Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS559

L20

CSU Cybersecurity Center
Computer Science Dept

Questions on past lectures

- Software reliability growth models: We saw them only briefly. For further details see
  - https://www.cs.colostate.edu/~malaiya/530/softwarereliability.pdf
  - Or take CS530 next semester
- Fuzzing: You can read further details in the articles mentioned. Also you can download some of the fuzzers (AFL etc) and try them.
- Hash functions: Look them up in cryptography texts/articles.

Happy Election day!

Colorado State University

Penetration Testing

How to get into a system and steal stuff

- Not legal in general
- Completely legal if you are hired and authorized to do Pen Testing. Very valuable service.
- Involves all kinds of bad/fun stuff.

Teaching How to Pick a Pocket or Two

- Fagin in Charles Dicken‘s Oliver Twist (1838)
- https://www.youtube.com/watch?v=2YVAmZBGdXw Fifth Av Theater

Quantitative Security

Colorado State University

Yashwant K Malaiya

CS 559

Penetration Testing

CSU Cybersecurity Center
Computer Science Dept

What is Penetration Testing?

- Definition: A penetration test is a method of evaluating the security of a computer system and/or network by simulating an attack from a malicious source
  - malicious source: also known as a Black Hat Hacker
- A Pen Tester vs a Hacker
  - Prior approval
    - Pen Tester's have prior approval from Senior Management.
    - Hackers need no approval.
  - Technical Skills and Tools
    - A Pen Tester's uses his technical skills & tools to identify weaknesses that needs fixing.
    - A hacker wants to exploit weaknesses for profit or satisfaction
  - Social Engineering Skills
    - Pen Tester's social engineering penetration attempts are there to raise awareness
    - Hackers social engineering attacks are to steal/damage data

Ack: NASA-Ames, 2010

Where are details?

- We will only look at higher level considerations.
- There are numerous interesting details that will take many hours of discussions/demonstrations. It can take a year to become an expert.
- Many powerful tools are in public domain and can be downloaded and installed.
- For example, you can run Kali Linux in a virtual machine.
  - It has a number of powerful tools included: Vulnerability analysis, Wireless attacks, Exploitation tools, Password attacks, Sniffing and Spoofing etc.
- Caution: Much of the information available has been created by those who wish to sell their services.

Penetration Testing vs Vulnerability Assessment

- **Vulnerability Assessment**: *process of identifying, evaluating, and classifying security vulnerabilities based on the risk they present*
  - Typically conducted by in-house staff using authenticated credentials; does not require a high skill level.
  - Planned internally by the organization. Known timing.
  - Unreliable at times and high rate of false positives. *(that is claim)*
  - Vulnerability assessment invites debate among System Admins.
  - Produces a report with mitigation guidelines and action items.

- **Penetration Testing**: *(pen testing or ethical hacking), is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit*
  - Generally an independent outside service; requires a great deal of skill
  - Focused in scope and may include targeted attempts to exploit specific vectors (Both IT and Physical)
  - Unpredictable for the internal people.
  - Highly accurate and reliable. *(that is claim)*
  - Penetration Testing = Proof of Concept against vulnerabilities.
  - Produces a binary result: Exploitable holes identified and proven.

Ack: NASA-Ames, Penetration Testing and Vulnerability Assessment, 2010

Scope of Penetration Testing

- Targeted Reconnaissance and penetration
  - Targeted exploitation of vulnerabilities.
  - Network/Firewall Vulnerability Testing
  - Web Application Vulnerability Testing
  - Cloud Computing Penetration Testing
  - Mobile app Penetration Testing
- Social Engineering (Phishing, pharming, spear-phishing)
  - Can you tell me what my password is?
- Physical facilities audit (Unlocked terminals, unsecure building)
  - Sorry, I forgot my badge...
- Wireless Access
  - Detection of rogue or weakly encrypted AP's. (TKMaxx breach etc)
- Dumpster Diving
  - I've found someone's Tax forms with SSN.

Pen Testing Metrics

Program Level Metrics

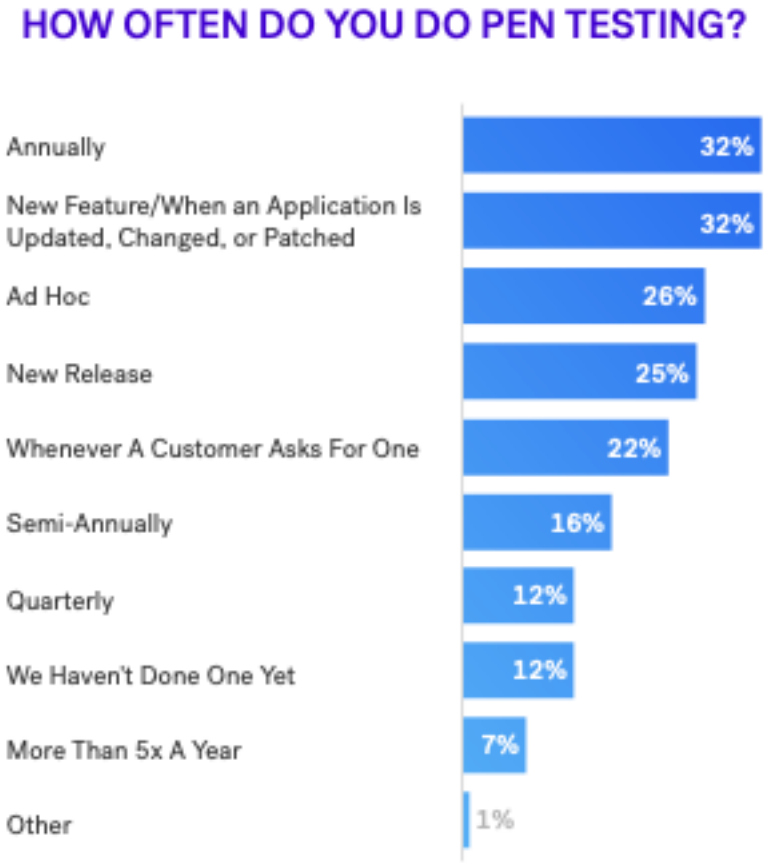
- Application Portfolio Coverage
  - An organization should apply security controls in a risk-based manner across its entire application portfolio.
  - Coverage = # of applications tested/ total # of applications
    - Applications include web, mobile, APIs
- Test Frequency & Time to Fix
  - a penetration test on critical applications two to four times a years, or upon major changes.
  - Critical findings should be fixed as soon as possible.

Engagement Level Metrics

- Vulnerability Types
  - How real-world vulnerabilities map to recognized vulnerability categories
  - Their criticality
  - Applying fixes

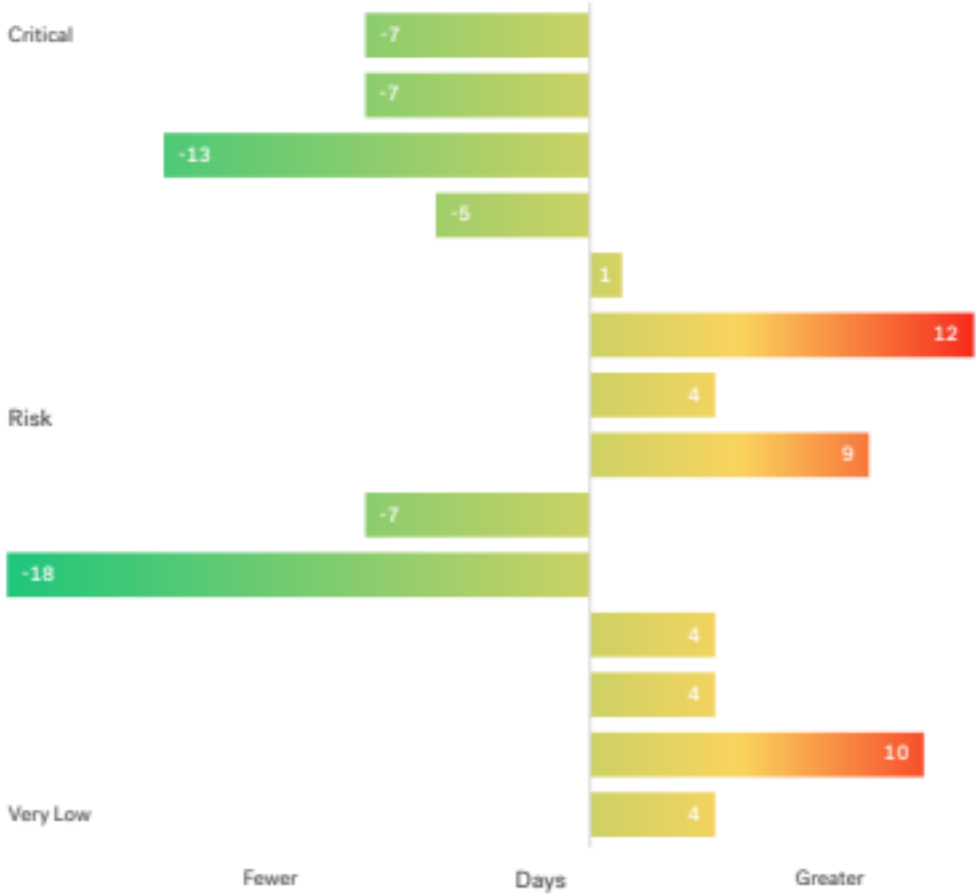
Pen Test Metrics 2018

HOW OFTEN DO YOU DO PEN TESTING?



Colorado State University

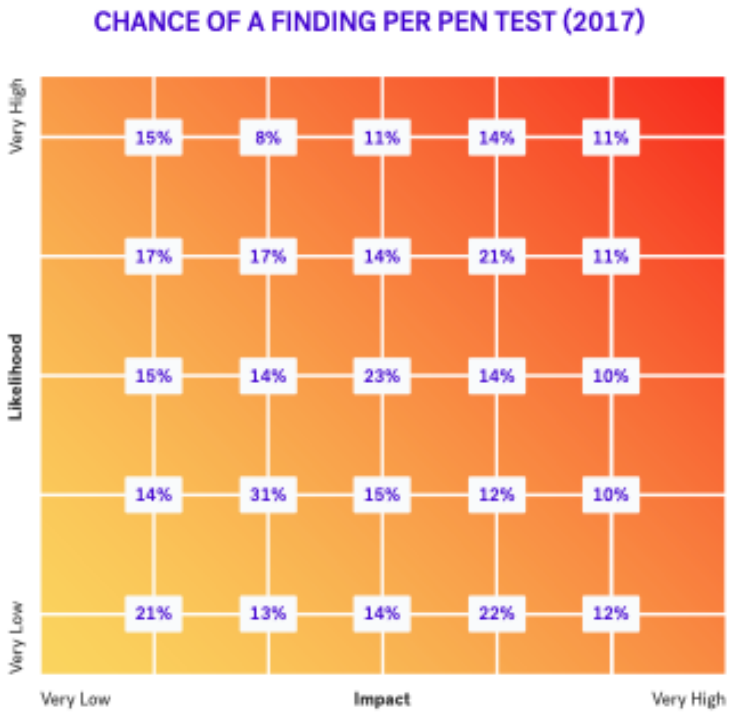
RELATIVE DAYS FOR ORG TO RESOLVE RISK (2017)

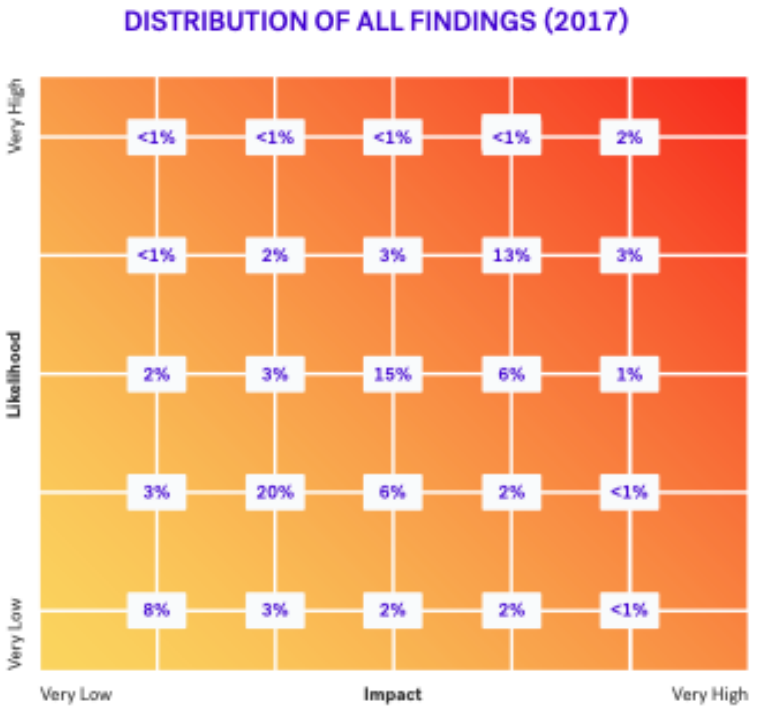


Data from Cobalt's pen testing as a service platform, based on 250+ pen tests conducted in 2017

Colorado State University

Chances of finding



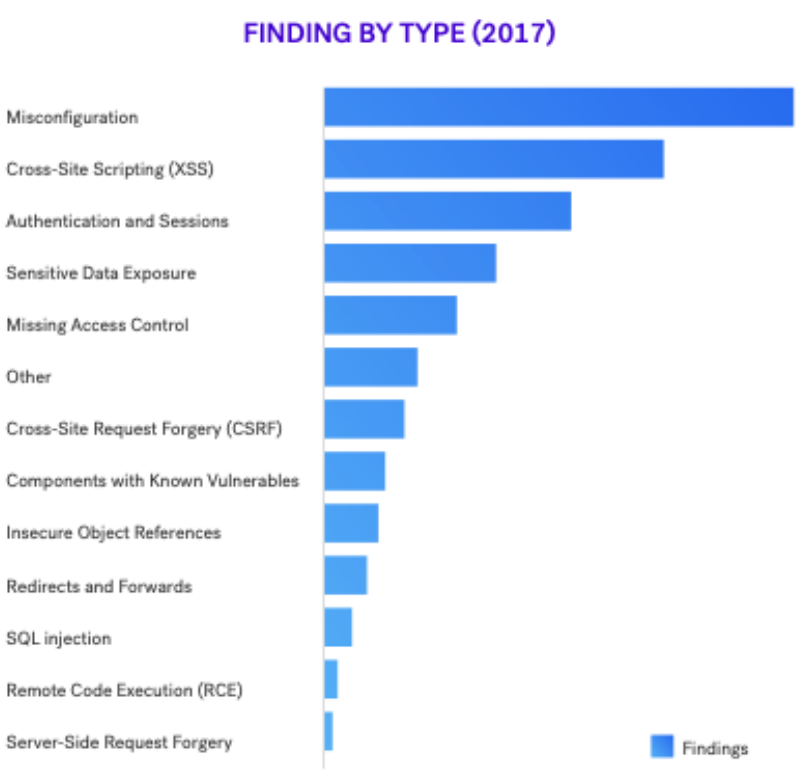


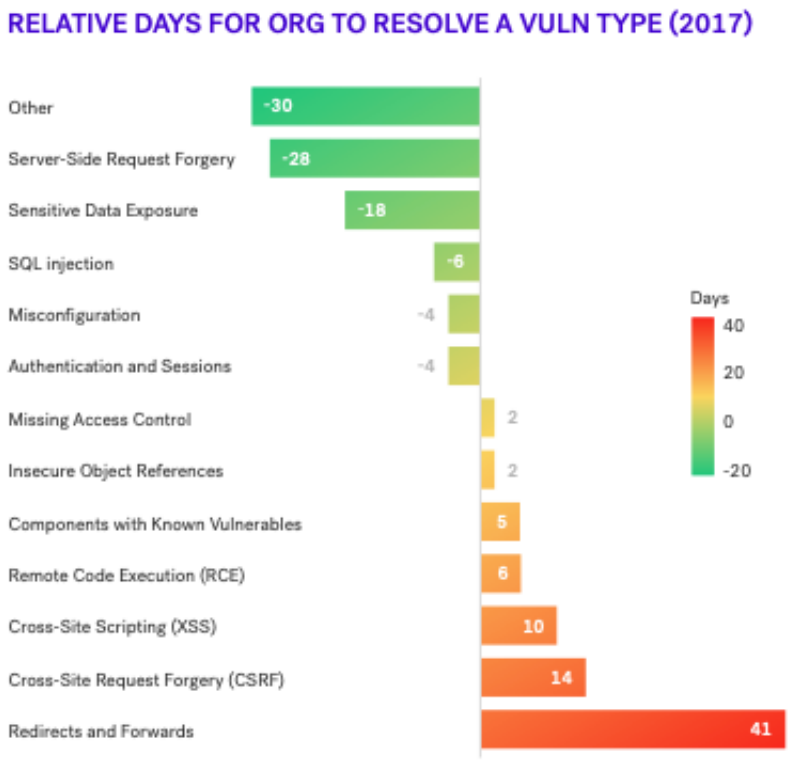
Note: multiple findings are likely.

Colorado State University

Vulnerability Types

a. How real world vulnerabilities map to common references like the OWASP Top 10 categories.

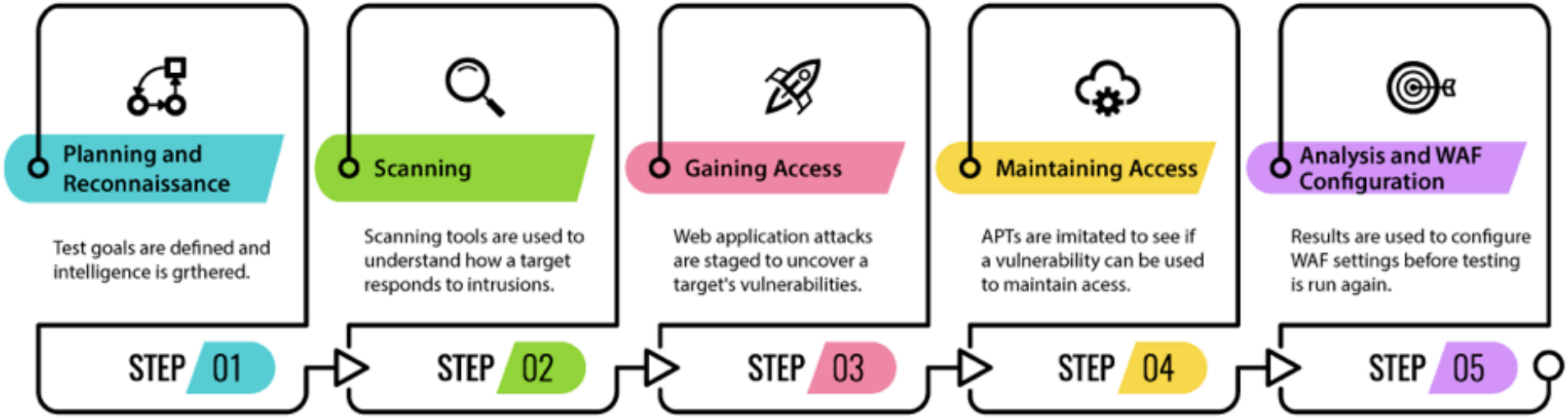




b. RELATIVE DAYS FOR ORG TO RESOLVE A VULN TYPE (2017)

Colorado State University

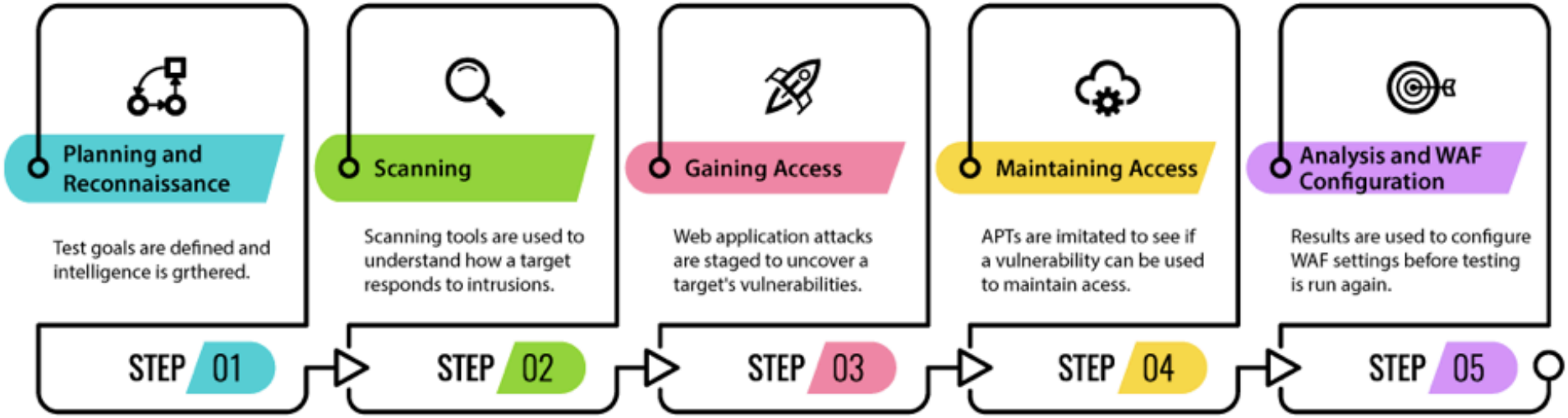
Pen Testing Stages



1. Planning and reconnaissance
   - Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.
   - Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.
2. Scanning
   - Network scanning and topology tracing, id OS and applications, Port scanning to find open ports and services, find net addresses of live hosts, firewalls, routers, etc. vulnerability scans to id potential vulnerabilities.
3. Gaining access:
   - This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

Sources: 1, 2

Pen Testing Stages



4. Maintaining access: See if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access.

- The idea is to imitate advanced persistent threats (APTs), which often remain in a system for months in order to steal an organization's most sensitive data.

5. Analysis and remediation: The results of the penetration test are then compiled into a report with

- Specific vulnerabilities that were exploited, Sensitive data that was accessed
- The amount of time the pen tester was able to remain in the system undetected
- This information is analyzed help configure an enterprise's WAF (web protection firewall) settings and security solutions to patch vulnerabilities and protect against future attacks.

Sources: 1, 2

Pen Testing Tools

- 1. The Network Mapper (also known as "NMAP")
  - NMAP can take the raw data packets which have just been created and use that to determine the following:
    - What hosts are available on a particular network trunk or segment
    - The information about the services which are being provided by these hosts
    - What operating system is being used (this is also known in technical terms as "Fingerprinting")
    - The versions and the types of data packet filters/firewalls are being used by any particular host
- 2. Metasploit: a package of different Pen Testing tools
  - with a built-in network sniffer, and various access points from which to mount and coordinate various kinds of Cyber based attacks.
  - This is accomplished via a quick, four step processes:
    - Determine which prepacked exploit should be used (or customize your own)
    - Configure this particular exploit with both the remote port number and IP address
    - Ascertain which payload should be used
    - Configure the payload with both the local port number and IP address
    - Launch the exploit at the intended target
  - This tool also comes with a "Meterpreter" which displays the results after an exploit has occurred

https://resources.infosecinstitute.com/category/certifications-training/pentesting-certifications/top-pentesting-tools/#gref

Pen Testing Tools

- 3. Wireshark: an actual network protocol and data packet analyzer
  - live information and data can be collected from: IEEE 802.11, Bluetooth, SSL/TLS, …WEP, ..Any Ethernet based connections
  - useful in analyzing the Security risks when information and data are posted to forms on Web based applications. These threats include data parameter pollution, SQL injection attacks, and memory buffer overflows.
- 4. The Web Application Attack and Audit Framework (also known as the "W3AF")
  - can root out threats such as:
    - User-Agent Faking
    - Custom Headers to Requests
    - DNS Cache Poisoning (this is also known as "DNS Spoofing," and it occurs when the DNS Name Servers return an incorrect IP address. As a result, the legitimate network traffic is diverted to the Cyber attacker's computer)

Pen Testing Tools

- 5. John the Ripper: primarily to launch Dictionary Attacks
  - Pen Test password databases which are both online and offline.
- 6. Kali Linux: Debian-derived Linux distribution designed for digital forensics and penetration testing
  - Numerous preinstalled penetration-testing programs, including Armitage (a graphical cyber attack management tool), Nmap (a port scanner), Wireshark (a packet analyzer), John the Ripper password cracker, Aircrack-ng (a software suite for penetration-testing wireless LANs), Burp suite and OWASP ZAP web application security scanners

Pen Testing Costs (examples)

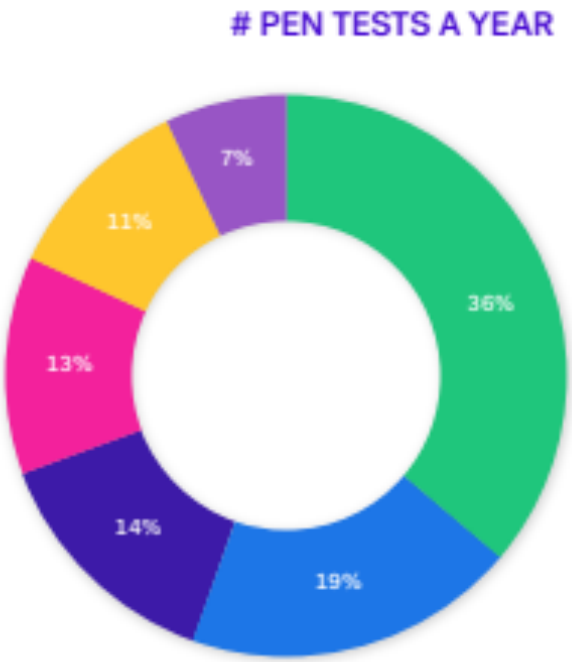
- From a vender, includes Pre-Test Discovery to define goals and a detailed Final Report
  - Up to 1 External IP starting at $1,195
  - Vulnerability Scan and Pen Test bundles as low as $1,495
  - Web Application Pen Tests starting at $2,500.
- From RSI
  - can cost $4,000-$100,000. On average, a high quality, professional pen test can cost from $10,000-$30,000, depending on
    - Organization size, complexity, scope, remediation
    - Methodology, Experience
    - External (common)/Internal Testing

How Often Should we Perform a Penetration Test?

- Regularly, at least once a year
  - Many regulations, such as PCI DSS, SOX, and HIPAA require an annual penetration test from a third party.
- Other times when
  - new network infrastructure or applications added
  - significant upgrades /modifications to applications or infrastructure
  - offices in new locations established
  - Security patches applied
  - end-user policies modified
- Example policy:
  - critical findings customer facing applications be fixed within 48 hours, high severity findings within 10 days, medium severity within 30 days, and low severity within 90 days.
- Typical value
  - 2016 av time to fix critical pen test findings = 17.6 days.
  - 2016 distribution: critical 9%, High 6%, Med 14%, Low 72%

How many pen tests do you do a year?

a. In 2017, cobalt.io collected data from 75 survey respondents in security, management, operations, DevOps, product, and developer roles



b. WHAT IS MOST CHALLENGING ABOUT PEN TESTING APPLICATIONS?

Source of data

Colorado State University

PCI Data Security Standard (PCI DSS v3)

Payment Card Industry Data Security Standard (PCI DSS) Requirement 11.3 Penetration Testing Guidance (pdf)

- Penetration Testing Components: Understanding of the different components that make up a penetration test and how this differs from a vulnerability scan including scope, application and network layer testing, network segmentation checks, and social engineering
- Qualifications of a Penetration Tester: Determining the qualifications of a penetration tester, whether internal or external, through their past experience (>1y) and certifications.
- Penetration Testing Methodologies: Detailed information related to the three primary parts of a penetration test: pre-engagement, engagement, and post-engagement.
- Penetration Testing Reporting Guidelines: Guidance for developing a comprehensive penetration test report that includes the necessary information to document the test as well as a checklist that can be used by the organization or the assessor to verify whether the necessary content is included.

For further information

- The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, Patrick Engebretson, Syngress, 2nd edition (August 15, 2013)
- Learn Kali Linux 2019: Perform powerful penetration testing using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark Paperback, Glen D. Singh, Packt Publishing (November 14, 2019)
- Full Ethical Hacking Course - Network Penetration Testing for Beginners (2019), 15 hours Video
- A sample Penetration Test Report.

Quantitative Security

Colorado State University

Yashwant K Malaiya

CS 559

Attacks

CSU Cybersecurity Center
Computer Science Dept

Attacks

- Assets and threats
- Attack types
- Attack surfaces
- Attack trees

Based on Computer Security Principles and Practice, Fourth Edition, William Stallings and Lawrie Brown

Vulnerabilities, Threats and Attacks

- Categories of vulnerabilities
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)
- Threats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- Attacks (threats carried out)
  - Passive – attempt to learn or make use of information from the system that does not affect system resources
  - Active – attempt to alter system resources or affect their operation
  - Insider – initiated by an entity inside the security parameter
  - Outsider – initiated from outside the perimeter

Table 1.3

Computer and Network Assets, with Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Passive and Active Attacks

Passive Attack

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
  - Release of message contents
  - Traffic analysis

Active Attack

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
  - Replay
  - Masquerade
  - Modification of messages
  - Denial of service

Attack Surfaces

Consist of the reachable and exploitable vulnerabilities in a system

Examples:

- Open ports on outward facing Web and other servers, and code listening on those ports
- Services available on the inside of a firewall
- Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
- Interfaces, SQL, and Web forms
- An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surface Categories

Network Attack Surface

- Vulnerabilities over an enterprise network, wide-area network, or the Internet
- Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks

Software Attack Surface

- Vulnerabilities in application, utility, or operating system code
- Particular focus is Web server software

Human Attack Surface

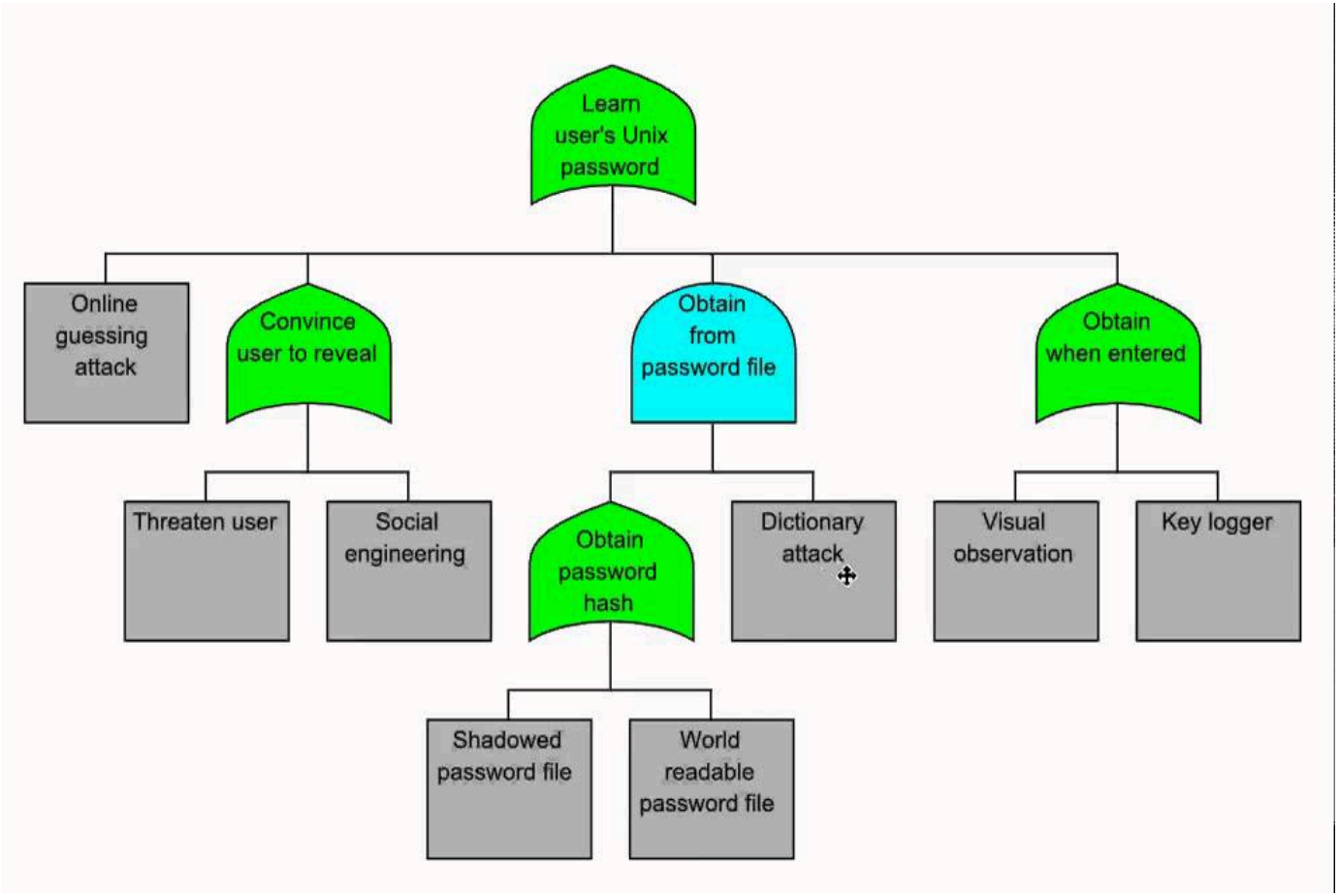
- Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

Attack Tree

An attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities

- The security incident that is the goal of the attack is represented as the root node of the tree, and the ways that an attacker could reach that goal are iteratively and incrementally represented as branches and subnodes of the tree.
- Each subnode defines a subgoal, and each subgoal may have its own set of further subgoals etc.
- The final nodes on the paths outward from the root, i.e., the leaf nodes, represent different ways to initiate an attack.
- Each node other than a leaf is either an AND-node or an OR-node.
  - To achieve the goal represented by an AND-node, the subgoals represented by all of that node's subnodes must be achieved;
  - and for an OR-node, at least one of the subgoals must be achieved.
- Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared.

Attack Tree Example 1



aa

Attack Tree Example 2

- Figure in next slide shows an example of an attack tree analysis for an Internet banking authentication application.
- The root of the tree is the objective of the attacker, which is to compromise a user's account.
- The shaded boxes on the tree are the leaf nodes, which represent events that comprise the attacks.
- The white boxes are categories which consist of one or more specific attack events (leaf nodes).
- Note that in this tree, all the nodes other than leaf nodes are OR-nodes.

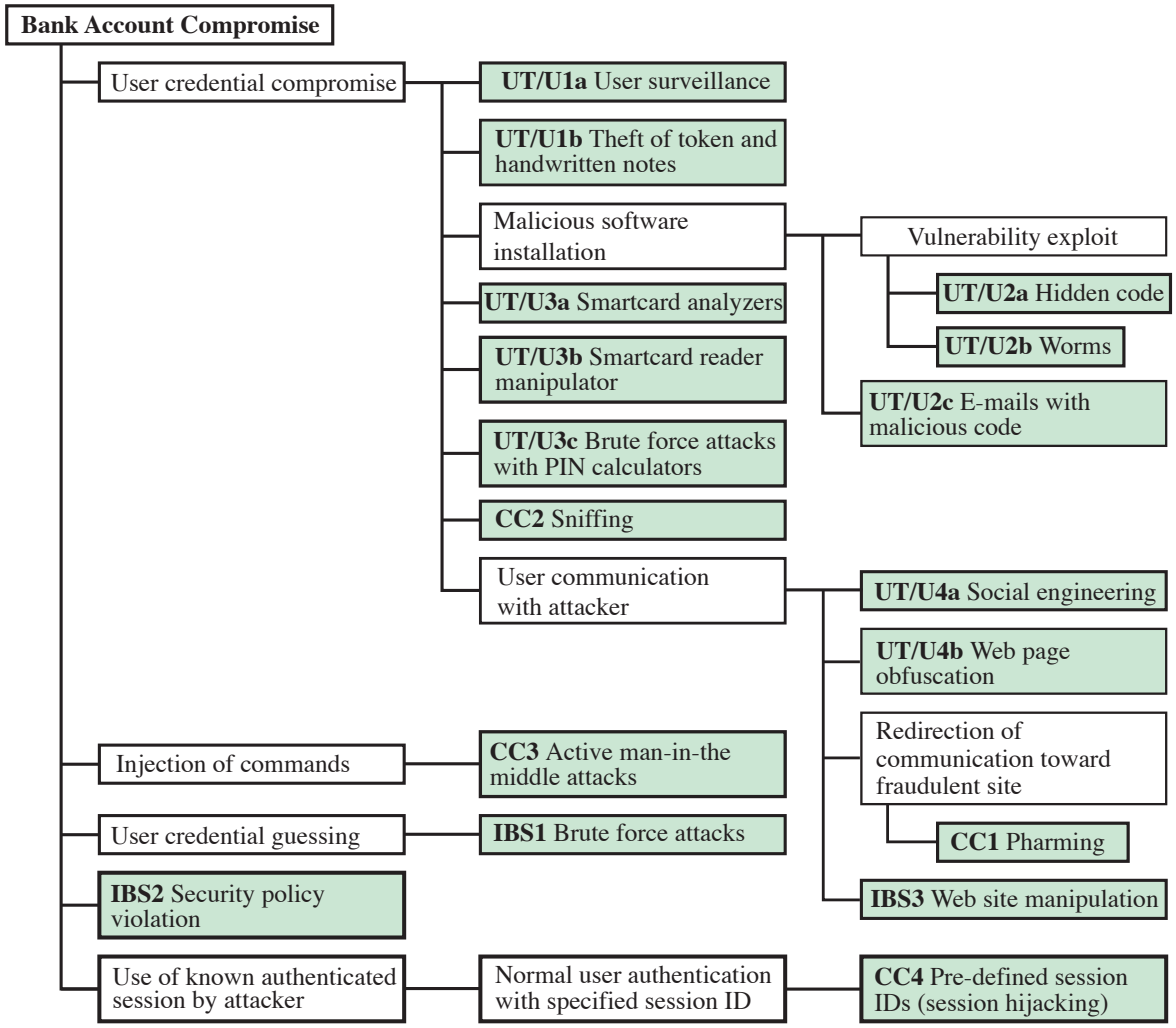


Figure 1.5 An Attack Tree for Internet Banking Authentication

Quantitative Security

Colorado State University

Yashwant K Malaiya

CS 559

Breach probability

CSU Cybersecurity Center
Computer Science Dept

Risk as a composite measure

Formal definition:

- **Risk** due to an adverse event e_i (a breach)

  $Risk_i = Likelihood_i \times Impact_i$

- $Likelyhood_i$ may be replaced by $frequency_i$, when it may happen multiple times a year.
- This yields the expected value. Sometimes a worst-case evaluation is needed.

In classical risk literature, the internal component of Likelihood is termed “Vulnerability” and external “Threat”. Both are probabilities. There the term “vulnerability” does not mean a security bug, as in computer security.

41

Risk as a composite measure

- Likelihood can be split in two factors

  $\text{Likelihood}_i = P\{\text{A security hole}_i \text{ is exploited}\}.$

  $= P\{\text{hole}_i \text{ present}\}.$

  $P\{\text{exploitation} \mid \text{hole}_i \text{ present}\}$

- $P\{\text{hole}_i \text{ present}\}$: an internal attribute of the system.
- $P\{\text{exploitation} \mid \text{hole}_i \text{ present}\}$: depends on circumstances outside the system, including the adversary capabilities and motivation.
- In the literature, the terminology can be inconsistent.

Caution: In classical risk literature, the internal component of Likelihood is termed "Vulnerability" and external "Threat". Both are probabilities. There the term "vulnerability" does not mean a security bug, as in computer security.

Annual Loss Expectancy (ALE)

Note the terminology is from the Risk literature.

- Annual loss expectancy (ALE)

  ALE = SLE x ARO

  – Where ARO is Annualized rate of occurrence.

- Note that ALE is essentially what we term as “risk”, with an annual time frame.

Estimating the Breach Probability

What factors impact the probability of an organization to be breached?

- Breach size
- Other factors:
- Default value of factor = 1
  - Specific value relative to the default value
- **Factors based on available data**
  - Organization's Country $F_{country}$
  - Organization's Industry Classification $F_{industry}$
  - Sensitive Data Encryption $F_{encryption}$
  - Organization's Privacy $F_{privacy}$
  - Business Continuity Management Team F_{BCM}
  - Data Breach Causes F_{breach_cause}

Modeling the Breach Probability

What factors impact the probability of an organization to be breached?

- Breach size
- Other factors:
- Default value of factor = 1
  - Specific value relative to the default value
- Do factors add or multiply?
  - Factors largely orthogonal: multiplicative
  - Factors overlap: additive
- Examples of multiplicative models
  - COCOMO Cost estimation model
  - RADC software defect density model
  - VLSI failure rate models

A look at the available data

- Some data is available at this time.
- Additional data collection and analysis is needed.