Security Audit M2 Cybersecurity

Introduction

Fault : Defect, imperfection or fault that occurs in hardware or software.

Error : Occurrence of an incorrect value in some unit of information within a system. Manifestation of a fault.

Failure : Deviation in the expected performance of a system.

Detection : Recognising that a fault/error has occurred.

Containment/Isolation : Isolating a fault and preventing its propagation throughout a system.

Recovery : Restoring the system to a stable (operational) state.

Repair : Repairing a faulty FRU

Reliability - Ability to function correctly over a specified period of time.

Availability - Probability that a system is performing at the instant t, regardless the number of times it has been repaired.

MTTF = Mean Time To Failure

MTTR = Mean Time To Repair

What is unavailability : Unplanned causes of downtime:

- Extended Planned Downtime
- Human Error
- Software (OS, Application, Database, Middleware) Failure
- Network Failure
- Disk / Hardware Failure
- Disasters (fire, tornado, earthquake, ...)

Planned causes of downtime:

- Backup
- Software Maintenance
- Hardware Maintenance
- Application / Database Upgrade
- Operating System Upgrade
- Hardware Upgrade

Dependancy Gaph :

Concepts

Cybersecurity : “Everything that results in protecting information and underlying technology from theft, manipulation and disruption”

Information system : Conventional support for information :

- Desktop / Server / Laptop / Printer / Network equipment (switches, routers, ...) / Hosted services and ressources / Professional and personal Mobile Phone / Phone System / Connexion Card, Access Token / Mobile storage devices : USB Keys, SD-RAM / Media reader, Game System / Credit card.

Security engineering : Tools, processes and methods required to design, implement, deploy, operate and test security of systems.

Information security : properties for information :

- Confidentiality
- Integrity
- Availibility
  CIA triangle

Goal : insure that Information is always Available ONLY to Authorized People

Properties : Confidentiality / Control / Integrity / Authenticity / Utility / Availability / Accessibility / Performance / Usability / Manageability.

Business assets :

- Availability : Make sure that IT services and resources are available for accredited users (employees, customers, partners, contractors).
- Integrity : Make sure that information as well as information processing is exact, reliable, trusted and eventually provable.
- Confidentiality : Make sure that IT services and resources are ONLY available to accredited users
- Authenticity (authentication and integrity)
- Traceability, Auditability, Non-repudiation
- Reputation / Branding
- Liability

Intro to risk management

Risk Analysis :

Threat :

- what from you want protect valuable assets.
- anything (man made or act of nature) that has the potential to cause harm (a.k.a Menace)

Threat Agent : Specific entity that manifests the threat (by carrying out an attack).

Vulnerability **:**

- Failure or Deviation of the Information System
- weakness that could be used to endanger or cause harm to an informational asset

Risk :

- when Threat exploits Vulnerability against Valuable Asset
- Probability that event will happen with a negative impact to an informational asset

ISO 27005/31000 Def :

Asset**:** anything that has value to the organisation;

Threat : a potential cause of an unwanted incident, which may result in harm to a system or organisation.

Vulnerability : a weakness of an asset or group of assets that can be exploited by one or more threats.

Risk : Probability of an event that will have an impact on objectives. Combination of the probability of an event and its consequence ; when Threat exploits Vulnerability against Valuable Asset

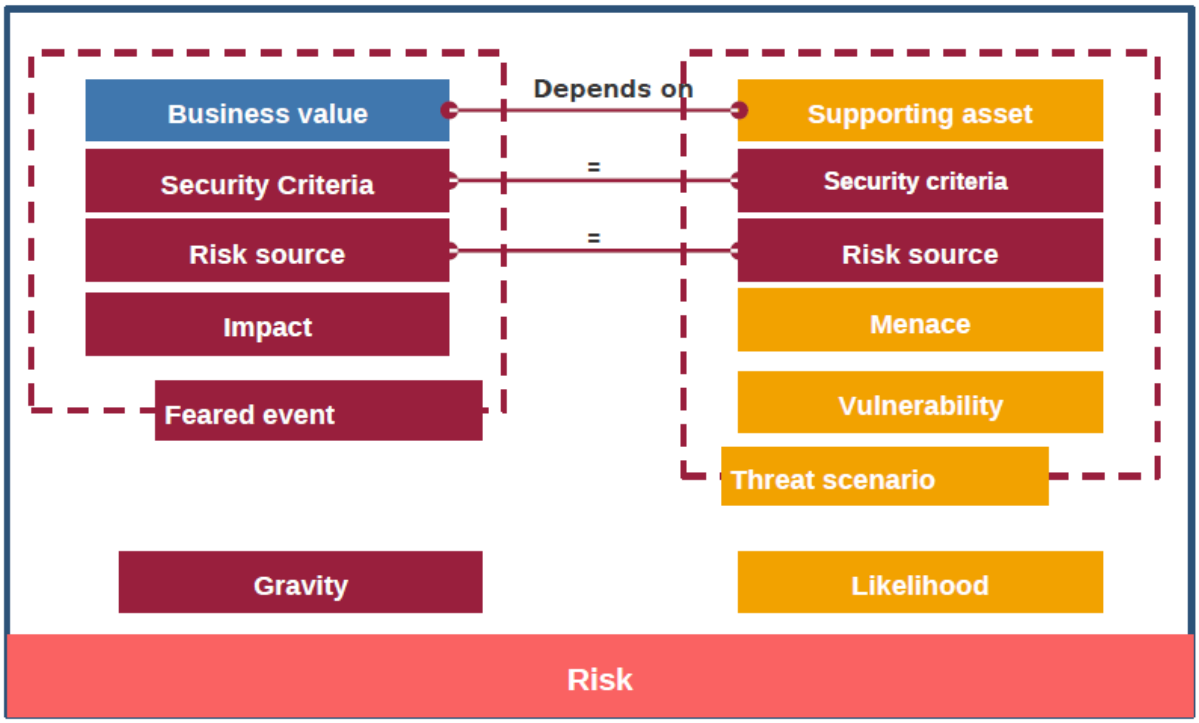
Exposure : State of the Asset being exposed to harmful event (threat)

Vector : Path or Means by which the threat impacts the asset

Incident : Event that indicates Asset compromised or impacted / Any attack, all attacks using vulnerability X, etc. / Service degradation

Attack : Act or action that exploits vulnerability accomplished by threat agent which impacts/damages Asset.

What is a risk?



Type of losses :

Productivity Loss = Losses that result from an organization's inability to deliver its products or services.

Response Loss = Losses that are associated with managing the event itself. This form of loss will be the most common across your analyses.

Replacement Loss = The costs associated with the replacement of a capital asset or a person.

Fines and Judgements = Penalties levied against an organization through civil, criminal or contractual actions, usually the result of a Confidentiality related scenario.

Competitive Advantage = Losses associated with a diminished competitive advantage.

Reputation Damage = Losses associated with an external actor's perception of your organization whereby its main value proposition is diminished.

Security as a process :

1. Identify the assets at risk
2. Ascertain enemies interested in it and assess capabilities
3. Select application technologies
4. Evaluate vulnerabilities for each component
5. Identify defensive solutions
6. Estimate cost including damage

ALE = Annual Losses Expectancies

Risks and Threat

What : Equifax, a US credit reporting agency, reported that information about 145 million people, have been compromised. Attackers used a vulnerability of Apache Struts.

WannaCry :

➔ Ransomware worm targeting Windows OS, spreading via SMB and leading to encrypt data on filesystem. The infection used a vulnerability in SMBv1 (Shadow Brokers 1st batch – ETERNALBLUE). Despite patches made available 2 months before, morev than 300,000 computers across 150 countries are believed to have been impacted

SolarWinds / SunBurst :

➔ In the SolarWinds attack, the hackers executed an attack that exploited a vulnerability in supply chain for management software created by a company called SolarWinds. That software, which is called Orion, is widely used by Fortune 500 companies and government agencies, and international companies. Hackers compromised SolarWinds' software and inserted their own malicious malware (called Sunburst), which then pushed out as a regular update to Orion.

KRACK :

➔ Key Reinstallation AttaCK (KRACK) – Attack against WPA2 protocol 4-way handshake. Attacker collects and replays retransmissions of message 3 of the 4-way handshake, causing re-use of previously used key.

CVE – Common Vuln Enum // NIST NVDB / cvedetails.org

CWE – Common Weaknesses Enum // cwe.mitre.org

CVSS – Common Vuln Severity Score

Methods and standards (ISO2700x, EBIOS, OSSTMM, FAIR, ATT&CK)

Purpose of InfoSec Standards :

- Protection of informational assets : way to all agree on the same language
- Sign (if not Proof) of Trust
- Potential Differentiatior (from Competition)
- Profitability : security is not a source of revenu : this is a cost → stickinig with standard is a cost
- Respect of Legislation and Rules
- Public Image

RGPD (EU) / HIPAA – Heath Information Protection Assurance Act.

Auditing : compare implementation with standards

ISMS : Information Security Management System.

ISO 27000 Standards : Risk Assessment.

Risk Assessment Language :

- What is at stake ? **Security Criteria**
- What to protect ? **Business Value**
- From who to protect ? **Risk Sources**
- Why do I want to protect ? **Feared Event**
- From what to protect ? **Threat Scenarios**
- What are the risks ? **Risks**
- How to protect ? **Treatment and mitigation measures**
- What are the acceptable risks ? **Residual risks / Security debt**

ISO 27005 – Risk Analysis

Step 1 : Context Study

Goal : Definition of perimeter and evaluation criteria for the risk analysis

The context study defines the criteria and metrics to quantify :

- Impact (categories/level)
- Potentiality of scenarios
- Criteria for Acceptance.

Step 2 : Identify Assets

Goal: mapping of valuables / discovery of perimeter

Identification of assets to insure :

- That no asset has been ignored or forgotten ;
- That the perimeter of risk analysis is clearly defined.

Step 3 : List Threats and existing Countermeasures

Goal : Identify Threats, Vulnerabilities and Countermeasures.

Based on the Context Study :

- Identify threats against assets ;
- Identify countermeasures ;
- Identify existing vulnerabilities.

Step 4 : Estimate Security Issue

Goals : Evaluate security needs for perimeter

Based on interviews of stakeholders, quantify needs/requirements for the security of assets.

Step 5 : Define Risk Scenarios

Goal : Define the risk scenarios

Risk Scenario : exploitation, by a threat of existing vulnerability on given asset.

Step 6 : Estimation of Risk Scenarios

Goal : Estimate impact and likelihood of scenarios

From the list of scenarios and used scales :

- Quantify impact;
- Quantify likelihood

Step 7 : Classify Risk Scenarios

Goal : Evaluate and Classify the Risk Scenarios

- Evaluate criticality of scenarios : **Criticality = Likelihood x Impact**
- Classify scenarios to identify remaining risks.

Methods : MEHARI (MEthode Harmonisée d'Analyse de Risques) / EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) / Octave / OSSTMM (Open Source Security Testing Methodology Manual)

Audit Cookbook

Compliance : Done to satisfy external requirements / Driven by business needs, not technical demands or events / Checklist based.

Security is: Done to protect assets and resources / Motivated by a need to defend assets against threats / Risk-based / Continuous and never ending.

Security + Compliance: Compliance establishes a baseline security posture / Security identifies and addresses all known risks to assets.

Audit : Risk Assessment / Assessment and Evaluation of conformance with security policy and set of security rules.

Why : Evaluate and validate security practices / Detect “forgotten/ignored” stakes or weaknesses.

Who can perform an audit : *AUTHORIZED* personal (System/network administrator, consultant, contractor) / Technical and Business Knowledge / Excellent Communication Skills / Certified

→ *Trained and Educated people*

You are selling a Service so.... Sell something :

- Tools customization
- Knowing what offers and market rates are
- Is this assessment for you?
- Fixed pricing or daily rate
- What does the client want?
- Can you provide what they want?

Scope of the work :: Understand customer’s requirements

- Black, gray, white box testing or red teaming
- How long assessment will take
- What to expect from the assessment
- Client contacts from project manager to network adminstrators in case of emergencies

Use methodologies/strategies that you have created / Remember to log/record everything / Secure communication with clients.

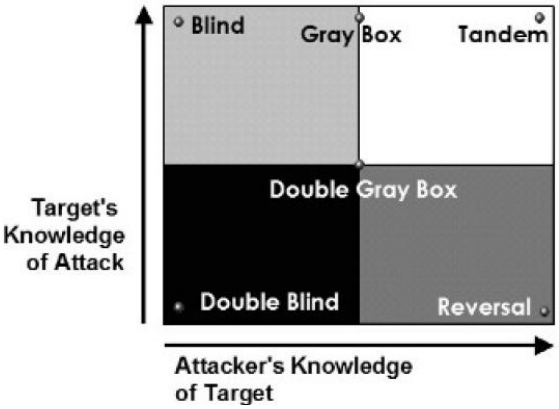
" White Box " :

- 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.

" Black Box " :

- Partial knowledge and/or access to the
- Information System (organization, documents
- procedures, sites, people);
- Reveal/spot weaknesses :

Ex: penetration testing.



Red team : Offensive research and exercices (Red team) is important to maintain the state-of-the-art knowledge and understanding of opponents' strategies.
Blue team : Defensive research and exercices (Blue team) is extremely important to achieve sustainability and resilience.

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

Phases - Pentesting
More Offensive and steath process :

- Reconnaissance
- Scanning and Enumeration
- Gaining Access
- Maintaining Access
- Covering Tracks

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 ?

- 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

Pre-Engagement

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

Reco / Collect information :

- Collect information on the target :
  - *Pentest – gather information passively*
  - Documentation : policies, “chartes”, etc ...
  - Interview
  - Research : Google, Whois, DNS, department of commerce, Wayback machine ...

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

Reconnaissance :

- Check social network (LinkedIn, twitter, FB,...)
- Google dorks
  - *site:<Target> ext:doc,docx,xlsx,pdf*
- Shodan

Cartography – Enumeration :

- Detection of systems and services , cartography :
  - Locating and visiting sites and buildings (if possible)
  - Documentation
  - Asset Management Tools or Network Management
  - 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,
    - ...

Vulnerability Analysis :

- Monitor your scan with sniffer
- Check exploitability manually or script (NSE, bash, powershell, ...)
- Identify false positives
- Focus on critical assets (risk analysis)

Credential attacks :

- Use a target-specific dictionnary (based on reco)
- Use various strategies

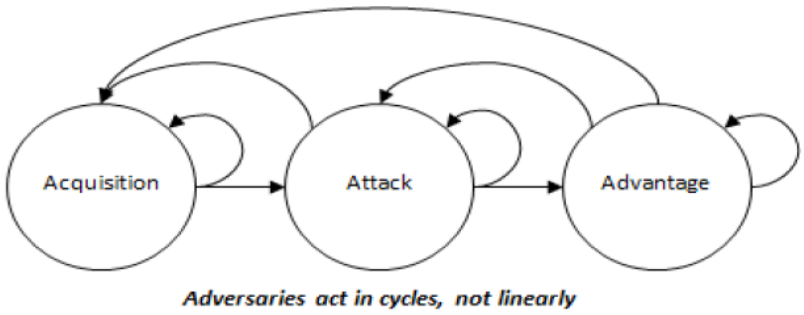
    - Craking, guessing, sniffing, …
- Pass-the-hash (in windows env)
- Hashcat, GPU or cloud based cracker

Exploitation :
- Script for checking availability of targeted service
- Embed reverse connection in payload
- To exfiltrate or reverse tunnel, use common protocols (DNS or HTTPS)
- To avoid crashing targeted Windows, use psexec, WMIC, …

Post-Exploitation :
- Be stealth (ex: no scan or activity easily detected)
- Use sniffer, host-based debugging tools
- Check for established connections (with netstat) or authorized relationships

Document, snapshots, video captures

- Take and Secure Position
- Progress
- Move Deeper and Deeper
    - Keeping account/service access
    - Priviledge escalation
    - Lateral movement / pivoting
    - Extraction / RAT



Threat Modeling and Attack Trees

MITRE Adversarial Tactics, Techniques, and Common Knowledge (**ATT&CK®**) framework.

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.

Tools :

Prepare the Tools

- Safe, Trusted and Autonomous Platform for execution and storage of resulting data.
- Dedicated system (laptop, VM, ...)
- USB-based bootable (such as Kali)
- Retrieve, install and configure necessary tools.
- Eventually development.
- Get used and trained.
- Verify ALL tools used are untampered with.

Security Scoreboards :

Pre-assessment / evaluation using scoreboards to measure and improve security practices

- Using MeHari Quick diagnostic
- Using CIS Top 20 Critical Controls
    - https://www.cisecurity.org/controls/

Discovery Tools :

- Information :
    - WhoIS, Recon-ng, Maltego, The Harvester, Spiderfoot, ...
- DNS :
    - Dig, DNSenum, ...
- IP Topology
    - IP : Traceroute, mtr, 0trace, ...
    - SNMP : SNMPWalk, snmpcheck, ...
    - SMB : LinNeighborood, NBTscan
- Network or System Administration
    - HP-Openview, N-View, Nagios
- Wi-Fi : Kismet
- Bluetooth: BTScanner
- Services :
    - Nmap, masscan
- Google
- Shodan
- Censys, ...
- Facebook, LinkedIn, ...

Discovery – Search Engines :

- censys.io
- https://shodan.io
- https://viz.greynoise.io
- https://zoomeye.org
- https://netograph.io
- https://wigle.net
- https://intelx.io
- https://fofa.so
- https://hunter.io
- https://haveibeenpwned.com
- ZoomEye.org
- PublicWWW.com
- Pulsedive.com

- intelx.io
- reposify.com

Network Flow Analysis :
- Tcpdump
    - Wireshark
    - Etherape
    - Ntop(ng)

Checking Configuration
- HIDS – Host Based Intrusion Detection
    - Windows Security Center
    - MBSA – Microsoft Baseline Security Analyzer
    - Lynis (linux)
    - Debsecan (debian)
    - Sara (Unix)
    - JASS (Solaris)
    - Scripts such as Checkperms
    - Sysinternals Utilities from Microsoft

Vulnerabilities Scanners :
- Framework :
    - Nessus/OpenVAS, Nuclei,
    - Nikto, Wikto, W3af, wapiti, arachni,
    - BlueSnarf
    - Metasploit
- Sending Virus Samples
- Code Injection, Packet Injection (ncat, scapy)
- XSS (Cross Site Scripting)

Fuzzer :
Testing based on random generation of data (either properly formatted and syntaxically correct, or not)
- Application
- Protocols
- File format

Using Firefox as Security Tools :
Testing based on use of Firefox add-ons
- FireCAT – catalog of Auditing Tools
- FoxyProxy – advanced proxy management
- Firebug – edit/debug of CSS, HTML, Javascript
- Flashbug
- Firecookie
- Modify Headers
- XSSme, RegEx Tester

OWASP Top 10 Tools :
A1: Injection – ZAP
A2: Cross-Site Scripting (XSS) - BeEF
A3: Broken Authentication and Session Management - HackBar
A4: Insecure Direct Object References - Burp Suite

A5: Cross-Site Request Forgery (CSRF) – Tamper Data
A6: Security Misconfiguration – Watobo
A7: Insecure Cryptographic Storage N/A
A8: Failure to Restrict URL Access - Nikto/Wikto
A9: Insufficient Transport Layer Protection - Calomel
A10: Unvalidated Redirects and Forwards – Watcher

Toolbox for analysis :

- OSS – keywords based tools
  - RATS, Splint, Flawfinder
- Static Code Analyzer
  - CodeQL, Coverity SWAT , HP Fortify SCA
- Dynamic Code Analyzer
- Protocol Validation (formal or not)
  - Tamarin, Avispa, ProVerif, Scyther

More detailed information on www.dwheeler.com

But also :

- Code Reading (see Software Security)
- Design Analysis
- Protocol Validation (formal or not)
- …

Social Engineering :

- Social Engineering Toolkit (SET)
- Maltego
- Google
- Scythe Framework
- Creepy
- Metasploit
- Recon-NG Framework
- Portable Virtual Box
- Hyperion & Veil

Social Eng. Tools :

- Social Engineer Toolkit http://trustedsec.com
- Gophish:https://github.com/gophish/gophish
- SocialFish:https://github.com/UndeadSe/SocialFish
- Modlishka:https://github.com/drk1wi/Modlishka
- CredSniper:https://github.com/ustayready/CredSniper
- ReelPhish:https://github.com/fireeye/ReelPhish

Hands on labs

Report :

- Analysis and synthesis in report
- Achievement of audit
- Readable and adapted to audience
- From executive summary to detailed annexes
- Adapted to the business objectives
- Definition of an action plan

Audience :

- Executive
- Stockholders
- Managers
- Operational staff
- Technical staff (techno-geek)

Content :

- Title, Introduction, legal
- Executive Summary
- Prioritized recommendations (with cost)
- Report (following the structure of MEHARI domains)
- Conclusion and detailed recommendations
- Annexes