Security Testing

Truc Huynh & Mohammad

3/16/2022

# Security Testing and Cyber-Security: Use Case Simulated Man in The Middle Attack and Prevention

## Author:

* Truc Huynh
* Mohammed Alswairki
* [Link to Research Paper-Word File](https://ind657-my.sharepoint.com/:w:/g/personal/huyntl02_pfw_edu/EREQ8HZ5ZnpEmlgh66AqLR0Bc5Aj6R21wPnLuFMnwC4k5g?e=LA2CBC)

## Keywords:

* Software Testing: security testing uncovers vulnerabilities of the system and determines that the data and resources of the system are well protected
* Software Testing Life Cycle(STLC): Software Testing Life Cycle (STLC) is a sequence of specific activities conducted during the testing process to ensure software quality goals are met. STLC involves both verification and validation activities. There are 6 steps of STLC: Requirement Analysis, Test Planning, Test Cases Designing, Test Environment Setup, Test Execution, Test Closure.
* Software Quality: Computer programs, procedures, and possibly associated documentation and data pertaining to the operations of the system (IEEE). Four component that need to assure the quality of the software development: code, procedures, documentation, data to operating the software system (from [2])
* Secure Software Testing: testing methods that determine software products protects data and maintains security specification as given.
* Secure Programing Practice: is the practice of developing computer software in such a way that guards against the accidental introduction of security vulnerabilities
* Security Breaches: A security breach happen when a system fail in its security processes and cause unauthorized party access to the system. A security breach can happen by software problems (error, fault, failures), outdated security technology, ransom ware, malware …
* Media Access Control (MAC Address): is a permanent, physical, unique address assigned to network interface by manufacturer. ## I. Abstract:
* The paper introduces security testing principles.
* The paper also discuss about types of security testing.
* The relationship between STLC, SDLC, and security testing
* A Use case of simulating Man-In-The-Middle Attack on a system, and the tools that can be used in an Man-In-The-Middle Attack (Python, Kali Linux, Web Application Security Testing)
* Overview of Penetration Testing Methods(Pen Testing) and its related work

## II. Introduction:

### A. Software Security Testing:

* Security Testing or Software Testing Security determines that software protects data and maintains security specification as given. Another word to say: “security testing uncovers vulnerabilities of the system and determines that the data and resources of the system are well protected”. It ensures that the software system and application are free from any threats or risks that can cause a loss.
* To understand and implement good security test plans we must understand what is software quality, software development framework (SDLC) software testing lifecycle (STLC), and software requirements.
* We also need to understand major issues that cause security breaches.
* Security-related bugs can differ from traditional bugs in a number of ways:
  + Security testing is often fundamentally different from traditional testing because it emphasizes what an application should not do rather than what it should do, as pointed out in [9],
  + Malicious attackers do intelligently search for vulnerabilities. If they succeed, they cause problems for other users, who may be adversely affected. Compounding the problem, malicious hackers are known to script successful attacks and distribute them.[9]
  + Since most developers are not currently trained in secure programming practices, security analysts carry a greater burden in verifying that secure programming practices are adhered to.[9]
  + Many security requirements can be neither refined nor dropped even if they are untestable. e.g.  ”an attacker should never be able to take control of the application,” would be regarded as untestable in a traditional software development setting [9]
* The result is that secure software development is intrinsically harder than traditional software development. Therefore, testing also has an expanded role. Software testing also has other strengths that can be leveraged during secure software development
  + Testing can help confirm that the developers did not overlook some insecure programming practices.
  + A vulnerability is usually taken more seriously if there is a known exploit for it, but developing exploits is the domain of penetration testing
  + Testing can be used to help identify and mitigate risks from third-party components, where development artifacts like source code and architecture diagrams are unavailable.
  + Testing can be used to provide metrics of software insecurity and help raise the alarm when software is seriously flawed from the security standpoint.
  + Every design artifact views the software system at a certain level of abstraction. Attackers like to find the abstractions used by developers and work their way around them. No person or group can view a software system at all possible levels of abstraction, but testing can help by perhaps finding (at least some) flaws that are not visible in the design artifacts.[9]
* It is often said that security testing is only a small part of secure programming [10]. In fact, it is very difficult to find all security related problems in a software system. Thus, no effective mitigation strategy should be overlooked.

### A. Software Security Testing Goal:

* To identify the threats in the system.
* To measure the potential vulnerabilities of the system.
* To help in detecting every possible security risk in the system.
* To help developers in fixing the security problems through coding.

### B. Software Security Testing Principle:

* Confidentiality
* Integrity
* Authentication
* Authorization
* Availability
* Non-repudiation

### C. Major Focus Areas in Security Testing:

* Network Security
* Web Application Testing (Client-side and Server-side)
* System Security

## D. Test Case Designing for Security Testing:

* Test if users can directly access bookmarked web page without login.
* Test if system restrict users to download the file without log in.
* Test if previous accessed pages should not accessible after log out (i.e. Sign out and then press the Back button to access the page accessed before).
* Test if the industry standard username & password rules is enforced.
* Test if sensitive information ( passwords, ID numbers, credit card numbers, etc.) are stored as plain text. They should be encrypted and in asterix format.
* Test if bookmarking is disabled on secure pages by default.
* Test if source code is invisible to users.
* Test if older version web browsers can access the app (older version web browsers does not support SSL).
* Test if multiple attempt is being blocked.
* Test if system completely log out current user after time out.
* Test if users connection are stable and secure.
* Verify that relevant information (upload, download, activities) are written to the log files and that information should be traceable.
* Test if the SSL encryption is done correctly and verify the integrity of the information.
* Prevent same username to log in at the same time.
* Check if important credential update immediately.
* Test if error messages doesn’t contain important information.

## III. Related Work:

### A. Types of Security Testing:

There are seven types of Security Testing: - Vulnerability Scanning: Vulnerability scanning is performed with the help of automated software to scan a system to detect the known vulnerability patterns. - Security Scanning: Security scanning is the identification of network and system weaknesses. Later on, it provides solutions for reducing these defects or risks. Security scanning can be carried out in both manual and automated ways. - Penetration Testing: Penetration testing is the simulation of the attack from a malicious hacker. It includes an analysis of a particular system to examine for potential vulnerabilities from a malicious hacker that attempts to hack the system. - Risk Assessment: In risk assessment testing security risks observed in the organization are analyzed. Risks are classified into three categories (low, medium, and high). This testing endorses controls and measures to minimize the risk. - Security Auditing: Security auditing is an internal inspection of applications and operating systems for security defects. An audit can also be carried out via line-by-line checking of code. - Ethical Hacking: Ethical hacking is different from malicious hacking. The purpose of ethical hacking is to expose security flaws in the organization’s system. - Posture Assessment: It combines security scanning, ethical hacking, and risk assessments to provide an overall security posture of an organization.

### B. Pen Testing:

Simulate Man-In-The\_Middle Attack on a system. Pre-requirments knowledge: - Python Scapy Package: Scapy is a powerful Python-based interactive packet manipulation program and library. It is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, store or read them using pcap files, match requests and replies, and much more. It is designed to allow fast packet prototyping by using default values that work. - Kali Linux: is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering [11].(Over 600 penetration testing tools pre-installed) - Cyber Security principles: Applied Cyber Security Principle to find weakness in the system (by pass filter if using same MAC address), network topology - Networking Principles: Understand MAC Address, Access Point, Various Networking Devices, Address Resolution Protocal (ARP), Domain Name Server (DNS) - OSI Model and TCP/IP Model: Understand Layers Architecture of OSI Model and TCP/IP Models, Understand IPV4 and IPV6 - Web Aplication Structures: (Client Server Model) - Python Programming: String Manipulation, Parsing HTML, Sending & receiving HTTP requests, Netfilterqueue, Socket Programming, Data Structures, OOP

Popular tools that is used in Man-In-The\_Middle Attack: - MAC Address Changer - Network Scanner - ARP Spoofer (ARP Cache Poisoning) - Packet Sniffer - DNS Spoofer (DNS Cache Poisoning) - File Interceptor

## Problem:

In this use case, I will demonstrate how to implement man-in-the-middle-attack on a private network (private system that we don’t have permission to get access). A private Network can only access by devices within its network. All tools will be write from scratch and source code can be found at [13]. Please take look at Pre-requirement section if you not sure about topics that I mention in the next sections. The benefit of writing script attack is that you can schedule the whole script as one and automate the process.

Private Network are usually exist on a physical building with the access within that building. However, it now had been extend to mobile technology with performance-critical data transfer. Which being say, cyber security engineer has more work to do. Private Networks are more secure than public network, however it won’t be secure if an adversary get access to one of the computer in the network. Man-In-The-Middle can be established just by one computer being hack, and spread out to many other devices within the network. Depend on the size of the attack, it can cause millions lost.

### A. System under normal operation:

Under normal operation, each client is connected to an access point within the organization (inside its building). Please notice access to the private network only can be grant within access point within the building (wire and wireless)

### B. Hackers Gain Access to The System:

Access can be gained in many ways insider attack, malware backdoor , code Injector, malware package… I will not focus on how the hackers gain access to the system. However, my focus is to simulate the strategy that hacker spread out the virus after gaining access and control the system.

Hacker can use a remote devices that set up within the building, or gain control to one of the devices within the organization to perform the task. They start with one device then spread attack to all other devices. Each of the devices get access by the hacker can become bots and sending out information, or spread out the virus to other devices within the network. Some virus can contain themselves, create back door, and by pass security scanner by changing its MAC address or IP address. Depend on how many devices hackers want to control, they usually need a super computer to handle the task.

The plan of attack is: - Step 1: Get Access to one computers: - Through a USB stick equipped with a custom Linux version - Enable backdoor on user’s computer

Images by Truc Huynh

* Step 2: Established Man-In-The-Middle:
  + Redirect the flow of packet by running ‘ARP Spoofer’.
  + ‘ARP Spoofer’ will run ‘Network Scanner’ to get all the IP and Mac Address on the network.
  + Then store the result, and run ‘Mac Address Changer’ to change our MAC address hacking devices (USB stick or remote computer) to a physical MAC address of a local computer (in the private network).

Images by Truc Huynh

* Step 3: Gather information
  + Using ‘Packet\_Sniffer’ to read packet and data flow through the hacker interface
  + Use the information that ‘Packet Sniffer’ collect to create a suitable plan for spreading the virus to other machine within the network
* Step 4: Modify Data, spread virus
  + Using the plan that create on step 3 to make an attack on other computers. Depend on security structure on the network using ‘DNS Spoofer’ or ‘File Interceptor’ (or both)
  + Using ‘File Interceptor’ to modify HTTP data that send over HTTP, replace a user’s download request with a completely different file (virus, backdoor…)
  + Using ‘DNS Spoofer’ (modify data in DNS Layer) to redirect the destination on the computer on network (e.g. to a fake website) so that hacker can install a backdoor on other local computer.
  + Slowly spread and contain them-self, avoid detect by the network administrator, or any security system on the network

Images by Truc Huynh

* Step 5:
  + Decide if the attack is sucess or not, make sure the attack don’t create any evidence that lead to the hacker(protocal tracing)

## Reference:

* IEEE: [Advance Technology for Humanity](https://www.ieee.org/) [1]
* ISO 9000-3: [Quality management and quality assurance standards](https://www.iso.org/standard/26364.html) [2]
* SWEBOK V3.0: [Guide to the Software Engineering Body of Knowledge](https://ieeecs-media.computer.org/media/education/swebok/swebok-v3.pdf) [3]
* [Tutorial Point: STLC Tutorial](https://www.tutorialspoint.com/stlc/index.htm) [4]
* [Software Testing | Security Testing](https://www.geeksforgeeks.org/software-testing-security-testing/?ref=lbp) [5]
* [Security Testing: Types, Tools, and Best Practices](https://www.neuralegion.com/blog/security-testing/) [6]
* [API Security: The Complete Guide](https://www.neuralegion.com/blog/api-security/) [7]
* [STLC (Software Testing Life Cycle) Phases, Entry, Exit Criteria (guru99.com)](https://www.guru99.com/software-testing-life-cycle.html) [8]
* Fink, G. & Bishop, M. “Property-Based Testing: A New Approach to Testing for Assurance.” ACM SIGSOFT Software Engineering Notes 22, 4 (July 1997): 74-80.[9]
* McGraw, Gary & Potter, Bruce. “Software Security Testing.” IEEE Security and Privacy 2, 5 (Sept.-Oct. 2004): 81-85. [10a]
* McGraw, Gary. “Application Security Testing Tools: Worth the Money?” Network Magazine, November 1, 2004. (2004). [10b]
* <https://www.kali.org/?msclkid=ccbd3c3faa2511ecbe541363c15a4582> [11]
* <https://pypi.org/project/scapy/?msclkid=33343ba2aa2611eca8b9c3abfd8b35c1> [12]
* <https://github.com/jackyhuynh/ethical-hacking-using-python> [13]
* <https://www.udemy.com/course/learn-python-and-ethical-hacking-from-scratch/learn/lecture/10800892#overview> [14]