Network Security - Ex. 3

Submission date: 25/7/2014

1 Instructions

Choose one of the following topics and implement the requirements. State in comments to the code and verbally if you use any software that you did not write and exactly what functions that software performs. The exercise will be graded based on the submitted code, a presentation of a functioning system and questions during the presentation. Questions may involve the internal workings of attacks, even if they are carried out by software you did not write. The work and submission can be done in pairs.

2 Topics

1. **ARP poisoning**. Install a LAN with at least three separate IP addresses on at least two separate computers. The IP addresses must include an IP gateway (router), an attacker and a target. Show how the attacker can poison the ARP table of the target, replacing the router's MAC address with the attacker's address. Show how packets sent from the target to an address outside the LAN are received by the attacker. If you choose this topic then you must write the attack code yourself.

2. **XSS**. Install a web server that hosts a web site with a reflected XSS vulnerability. Send an e-mail to the target with a link to the server such that clicking the link causes the target's browser to explicitly display the cookie of the session between the target and the server. The browser and server must be implemented on separate machines.

3. **SSL Strip**. Install a web server that hosts a simple web site that has both text and an image on its single web page. Access this site with both HTTP and HTTPS and show (e.g. by wireshark) that in the first case the whole web page is in the clear and in the second case the whole web page is encrypted. Insert a man-in-the-middle and implement the SSL Strip attack. Show that traffic between the browser and MITM

is in the clear, while traffic between the MITM and server is SSL/TLS protected.

4. **Private equality function**. Implement a two-party protocol between Alice and Bob privately computing the equality function on strings of length at most 128 bits. In other words, Alice has input $x \in \{0,1\}^{128}$, Bob has input $y \in \{0,1\}^{128}$ and the result of the computation is 1 if $x = y$ and the result is 0 if $x \neq y$. Assume that both parties are honest but curious, so for example there is no need to implement cut-and-choose techniques.