M2 CyberSecurity
Threat and Risk Analysis, IT Security Audit and Norms

Security Assessment of Information System
Standards, Methods and Tools

Florent Autréau - florent.autreau@imag.fr
2016 /2017

Exercise 6

- Cheating – Fake Exam
  - Exam situation : write down the 100 first digits of PI
  - Describe the strategies used for cheating and the potential countermeasures

What is a Security Audit ?
For what Purpose ?

Information Security Audit

- Audit :
  - Risk Assessment
  - Assessment and Evaluation of conformance with security policy and set of security rules.
- Reference : Set of rules defining organization, procedure and/or technology to ensure information security.

Why assessing Information Security ?

- Evaluate and validate security practices (control, quality processes);
- Validate procedures to alert, react and handle incident or disaster;
- Detect “forgotten/ignored” stakes or weaknesses;
- Educate users, management, employees to Information Security and Risk Management.

Phases of the Audit

- Preparation
- Documentation Review
- Interviews, talks, visits
- Technical Investigation, Data Collection
- Data Analysis
- Synthesis and report writing
- Report Presentation
- Planning corrective actions

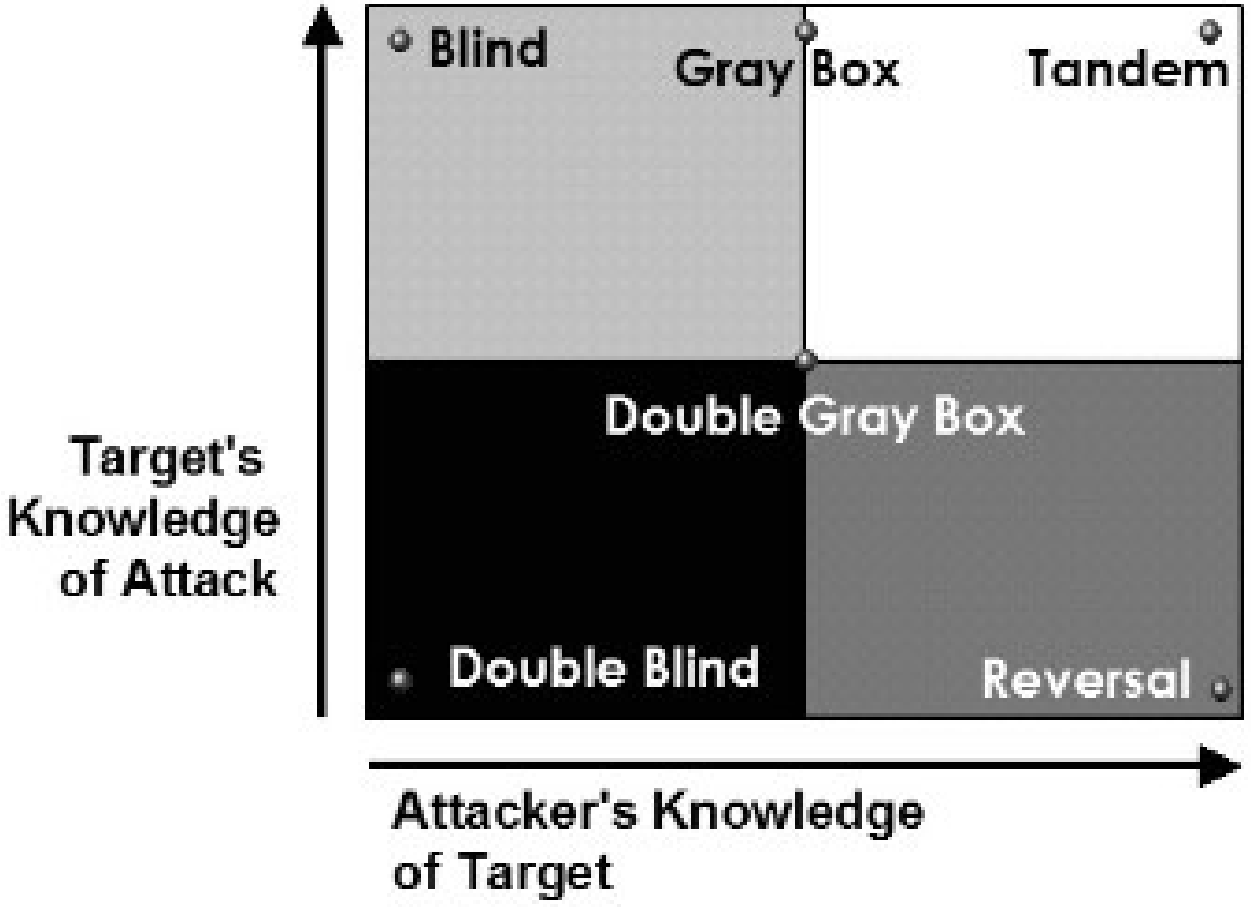

OSSTMM
Discovery:
Obtaining and analysis of the existing system documentation
Enumeration Verification:
Testing of the operating systems, the configuration and services in comparion with the system documentation
Vulnerability Research & Verification:
Vulnerability research and analysis by penetration tests
Integrity Testing:
Integrity testing of all results
Security Mapping:
Mapping of the measured security. Mapping of the results on systems and services.
Risk Assesment Value:
Calculation of the RAV and risk classification of the weaknesses found.
Reporting:
Mapping of the results and giving of recommendations

InfoSec Audit (1)

- "White Box "
  - audit in situ;
  - Access to buildings, organization, data, processes, documentation and procedures;
  - Access to people with interviews of managers and people in charge of operation.

InfoSec Audit (2)

- " Black Box "
  - Partial knowledge and/or access to the Information System (organization, documents procedures, sites, people);
  - Reveal/spot weaknesses :
- Ex: penetration testing.


Blind
Gray Box
Tandem
Double Gray Box
Double Blind
Reversal
Target's Knowledge of Attack
Attacker's Knowledge of Target

Who can perform an audit ?

- *AUTHORIZED* personal
    - System/network administrator, consultant, contractor
- Technical and Business Knowledge
- Excellent Communication Skills
- Certified (ex: ISO Lead Auditor)

Trained and Educated people

Limitations

- Based on interviews with declarations and claims that can be twisted (intentionally or not);
- Context and time dependent;
- Snapshot / view.

How to perform an Audit ?

Where to start ?

- Define the contract : daily job, mission, contract, order, ...
- Define the type of audit (host-based, network-based, 'white-box', 'black-box', penetration testing, ...)
- Define perimeter and schedule
- List people to be involved

How to perform an Audit ?

- Define the type of Audit, Target, Perimeter
- Prepare the Tools
- Review Policies and Documentation
- Data Collection
- Analyze and Synthesis
- Writing the Report
- Presentation
- Planning Corrective Actions

Collect information

- Collect information on the target :
  - Documentation : policies, “chartes”, etc ...
  - Interview
  - Research : Google, Whois, DNS, department of commerce ...

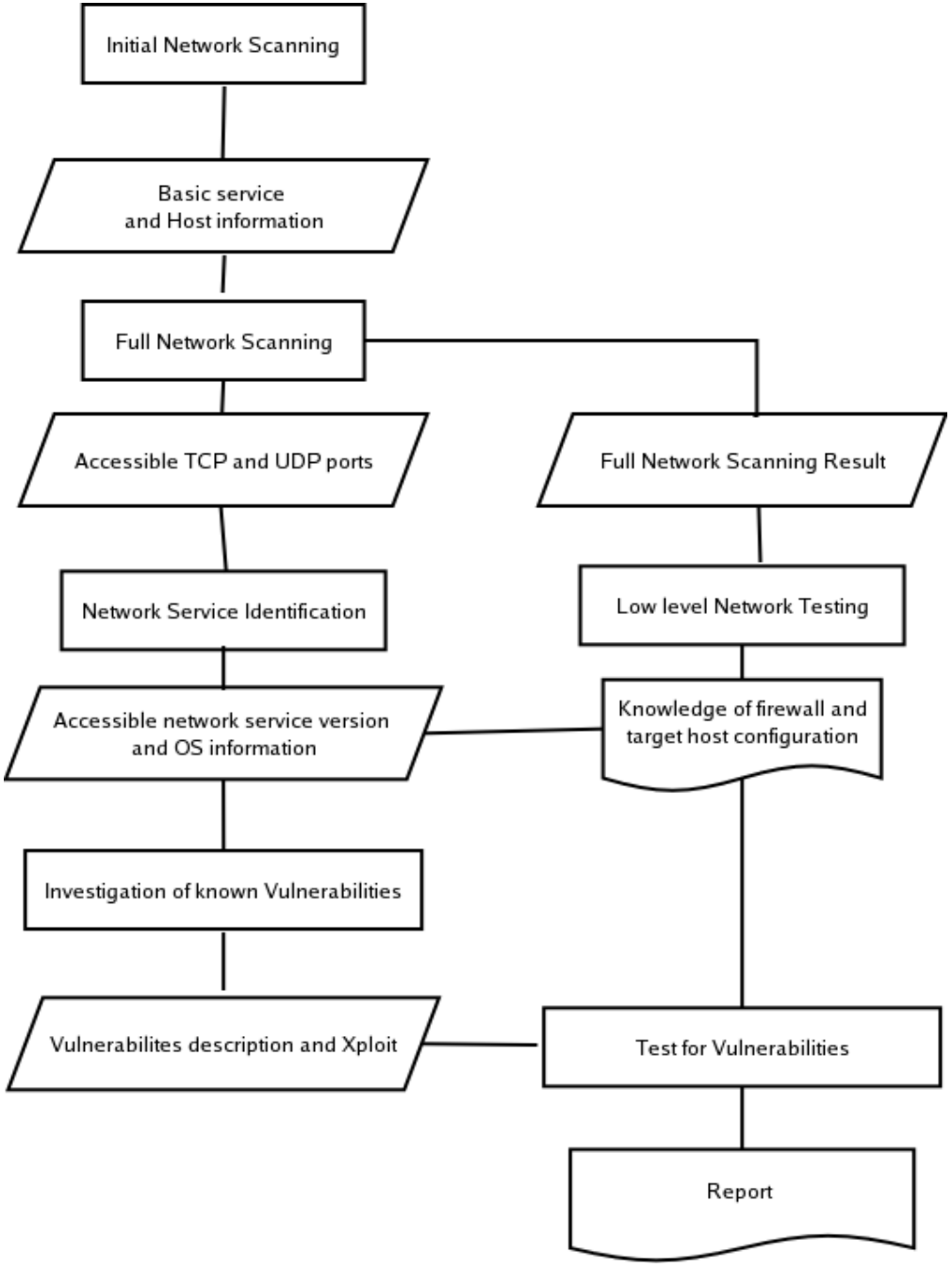
Goal: Identify systems, processes, applications, people, organizations as well as documents

Cartography

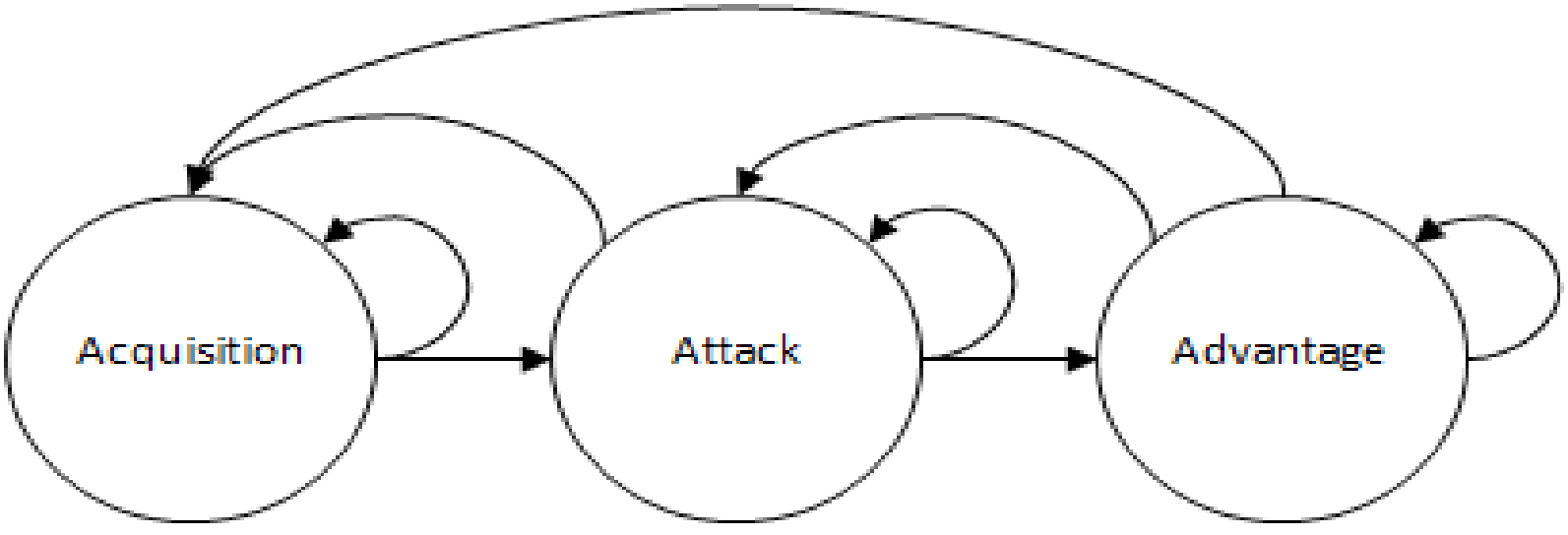
- Detection of systems and services , cartography :
  - Locating and visiting sites and buildings (if possible)
  - Documentation
  - Asset Management Tools or Network Management
    - Ex: HP OpenView, Lan Manager, Nagios, ...
  - Network Topology : IP routing, SMTP ...
  - Detection of ports/services
  - Identification of systems

Looking for Vulnerabilities

- Scan and exploitation of vulnerabilities :
  - Physical (garbage dumping, wires, access to resources)
  - Network (filtering policies, equipments)
  - Systems (patches, active services)
  - Applications
    - Web Server,
    - Database,
    - Mail Server,
    - Directory,
    - ...


Initial Network Scanning
Basic service and Host information
Full Network Scanning
Accessible TCP and UDP ports
Full Network Scanning Result
Network Service Identification
Low level Network Testing
Accessible network service version and OS information
Knowledge of firewall and target host configuration
Investigation of known Vulnerabilities
Vulnerabilites description and Xploit
Test for Vulnerabilities
Report

- Take and Secure Position
- Progress
- Move Deeper and Deeper



Adversaries act in cycles, not linearly

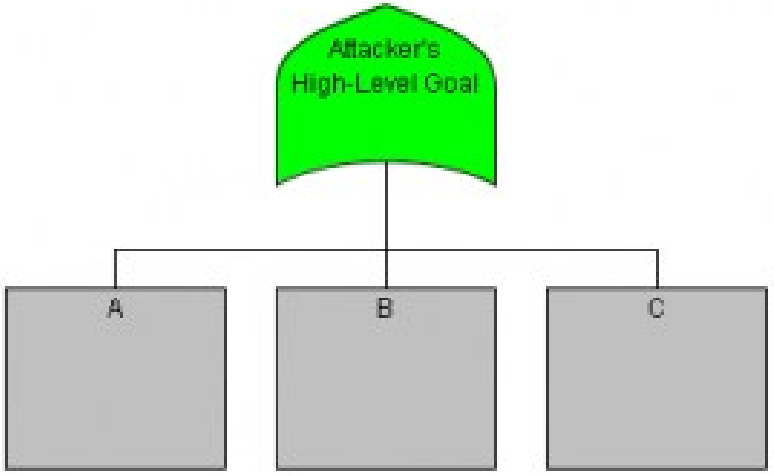
Attack Trees

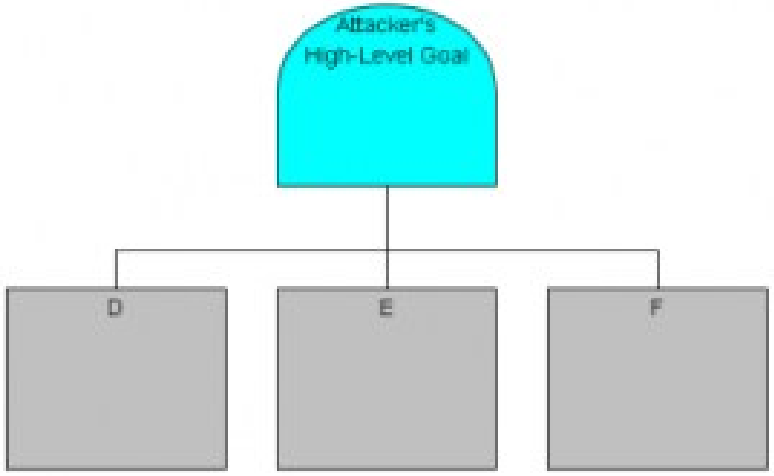
Attack trees are a graphical and mathematical construct (similar to decision tree diagrams) used to

- Identify potential hostile activities (greatest risk);
- Determine effective strategies for reducing the defender's risk to an acceptable level;
- Describe the potential interactions between the adversary and the defender;
- Provide a communication mechanism for security analysts;
- Capture what is known (facts) and believed (assumptions) about the system and its adversaries, and store the information in a form that can subsequently be retrieved and understood by others.

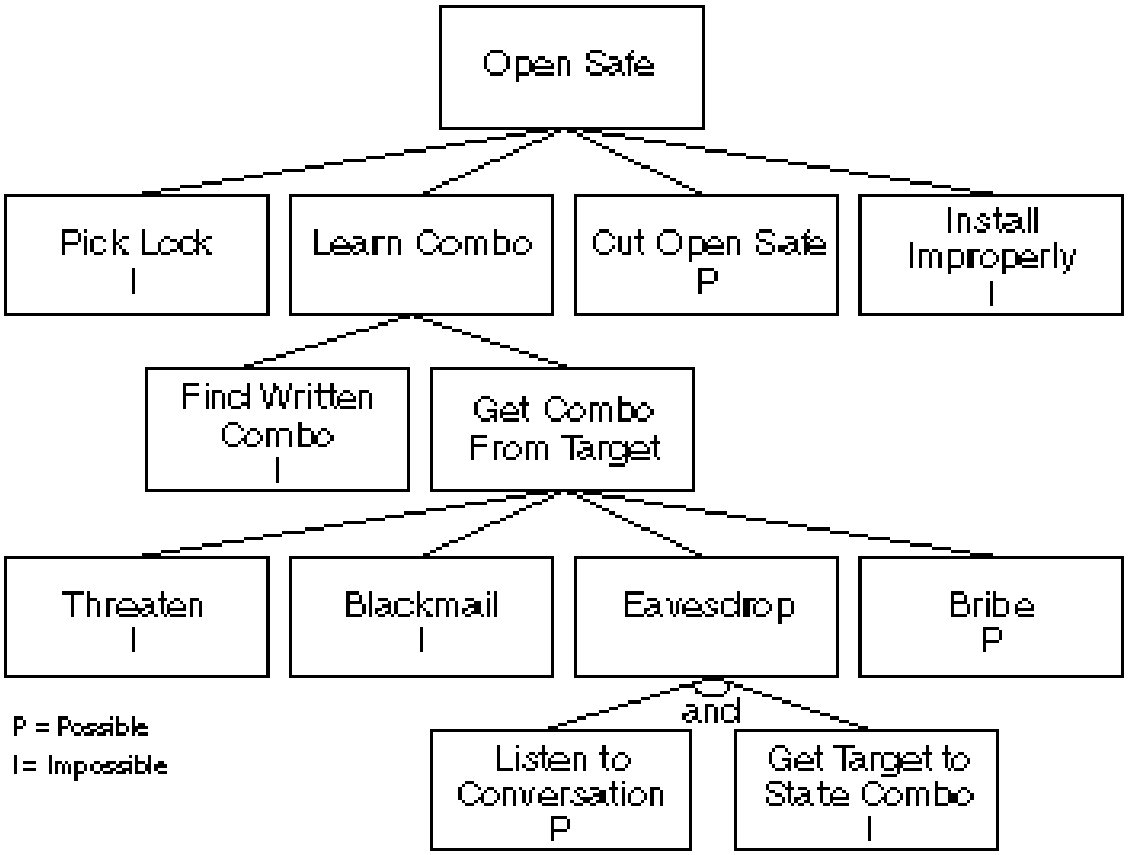
Attack Trees

- Goals / Objectives
- Nodes : Steps with properties/values (potentiality, proba, cost)
- AND/OR relationships





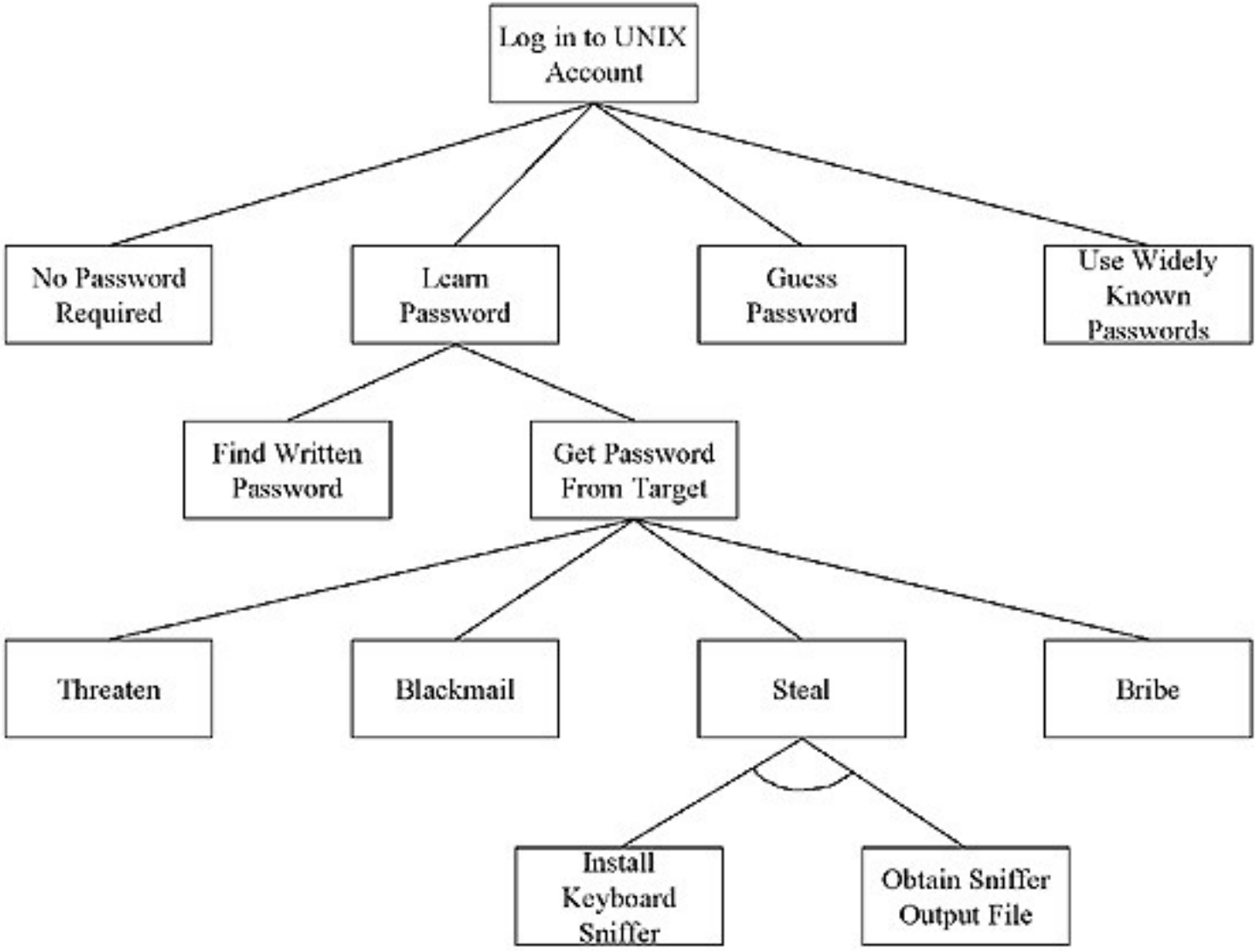
How to open a safe (from www.schneier.com)



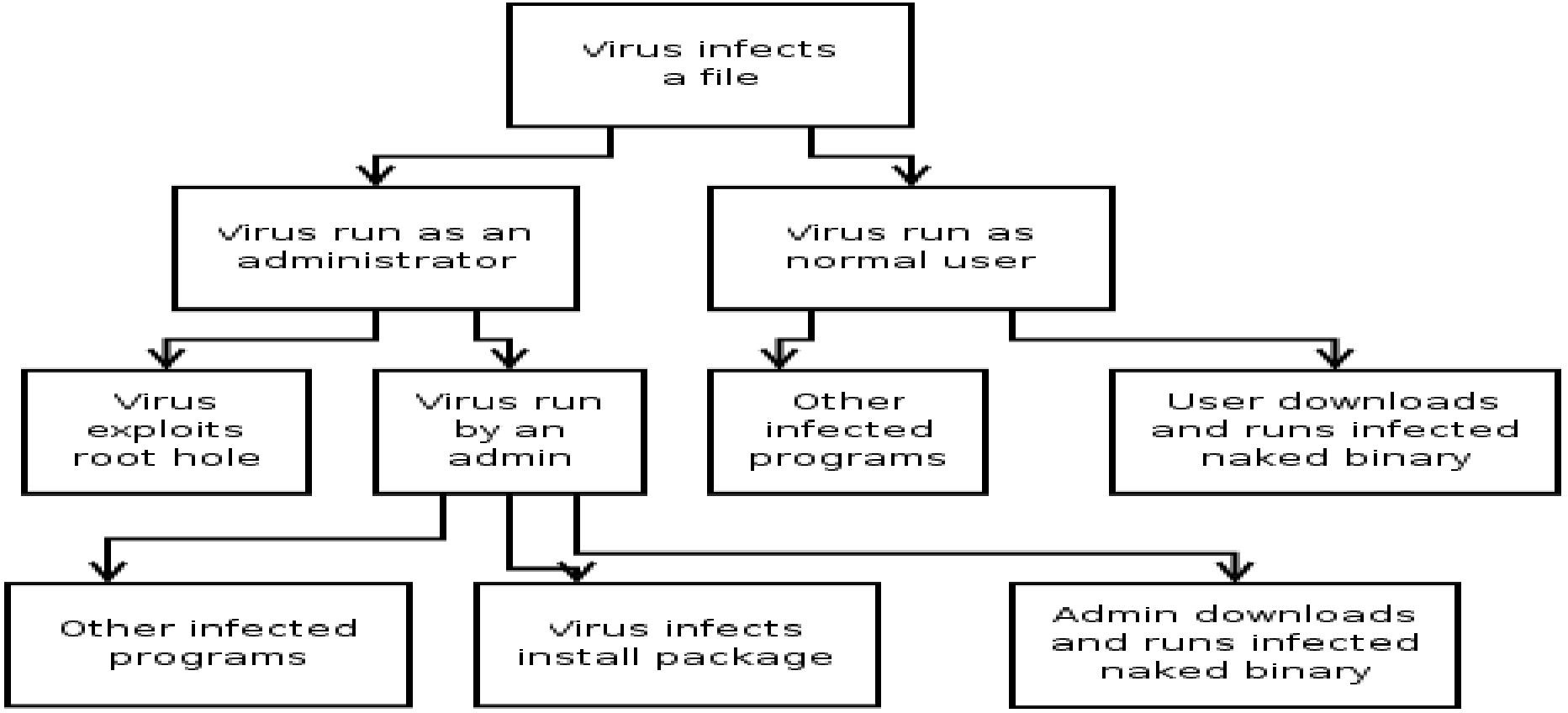
Attack/Fault Tree Analysis

FTA : Fault Tree Analysis

- Start with target or undesired event to study
- Identify possible attacks and conditions
- Construct and evaluate the attack/fault tree
  - By break down
  - Specify frequency/probability/costs
- Risk mitigation / hazard control

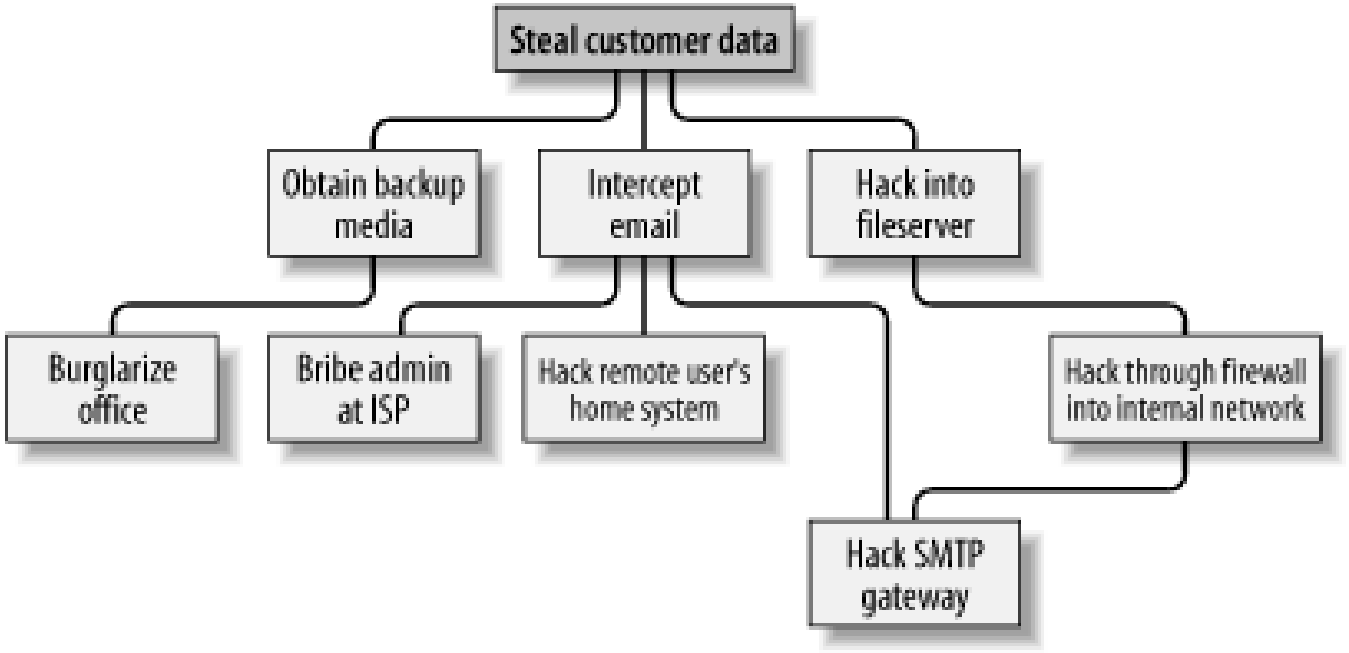

Log in to UNIX Account
No Password Required
Learn Password
Guess Password
Use Widely Known Passwords
Find Written Password
Get Password From Target
Threaten
Blackmail
Steal
Bribe
Install Keyboard Sniffer
Obtain Sniffer Output File

Attack Tree – Virus infection

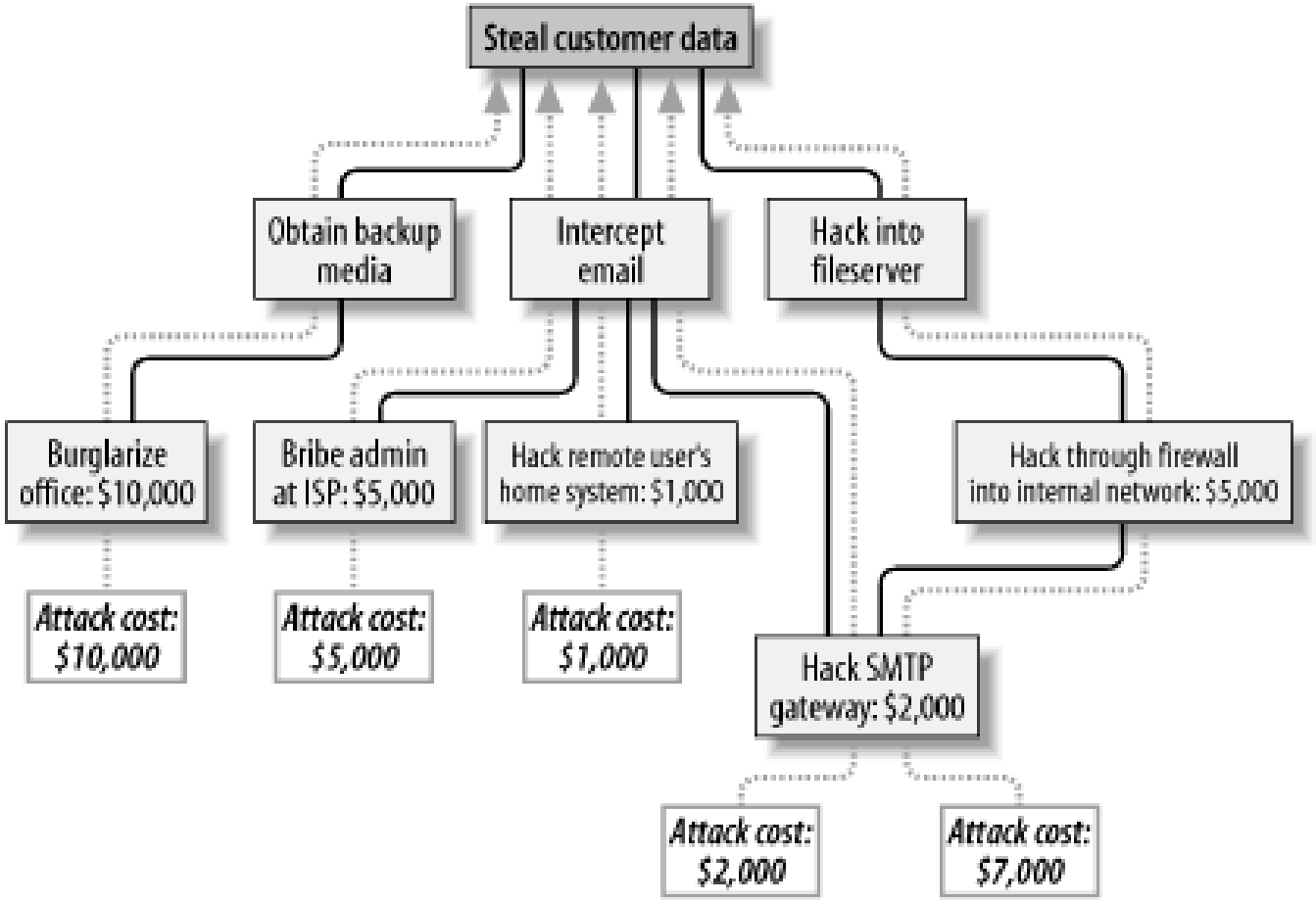


Attack Tree (start with root goal)

Attack Tree (with more details)



Attack Tree (with cost estimates)



Tutoring

Exercise 7

- Present a threat/attack tree for the scenarios used in Exercice 5 (as a preparation for lab):
    - Role : student in M2 CySec

      Target : any personal informational assets exposed/used while in F103 or other university Lab room.
    - Role : sysadmin working for the university

      Target : availability of lab systems in F103 or other room.

Exercice 8 - Attack Tree - IoT

Formaliser votre analyse sous la forme d'un arbre d'attaque en vous basant sur la catégorisation des vulnérabilités publiée par l'OWASP, OWASP - Internet of Things Top 10 - 2014 :

I1 Insecure Web Interface

I2 Insufficient Authentication/Authorization

I3 Insecure Network Services

I4 Lack of Transport Encryption

I5 Privacy Concerns

I6 Insecure Cloud Interface

I7 Insecure Mobile Interface

I8 Insufficient Security Configurability

I9 Insecure Software/Firmware

I10 Poor Physical Security

en traduisant les catégories (ex : pas d'authentification)

en identifiant l'objectif principal et le possible impact (ex : acces a interface administratif)

en précisant pour chaque noeud terminal (stratégie d'attaque) leur faisabilité, les contre-mesures possibles, ... (ex : authentification forte)