Experiment 8

Shashwat Shah
60004220126
TYBTech Comps B

Aim: To implement RSA digital signature

Theory: Algorithm.

Steps.

1) Sender A uses hashing algorithm to calculate the message digest (MD1) over the original message M.
2) Sender A now encrypts the message digest with its private key. Output of this process is called Digital Signature of A.
3) Now A sends the digital signature along the original message M.
4) When B receives the original message M and digital signature. It uses the same message digest algorithm as was used by A. and calculates its own message digest (MD2) for M.
5) Now B uses A's public key to decrypt the digital signature because it was encrypted by A's public key. Result of this process is the original MD1 calculated by A.
6) If MD1 == MD2, B accepts the original message and ensures that message has come from A, not someone posing as A.

Conclusion: Thus, we have successfully implemented RSA digital signature.

Experiment 9

Aim: Perform information gathering / Foot printing

Theory: Information gathering, also known as reconnais is a crucial initial phase in cybersecurity. It involves collecting as much relevant data as possible about a target system or network to identify potential vulnerabilities and attack vectors.

1) Passive Information Gathering - This involves gathering information without directly interacting with the targe which includes searching online public sources suc as social media, search engines, forums, etc.

2) Active Information Gathering - It involves more direct interaction with the target system. Techniques ma include port scanning, network mapping, and servic enumeration etc.

3) Foot printing - This is the process of collecting informat about the target organizations networks, systems and infrastructure, involves identifying IP addresses, domain names, network blocks, etc.

4) Enumeration - It involves gathering specific information about the targets systems, such as user accounts, network shares, installed softwar and services running on the network.

5) Social Engineering - This techniques involves manipulati individuals within the target organisation to divulge confidential information or perform actions that compromis

Security

Conclusion : Thus, we have learnt how important Information gathering is in cybersecurity and how to perform it using various tools.

Experiment 10

Shashwat Shah
60004220126
TY Btech Comps B

Aim: Perform packet capture and sniff IP traffic using wireshark.

Theory: Packet sniffers intercept packets of data flowing across a computer network in order to view their contents. This act is called packet sniffing.

Web pages and emails are not sent through the internet as one document, rather the sending side breaks them down into many little data packets. These packets are then addressed to an IP address at the receiving end, which has to send back an acknowledgement of each packet it receives.

These packets are not transferred from the sender to the receiver through a single direct connection. Instead, as each packet traverses the internet enroute to its destination, it passes through a number of traffic control devices such as routers and switches. Each time a packet passes through one of these traffic control devices, it is susceptible to capture and analysis.

Anyone who has access to a router can perform packet collection and subsequent analysis. Wireshark is arguably the most popular of packet sniffing tools.

Conclusion: Thus, we have performed packet capture and sniffed IP traffic using wireshark.

Experiment 11

Shashwat Shah
60004220126
T4 Btech Comps B

Aim: Perform SQL Injection

Theory: SQL injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application of a web page ~~or web~~ and retrieve the contents of the entire SQL database. They can also use SQL injection to add, modify, and delete records in the database.

An SQL injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle SQL server or others. Criminals may use it to gain unauthorized access to your sensitive data.

SQL injection attacks are one of the oldest application vulnerabilities. The OWASP (Open web Application Security Project), lists injections in their OWASP Top 10 2017 document as the number one threat to web application security.

Conclusion: Thus, we have learnt and performed SQL injection attack.