**Projekt 1 - ZBER DÁT**

**Zber dát - nástroje (napr. CISCO 3560)**

**CISCO MONITOR CAPTURE = Embedded Packet Capture**

* dostupný pre smerovače
* definícia veľkosti buffera v zariadení (miesto kam sa bude odkladať odchytená prevádzka)
* možnosť určiť pomocou access listov čo chcem odchytávať
* určenie portu, z ktorého bude odchytávaná prevádzka a v ktorom smere
* export odchytenej prevádzky (FTP, TFTP,...) vo formáte pcap a jeho následná analýza
* dostupný od IOS 12.4.20T

h[ttp://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/1089-cisco-router-embedded-packet-capture-configuration-usage-troubleshooting-exporting.html](http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/1089-cisco-router-embedded-packet-capture-configuration-usage-troubleshooting-exporting.html)

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/command/epc-cr-book/epc-cr-m1.html>

**CISCO IP TRAFFIC EXPORT**

* dostupný pre smerovače
* určenie odchytávaného portu
  + určenie portu, ktorým bude odchytená prevádzka odchádzať na zariadenie, kde sa budú tieto data ukladať (zariadenie musí byť v tej istej vlan ako port, ktorým data odchádzajú alebo musí byť priamo pripojené k portu = určuje sa MAC ADRESA zariadenia, na ktoré majú prísť odchytené data)
  + definícia buffera pre odchytené data a pomocou FTP/TFTP ich odoslanie na následnú analýzu
* dostupný pod IOS 12.3(4)T

<http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t11/ht_rawip.html>

<http://www.ciscozine.com/ip-traffic-export-how-to-mirror-traffic-on-a-router/>

**CISCO NETFLOW**

<https://en.wikipedia.org/wiki/NetFlow>

* zber dát na CISCO zariadeniach (bude treba určiť na ktorých)
* NetFlow collector - miesto kde sa budú dáta posielať a spracovávať
  + NFDUMP <http://nfdump.sourceforge.net/>
  + NFSEN <http://nfsen.sourceforge.net/>
* aplikácie pre analýzu dát: <http://techteapot.com/top-5-open-source-netflow-analyzers/>

**CISCO IPFIX**

<https://en.wikipedia.org/wiki/IP_Flow_Information_Export>

* informácie o toku z routerov, ale aj iných zariadení
* vychádza z Cisco NETFLOW verzie 9
* smerovače môžu informovať centrálnu stanicu
* preferuje SCTP transport protocol, ale aj TCP, UDP

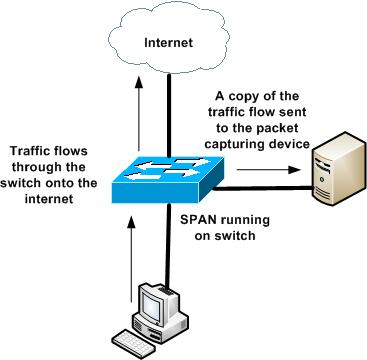
Rozdiel medzi Netflow a IPFIX  
<http://www.bradreese.com/blog/netflow-vs-ipfix-exporter.htm>

**SNMP**

* ako presne SMNP v našom prípade využiť pre zber dát

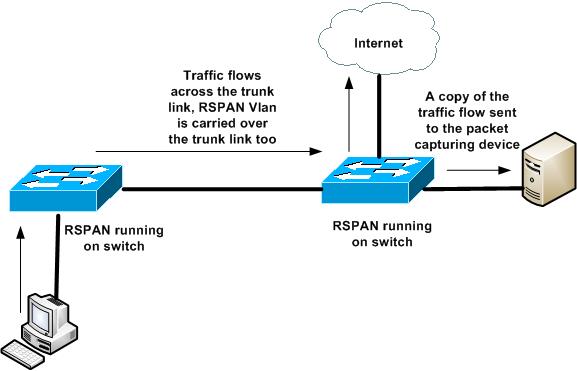
**PORT MIRRORING - SPAN**

* zber v rámci jedného switcha



**PORT MIRRORING - RSPAN**

* zber z viacerých switchov (budeme mať prístup?)



**Čo dokáže Cisco firewall (ASA 5505/5515/5520)?**

**Capture Data using ASDM** (Cisco Adaptive Security Device Manager)

<http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/110117-asa-capture-asdm-config.html#configurationPACKETCAP>

**Capture Data using CLI**

<http://www.techrepublic.com/blog/data-center/easy-packet-captures-straight-from-the-cisco-asa-firewall/>

**Zber dát z wifi AP (Linksys L2 dd-wrt, CISCO WLC)**

* priamo integrovane služby **packet capture** (zaleží od konkretného typu)  
  <http://www.linksys.com/ca/support-article?articleNum=140781>
* **PRTG Network Monitor**  
  <https://www.paessler.com/prtg/features>
* **LinkLog**  
  <http://www.leshylabs.com/blog/dev/2014-09-16-Capturing_Linksys_Log_Events_in_Linux.html>
* **DD-WRT**  
  možnosť preposielať pomocou IPTABLES traffic na monitorovacie PC
* **Cisco WLC: Per-client Packet Capture**  
  <http://wifinigel.blogspot.sk/2014/08/cisco-wlc-per-client-packet-capture.html>

–––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––––

**Sieťové nástroje - analýza toku dát**

<http://www.sectec.sk/sk/network-monitoring>

**dSniff**

* aplikacia urcna na odchytavanie prihlasovacich mien a hesiel, webovych stranok, obsahu mailov a podobne
* It handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pc Anywhere,
* NAI Sniffer, Microsoft SMB, Oracle SQL\*Net, Sybase and Microsoft SQL protocols.

OS: UNIX

**Capsa**

* Wired & wireless network real-time packet capturing -- (Packets never lies)
* Traffic & bandwidth monitoring -- (Which machines are downloading or watching online videos?)
* Advanced protocol analysis -- (What network protocols are used in your network? HTTP - web browsing, MSN - chatting.)
* Multiple network behavior monitoring -- (What the users are doing: web browsing, chatting?)
* Expert network diagnosis -- (Are there any attacks and problems in my network?)
* Network activity logging -- (Who and when visited which website/chatted with whom/sent email to whom?)
* Email contents preservation -- (Need to save a copy of all emails' contents sent/received by your employee in your network as evidence?)
* Quick & intuitive reports -- (Need rich charts and graphs in your presentations and reports? )
* In-depth packet decoding -- (What is the original information in network communications?)

OS: Windows (TRIAL verzia je dost okliestena)

**CommView**

* vo dvoch verziach: Ethernet a WiFi
* Protocols distribution, bandwidth utilization, and network nodes charts and tables.
* Detailed IP connections statistics: IP addresses, ports, sessions, etc.
* VoIP analysis: H.323 and SIP (TMC'S Internet Telephony Magazine product of the year award)
* WEP and WPA2-PSK decryption (wireless edition only)
* Multi-channel capturing using several USB adapters (wireless edition only)
* Packet injection using a packet generator
* User-defined packet filters and alarms
* TCP and UDP stream reconstruction
* Packet-to-application mapping
* Reporting
* Capture log file import and export

OS: Windows (TRIAL verzia funguje 30 dni)  
  
**Ettercap**

* IP-based: packets are filtered based on IP source and destination.
* MAC-based: packets are filtered based on MAC address, useful for sniffing connections through a gateway.
* ARP-based: uses ARP poisoning to sniff on a switched LAN between two hosts (full-duplex).
* PublicARP-based: uses ARP poisoning to sniff on a switched LAN from a victim host to all other hosts (half-duplex).

OS: UNIX, Windows, MAC OS X,

**Kismet**

* Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic

OS: UNIX, MAC OS X

**Microsoft Network Monitor**

* It enables capturing, viewing, and analyzing network data and deciphering network protocols
* Process tracking
* Grouping by network conversation
* Support for over 300 public and Microsoft proprietary protocols
* Simultaneous capture sessions
* Wireless Monitor Mode with supported wireless NICs
* Real-time capture and display of frames
* Reassembly of fragmented data
* Sniffing of promiscuous mode traffic
* Can read libpcap capture files
* API to access capture and parsing engine

OS: Windows

**ngrep**

* IPv4 and IPv6, Internet Protocol version 4 and version 6
* TCP, Transmission Control Protocol
* UDP, User Datagram Protocol
* ICMPv4 and ICMPv6, Internet Control Message Protocol version 4 and version 6
* IGMP, Internet Group Management Protocol
* Ethernet, IEEE 802.3
* PPP, Point to Point Protocol
* SLIP, Serial Line Internet Protocol
* FDDI, Fiber Data Distribution Protocol
* Token Ring, IEEE 802.5

OS: UNIX, MAC OS X, Windows

**netsniff-ng**  
<https://en.wikipedia.org/wiki/Netsniff-ng>

OS: UNIX

**tcpdump**

OS: UNIX, MAC OS X, Windows

**Wireshark**

OS: UNIX, MAC OS X, Windows

**Nmap**  
<https://en.wikipedia.org/wiki/Nmap>

* Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
* Port scanning – Enumerating the open ports on target hosts.
* Version detection – Interrogating network services on remote devices to determine application name and version number.
* OS detection – Determining the operating system and hardware characteristics of network devices.
* Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and Lua programming language.

Typical uses of Nmap:

* Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
* Identifying open ports on a target host in preparation for auditing.
* Network inventory, network mapping, maintenance and asset management.
* Auditing the security of a network by identifying new servers.
* Generating traffic to hosts on a network
* Find and exploit vulnerabilities in a network.

OS: UNIX, Windows

Ď**alšie nástroje**

<https://en.wikipedia.org/wiki/Metasploit_Project>

<https://en.wikipedia.org/wiki/Stockade_(software>)

<https://en.wikipedia.org/wiki/DenyHosts>

**IDS/IPS nástroje - detekcia toku dát**

[ttp://preventista.sk/info/spustite-siet-3-systemy-detekcie-a-prevencie-prieniku/](http://preventista.sk/info/spustite-siet-3-systemy-detekcie-a-prevencie-prieniku/)

**ACARM-ng** (Alert Correlation, Assessment and Reaction Module - next generation)

- open source IDS/IPS system, Linux

- <http://www.acarm.wcss.wroc.pl/>

- <https://en.wikipedia.org/wiki/ACARM-ng>

**AIDE** (The Advanced Intrusion Detection Environment)

- open source, UNIX like

-<http://aide.sourceforge.net/>

-<https://en.wikipedia.org/wiki/Advanced_Intrusion_Detection_Environment>

**BRO**

- open source, Linux/BSD/MAC

- <https://www.bro.org/>

- <https://en.wikipedia.org/wiki/Bro_(software>)

**Fail2ban**

**-** Unix like

-<http://www.fail2ban.org/wiki/index.php/Main_Page>

-<https://en.wikipedia.org/wiki/Fail2ban>

**OSSEC**

- open source, cross-platform

-<http://www.ossec.net/>

-<https://en.wikipedia.org/wiki/OSSEC>

**Samhain**

- UNIX, GPL

<http://www.la-samhna.de/samhain/>

<https://en.wikipedia.org/wiki/Samhain_(software>)

**Prelude**

- Linux, BSD, Win

- Propietary and GPL

-<http://www.prelude-siem.com/index.php/uk/>

-<https://en.wikipedia.org/wiki/Prelude_Hybrid_IDS>

**Snort**

- Open source, cross-platform

-<https://www.snort.org/>

-<https://en.wikipedia.org/wiki/Snort_(software>)

**Suricata**

**-** Open source, cross-platform

-<http://suricata-ids.org/>

-<https://en.wikipedia.org/wiki/Suricata_(software>)

**SAGAN**

- open source, Unix like

-<https://en.wikipedia.org/wiki/Sagan_(software>)

-<https://quadrantsec.com/sagan_log_analysis_engine/>