Summary-"An Interactive Visualization Tool for Teaching ARP Spoofing Attack"

This paper is an initiative of making understand students with the hands-on implemented visualization of most vulnerable protocol within Local Area Network namely Address Resolution Protocol. ARP is considered to be easily exploited by attackers if they are able to gain access to the same network. Thus, the main motive of this paper is to provide enhanced learning method to make students explain the ARP spoofing attack in a detailed way as if it is implemented in real time. Researchers developed a tool named Hacker Graphical User Interface (HGUI) using programming language Processing, which is as collaborative visualization hands-on tool developed to help students in understanding the ARP Spoofing mechanism. This tool is designed to cover all the anomalies of ARP spoofing like creation of normal packets, attacking those packets, animations showing the work flow of spoofing and the status visualization of ARP cache in real time.

Contextual groundwork includes understanding of following terminologies listed:

1. ARP (Address Resolution Protocol) mechanism
2. ARP Spoofing attacks in detail
3. Study related to ARP Spoofing tools and defense(tools like Cain and Abel and Ettercap, defense system like static ARP cache and secure ARP software)

Development of Hacker Graphical User Interface (HGUI):

1. Architecture: Constitutes centralised visualization module that communicates with users and controls other virtual machines including multiple attackers and victims.
2. Technologies Used: Includes programming through Processing for virtualization, Virtual machine for running KALI Linux through which attackers and victims can be included and finally the technological interface that connects this both such as various scripting and programming languages.
3. Items to visualize: This establishes the organised view of essential hardware that performs ARP spoofing like Router, Switch, attacker machine and victim or target machine.
4. Final flow of ARP Spoofing attack: This is all about how this tool works and all of its functionalities.

Survey and Conclusion:

In this phase developers evaluated the performance of students on the basis of their knowledge before and after getting familiarise with the HGUI tool. This performance helped them to get the clear vision of outcome of this tool and its influence of the understanding process of the students. Although the curiosity level in students towards this tool was not as much expected, but the outcomes were quite satisfactory resulting majority improvement of their performance in post-lab session. This survey concluded that HGUI tool helped students for learning ARP spoofing mechanism in detail and motivated them to study about similar hands-on tool that helps them to understand about such challenging topics very easily.