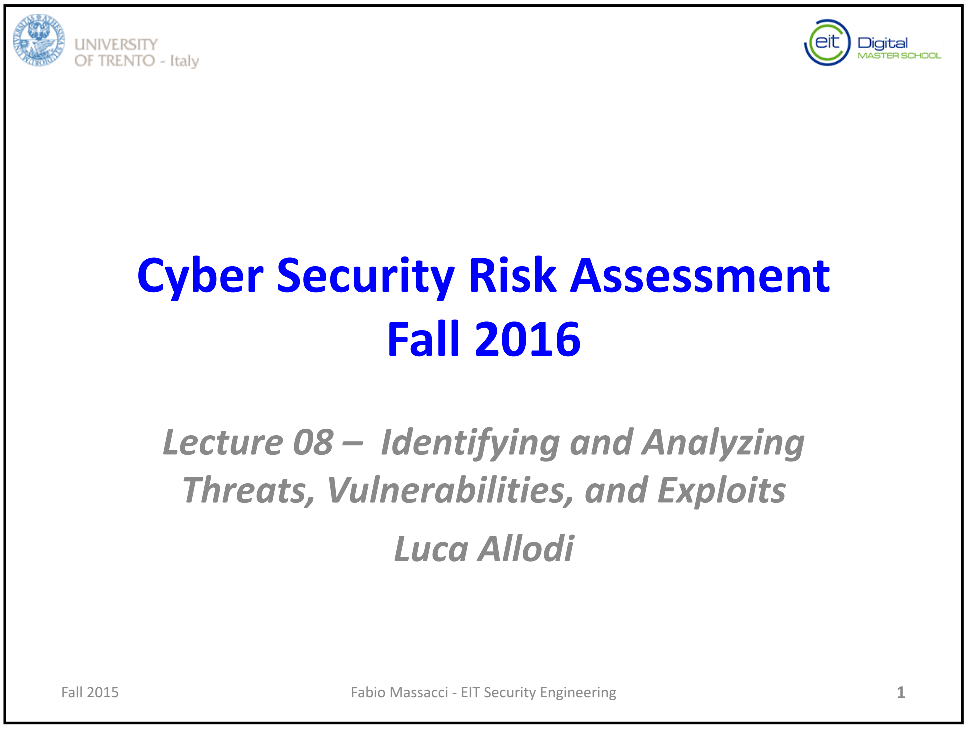
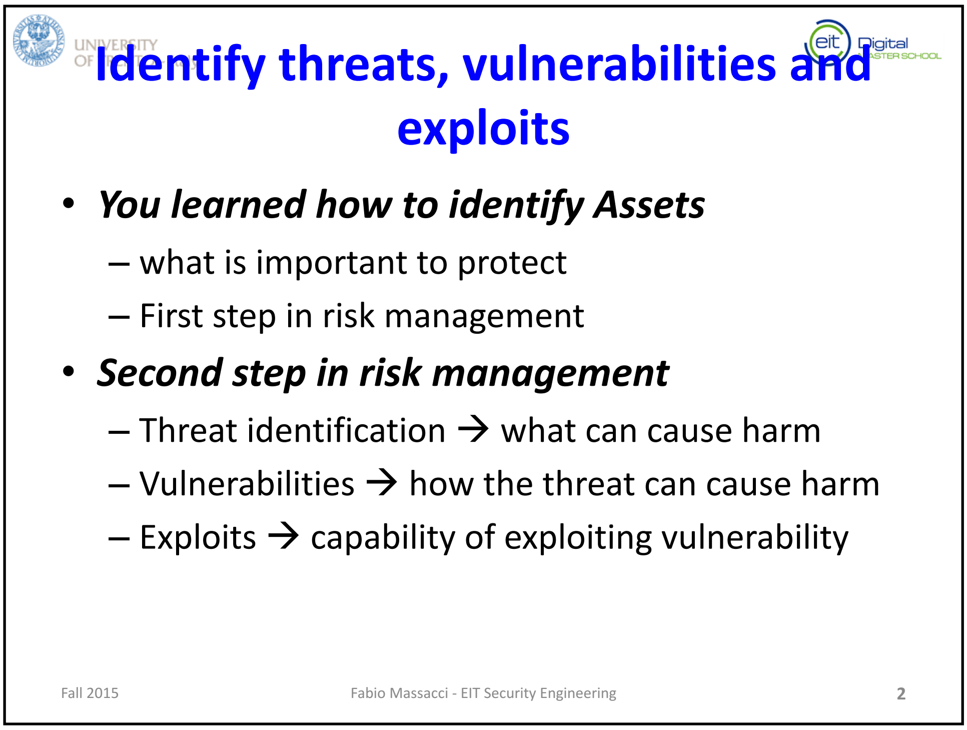


Cyber Security Risk Assessment Fall 2016

Lecture 08 – Identifying and Analyzing Threats, Vulnerabilities, and Exploits

Luca Allodi

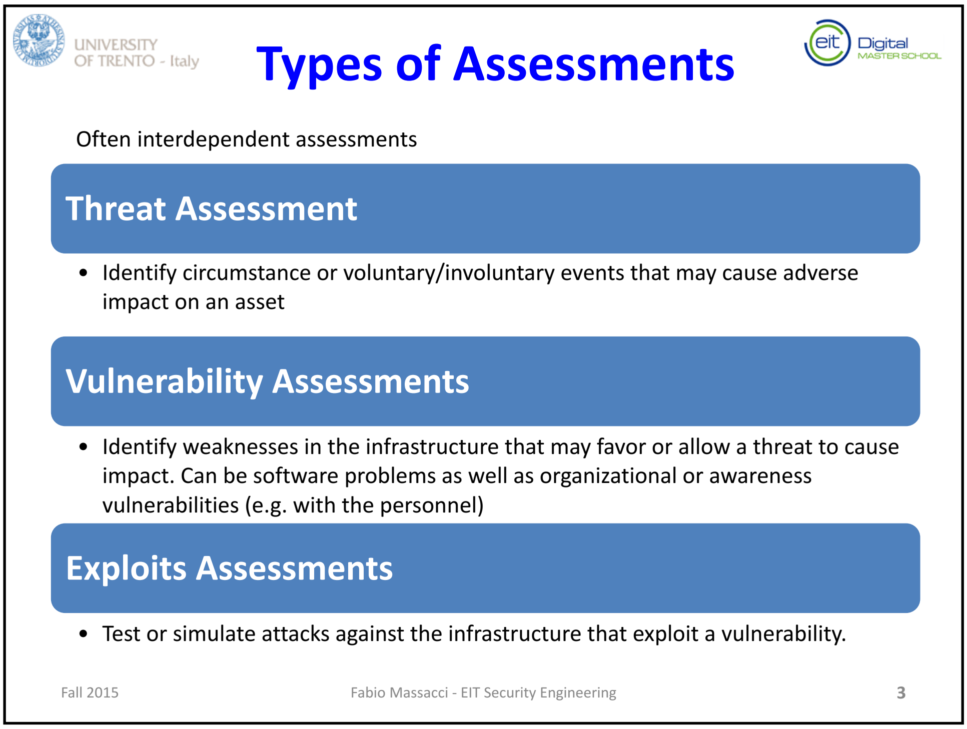
Fall 2015 Fabio Massacci - EIT Security Engineering 1



Identify threats, vulnerabilities and exploits

- ***You learned how to identify Assets***
  - what is important to protect
  - First step in risk management
- ***Second step in risk management***
  - Threat identification → what can cause harm
  - Vulnerabilities → how the threat can cause harm
  - Exploits → capability of exploiting vulnerability

Fall 2015 Fabio Massacci - EIT Security Engineering 2



UNIVERSITY OF TRENTO - Italy

Types of Assessments

Often interdependent assessments

Threat Assessment

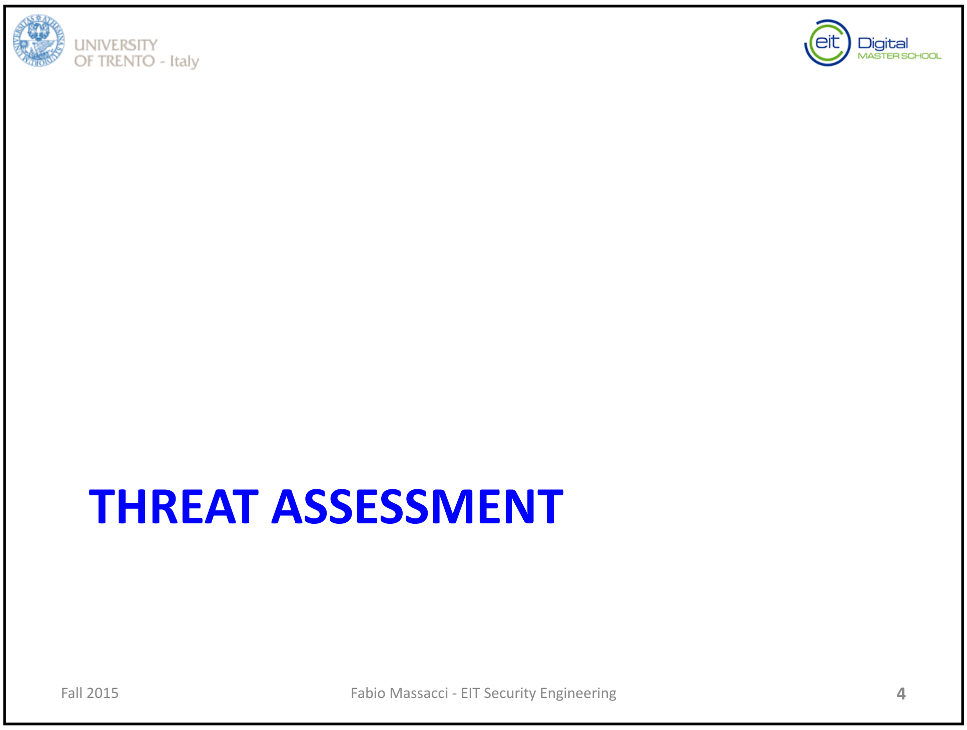
- Identify circumstance or voluntary/involuntary events that may cause adverse impact on an asset

Vulnerability Assessments

- Identify weaknesses in the infrastructure that may favor or allow a threat to cause impact. Can be software problems as well as organizational or awareness vulnerabilities (e.g. with the personnel)

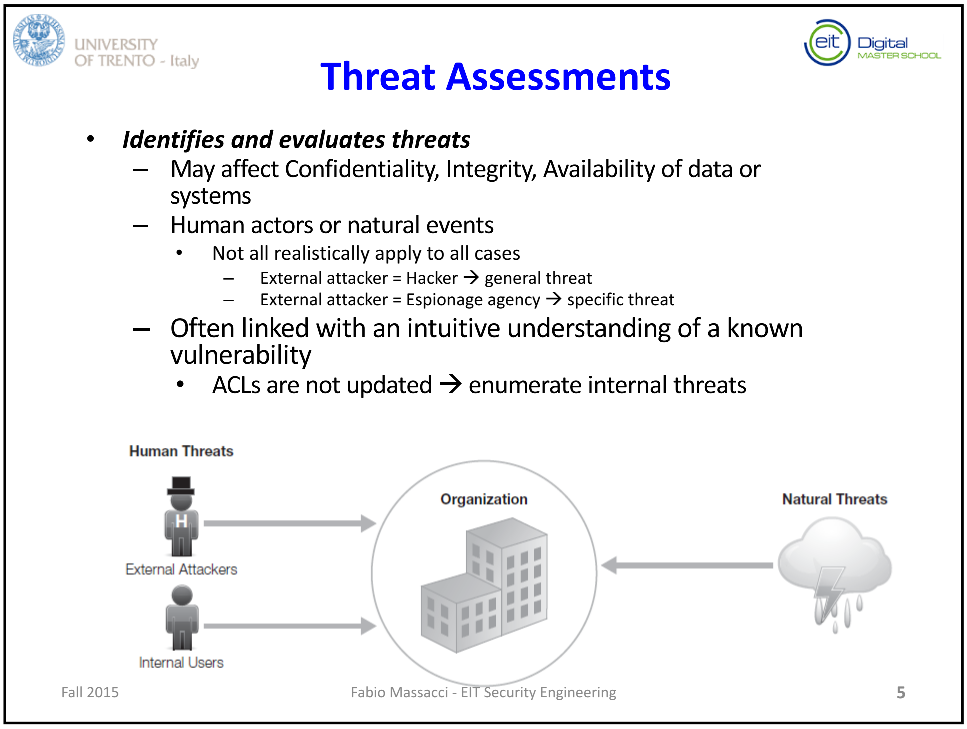
Exploits Assessments

- Test or simulate attacks against the infrastructure that exploit a vulnerability.



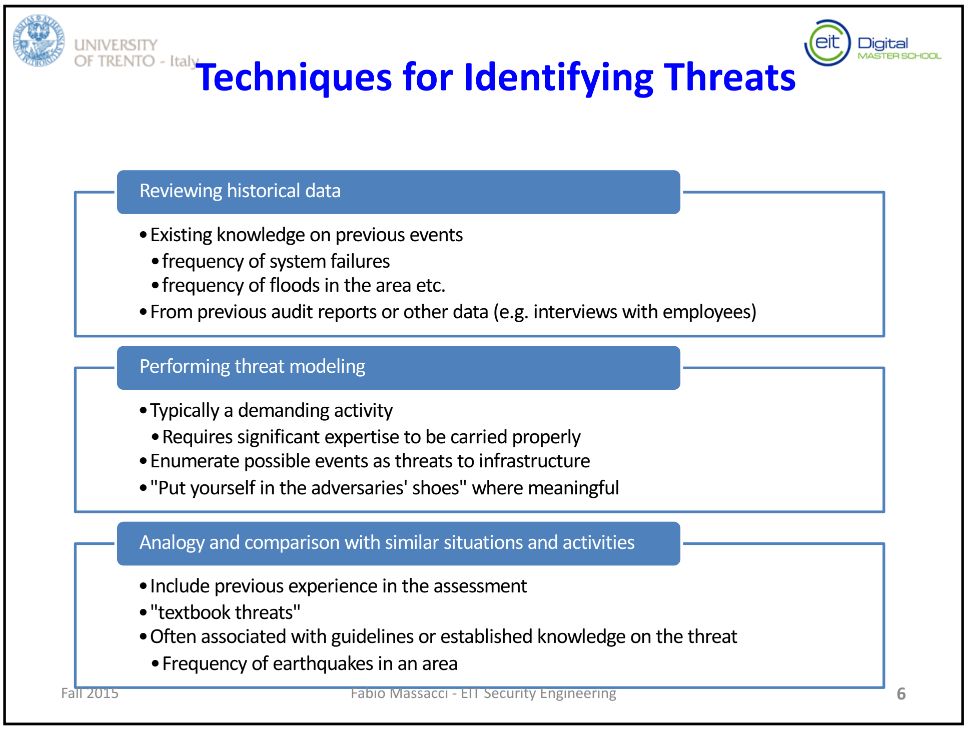
UNIVERSITY OF TRENTO - Italy

THREAT ASSESSMENT



Threat Assessments

- ***Identifies and evaluates threats***
  - – May affect Confidentiality, Integrity, Availability of data or systems
  - – Human actors or natural events
    - Not all realistically apply to all cases
      - – External attacker = Hacker → general threat
      - – External attacker = Espionage agency → specific threat
  - – Often linked with an intuitive understanding of a known vulnerability
    - ACLs are not updated → enumerate internal threats



Techniques for Identifying Threats

Reviewing historical data

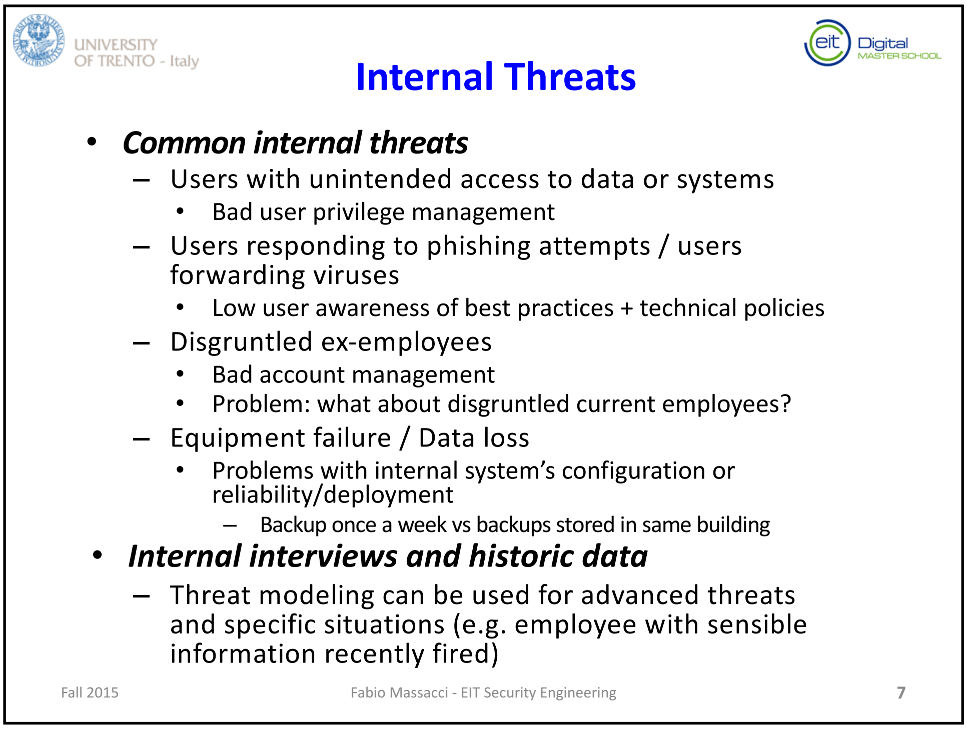
- Existing knowledge on previous events
  - frequency of system failures
  - frequency of floods in the area etc.
- From previous audit reports or other data (e.g. interviews with employees)

Performing threat modeling

- Typically a demanding activity
  - Requires significant expertise to be carried properly
- Enumerate possible events as threats to infrastructure
- "Put yourself in the adversaries' shoes" where meaningful

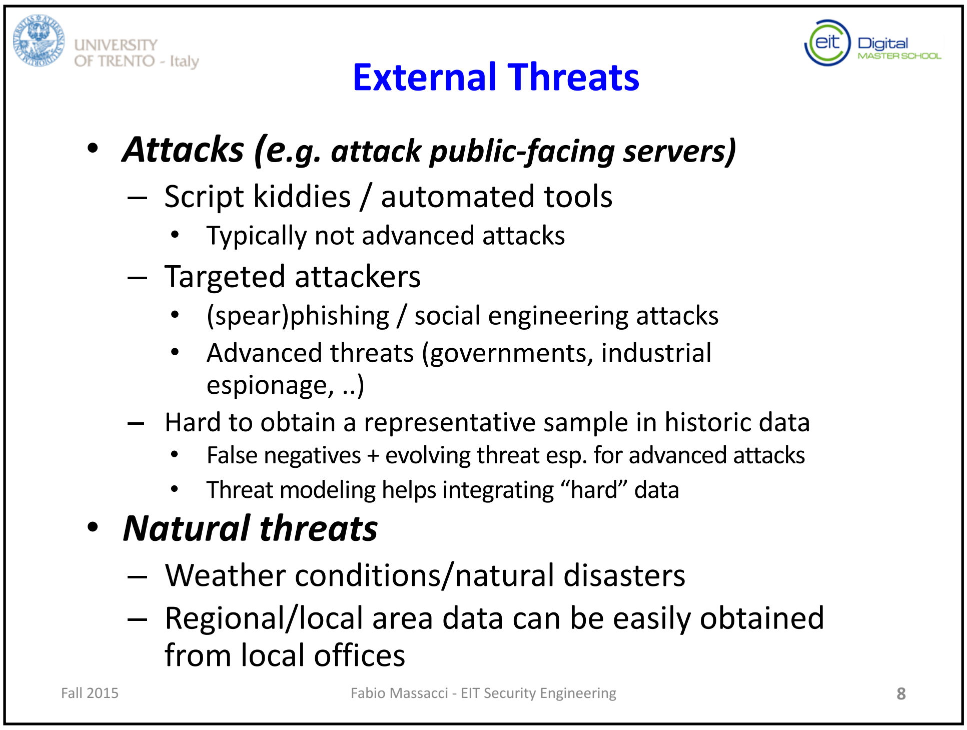
Analogy and comparison with similar situations and activities

- Include previous experience in the assessment
- "textbook threats"
- Often associated with guidelines or established knowledge on the threat
  - Frequency of earthquakes in an area



Internal Threats

- ***Common internal threats***
  - Users with unintended access to data or systems
    - Bad user privilege management
  - Users responding to phishing attempts / users forwarding viruses
    - Low user awareness of best practices + technical policies
  - Disgruntled ex-employees
    - Bad account management
    - Problem: what about disgruntled current employees?
  - Equipment failure / Data loss
    - Problems with internal system's configuration or reliability/deployment
      - Backup once a week vs backups stored in same building
- ***Internal interviews and historic data***
  - Threat modeling can be used for advanced threats and specific situations (e.g. employee with sensible information recently fired)



External Threats

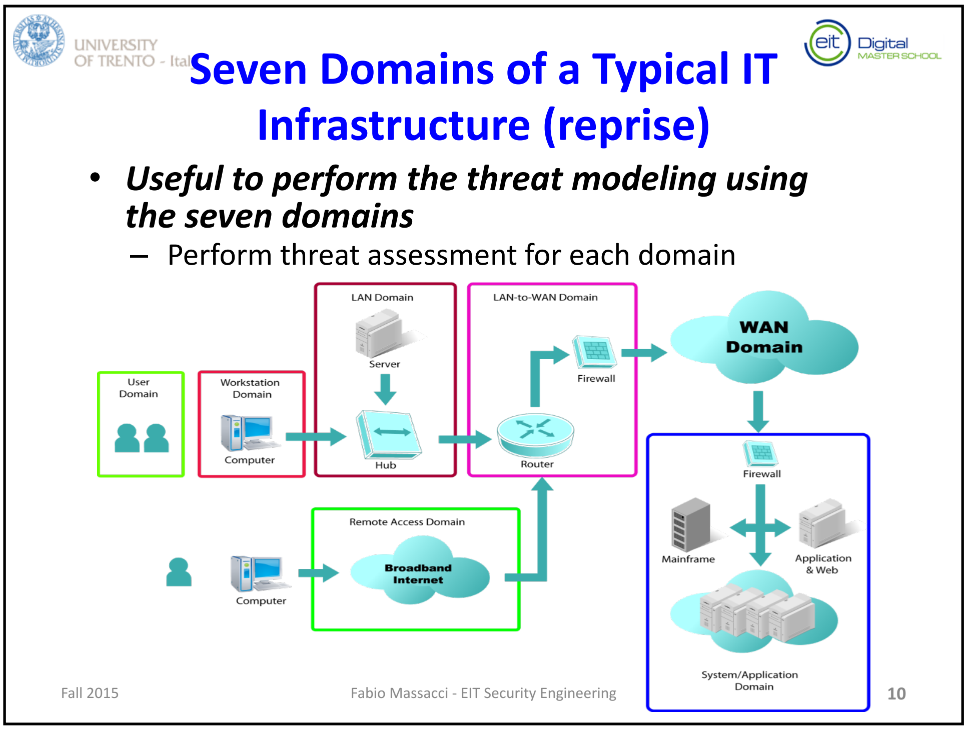
- ***Attacks (e.g. attack public-facing servers)***
  - Script kiddies / automated tools
    - Typically not advanced attacks
  - Targeted attackers
    - (spear)phishing / social engineering attacks
    - Advanced threats (governments, industrial espionage, ..)
  - Hard to obtain a representative sample in historic data
    - False negatives + evolving threat esp. for advanced attacks
    - Threat modeling helps integrating "hard" data
- ***Natural threats***
  - Weather conditions/natural disasters
  - Regional/local area data can be easily obtained from local offices

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Threat Modeling

- ***Mostly useful to protect against sentient or evolving attackers***
- ***Key idea: think as an adversary***
  - External attacker → what could he do to penetrate the infrastructure?
  - Internal attacker → what could a malicious user do? What could a non-malicious user do?
- ***Useful points to address:***
  - Assets:
    1. What system are you trying to protect?
    2. Is the system susceptible to attacks?
    3. Is the system susceptible to hardware or software failure?
  - Attackers:
    1. Who are the potential adversaries?
    2. How might a potential adversary attack?
    3. Who are the users?
    4. How might an internal user misuse the system?

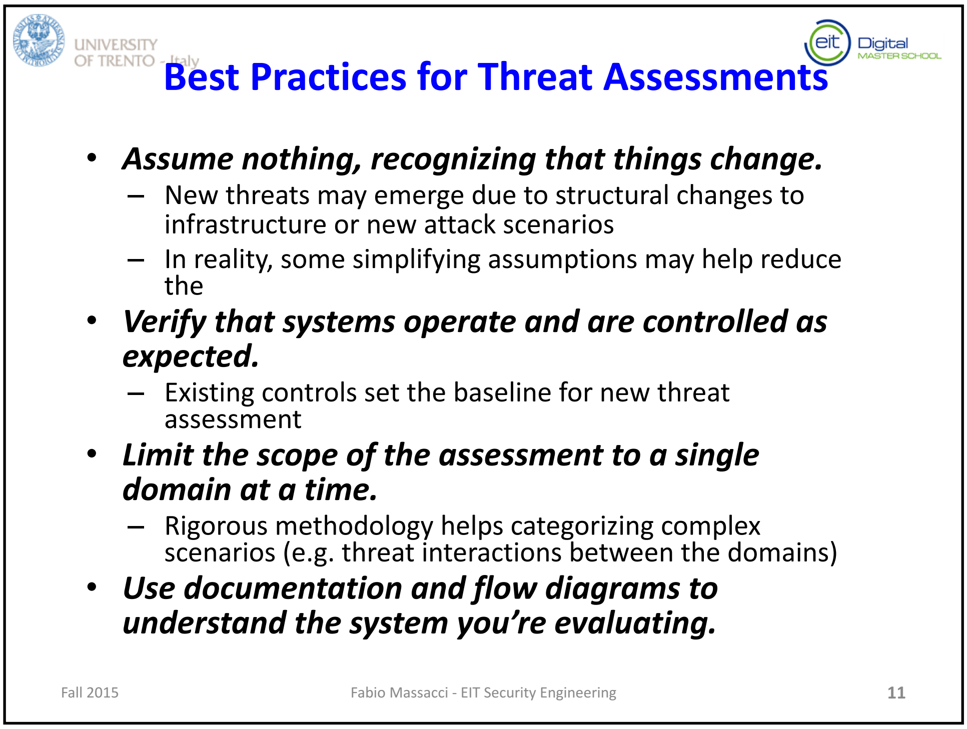


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

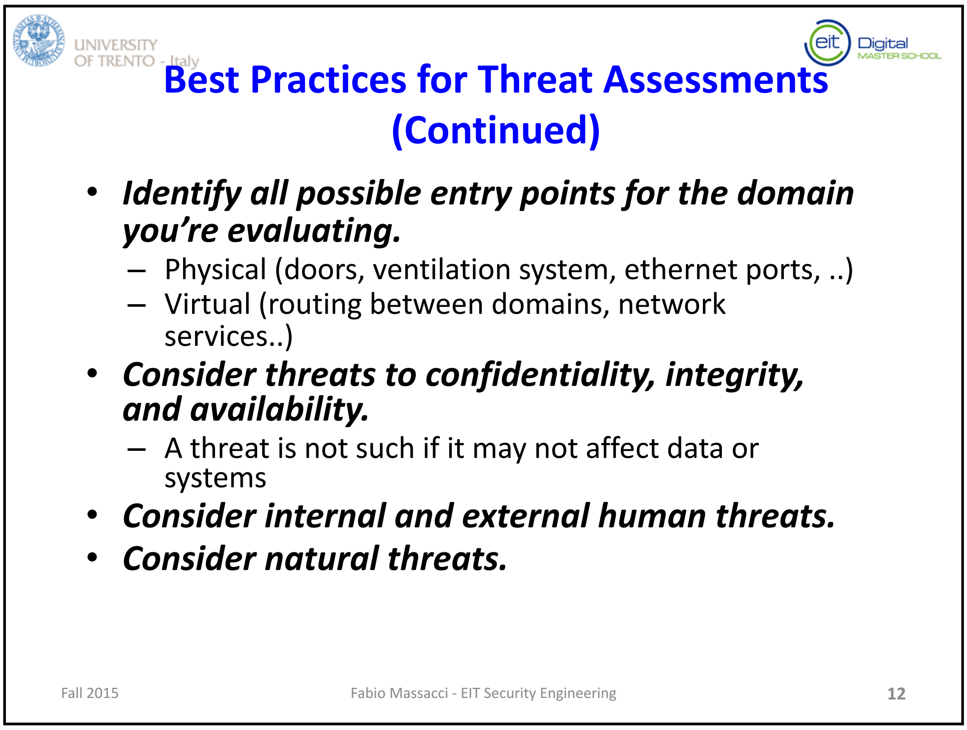
Seven Domains of a Typical IT Infrastructure (reprise)

- ***Useful to perform the threat modeling using the seven domains***
  - Perform threat assessment for each domain



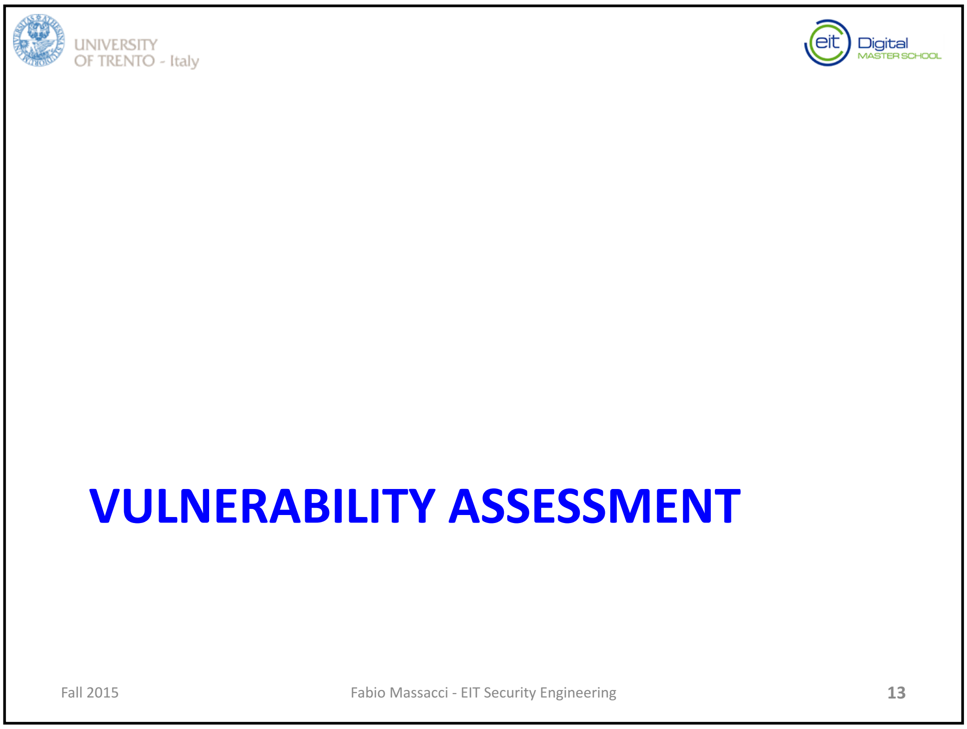
Best Practices for Threat Assessments

- ***Assume nothing, recognizing that things change.***
  - New threats may emerge due to structural changes to infrastructure or new attack scenarios
  - In reality, some simplifying assumptions may help reduce the
- ***Verify that systems operate and are controlled as expected.***
  - Existing controls set the baseline for new threat assessment
- ***Limit the scope of the assessment to a single domain at a time.***
  - Rigorous methodology helps categorizing complex scenarios (e.g. threat interactions between the domains)
- ***Use documentation and flow diagrams to understand the system you're evaluating.***



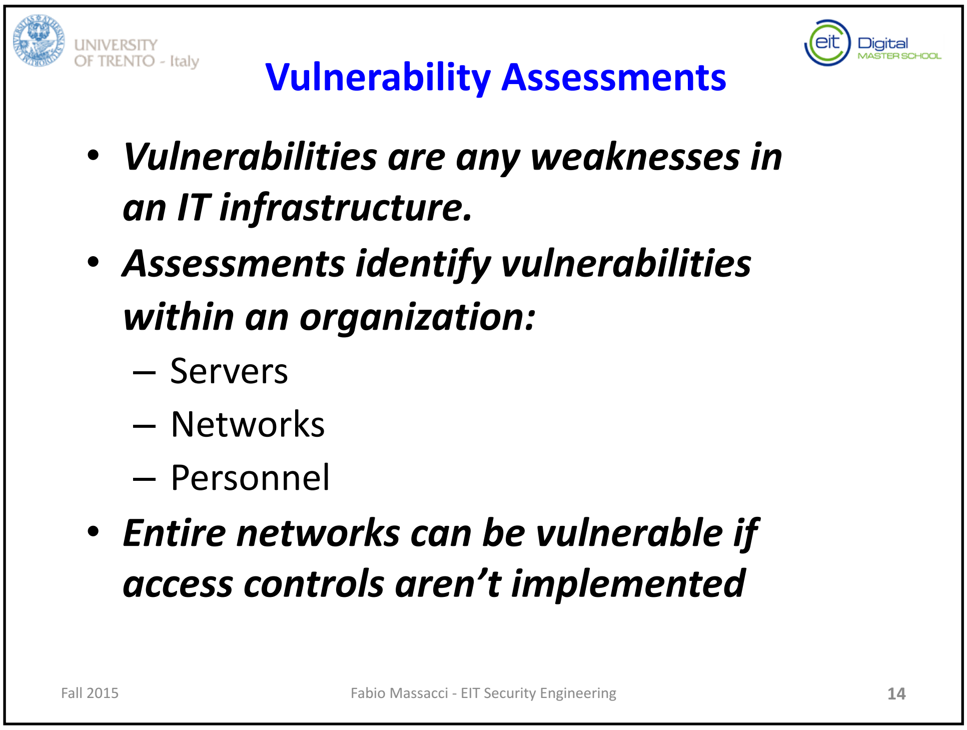
Best Practices for Threat Assessments (Continued)

- ***Identify all possible entry points for the domain you're evaluating.***
  - Physical (doors, ventilation system, ethernet ports, ..)
  - Virtual (routing between domains, network services..)
- ***Consider threats to confidentiality, integrity, and availability.***
  - A threat is not such if it may not affect data or systems
- ***Consider internal and external human threats.***
- ***Consider natural threats.***



UNIVERSITY
OF TRENTO - Italy

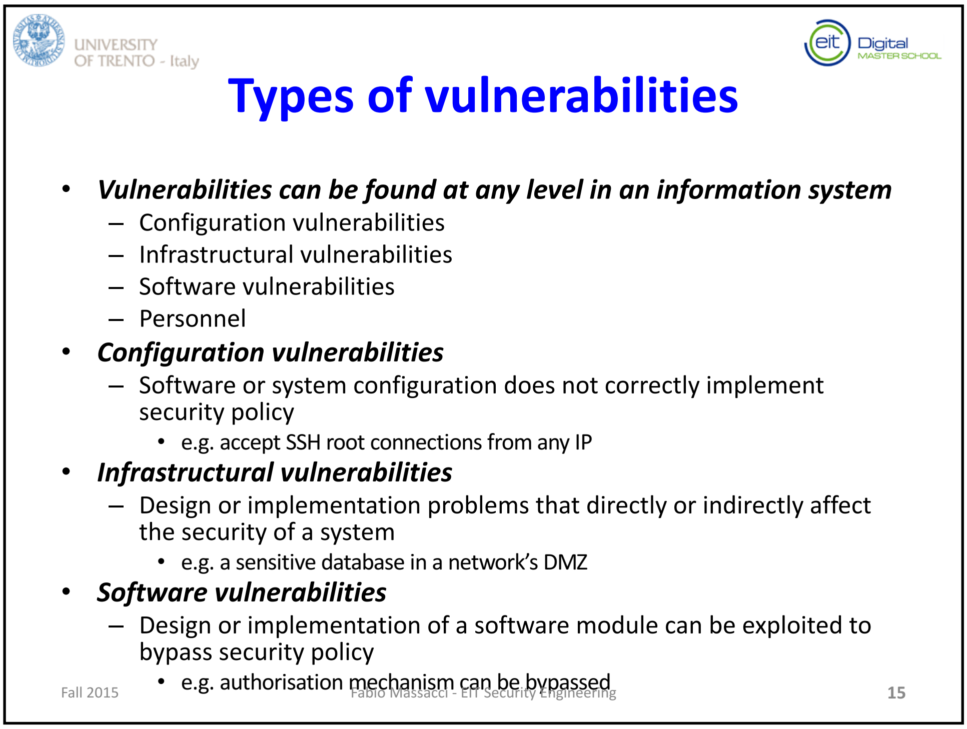
VULNERABILITY ASSESSMENT



UNIVERSITY
OF TRENTO - Italy

Vulnerability Assessments

- ***Vulnerabilities are any weaknesses in an IT infrastructure.***
- ***Assessments identify vulnerabilities within an organization:***
  - Servers
  - Networks
  - Personnel
- ***Entire networks can be vulnerable if access controls aren't implemented***

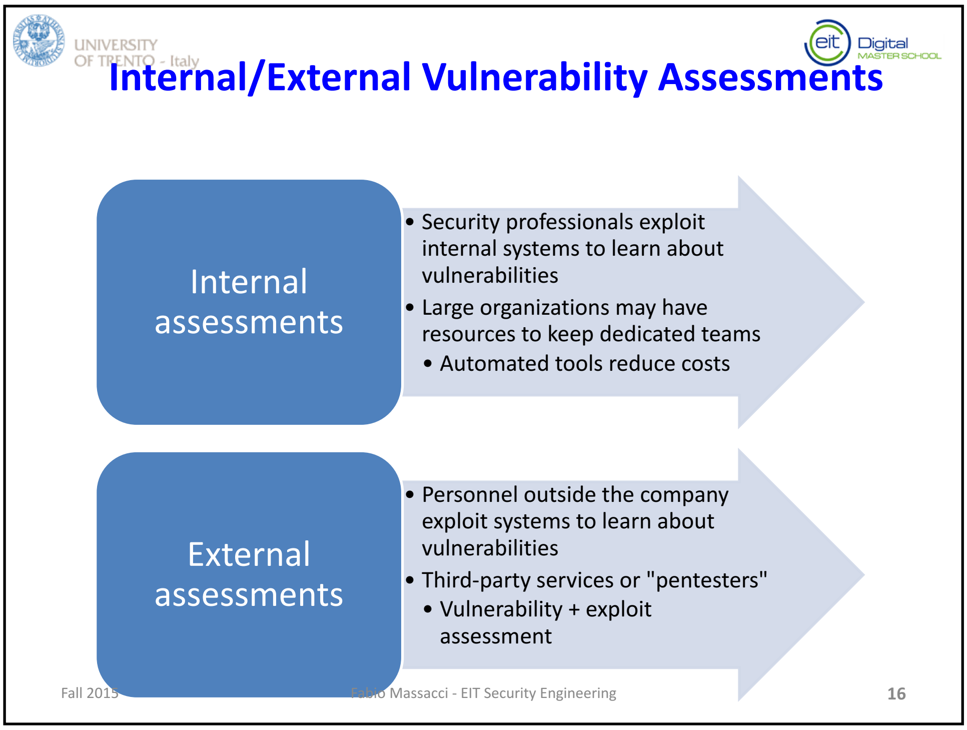


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Types of vulnerabilities

- ***Vulnerabilities can be found at any level in an information system***
  - Configuration vulnerabilities
  - Infrastructural vulnerabilities
  - Software vulnerabilities
  - Personnel
- ***Configuration vulnerabilities***
  - Software or system configuration does not correctly implement security policy
    - e.g. accept SSH root connections from any IP
- ***Infrastructural vulnerabilities***
  - Design or implementation problems that directly or indirectly affect the security of a system
    - e.g. a sensitive database in a network's DMZ
- ***Software vulnerabilities***
  - Design or implementation of a software module can be exploited to bypass security policy
    - e.g. authorisation mechanism can be bypassed



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

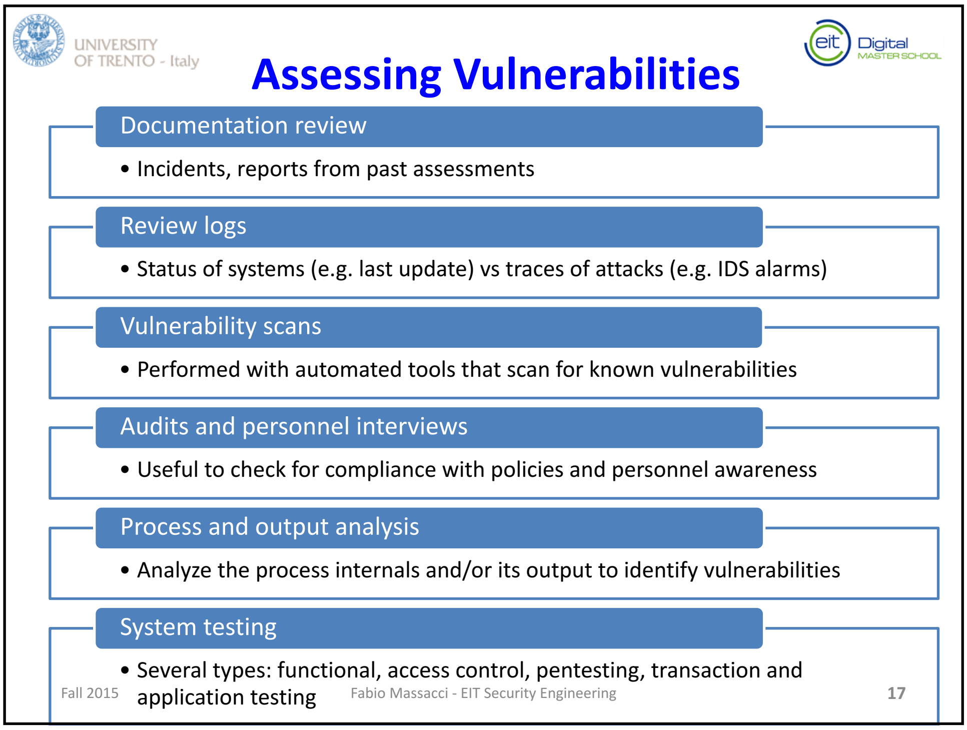
Internal/External Vulnerability Assessments

Internal assessments

- Security professionals exploit internal systems to learn about vulnerabilities
- Large organizations may have resources to keep dedicated teams
  - Automated tools reduce costs

External assessments

- Personnel outside the company exploit systems to learn about vulnerabilities
- Third-party services or "pentesters"
  - Vulnerability + exploit assessment



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Assessing Vulnerabilities

Documentation review

- Incidents, reports from past assessments

Review logs

- Status of systems (e.g. last update) vs traces of attacks (e.g. IDS alarms)

Vulnerability scans

- Performed with automated tools that scan for known vulnerabilities

Audits and personnel interviews

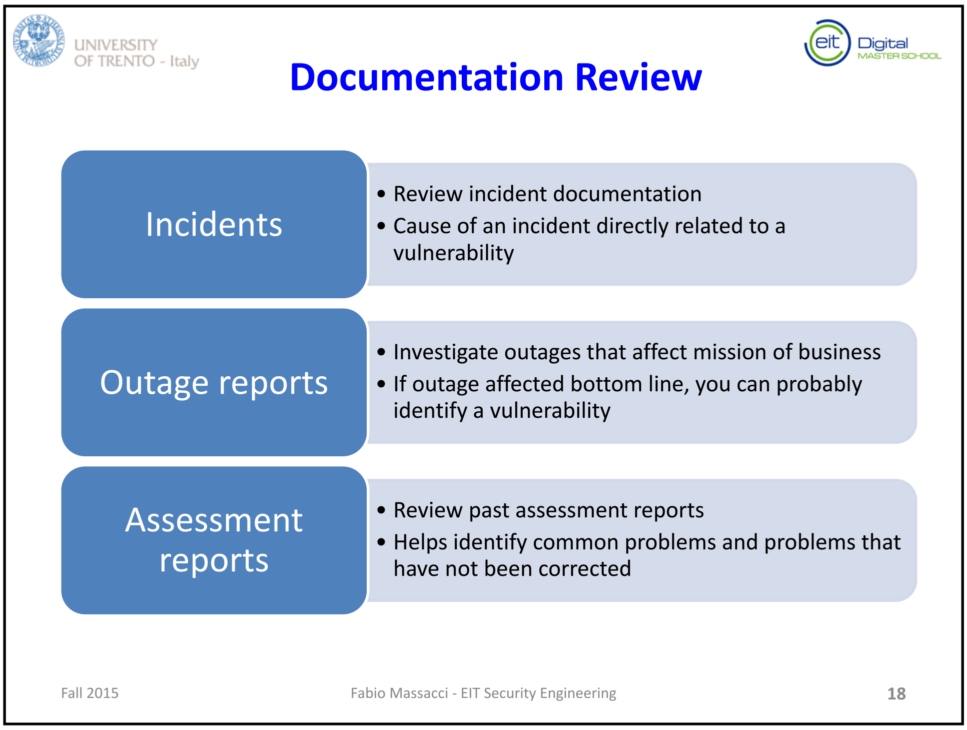
- Useful to check for compliance with policies and personnel awareness

Process and output analysis

- Analyze the process internals and/or its output to identify vulnerabilities

System testing

- Several types: functional, access control, pentesting, transaction and application testing



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Documentation Review

Incidents

- Review incident documentation
- Cause of an incident directly related to a vulnerability

Outage reports

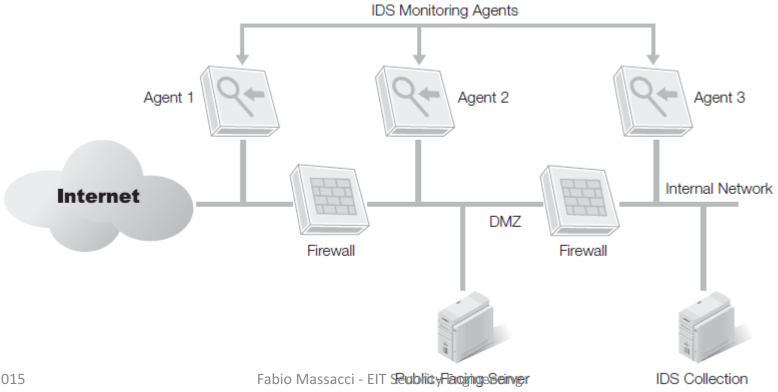
- Investigate outages that affect mission of business
- If outage affected bottom line, you can probably identify a vulnerability

Assessment reports

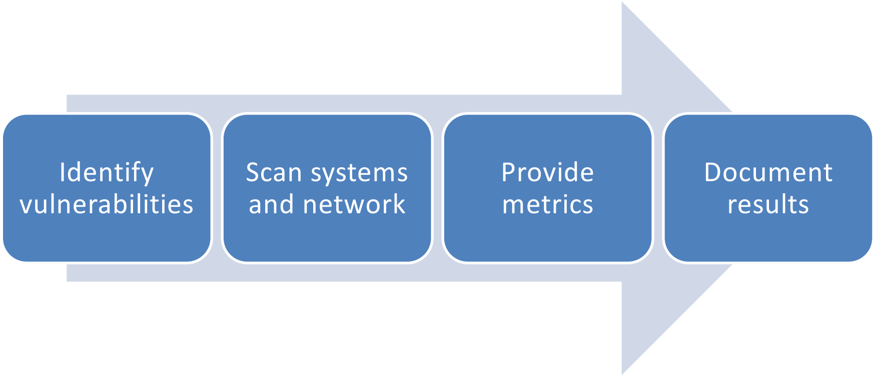
- Review past assessment reports
- Helps identify common problems and problems that have not been corrected

Intrusion Detection System Outputs

- ***IDS systems report logs of fired alarms***
  - Host, network systems
  - Signature-based vs behavioral
- ***Significance of logs depend on sensor position***
- ***High false positive rates → inspection can be expensive***



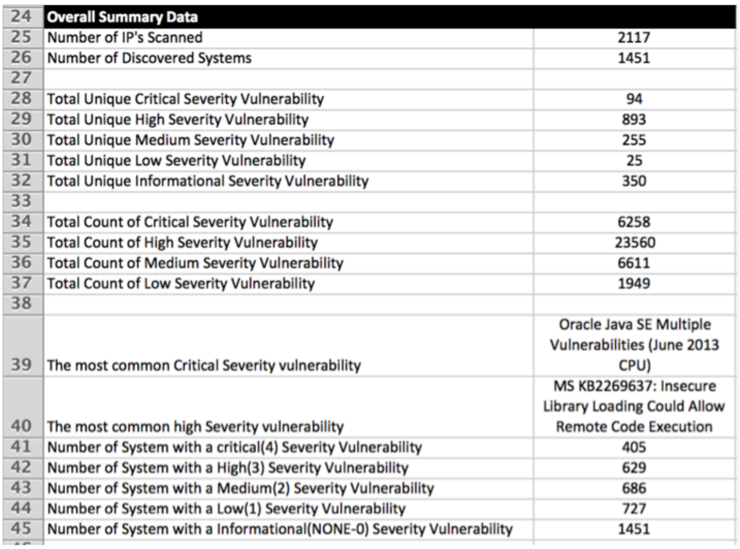
Vulnerability Scans and Other Assessment Tools



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Example of VA tool output (Nessus)



24	Overall Summary Data	
25	Number of IP's Scanned	2117
26	Number of Discovered Systems	1451
27		
28	Total Unique Critical Severity Vulnerability	94
29	Total Unique High Severity Vulnerability	893
30	Total Unique Medium Severity Vulnerability	255
31	Total Unique Low Severity Vulnerability	25
32	Total Unique Informational Severity Vulnerability	350
33		
34	Total Count of Critical Severity Vulnerability	6258
35	Total Count of High Severity Vulnerability	23560
36	Total Count of Medium Severity Vulnerability	6611
37	Total Count of Low Severity Vulnerability	1949
38		
39	The most common Critical Severity vulnerability	Oracle Java SE Multiple Vulnerabilities (June 2013 CPU)
40	The most common high Severity vulnerability	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
41	Number of System with a critical(4) Severity Vulnerability	405
42	Number of System with a High(3) Severity Vulnerability	629
43	Number of System with a Medium(2) Severity Vulnerability	686
44	Number of System with a Low(1) Severity Vulnerability	727
45	Number of System with a Informational(NONE-0) Severity Vulnerability	1451

UNIVERSITY OF TRENTO - Italy

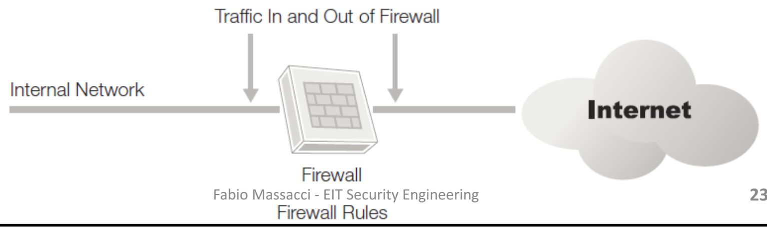
eit Digital MASTER SCHOOL

Audits and Personnel Interviews

- ***Audits performed to check compliance with rules and guidelines***
- ***VA audits check compliance with internal policies***
  - Checks to see if an organization is following the policies that are in place
- ***Audits can be:***
  - Manual
  - Automated, scripted
  - Personnel interviews

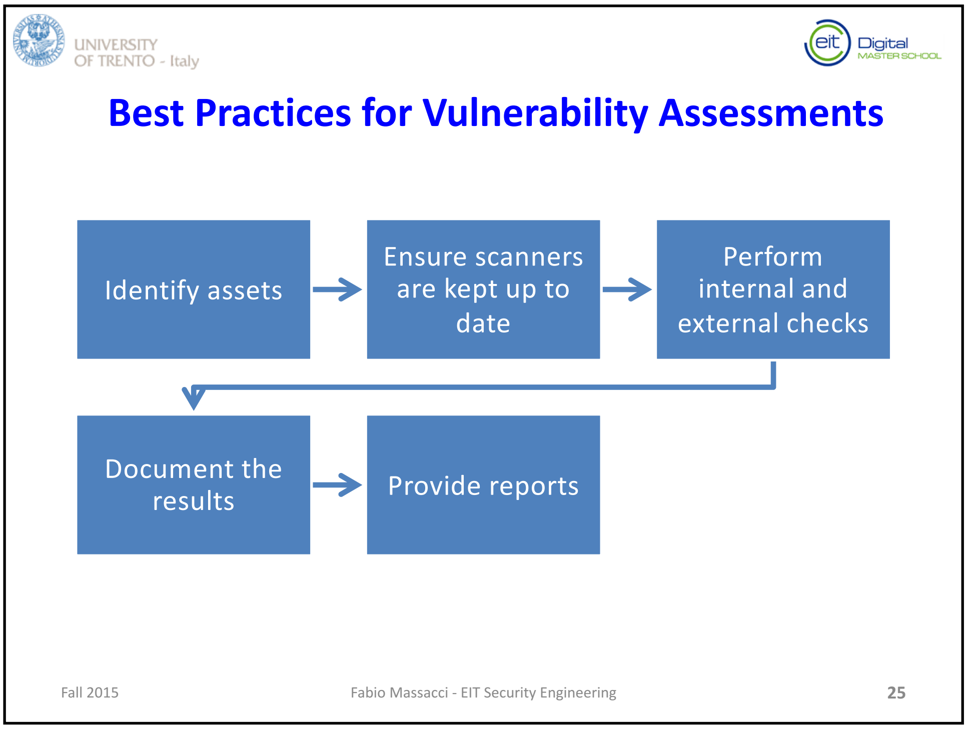
Process Analysis and Output Analysis

- ***Process analysis***
  - Requires understanding of internal process operations
  - White-box view allows for detailed analysis
  - Does not scale with process complexity
- ***Output analysis***
  - Less fine-grained, black-box view on input transformations
  - Can make analysis of complex systems manageable
  - May require the definition (documentation) of requisites
- ***Example:***
  - Firewall has five rule → Process analysis
  - Firewall has 100 rules → Output analysis



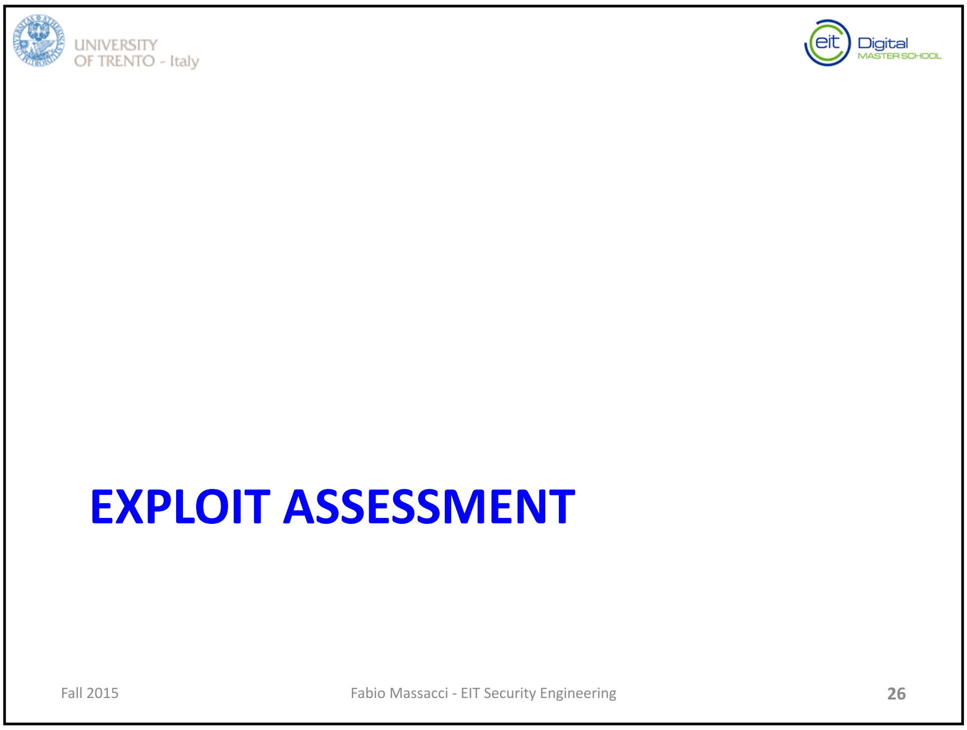
System Testing

- ***Functionality testing***
  - Mainly used for software development and deployment
  - Defined against requirements
  - Evaluate subsequent modifications
    - e.g. functionality extensions
- ***Access controls***
  - Verifying user rights and allocations
    - Security vs usability
- ***Penetration testing***
  - Verifying security countermeasures
  - Invasive w.r.t. VA → attack vs scan
- ***Tests transactions with applications***
  - Assures that incomplete transactions are not committed to back-end
  - Hardening vs some types of attacks, e.g. SQLi

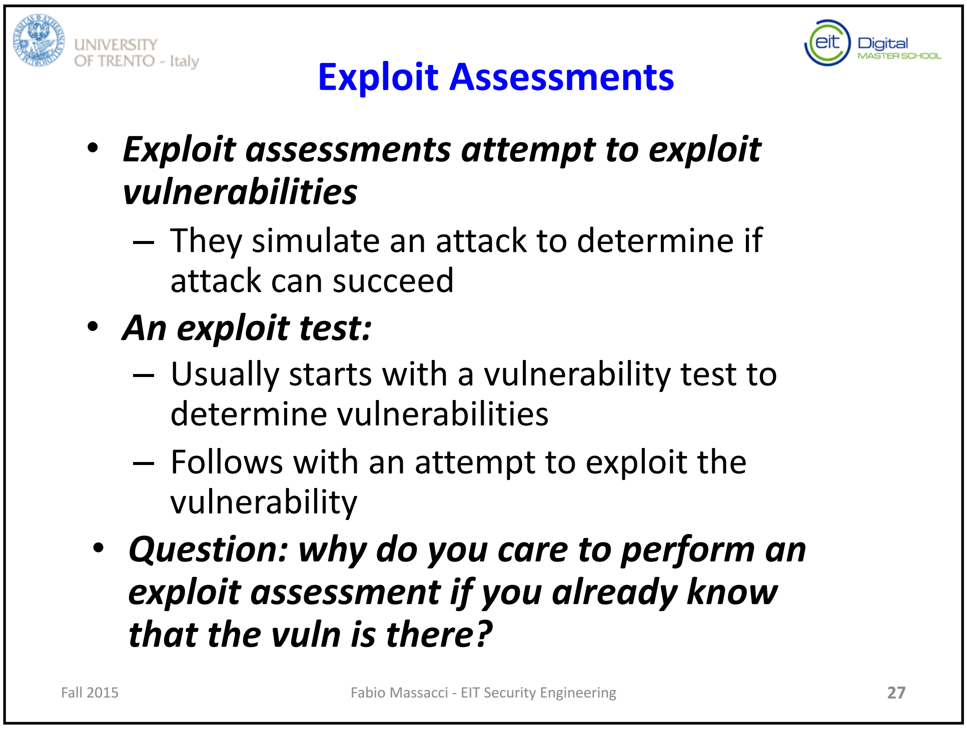


Best Practices for Vulnerability Assessments

Identify assets → Ensure scanners are kept up to date → Perform internal and external checks → Document the results → Provide reports

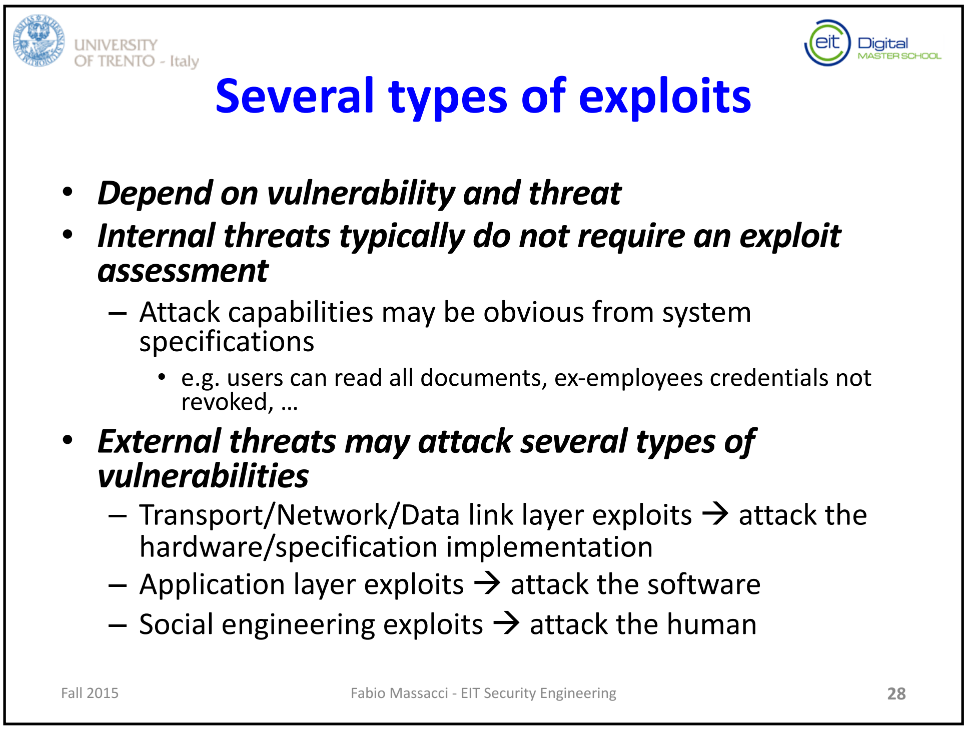


EXPLOIT ASSESSMENT



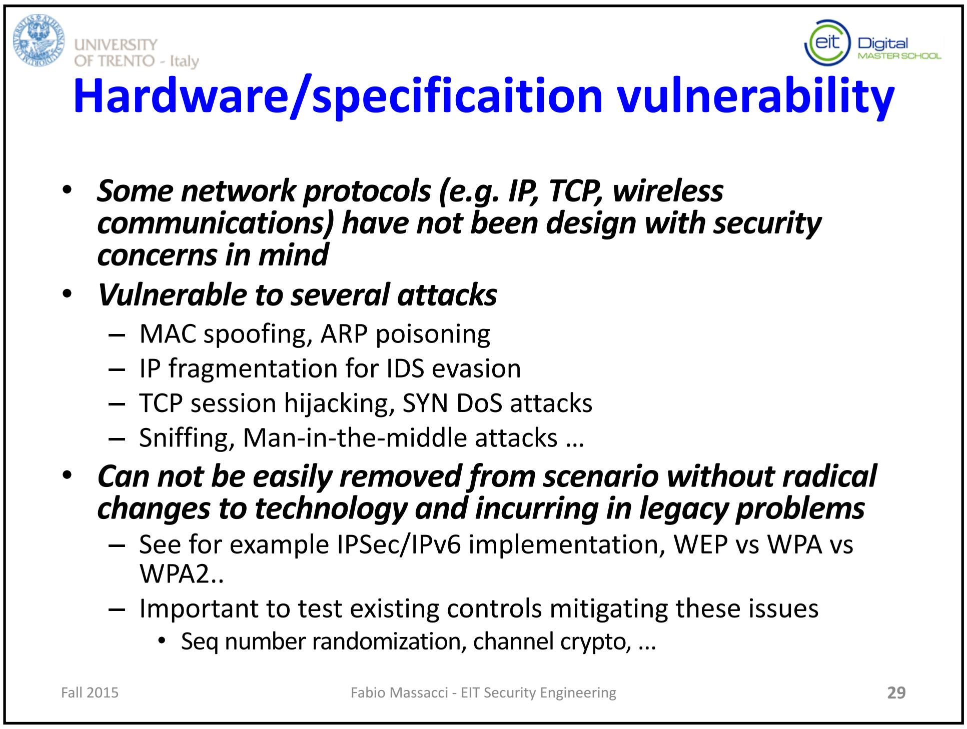
Exploit Assessments

- ***Exploit assessments attempt to exploit vulnerabilities***
  - They simulate an attack to determine if attack can succeed
- ***An exploit test:***
  - Usually starts with a vulnerability test to determine vulnerabilities
  - Follows with an attempt to exploit the vulnerability
- ***Question: why do you care to perform an exploit assessment if you already know that the vuln is there?***



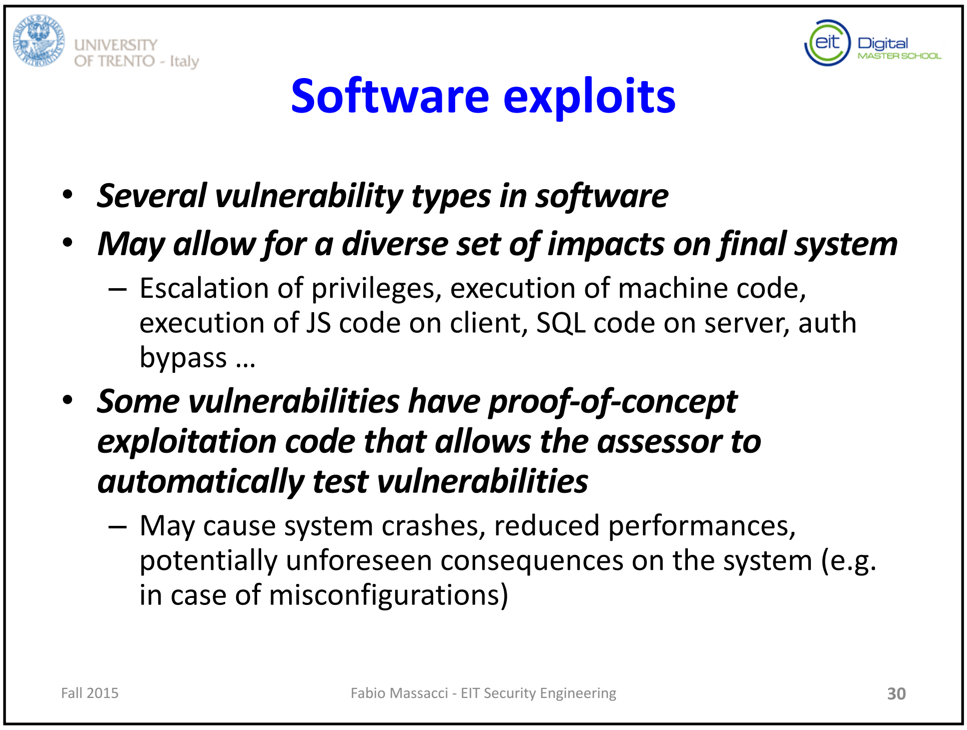
Several types of exploits

- ***Depend on vulnerability and threat***
- ***Internal threats typically do not require an exploit assessment***
  - Attack capabilities may be obvious from system specifications
    - e.g. users can read all documents, ex-employees credentials not revoked, …
- ***External threats may attack several types of vulnerabilities***
  - Transport/Network/Data link layer exploits → attack the hardware/specification implementation
  - Application layer exploits → attack the software
  - Social engineering exploits → attack the human



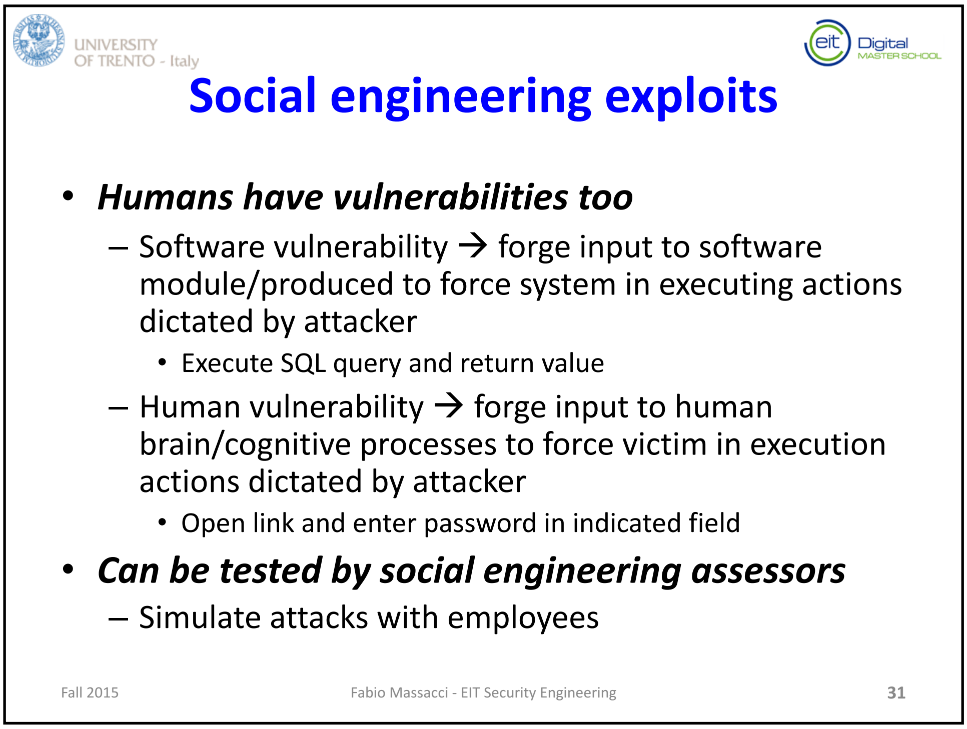
Hardware/specificaition vulnerability

- ***Some network protocols (e.g. IP, TCP, wireless communications) have not been design with security concerns in mind***
- ***Vulnerable to several attacks***
  - MAC spoofing, ARP poisoning
  - IP fragmentation for IDS evasion
  - TCP session hijacking, SYN DoS attacks
  - Sniffing, Man-in-the-middle attacks …
- ***Can not be easily removed from scenario without radical changes to technology and incurring in legacy problems***
  - See for example IPSec/IPv6 implementation, WEP vs WPA vs WPA2..
  - Important to test existing controls mitigating these issues
    - Seq number randomization, channel crypto, …



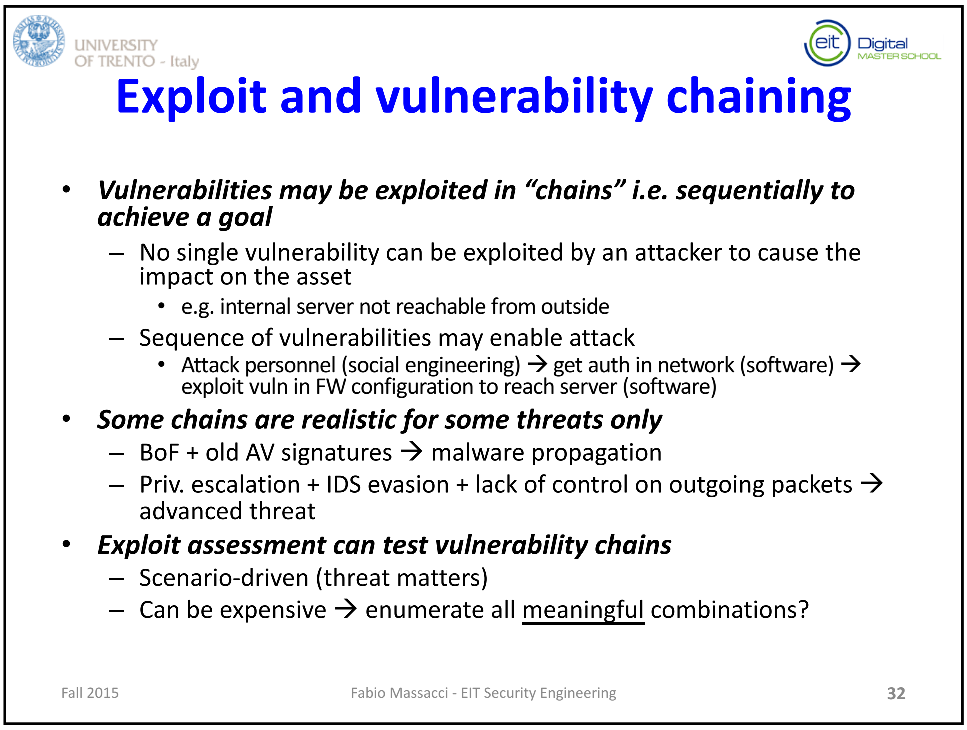
Software exploits

- ***Several vulnerability types in software***
- ***May allow for a diverse set of impacts on final system***
  - Escalation of privileges, execution of machine code, execution of JS code on client, SQL code on server, auth bypass …
- ***Some vulnerabilities have proof-of-concept exploitation code that allows the assessor to automatically test vulnerabilities***
  - May cause system crashes, reduced performances, potentially unforeseen consequences on the system (e.g. in case of misconfigurations)



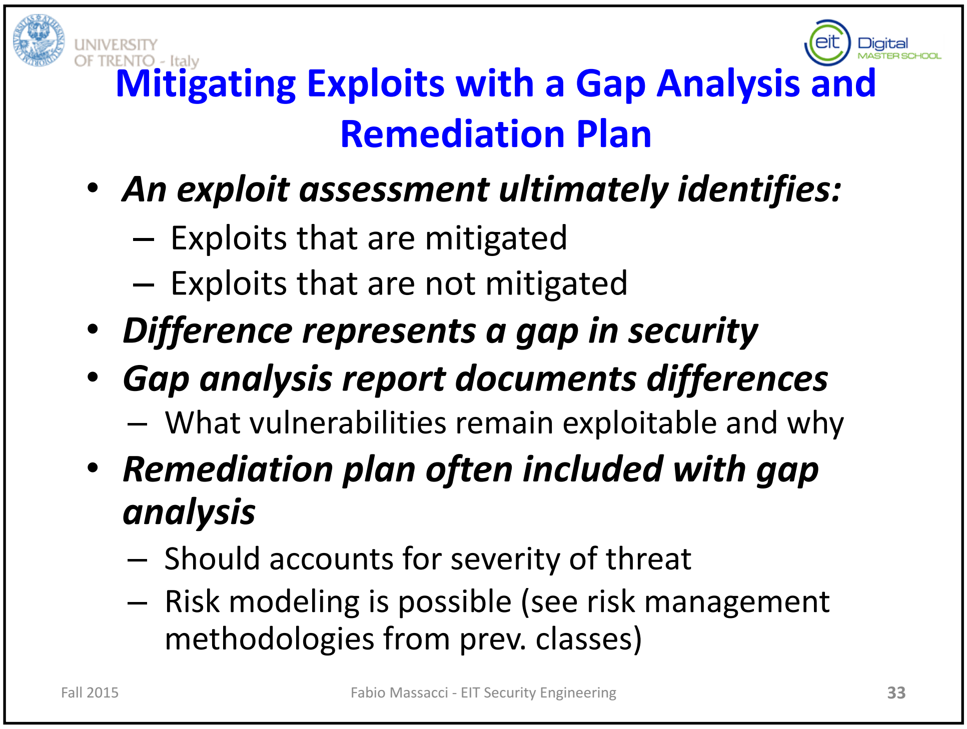
Social engineering exploits

- ***Humans have vulnerabilities too***
  - Software vulnerability → forge input to software module/produced to force system in executing actions dictated by attacker
    - Execute SQL query and return value
  - Human vulnerability → forge input to human brain/cognitive processes to force victim in execution actions dictated by attacker
    - Open link and enter password in indicated field
- ***Can be tested by social engineering assessors***
  - Simulate attacks with employees



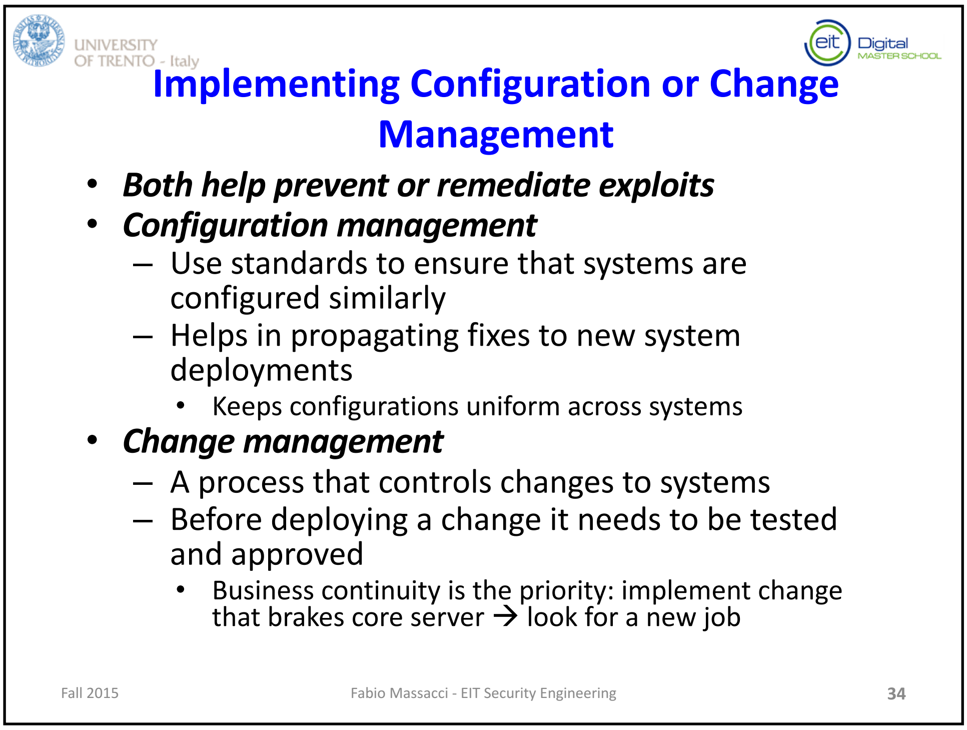
Exploit and vulnerability chaining

- ***Vulnerabilities may be exploited in "chains" i.e. sequentially to achieve a goal***
  - No single vulnerability can be exploited by an attacker to cause the impact on the asset
    - e.g. internal server not reachable from outside
  - Sequence of vulnerabilities may enable attack
    - Attack personnel (social engineering) → get auth in network (software) → exploit vuln in FW configuration to reach server (software)
- ***Some chains are realistic for some threats only***
  - BoF + old AV signatures → malware propagation
  - Priv. escalation + IDS evasion + lack of control on outgoing packets → advanced threat
- ***Exploit assessment can test vulnerability chains***
  - Scenario-driven (threat matters)
  - Can be expensive → enumerate all meaningful combinations?



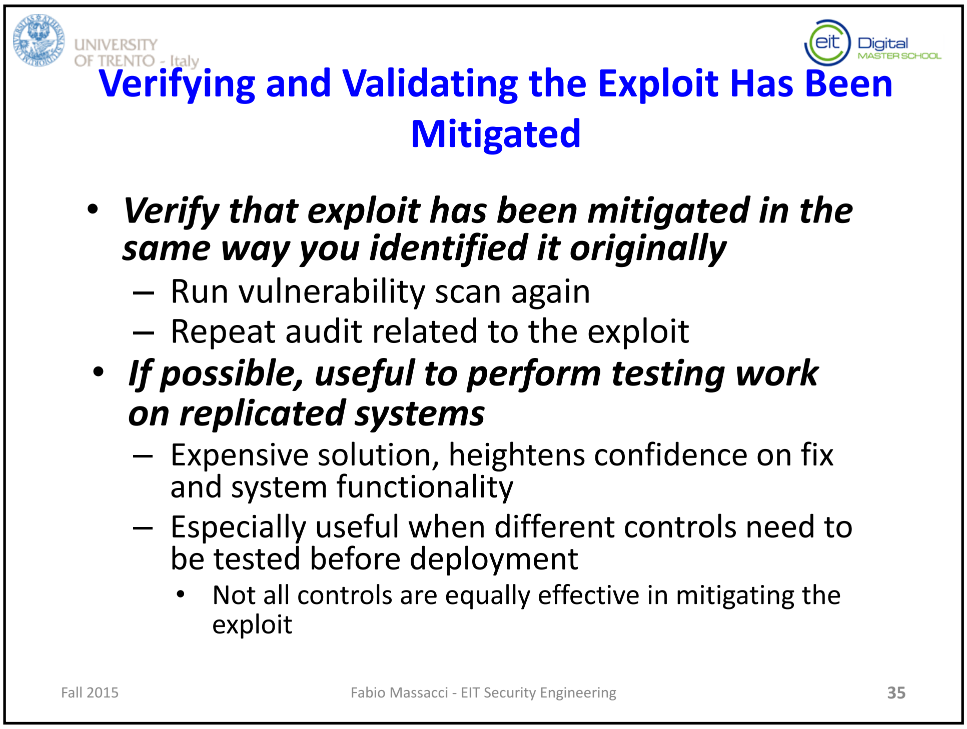
Mitigating Exploits with a Gap Analysis and Remediation Plan

- ***An exploit assessment ultimately identifies:***
  - Exploits that are mitigated
  - Exploits that are not mitigated
- ***Difference represents a gap in security***
- ***Gap analysis report documents differences***
  - What vulnerabilities remain exploitable and why
- ***Remediation plan often included with gap analysis***
  - Should accounts for severity of threat
  - Risk modeling is possible (see risk management methodologies from prev. classes)



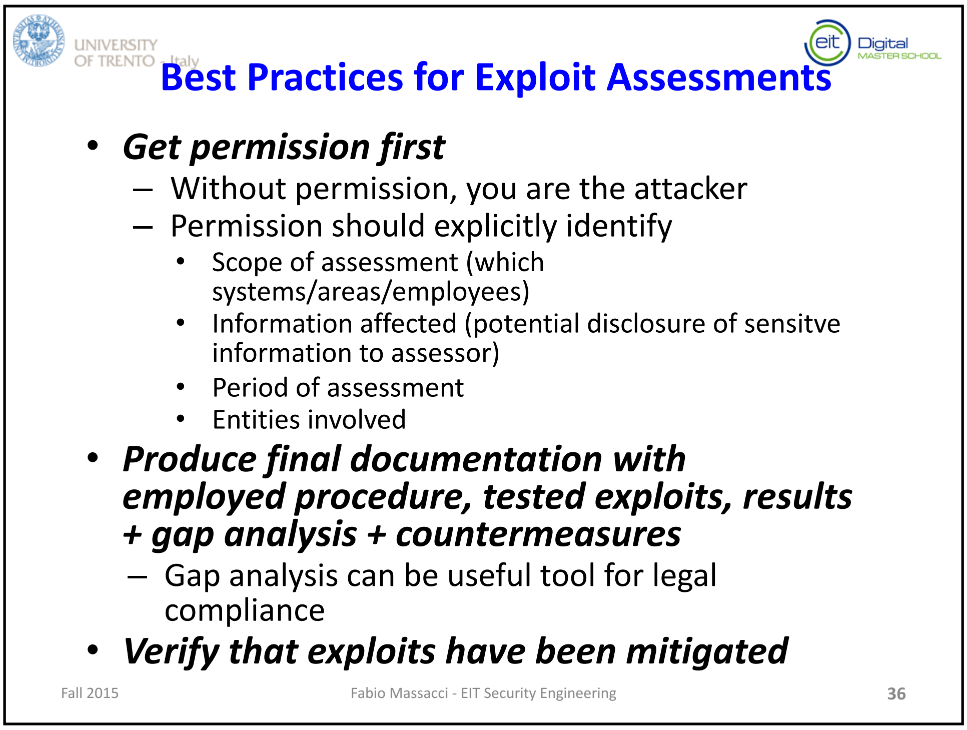
Implementing Configuration or Change Management

- ***Both help prevent or remediate exploits***
- ***Configuration management***
  - Use standards to ensure that systems are configured similarly
  - Helps in propagating fixes to new system deployments
    - Keeps configurations uniform across systems
- ***Change management***
  - A process that controls changes to systems
  - Before deploying a change it needs to be tested and approved
    - Business continuity is the priority: implement change that brakes core server → look for a new job



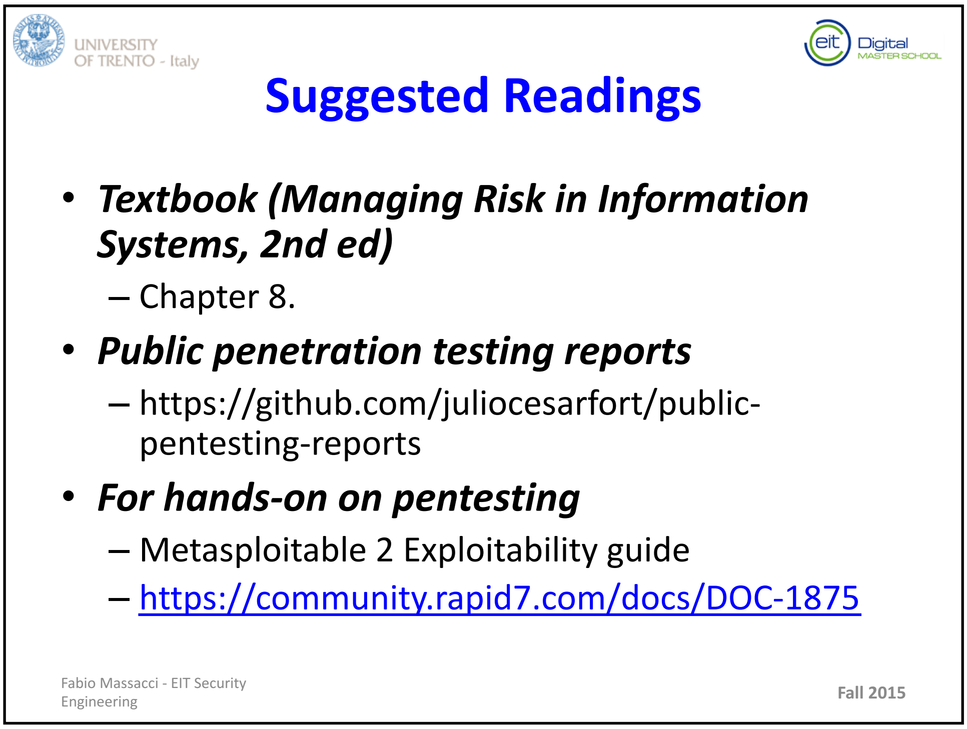
Verifying and Validating the Exploit Has Been Mitigated

- ***Verify that exploit has been mitigated in the same way you identified it originally***
  - Run vulnerability scan again
  - Repeat audit related to the exploit
- ***If possible, useful to perform testing work on replicated systems***
  - Expensive solution, heightens confidence on fix and system functionality
  - Especially useful when different controls need to be tested before deployment
    - Not all controls are equally effective in mitigating the exploit



Best Practices for Exploit Assessments

- ***Get permission first***
  - Without permission, you are the attacker
  - Permission should explicitly identify
    - Scope of assessment (which systems/areas/employees)
    - Information affected (potential disclosure of sensitve information to assessor)
    - Period of assessment
    - Entities involved
- ***Produce final documentation with employed procedure, tested exploits, results + gap analysis + countermeasures***
  - Gap analysis can be useful tool for legal compliance
- ***Verify that exploits have been mitigated***



Suggested Readings

- ***Textbook (Managing Risk in Information Systems, 2nd ed)***
  - Chapter 8.
- ***Public penetration testing reports***
  - https://github.com/juliocesarfort/public-pentesting-reports
- ***For hands-on on pentesting***
  - Metasploitable 2 Exploitability guide
  - https://community.rapid7.com/docs/DOC-1875