Project Proposal

Title:

Identification of Vulnerabilities of OPNsense Firewall in Using Phishing Attacks and Pen Testing of Virtual Home-Based Cloud Environment

Project Description:

This project focuses on identifying vulnerabilities in the OPNsense firewall using phishing attacks and performing penetration testing in a virtual home-based cloud environment. The project involves setting up a virtual environment with multiple virtual machines (VMs), including VMs running Windows Server and Ubuntu, and one VM running the OPNsense firewall. An attacker VM containing machine learning (ML) Python codes will be used to launch phishing attacks on the OPNsense firewall and other VMs.

The project aims to evaluate the security posture of the OPNsense firewall and the virtual home-based cloud environment against phishing attacks and identify potential vulnerabilities. By simulating phishing attacks and performing penetration testing, the project will help to determine the vulnerabilities of the OPNsense firewall and the impact of phishing attacks on the virtual environment.

Objectives:

- Identify vulnerabilities in the OPNsense firewall using phishing attacks

- Perform penetration testing of the virtual home-based cloud environment

- Evaluate the security posture of the OPNsense firewall and the virtual environment

- Determine if any manipulation can be done on the Windows Server or other VMs after phishing attacks on the OPNsense firewall

Scope of the Project:

The project scope includes setting up a virtual environment with OPNsense firewall, Windows Server, and Ubuntu VMs, simulating phishing attacks using ML Python codes from an attacker VM, and performing penetration testing to identify vulnerabilities in the OPNsense firewall and the virtual environment.

Technologies to Be Used:

- OPNsense firewall

- Virtualization software (VMware or VirtualBox)

- Windows Server and Ubuntu VMs

- Attacker VM with ML Python codes for phishing attacks

- Penetration testing tools (e.g., Metasploit, Burp Suite, ZAP)

Methodology:

1. Set up a virtual environment with OPNsense firewall, Windows Server, and Ubuntu VMs.

2. Configure an attacker VM with ML Python codes for phishing attacks.

3. Launch phishing attacks on the OPNsense firewall and other VMs using different network codes.

4. Perform penetration testing to identify vulnerabilities in the OPNsense firewall and the virtual environment.

5. Analyze the vulnerabilities of the OPNsense firewall and determine if any manipulation can be done on the Windows Server or other VMs.

Expected Outcome:

The project is expected to identify vulnerabilities in the OPNsense firewall using phishing attacks and provide insights into the security posture of the virtual home-based cloud environment. The results will help to determine the impact of phishing attacks on the OPNsense firewall and the virtual environment, and provide recommendations for improving the security of the OPNsense firewall and the virtual environment.