

CompTIA Security+

Network Security Solutions d.o.o.

<http://www.netsec.rs>

Dejan Levaja

Agenda :: Day II

•Infrastructure and Connectivity

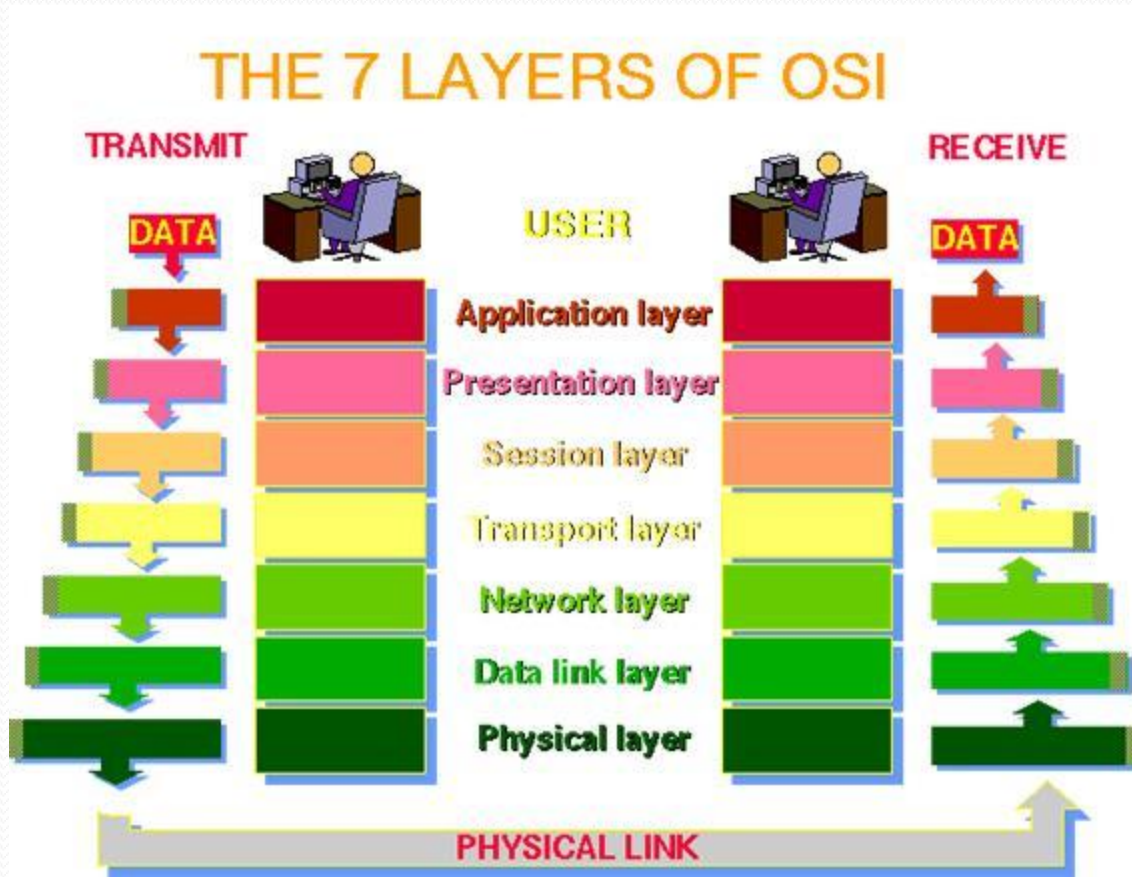
- Understanding Infrastructure Security
 - Working with Hardware Components
 - Working with Software Components
- Understanding the Different Network Infrastructure Devices
 - Firewalls
 - Hubs
 - Modems
 - Remote Access Services
 - Routers
 - Switches
 - Telecom/PBX Systems
 - Virtual Private Networks
 - Wireless Access Points
- Monitoring and Diagnosing Networks
 - Network Monitors
 - Intrusion Detection Systems
- Securing Workstations and Servers
- Understanding Mobile Devices
- Understanding Remote Access
 - Using Point-to-Point Protocol
 - Working with Tunneling Protocols
 - Using 802.1x Wireless Protocols
 - Working with RADIUS
 - TACACS/+
- Securing Internet Connections

- Working with Ports and Sockets
- Working with E-Mail
- Working with the Web
- Working with File Transfer Protocol
- Understanding Network Protocols
- The Basics of Cabling, Wires, and Communications
 - Coax
 - Unshielded Twisted Pair and Shielded Twisted Pair
 - Fiber Optic
 - Infrared
 - Radio Frequencies
 - Microwave Systems
- Employing Removable Storage
 - CD-R/DVD-R
 - Diskettes
 - Flash Cards
 - Hard Drives
 - Network Attached Storage
 - Smart Cards
 - Tape
 - Thumb Drives

Agenda :: Day II

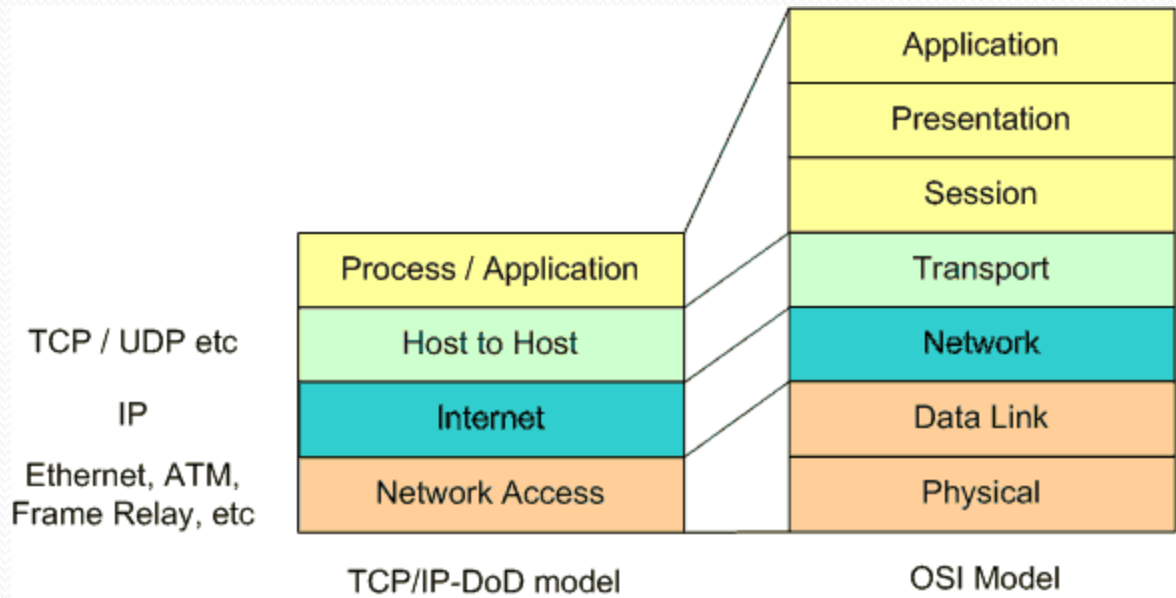
- **Monitoring Activity and Intrusion Detection**
 - Monitoring the Network
 - Recognizing the Different Types of Network Traffic
 - Monitoring Network Systems
 - Understanding Intrusion Detection Systems
 - Working with a Network-Based IDS
 - Working with a Host-Based IDS
 - Working with NIPS
 - Utilizing Honeypots
 - Understanding Incident Response
 - Working with Wireless Systems
 - Wireless Transport Layer Security
 - IEEE 802.11x Wireless Protocols
 - WEP/WAP
 - Wireless Vulnerabilities to Know
 - Understanding Instant Messaging's Features
 - Understanding IM Vulnerabilities
 - Controlling Privacy
 - Working with 8.3 File Naming
 - Understanding Protocol Analyzers
 - Understanding Signal Analysis and Intelligence
 - Footprinting
 - Scanning

TCP/IP



Hint: All People Seem To Need Data Processing

OSI vs DoD model



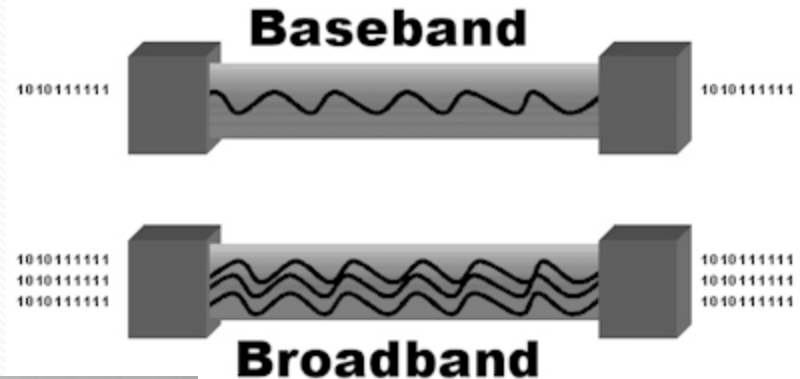
The Basics of Cabling, Wires, and Communications

- Coax

- Baseband signaling means that a single channel is carried through the coax.
- Broadband refers to multiple channels on the coax.
- Connector
- T connector
- Terminator
- Vampire tap

- Coax security

- Network instability
- Sniffing (Vampire tap)



The Basics of Cabling, Wires, and Communications

- UTP/STP
 - Unshielded Twisted Pair (UTP)
 - Shielded Twisted Pair (STP)
 - 7 categories
 - 1 : voice grade (POTS)
 - 7 : >1Gbps
- Fiber Optic
 - Hard to tap



The Basics of Cabling, Wires, and Communications

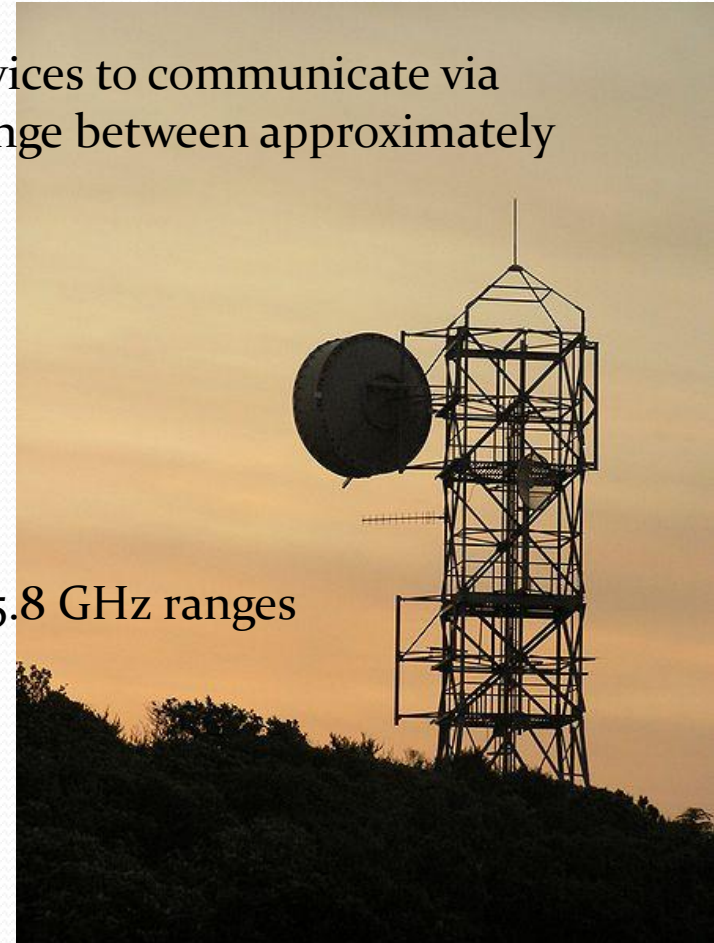
- Radio Frequencies

- Infrared

- Infrared technology allows computing devices to communicate via short-range wireless signals (frequency range between approximately 1 and 430 THz (terahertz))
 - Keyboards, mices....

- Microwave Systems (0,3 GHZ and 300 GHZ)

- GSM - 0.3 GHz to 1,9 GHz
 - Wireless 2,4GHz, 5GHz
 - Bluetooth 2,4Ghz
 - WiMax - 2.3 GHz, 2.5 GHz, 3.5 GHz and 5.8 GHz ranges
 - Satellites
 - Radars
 - GPS
 -



Protocols

- IP address vs port
- Socket
- API
- Protocols:
 - PPP
 - ARP
 - IP
 - ICMP
 - TCP
 - UDP
 - Telnet,SSH, SMTP, POP₃, IMAP₄, SNMP, DNS, NBT(SMB),HTTP, HTTPS, FTP, LDAP, LDAPS, RADIUS, TACACS
- Vežba:
 - Na kojim portovima rade navedeni protokoli ?
- Vežba:
 - Gde na Win/Lin OS stoje podaci o portovima/servisima?

Point to Point Protocol (PPP)

Web

- HTTP, TCP 80, clear text
- HTTPS, TCP 443

Understanding the Different Network Infrastructure Devices

- Routers
- Route
 - static
 - dynamic
- Protocols
 - Routing Information Protocol (RIP)
 - RIP is a IGP distance-vector routing protocol, which employs the hop count (max 15) as a routing metric.
 - Open Shortest Path First (OSPF)
 - Border Gateway Protocol (BGP)

Comparing BGP and OSPF (1)

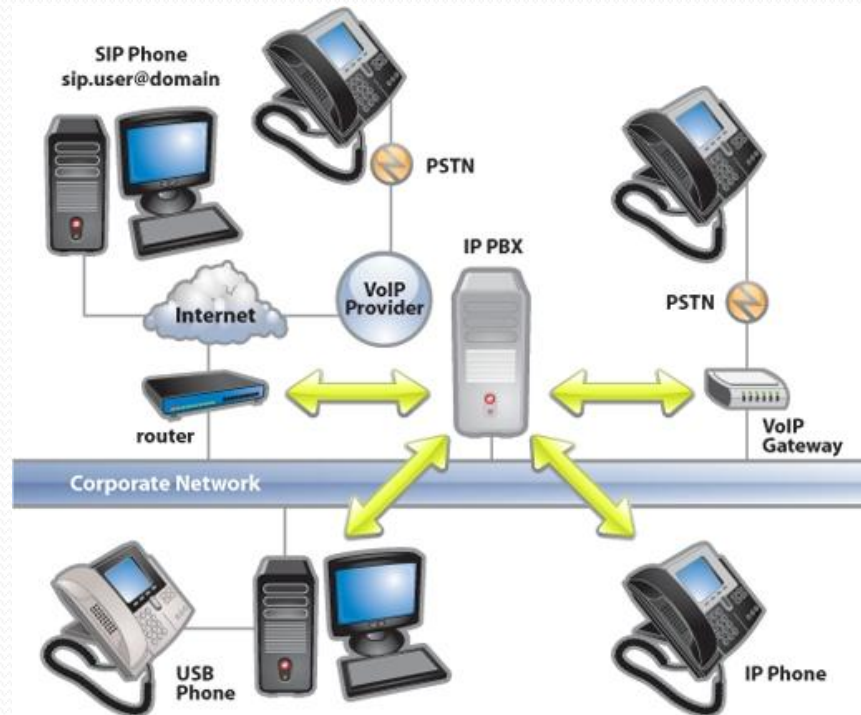
OSPF	BGP
IGP : Interior Gateway Protocol	EGP : Exterior Gateway Protocol
Protocol that directly rides IP Protocol number: 89	Protocol that rides TCP Port number: 179
Link-state protocol propagates link-state information	Path vector protocol propagates path information
With every change, LSA, chain propagation	With every change, UPDATE, chain propagation

Understanding the Different Network Infrastructure Devices

- Firewalls
 - Packet filter firewall
 - port, ip
 - Proxy firewall
 - nat, cache, web protocols
 - Stateful inspection firewall
 - [Application layer gateway]
- Hub
- Switch
- Modem

Understanding the Different Network Infrastructure Devices

- Telephony
 - PBX (Private Branch Exchange)
 - POTS (Plain Old Telephone System)
 - PSTN (Public Switched Telephone Network)
 - VoIP (Voice over IP)



Understanding the Different Network Infrastructure Devices

- WiFi(2,4GHz – 5 GHz)
 - Wireless Access Point (WAP)
 - IEEE 802.11 – Wireless Ethernet
 - Ad-Hoc mode
 - Infrastructure mode
 - SSID (WAP name)
 - BSSID (WAP MAC address)
 - WAP Association
- Wireless standards
 - 802.11 - 1997., max 2Mbps, 2.4GHz
 - 802.11b – 1999., max 11Mbps, 2.4GHz
 - 802.11a – 1999., max 54Mbps, 5GHz
 - 802.11g – 2003., max 54Mbps, 2.4GHz
 - 802.11n – 2009., max 600 Mbps, with the use of four spatial streams at a channel width of 40 MHz
 - 802.16m – WiMax, max 1Gbps, 2.3, 2.5 and 3.5Ghz, long range system!



Understanding the Different Network Infrastructure Devices

- Wireless security
 - WEP- 1997.,
 - Authentication: Open System, Shared Key
 - Encryption: RC4 + IV (Inicialization Vector (24bit, clear text))
 - WPA – 2003., upgrade from WPA, same hardware
 - WPA2 – 2004.,
 - Encryption: AES, TKIP
 - WPA PSK – password auth
 - WPA Enterprise – certificate auth
- Wireless vulnerabilities
 - Site surveying
 - War driving
 - Rogue Access Point
 - Jamming
- Demo
 - Kismet
 - Sniffing



Vulnerabilities of Web Add-ins

- ActiveX
 - ActiveX is a Microsoft technology that is used to add functionality to Windows programs.
 - ActiveX controls are often used to enable Microsoft's Internet Explorer browser to view and use multimedia content embedded in web pages (for example, Flash applications). They are also used to add new functions to the browser (for example, toolbars).
 - Authenticode identifies the publisher of signed software and verifies that it hasn't been tampered with, before users download software to their PCs.
- Common Gateway Interface (CGI)
 - Older form of server side scripting
- Cookies
 - Cookies are text files that a browser maintains on the user's hard disk in order to provide a persistent, customized web experience for each visit.

Vulnerabilities of Web Add-ins

- Cross-site scripting (XSS)
 - Persistent vs NonPersistent
 - Demo
- Input Validation
- Java Applets (Sun)
 - A Java applet is a small, self-contained Java application that is downloaded from a server to a client and then run from the browser.
 - A Java "applet" (so-called because it is a little application) is a fully contained program.
- Javascript (Netscape)
 - Must be placed inside an HTML document to function. It runs in browser.
 - JavaScript is text that is fed into a browser that can read it and then is enacted by the browser.

Vulnerabilities of Web Add-ins

- Signed Applets
 - A signed applet doesn't run in the Java sandbox, and it has higher system access capabilities.
- Popup (Popunder)
 - Both popups and popunders are opening pages or sites that you did not specifically request and may only display ads or bring up applets that should be avoided

Employing Removable Storage

- Removable storage (removable media) refers to any type of storage device that can be removed from the system.
 - CD-R/DVD-R
 - Diskettes
 - Flash Cards
 - Hard Drives
 - Network Attached Storage
 - Tape

Monitoring Network Systems

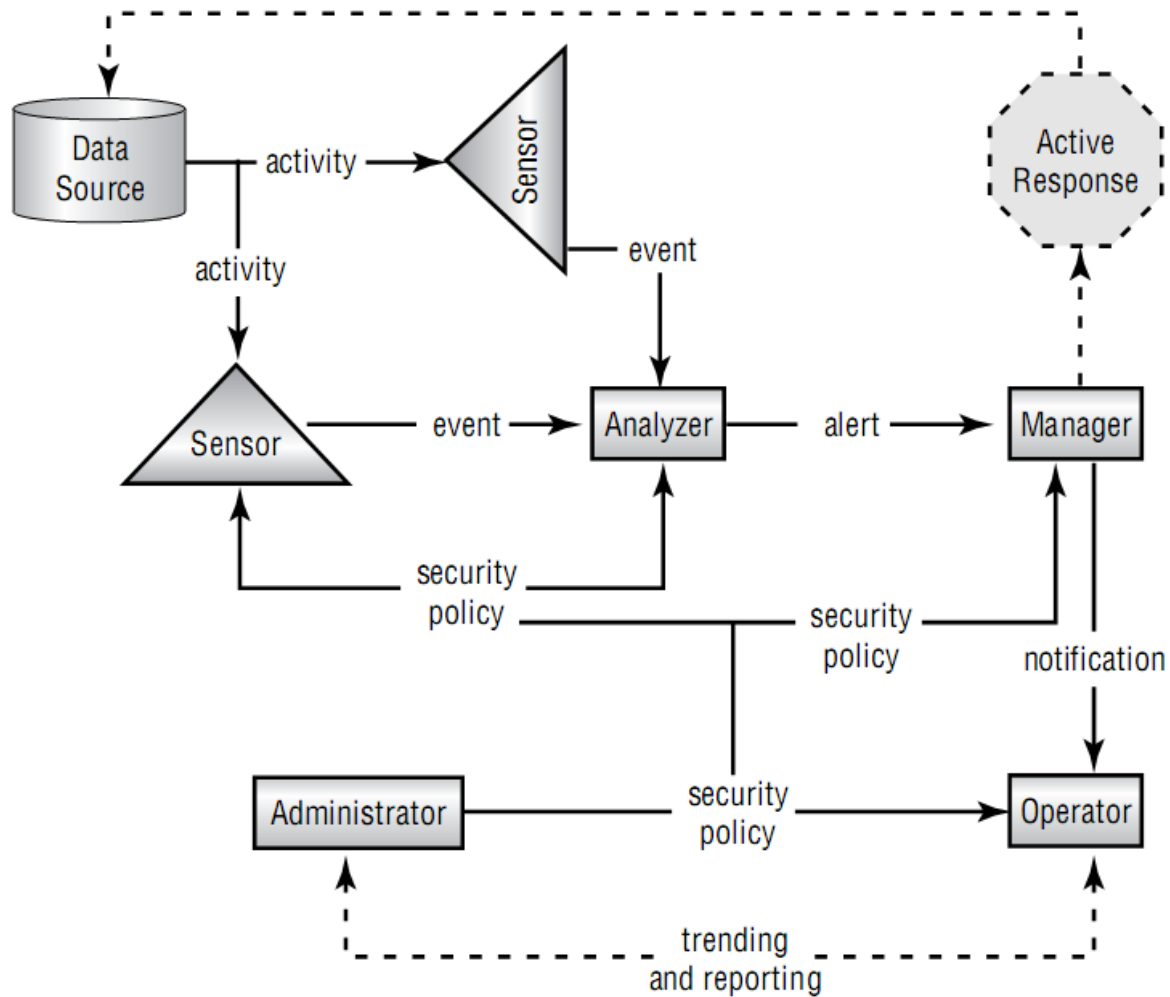
- Monitoring
 - Host (what is host?)
 - Network
 - Tap
 - Switched Port Analyzer (SPAN) or Port Mirroring
 - L2 vs L3 sniffing (evesdropping)

Understanding Intrusion Detection Systems

- Intrusion detection (ID) is the process of monitoring events in a system or network to determine if an intrusion is occurring. An IDS reports and monitors intrusion attempts.
- An intrusion is defined as any activity or action that attempts to undermine or compromise the confidentiality, integrity, or availability of resources.
- Terminology:
 - Activity - element of a data source that is of interest to the operator.
 - Alert - a message from the analyzer indicating that an event of interest has occurred. The alert contains information about the activity as well as specifics of the occurrence.
 - Analyzer - The analyzer is the component or process that analyzes the data collected by the sensor.
 - Data source - The data source is the raw information that the IDS uses to detect suspicious activity. The data source may include audit files, system logs, or the network traffic as it occurs.

Understanding Intrusion Detection Systems

- Event
- sus
- Ma
- to 1
- No
- ma
- Op
- IDS
- Ser
- dat



es that a
 ator uses
 he IDS
 or the
 n the

Understanding Intrusion Detection Systems

- Signature-based-detection IDS
 - also commonly known as misuse-detection IDS (MD-IDS), is primarily focused on evaluating attacks based on attack signatures and audit trails.
- Anomaly-detection IDS
 - an anomaly-detection IDS (AD-IDS), also commonly known as behavior-based IDS, looks for anomalies, meaning it looks for things outside of the ordinary. Typically, a training program learns what the normal operation is and then can spot deviations from it.
- Network-based IDS (NIDS)
 - Placing the NIDS
 - Snort, Cisco, MS TMG 2010....
- Host-based IDS (HIDS)
 - Tripwire (file based)
- Passive Response
 - Logging
 - Notification
 - Shunning

Understanding Intrusion Detection Systems

- Active response
 - Terminating processes or sessions
 - Network configuration changes
 - Deception
- IDS vs IPS (NIPS)
- Hands on
 - Vežba:
 - Pregled logova u Windowsu
 - Zadatak:
 - Skript koji prikazuje failed logon evente
 - Instaliranje WinPcap-a
 - Instaliranje Snort-a
 - Vežba:
 - Pregled logova u Linuxu
 - Instaliranje Wiresharka

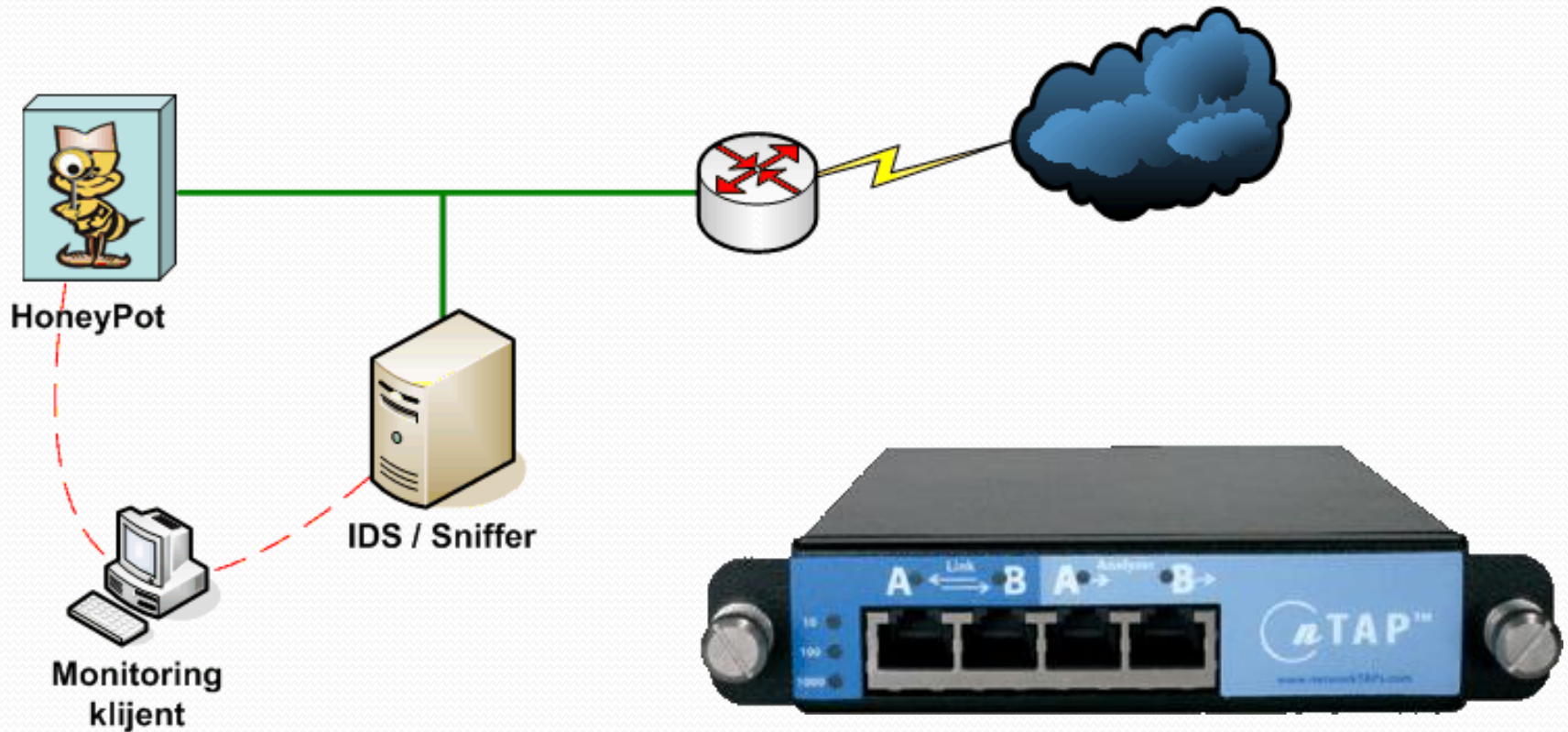
HoneyPots / HoneyNets

- HoneyPot je sistem čija je osnovna namena da bude napadnut



HoneyPots / HoneyNets

- Tipična konfiguracija
- Tarpit == HoneyPot (or not?)

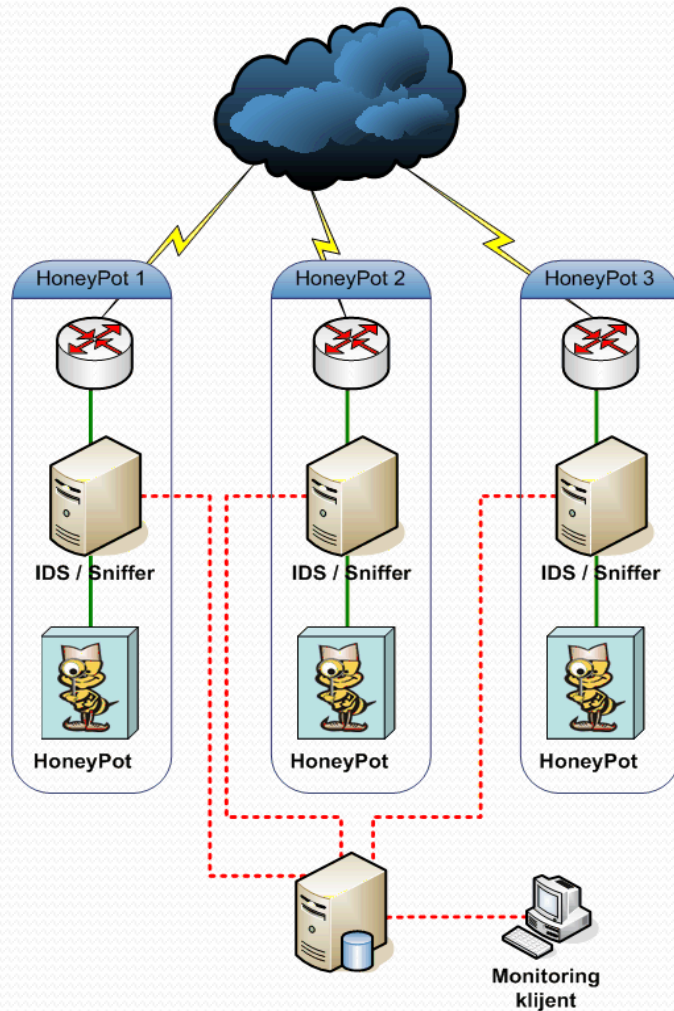


HoneyPots / HoneyNets

- Prevencija
- Detekcija – *no false positives*
 - IDS
- Protivmera
- Analiza
- Edukacija

HoneyPots / HoneyNets

- HoneyNet – više HoneyPotova



HoneyPots / HoneyNets

- Vežba:
 - Konfigurisanje HoneyBot-a
(<http://www.atomicsoftwaresolutions.com/honeybot.php>)
- Više o HoneyX:
 - <http://www.honeynet.org>
 - <http://honeyblog.org/>
 - <http://netsec.rs/UserFiles/File/HoneyPots%20for%20Windows.zip>