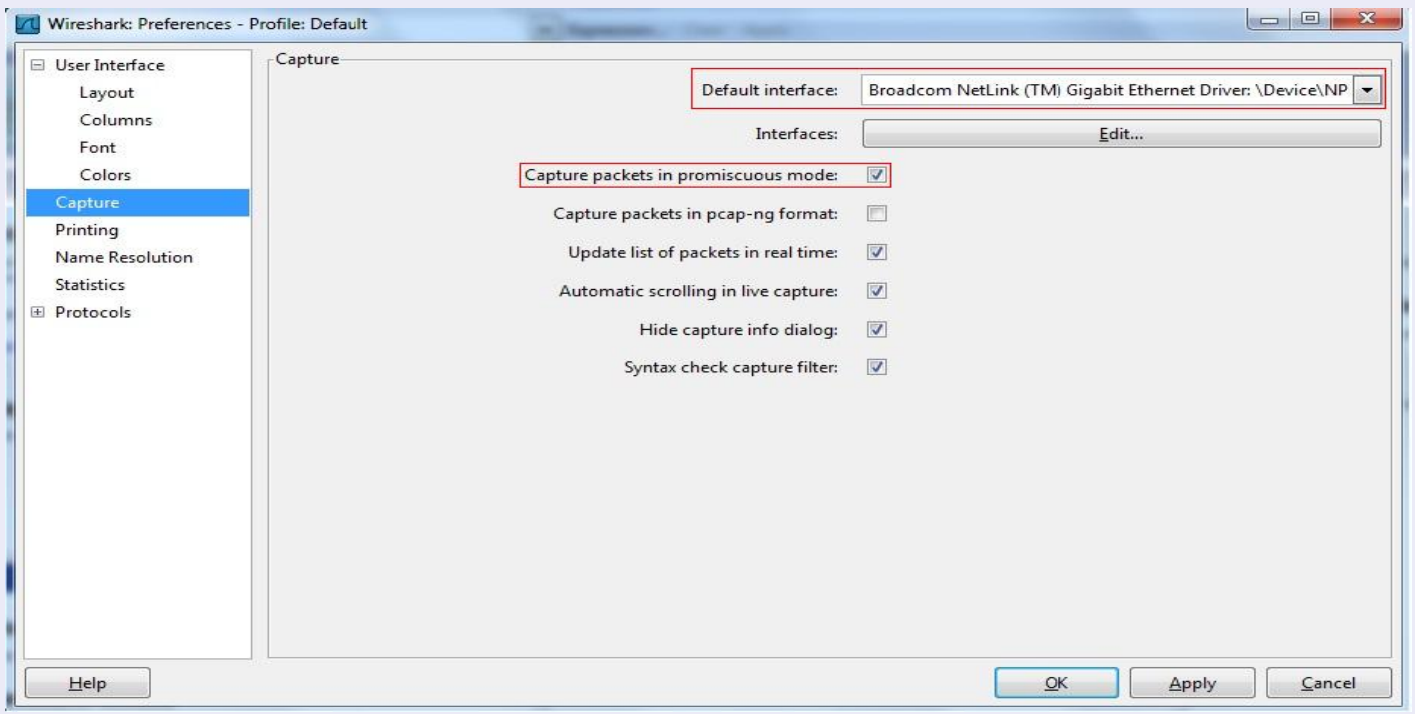
- Výborný nástroj pro analýzu přenášeného obsahu.
- Vyzkoušejte zachycení komunikace: z libovolného IM klienta, ze vzdálené správy směrovače přes protokol Telnet, z přenosu souboru protokolem TFTP.



Extra nastavení

Změna vlastností defaultního profilu

- Vyberte v hlavním menu **Edit** → **Preferences...**.
- V sekci „Capture“ lze vybrat rozhraní a zvolit promiskuitní režim jako defaultní (platné od příštího spuštění nástroje).



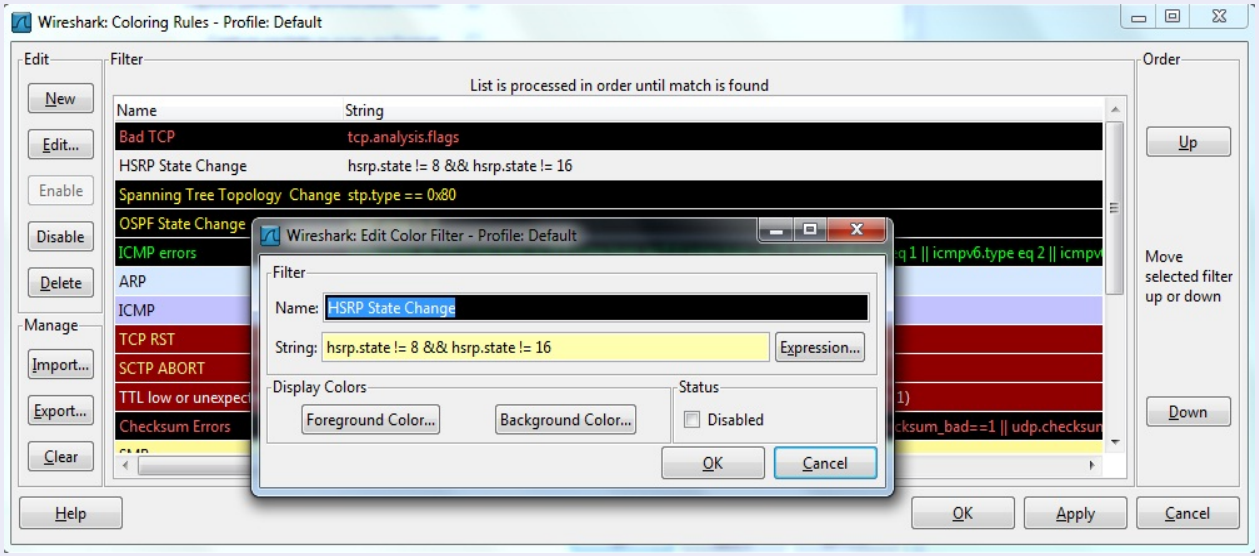
Extra nastavení

Změna formátu času

- Vyberte v hlavním menu **View** → **Time Display Format** →..
- Neznám defualtní nastavení, ale pro řešení různých problemů je nutné nastavení měnit(někdy stačí minuty jindy milisec).
- Čas i datum se bere ze systému - pozor na správné nastavení.

Změna barevných profilů

- Vyberte v hlavním menu **View** → **Coloring Rules..**



Odposlouchávání jako typ síťového útoku

Nástroj Caine & Abel si představíme hned několikrát v tomto kurzu. Na tomto místě ho použijeme k demostraci síťového útoku ARP spoofing. Co nás bude a nebude zajímat?

- Nejde nám o to v kurzu trénovat typy útoků!!!
- Tento typ útoku bude jediný, který si v laboratorních podmínkách vyzkoušíme.
- Uvidíte, zda teoretický princip skutečně chápete a zdali jste schopni tento typ triviálního útoku odhalit.
- Dále v této prezentaci si zopakujeme základní principy některých síťových útoků, které nám stačí k tomu, abychom věděli, jak zabezpečit síť a dále kde hledat bezpečnostní mezery (např. při forenzní analýze).

ARP Poisoning/ARP Spoofing

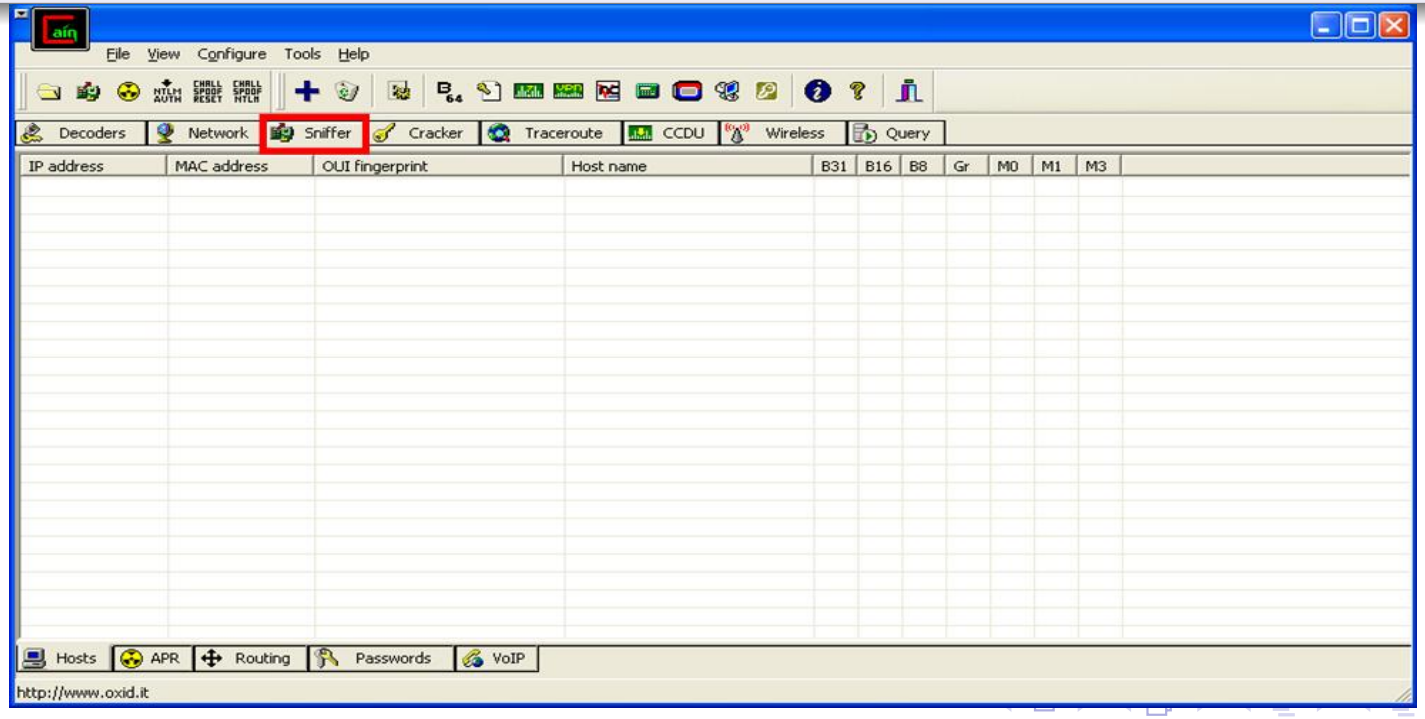
Základní charakteristika

- Nikoli běžná metoda odposlouchávání provozu ale útok na přepínač, typ Man in The Middle,
- výsledkem útoku je, že umožní odposlouchávat síťový provoz (např. konkrétního hosta), jako dříve zmíněné metody,
- k pochopení tohoto typu útoku je klíčové znát přesně, jak funguje protokol ARP (Address Resolution Protocol).
- Co víte o ARP spoofingu? Jak probíhá podrvžení MAC adresy?
- Jaké existuje zabezpečení proti tomuto typu útoku?

Otevřete si ve Wiresharku dump, který máte připravený v moodlu. Identifikujte chování běžného ARP dotazu a ARP spoofingu.

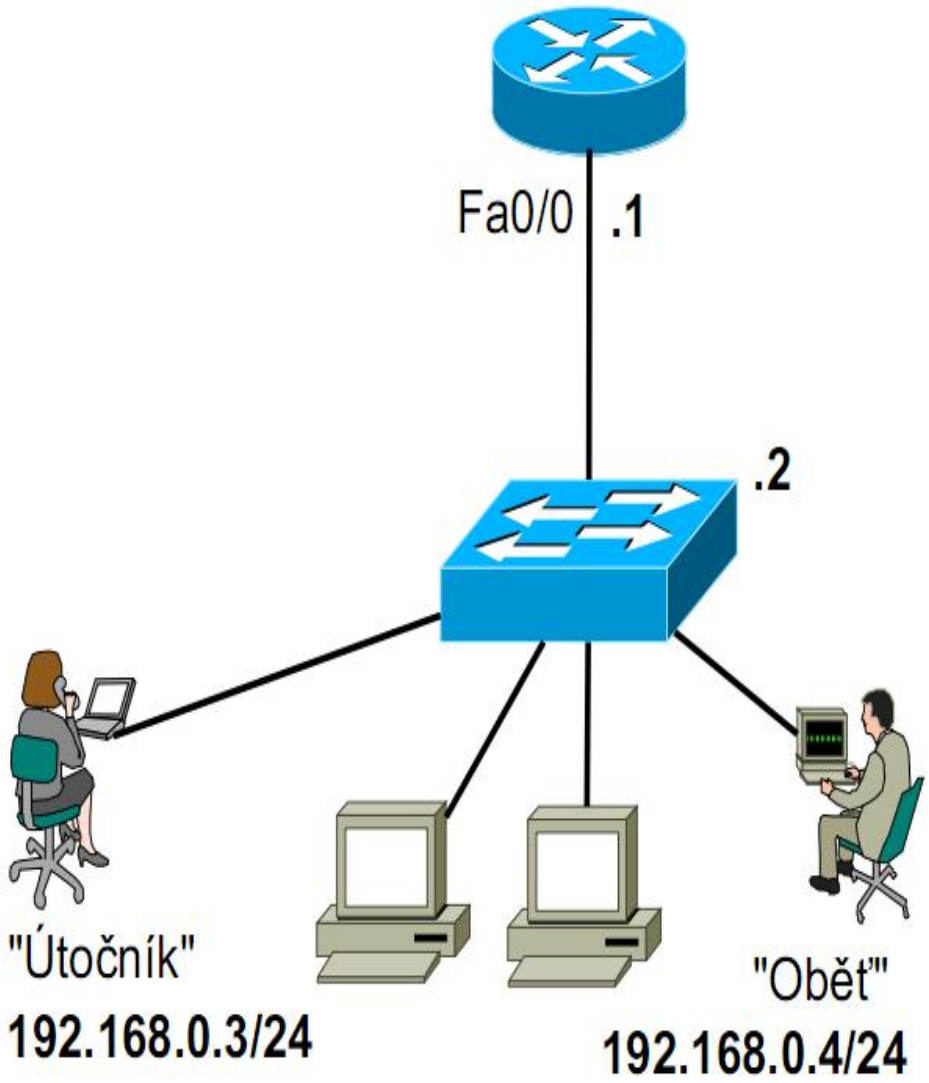
Caine & Abel

- 6. příčka v Top Security Tools, GUI nástroj pod OS Windows,
- dle oficiálních stránek „Password Recovery Tool“, freeware,
- obsahuje obrovské množství integrovaných funkcí jako např. síťový sniffer, cracker (slovníkový a brute-force útok), ARP spoofing, hash dump, ...
- oficiální stránky nástroje: http://www.oxid.it//.



Topologie příkladu pro ARP Spoofing

- Nastavte adresu rozhraní směrovače a IP adresu VLAN1 na přepínači.
- Na přepínači nastavte možnost vzdáleného přístupu protokolem Telnet.
- Cíl: útočník bude zachytávat provoz mezi „Obětí“ přistupující na přepínač pomocí protokolu Telnet a přepínačem.
- Funkčnost ověřte programem Wireshark.



Caine & Abel

Vykonáním samotného útoku se nebudeme příliš zabývat a použijeme připravené video (moodle).

- Protokolem ICMP ověřte konektivitu mezi hosty.
- Před začátkem simulace útoku spuste na všech PC Wireshark.
- Ve Wiresharku sledujte, jak se projeví sken sítě (identifikace zařízení na síti).
- Pozorujte ve Wiresharku, jak „Útočník“ podvrhne MAC. Zkontrolujte obsah ARP tabulek.
- Připojte se vzdáleně z „Oběti“ na přepínač přes protokol Telnet a vypište běžící konfiguraci.
- Na PC, kde sedí „Útočník“ ve Wiresharku zobrazte obsah přenášený protokolem Telnet (mezi obětí a přepínačem).
- Aplikujte Vámi navržené zabezpečení před tímto typem útoku a celý postup opakujte.

Nejběžnější síťové útoky

Chcete-li, co nejlépe zabezpečit Vaší počítačovou síť před útoky, je důležité chápat základní teoretické principy, jak takové útoky probíhají. Díky tomu jste schopni určit, jakých bezpečnostních mezer ve Vaší konfiguraci může útočník využít.

Běžné síťové útoky

- ARP Spoofing/ARP Poisoning (Již známe).
- MAC Address Table Overflow/MAC Address Flooding.
- VLAN Hopping.
- Útoky na Spanning-tree.

Odpovězte na níže uvedné otázky

- Popište základní princip útoku.
- Navrhněte vhodné zabezpečení.

Děkuji za pozornost!