ARP SPOOFING DETECTION APPROACH FOR NETWORK INTRUSION DETECTION SYSTEM

Requirements and Specification Document

25th March 2018

Version Major

Serial No.	Name	Enrollment Number
1	Abhishek Kanhar	16114005
2	Anil Kumar	16114012
3	Anoop Singh	16114016
4	Hasanwala Faizal	16114030
5	Rahul Singh	16114052

1. Project Abstract

The software will protect the organization from internal attacks of ARP spoofing, in which one machine on network tries to impersonate other machine on network with intentions to harm the network or gain information from network. Software will provide additional security, without having to change kernel level implementation on machine or need on any hardware. The web interface of software will allow system administrators to overview current status of whole network and emergency notifications on the interface itself. Web interface will also provide weekly and monthly statistics on attack on network and from where they were originated. For an normal employee access will be limited to the viewing current status and weekly analysis of his/her machine. Each employee will be provided credentials to login at the time on software installation on his/her machine.

2. Document Revision History

Revision 1.0 25th March 2018 - initial version

3. Customer

The customer for software is bank with large internal network of PCs. The internal network also connects to important PC and server of bank. Bank deals with regular cyber attack on their infrastructure. Many of the attacks occurs through the malware infected PCs. The software developed will be used by two major actors

1) System Administrator
2) Bank Employee

System administrator assumes the task of reviewing and analyzing attacks on network. Whereas the bank employee is the actor on whose machine software will be installed. He or she is responsible for alerting the administrator about the attack, as soon as our software alerts him or her.

This software can be potentially used by any organization who faces such cyber security threats. Any organization with large internal network can be a potential customer. Untrained employees in such organization are threats to such internal attacks, which can be simply initiated from a malicious mail. The main actors in any such cases will remain same.

4. Competitive Landscape

Currently there are many software present in the market which provide such security features. A variety of software features (similar to ours) are present in market. Competitors having considerable market share are considered here.

1) *Arpwatch*
    a) Strengths
        i) Doesn't require any extra hardware.
        ii) No need to change default IP stack.
    b) Weakness
        i) Takes too much time for detection of attack.
        ii) Complex user interface.

2) *Secure ARP (protocol)*
    a) Strengths
        i) 100% immune to attacks.
        ii) Validates the ARP request by removing ARP's stateless property.
    b) Weakness
        i) Requires to change default IP stack.
        ii) Slow due to cryptographic calculations.
        iii) Complex user interface.

Our software is different from competitors in following manner.

1) Doesn't need to change current IP stack.
2) No need of extra hardware.
3) Fast response.
4) Fast detection of attacks.
5) Provides easy to use Web User Interface.

5. System Requirements

Functional Requirements

Requirement 1: (Must have)

- User(employee) initiates installation of the software on his system.
    - He or she is prompted to enter his/her employee details.

- Software makes request to web application with employee details.
    - Web application registers the employee and return success message.
    - If employee is already registered then error message is returned.
- Software displays message to employee

R 1.1:
- Input: User initiates the installation
- Output: Software asks for employee name and ID number.

R 1.2:
- Input: Employee ID and name.
- Output: Message sent by central web application
    - If message is success message. Provide URL of central web application to user and his/her credentials for login.
    - If message is error message. Display error message.
- Processing
    - Central web application will register the employee and his machine number.
    - If employee is already registered then. Application will generate error.
    - If registration is successful then. Application will generate password for employee.

Requirement 2: (Must have)
- Software should detect attacks and immediately report to the employee using the machine.
- Also a message should be dispatched to the central web application to alert the system administrator.
- The infected computer should be shut down by the administration.

R 2.1:
- Input: ARP spoofing is detected (Input will not be from user)
- Output: Notification displayed to employee using the machine.
- Processing
    - Software sends alert message to central web application
    - Central web application updates network status as ‘under attack’.
    - System administration is sent an alert message.

R 2.2: (For administrator)

- Input: Infected computer's ID and alert message.
- Output: Infected PC shut down/ disconnected and database updated.
- Processing
    - Software issues a request to administration to shut down the infected PC.
    - The infected PC's id and date/time of the infection are stored in the database.

Requirement 3: (must have)

- Login page for normal employee and administrator.

R 3.1:

- Input: Username and password
- Output: Success or failure message
- Processing
    - Central web application checks for the username and password entered.
    - If username and password combination is correct. Then returns 'Login Success'
    - If username is correct but password is incorrect. Then returns 'Invalid Password'.
    - If username in not registered. Then returns 'User not registered. User credentials were provided during installation'.

Requirement 4: (must have)

- Administrator should be able to see the stats of the company's infections for the last 30 days.
- Normal user should be able to the stats for his machine for the past 30 days.
- Appropriate charts should be plotted for the above data.

R 4.1: (For Backend)

- Input: No input required (Automatic monthly cycle)
- Output: Appropriate stats data (Input for statistical representation) is provided to the frontend.
- Processing
    - Whenever a request for stats is issued, the system checks whether the request is issued by admin or a normal employee.
        - If normal employee, the data for his machine is fetched and sent to the frontend .

        - If admin, the data for all the machines is fetched and sent to the frontend.

R 4.1: (For Frontend)

- Input: Stats data in appropriate format (From the backend)
- Output: Charts and stats for the given stats data in a presentable manner
- Processing
    - For the normal employee data:
        - A Bar chart for the last month's data, with days on x-axis and number of infections on y-axis.
    - For admin data:
        - A stacked bar chart with days on x-axis and number of attacks by employees (stacked) on x-axis.
        - A Pie chart showing the percentage of attacks coming from every employee's machine.
    - The statistics should be presented in a manner so that they can be readily printed as a report.

Requirement 5: (useful)

- Forgot password functionality for normal employee.
- Forgot password button on login page.

R 5.1:

- Input: Normal employee clicks 'Forgot password?' button.
- Output: Application asks for employee details.

R 5.2:

- Input: Employee enters his or her details.
- Output: Application responds with message.
- Processing:
    - If employee with provided details is found then application forwards request to administrator, and returns 'Request forwarded to administrator'.
    - If employee is not found then returns 'No such user found'.

R 5.3:

- Input: Administrator gets forgot password request
- Output: Administrator issues new password.
- Processing:

- Administrator verifies the forgot password request and issues new password.

Non-Functional Requirements

- Operability
  - There will be only one time installation. After that software on machine will need no inputs from employee.
  - For central web application, UI for both normal employee and system administration will be provided to ease the operability.
- Documentation
  - Documentation for central web application will be provided.
  - Installation guide for software will be provided, also installation will be assisted by one of developers.
- Speed
  - Web application will run on any hosting platform.
  - Software will run in background with no user interaction, so no speed concern
- Memory Usage
  - Web application will run on any system with little as 1 GB RAM.
  - For smooth usage, in case of spoof detecting software minimum memory of 256 MB is recommended for software only.
- CPU Usage
  - Web application run in separate system, so no issue with CPU usage.
  - Spoof detection software will run on any machine.
- Storage Usage
  - Web application uses database for storing all information provided by spoof detection software. So large database is needed.
  - Spoof detection software will need around 50 MB of storage space.
- Backup
  - Weekly backup of data will be taken of database hosted on central web application.
- Updates
  - Updates will be silent for both spoof detection software.
  - Central web application will be unusable for ~20 seconds while updating.

External dependencies

List of all external entities required by central web application and spoof detecting software:

1) A web server to host central web application.
2) A database to store attacks information.
3) Linux operating system for running of spoof detector.

Use case diagram