

# CompTIA Security+

Network Security Solutions d.o.o.

<http://www.netsec.rs>

Dejan Levaja

# Agenda :: Day I

- **General Security Concepts**

- Understanding Information Security
  - Securing the Physical Environment
  - Examining Operational Security
  - Working with Management and Policies
- Understanding the Goals of Information Security
- Comprehending the Security Process
  - Appreciating Antivirus Software
  - Implementing Access Control
  - Understanding Authentication
- Authentication Issues to Consider
- Distinguishing between Security Topologies
  - Setting Design Goals
  - Creating Security Zones
  - Working with Newer Technologies
  - Addressing Business Concerns
  - Dealing with Telephony Issues

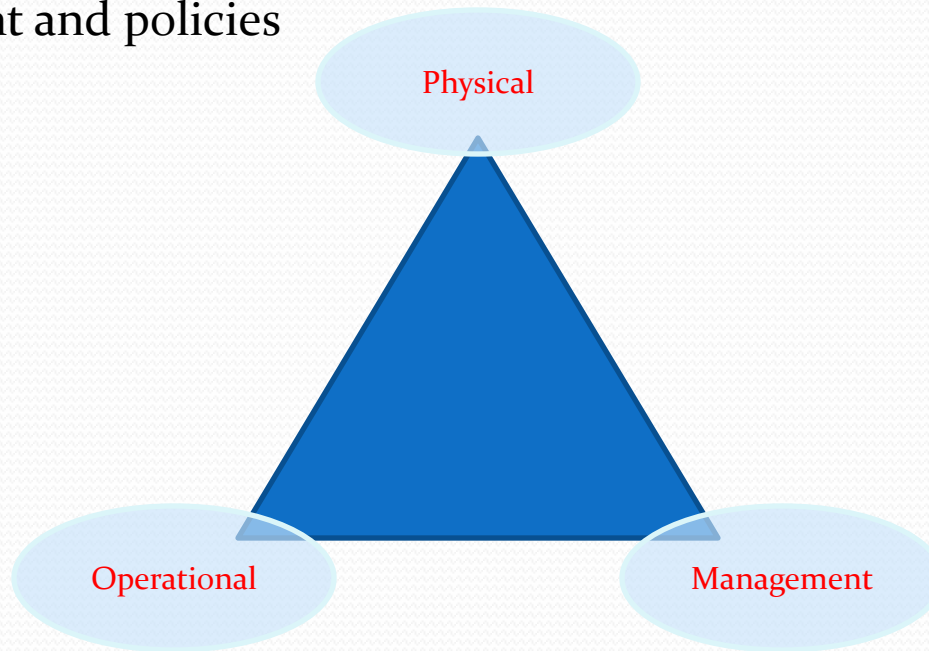
- **Identifying Potential Risks**

- Calculating Attack Strategies
  - Understanding Access Attack Types
  - Recognizing Modification and Repudiation Attacks
  - Identifying Denial-of-Service and Distributed Denial-of-Service Attacks
- Recognizing Common Attacks

- Back Door Attacks
- Spoofing Attacks
- Man-in-the-Middle Attacks
- Replay Attacks
- Password-Guessing Attacks
- Privilege Escalation
- Identifying TCP/IP Security Concerns
  - Working with the TCP/IP Suite
  - Understanding Encapsulation
  - Working with Protocols and Services
  - Recognizing TCP/IP Attacks
- Understanding Software Exploitation
- Understanding OVAL
- Surviving Malicious Code
  - Viruses
  - Trojan Horses
  - Logic Bombs
  - Worms
  - Antivirus Software
- Understanding Social Engineering
- Introducing Auditing Processes and Files

# Understanding Information Security

- definition of security
- Complexity
  - Physical security
  - Operational security
  - Management and policies



# Securing the Physical Environment

- Physical security (and any other)
  - Who?
  - Why?
  - What?
- Physical security is relatively easy to accomplish!
  - Security staff
  - CCTV
  - Document shredding
- I step: making a physical location less tempting as a target
- II step: detecting a penetration or theft
- III step: recovering from a theft or loss of critical information or systems

# Survey your physical environment

- 1. How would you gain access to the building? Is a key or code required? Is there any security—a guard, a receptionist, or cameras? Are they highly visible, or does someone have to look to even know they are there?
- 2. How would you gain access to the floor the server is on? Is the elevator keyed, or can anyone use it? Do the doorways to the stairs only open outward, or can anyone walk up and enter?
- 3. How would you find the server? Is it sitting in the middle of the office, or is it in a separate room? If the latter, is the door to that room secured? How is it secured—by key, badge, punchpad?
- 4. After you reach the server, would anyone see what you're doing? Does the server room have glass windows? Is there a camera overlooking the server? Is the server viewable from a distance? Would anyone question why you were there?
- 5. If you do use cameras for surveillance, where are the tape machines? Are they located near the server so someone can steal the evidence of their crime as well?

# Examining Operational Security

- Operational security focuses on how your organization does that which it does
  - tech stuff : computers, networks, and communications systems as well as the management of information
- Very complex!
- Hard to accomplish!
- Problems: old systems and custom apps (password policy? protocols? ports?...)
- You can install hardware and software to improve security, but management may decide these measures cost too much to implement.

# Survey your operational environment

- How do users on your network access the Internet? Do any users use dial-up connections within the office? Do they use dial-up access when they take their laptops home with them? Are proxy servers in use? Do you use private or public IP addresses? If you are using private IP addresses, are you using something as simple as Internet Connection Sharing or as complex as Network Address Translation (both perform the same function, but the latter offers more functionality and security)?
- Are there wireless access points on the network? Can a mobile user with a laptop configure their settings to join the network? What is the range of your access points? Are signals stopped at the perimeter, or can someone sitting in the parking lot access the network?
- Are dial-in connections allowed? Can users call in from home? Can they call in from hotel rooms? Do you verify the number they are calling from or merely allow anyone in with a correct username/password combination?
- Do you use Terminal Services? Are thin clients employed/allowed? Are entire sessions on the server run remotely? Is remote administration enabled?
- Do your users have shares on their laptops that would potentially compromise the laptop's data security?
- What ports are open on your routers and firewalls (or on a user's personal firewall solution)?

# Working with Management and Policies

- Management and policies provide the guidance, rules, and procedures for implementing a security environment.
- Policies, to be effective, must have the full and uncompromised support of the organization's management team.
- Policies
  - who, what,when, where, why,how...
  - Administrative policies
  - Disaster recovery plans
  - Information policies
  - Security policies
  - Software design requirements
  - Usage policies
  - User management policies
- [http://www.sans.org/reading\\_room/whitepapers/policyissues/492.php](http://www.sans.org/reading_room/whitepapers/policyissues/492.php)

# Understanding the Goals of Information Security

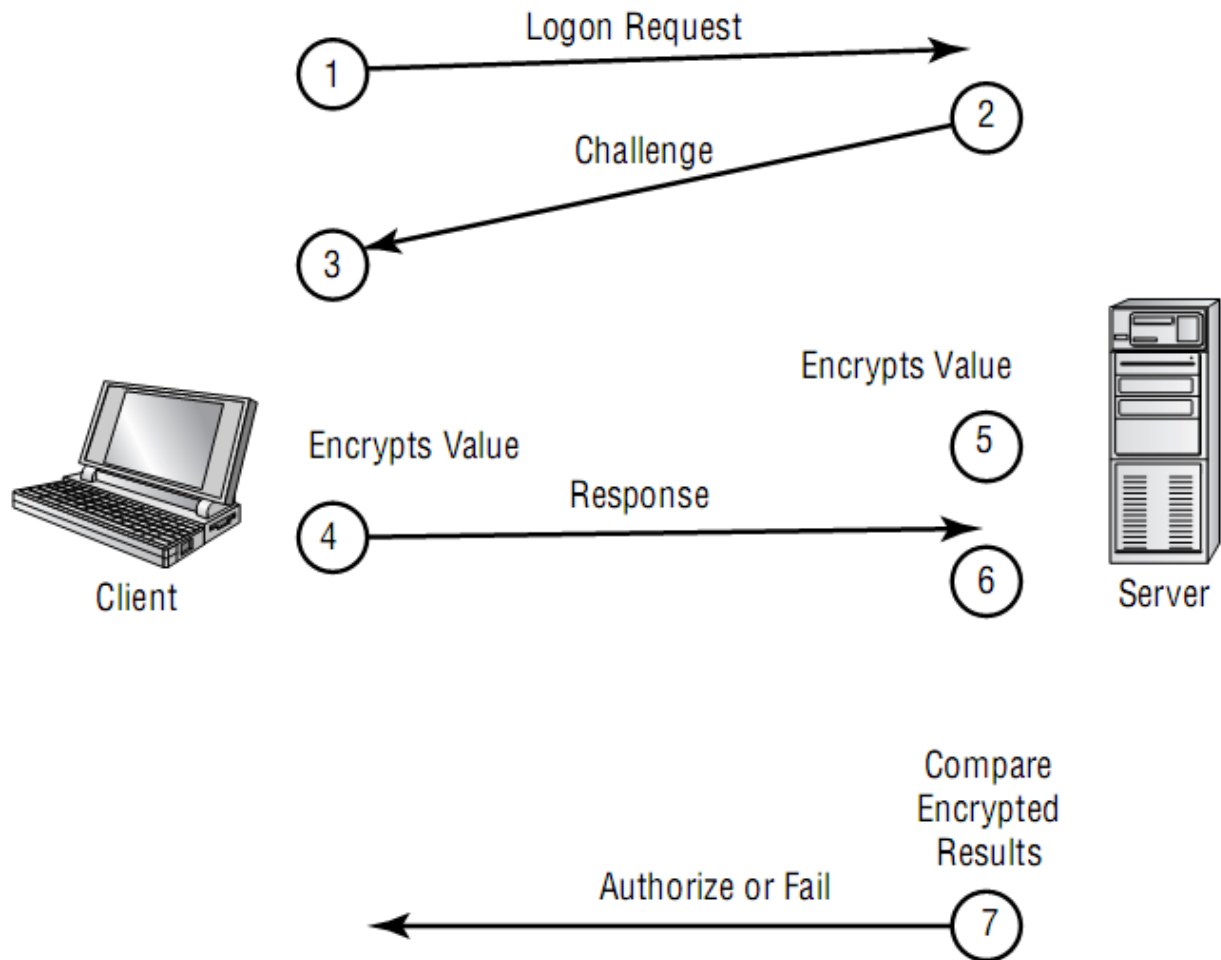
- Easy to express but extremely hard to carry out!
- Prevention of incidents
- Detection
- Response

# Implementing Access Control

- Access control defines how users and systems communicate and in what manner.
- The Mandatory Access Control Method
  - static model that uses a predefined set of access privileges for files on the system.
  - MAC uses labels to identify the level of sensitivity that applies to objects.
- The Discretionary Access Control Method
  - DAC model allows the owner of a resource to establish privileges to the information they own.
- The Role-Based Access Control Method
  - RBAC model allows a user to act in a certain predetermined manner based on the role the user holds in the organization. The roles almost always shadow the organizational structure.
  - MS Active Directory

# Understanding Authentication

- Authentication proves that a user or system is actually who they say they are.



# Understanding Authentication

- Mutual Authentication
  - MS CHAP v2
- Password Authentication Protocol
  - Password in clear text!!!
- Security Tokens
  - hardware(OTP...)
  - Software (OS services, impersonation, user logon session...)
- Smart Cards
- Username/Password

# Authentication Issues to Consider

- Weak passwords (R2D2, C3PO...)
- Shared passwords
- Identification proofing – lost your password?
- *Add your favorite password problem here \_\_\_\_\_ .*
- Finger or not (to) finger...biometrics sucks
  - false positives
  - false negatives
  - detachable authenticators ☹️
  - hygiene
  - .....
- Price?

# Distinguishing between Security Topologies

- The security topology of your network defines the network design and implementation from a security perspective.
- Security topology covers four primary areas of concern:
  - Design goals
  - Security zones
  - Technologies
  - Business requirements
- Setting Design Goals
  - confidentiality
  - integrity
  - availability
  - accountability

# Distinguishing between Security Topologies

- CIA(+A)
  - Confidentiality
    - Meeting the goal of confidentiality is to prevent or minimize unauthorized access to and disclosure of data and information.
  - Integrity
    - Data must be untampered with and unchanged
  - Availability
    - Prevent data loss
    - Practice: Calculate availability per year
      - 99% =
      - 99.9% =
      - 99.99% =
      - 99.999% =
      - 99.9999% =
  - Accountability
    - who is responsible?

# Creating Security Zones

- Security zone describes design methods that isolate systems from other systems or networks.
  - hardware (router, switch, fw...)
  - software (IPSec,...)
- Zones:
  - Internet
    - Big bad jungle
  - Intranet
    - My network
  - Extranet
    - Extranets extend intranets to include outside connections to partners.
  - Demilitarized zone (DMZ)
    - Separates public from private network
- Intrusion vs Extrusion
- Designing Security Zones

# Working with Newer Technologies

- Virtualization Technology
  - Server
    - VMWare (~100% of fortune 100 😊 )
    - Xen
    - Hyper-V
  - Desktop
    - VMWare
    - Microsoft
    - Sun
    - ....
- Virtual Local Area Networks
  - Broadcast problem solved 😊
  - VLANs can increase security by allowing users with similar data sensitivity levels to be segmented together.

# Working with Newer Technologies

- Network Address Translation
  - Private IP to Public IP
  - Network hiding
  - NAT provides a simple, inexpensive firewall for small networks.
    - Practice: write down private IP ranges
- Port Address Translation
  - Single public IP
  - Microsoft's Internet Connection Sharing
- Tunneling
  - Tunneling refers to creating a virtual dedicated connection between two systems or networks.
  - Most popular being the Layer 2 Tunneling Protocol (L2TP) *Sic!*
  - PPTP
  - IPSec
- VPNs

# Addressing Business Concerns

- Security per se or not?
- Addressing Business Concerns
  - Identifying Assets
    - Asset identification is the process in which a company attempts to place a value on the information and systems it has in place.
  - Assessing Risk
  - Identifying Threats
    - Internal
    - External
  - Understanding Vulnerabilities
    - OS
    - Protocols
    - Apps
    - Telephony
      - VoIP, PSTN PBX, wardialing...

# HANDS ON

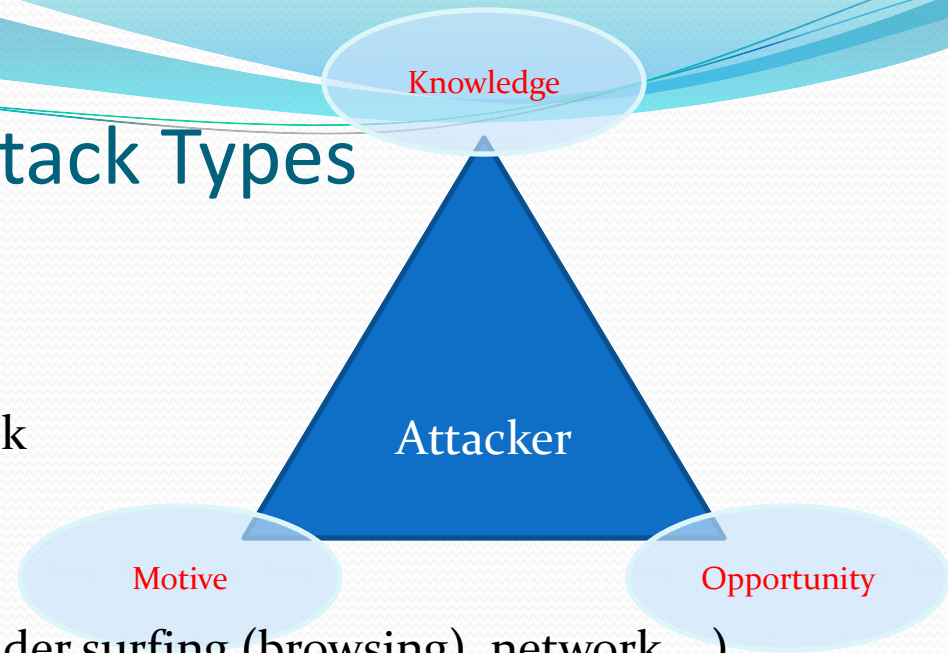
- Update Linux
- Update Windows

TEST

# Identifying Potential Risks

# Understanding Access Attack Types

- Attack goals:
  - Access attack
  - Modification and repudiation attack
  - Denial-of-service (DoS) attack
- Access Attacks
  - Eavesdropping :: passive :: (Shoulder surfing (browsing), network,...)
  - Snooping :: active :: (Dumpster diving, Piggybacking, file snooping/searching...)
  - Interception :: active/passive :: (Government agencies 😊)
- Recognizing Modification and Repudiation Attacks
  - repudiation vs nonrepudiation



# Understanding Access Attack Types

- Identifying DoS and DDoS attacks
  - TCP Syn Flood
  - Ping Of Death
  - BoF *Sic!!!*
  - *zombies, masters i IRC*
  - botnets
  - DoS protection?

# Recognizing Common Attacks

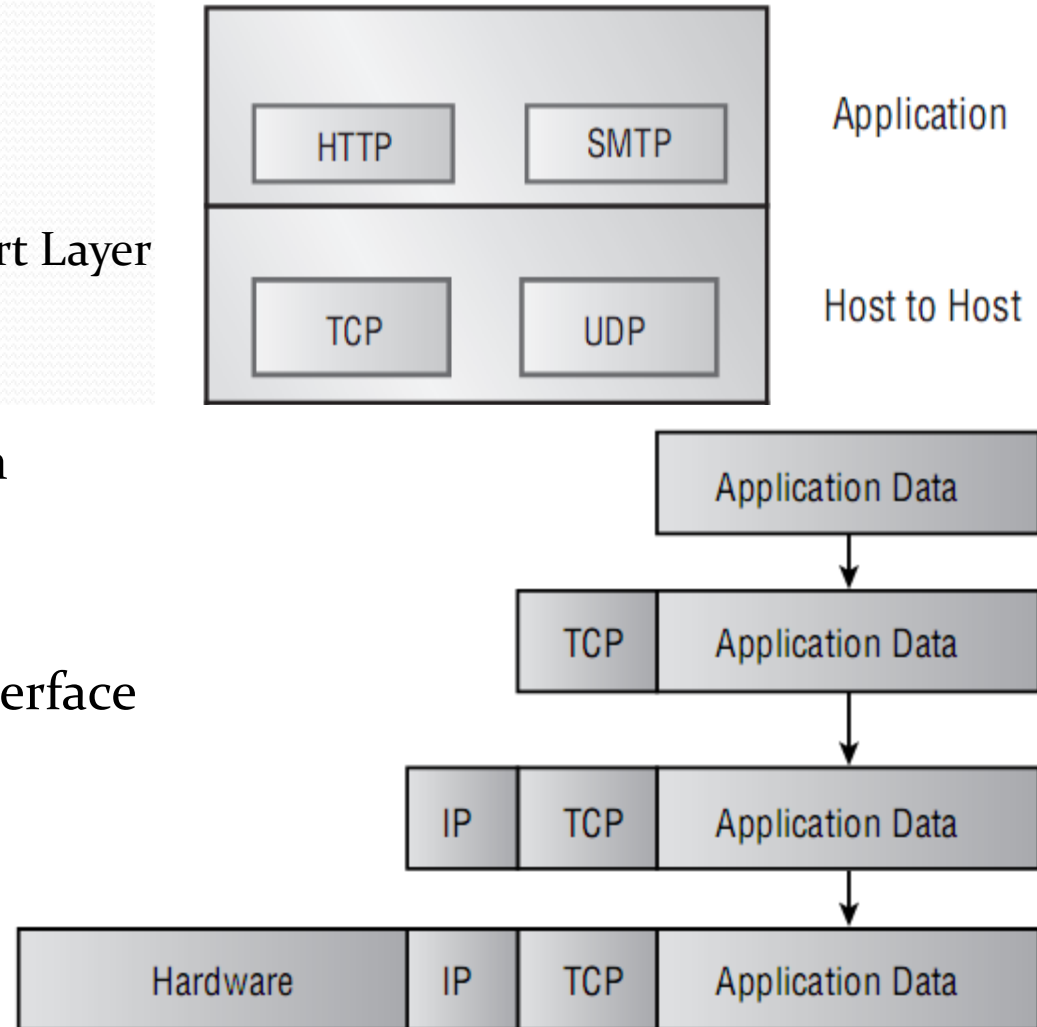
- Back Door Attacks
  - BackOrrifice, NetBus – you’ve got to be kidding? It’s so 90’s 😊
  - PoisonIvy, BitFrost – so 2010! (not in your book!)
- Spoofing Attacks
  - IP spoofing (nmap)
  - DNS spoofing
  - DNS poisoning
- Man-in-the-Middle Attacks
  - SSL
  - Wireless
  - LAN
- Replay Attacks

# Recognizing Common Attacks

- Password-Guessing Attacks
  - Brute-force attack
  - Dictionary attack
  - salt, rainbow tables...
- Privilege Escalation

# Identifying TCP/IP Security Concerns

- History
- DoD (TCP) model
  - The Application Layer
  - The Host-to-Host or Transport Layer
  - The Internet Layer
  - The Network Interface Layer
- Understanding Encapsulation
- Well-Known Ports
- TCP Three-Way Handshake
- Application Programming Interface



# Recognizing TCP/IP Attacks

- Sniffing the Network
  - Wireshark, tcpdump, netmon....
  - Hub vs Switch
- Scanning Ports
  - nmap, telnet...
- TCP Attacks
  - TCP SYN (or TCP ACK Flood Attack) **Sic!!!**
  - TCP Sequence Number Attack
    - hijacking
- UDP Attacks
  - UDP flooding
- ICMP Attacks
  - Smurf
  - ICMP Tunneling

# Understanding Software Exploitation

- Database exploitation
- Application exploitation
- Understanding OVAL
  - Open Vulnerability and Assessment Language
  - <http://oval.mitre.org>
- E-mail exploitation
- Spyware
- Rootkits

# Surviving Malicious Code

- Malicious code refers to a broad category of software threats to your network and systems, including viruses, Trojan horses, bombs, and worms.
- Viruses
  - polymorphic
    - Polymorphic viruses change form in order to avoid detection.
  - stealth
    - A stealth virus attempts to avoid detection by masking itself from applications.
  - retroviruses
    - A retrovirus attacks or bypasses the antivirus software installed on a computer.

# Surviving Malicious Code

- multipartite
  - A multipartite virus attacks your system in multiple ways.
- armored
  - An armored virus is designed to make itself difficult to detect or analyze.
- companion
  - A companion virus attaches itself to legitimate programs and then creates a program with a different filename extension. This file may reside in your system's temporary directory.
- phage
  - A phage virus modifies and alters other programs and databases.
- macro viruses
  - A macro virus exploits the enhancements made to many application programs.
- Symptoms of a Virus Infection

# Surviving Malicious Code

- Identifying Hoaxes
  - “Good time”, “Irina”
- Trojan Horses
- Logic Bombs
- Worms
- Antivirus Software

# Understanding Social Engineering

- Phishing
- Pharming

# Introducing Auditing Processes and Files

- security logs
- audit logs

# HANDS ON

- Identify running processes on a:
  - Windows machine
  - Linux machine

# Introducing Auditing Processes and Files