Ex. No: 1

Date: 12/08/2024

Aim: To study and write about the different wireless network components and features of any one of the Mobile Security Apps.

Description:

Wireless Network Components

A wireless network consists of several key components that work together to provide wireless connectivity. The main components are,

1. **Clients**: These are the enduser devices such as smartphones, tablets, laptops, and desktop computers that connect to the wireless network.
2. **Access Points (APs)**: These devices allow wireless clients to connect to a wired network. They broadcast a network name (SSID) that clients can connect to.
3. **Routers**: Routers direct data traffic between different networks, such as between a local network and the internet.
4. **Switches**: These devices connect multiple devices on a wired network and use MAC addresses to forward data to the correct device.
5. **Firewalls**: Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules to protect the network from unauthorized access.
6. **Ethernet Cables**: While wireless networks eliminate the need for physical cables between devices Ethernet cables are still used to connect the wireless network components to the internet and other wired networks.

Features of a Mobile Security App: Norton Mobile Security

Norton Mobile Security is a comprehensive mobile security app that offers a range of features to protect your device and data:

1. **Malware Protection**: It scans and removes malware, spyware, and other malicious software from your device.
2. **AntiTheft**: If your device is lost or stolen, you can remotely lock it, wipe data, or even locate it using GPS.
3. **Privacy Advisor**: This feature helps you understand and manage app permissions to protect your personal information.
4. **Secure Web Browsing**: Norton provides a secure browser that protects you from phishing attacks and other online threats.
5. **Call and Text Blocking**: You can block unwanted calls and texts to avoid spam and potential scams.
6. **App Advisor**: This feature analyzes apps for potential privacy and security risks before you download them.
7. **VPN (Virtual Private Network)**: Norton includes a VPN to encrypt your internet connection and protect your data from being intercepted.

These features make Norton Mobile Security a robust tool for safeguarding your mobile device and personal information.

Result:

Thus, the different wireless network components and features of Norton Mobile Security Apps were studied and written.

Ex. No : 2

Date: 12/08/2024

Aim: To study and write about the features of firewall in providing network security and to set Firewall Security in windows.

Description

Features of Firewalls in Providing Network Security

Firewalls are a crucial component of network security, acting as a barrier between trusted internal networks and untrusted external networks. Some key features of firewalls are,

1. **Traffic Filtering**: Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules. They allow or block traffic based on factors such as source and destination IP addresses, port numbers, and protocols.
2. **Intrusion Prevention**: Firewalls help prevent unauthorized access by blocking malicious traffic, such as viruses, backdoors, phishing emails, and denial-of-service (DoS) attacks.
3. **Insider Threat Protection**: Firewalls can restrict certain types of outgoing traffic, helping to identify suspicious activity and mitigate data exfiltration.
4. **Logging and Monitoring**: Firewalls log traffic details for analysis, providing visibility into who is accessing the network and what they are trying to do.
5. **Network Segmentation**: Firewalls can create separate segments within a network, isolating sensitive data and systems from less secure areas.
6. **Application Layer Filtering**: Advanced firewalls, such as NextGeneration Firewalls (NGFWs), can inspect traffic at the application layer, providing deeper inspection capabilities.

Setting Up Firewall Security in Windows

To set up firewall security in Windows, follow these steps:

1. **Open Windows Security**: Press the Windows key, type "Windows Security," and select the app from the search results.
2. **Navigate to Firewall & Network Protection**: In the Windows Security window, click on "Firewall & network protection" under the "Protection" section.
3. **Select Network Profile**: You will see three network profiles: Domain network, Private network, and public network. Select the appropriate profile based on your network type.
4. **Turn on Microsoft Defender Firewall**: Under the selected network profile, ensure that the

"Microsoft Defender Firewall" switch is turned on. This helps protect your device from unauthorized access.

5. **Configure Advanced Settings**: For more detailed control, click on "Advanced settings" to open the Windows Defender Firewall with Advanced Security. Here, you can create, modify, or delete inbound and outbound rules, as well as connection security rules.

6. **Create Rules**: To create a new rule, click on "New Rule" in the Actions pane5. Follow the wizard to specify the rule type (inbound, outbound, or connection security), the protocol, port number, andIP addre ss range. Configure the action (allow or block) and apply the rule to the appropriate network profiles.
7. **Review and Save**: After configuring the rules, review them to ensure they meet your security requirements. Save the changes and close the firewall settings.

By following these steps, you can effectively set up firewall security in Windows to protect your network from unauthorized access and various threats.

Result:

Thus, the features of firewall in providing network security and to set Firewall Security in windows were studied and written successfully.

Ex. No: 3

Date: 19/08/2024

Aim: To analyse and write the steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome).

Description:

Steps to Ensure Security in Mozilla Firefox

1. **Update Firefox**: Ensure that you are using the latest version of Firefox1. Updates often include security patches and new features.
2. **Enable Enhanced Tracking Protection**: This feature blocks trackers and malicious content by default. You can customize the settings to block trackers, crypto miners, and finger printers.
3. **Use Private Browsing Mode**: This mode prevents Firefox from saving your browsing history, cookies, and temporary files.
4. **Manage Addons and Extensions**: Only install addons from trusted sources. Remove any unnecessary or suspicious extensions.
5. **Use a VPN**: A VPN encrypts your internet connection, providing an additional layer of security, especially when using public Wi-Fi.
6. **Clear Browsing Data Regularly**: Remove cookies, cache, and history to prevent tracking and improve performance.
7. **Enable DNS over HTTPS (DoH)**: This feature encrypts DNS queries, enhancing privacy and security.
8. **Use Strong Passwords**: Store and manage your passwords securely using a password manager.
9. **Enable TwoFactor Authentication (2FA)**: Add an extra layer of security to your accounts by enabling 2FA.
10. **Review Permissions**: Regularly check and manage permissions for websites and extensions to ensure they only have access to necessary data.

By following these steps, you can significantly enhance the security of your browsing experience in both Mozilla Firefox.

Result:

Thus, the steps to ensure Security of Web browser Mozilla Firefox were analysed.

Ex. No: 4

Date: 19/08/2024

Aim:

To study and write a note on different types of vulnerabilities for hacking websites / Web Applications.

Description:

Types of Vulnerabilities for Hacking Websites/Web Applications

Web applications are often targeted by hackers due to various vulnerabilities that can be exploited1. Some common types of vulnerabilities are,

1. **SQL Injection**: This occurs when an attacker inserts malicious SQL code into a query, allowing th em to manipulate the database and access sensitive information.
2. **CrossSite Scripting (XSS)**: XSS vulnerabilities allow attackers to inject malicious scripts into web pages viewed by other users, potentially stealing cookies, session tokens, or other sensitive information.
3. **Broken Authentication**: This vulnerability occurs when authentication mechanisms are improperly implemented, allowing attackers to compromise passwords, keys, or session tokens.
4. **Security Misconfigurations**: Misconfigured security settings can expose web applications to various attacks, such as directory traversal or remote code execution.
5. **Sensitive Data Exposure**: This happens when web applications fail to protect sensitive data, such as credit card numbers, personal information, or passwords, leading to data breaches.
6. **Cross Site Request Forgery (CSRF)**: CSRF attacks trick users into performing actions they did not intend to, such as changing account details or initiating transactions1.
7. **Insecure Deserialization**: This vulnerability allows attackers to execute arbitrary code or gain unauthorized access by exploiting insecure deserialization processes.
8. **Using Components with Known Vulnerabilities**: Web applications that use outdated or

vulnerable components can be exploited by attackers to gain access to the system.

9. **Broken Access Control**: This occurs when access controls are not properly enforced, allowing attackers to access restricted resources or perform unauthorized actions.
10. **Server-Side Request Forgery (SSRF)**: SSRF vulnerabilities allow attackers to send crafted requests from a vulnerable web application to access internal systems or services.

Preventive Measures

To protect web applications from these vulnerabilities, consider the following preventive measures:

1. **Input Validation and Sanitization**: Validate and sanitize all user inputs to prevent SQL injection and XSS attacks.

2. **Use Prepared Statements**: Use prepared statements and parameterized queries to prevent SQL injection.
3. **Implement Strong Authentication**: Use multifactor authentication and strong password policies to protect against broken authentication.
4. **Regular Security Audits**: Conduct regular security audits and vulnerability assessments to identify and fix security misconfigurations.
5. **Encrypt Sensitive Data**: Encrypt sensitive data both in transit and at rest to prevent data exposure.
6. **Implement CSRF Tokens**: Use CSRF tokens to protect against cross-site request forgery attacks.
7. **Secure Deserialization**: Use secure deserialization libraries and practices to prevent insecure deserialization.
8. **Update Components**: Regularly update and patch all components and libraries to address known vulnerabilities.
9. **Enforce Access Controls**: Implement and enforce strict access controls to prevent broken access control.
10. **Monitor and Log Activities**: Monitor and log web application activities to detect and respond to potential attacks.

By understanding these vulnerabilities and implementing preventive measures, you can significantly enhance the security of your web applications.

Result:

Thus, the different types of vulnerabilities for hacking websites / Web Applications were studied and written successfully.

Ex.No: 5

Date: 26/08/2024

Aim: To analyse the Security Vulnerabilities of E-commerce services and E-Mail Application.

Description:

The security vulnerabilities for both e-commerce services and email applications:

E-commerce Services

1. **Online Payment Fraud**: This includes identity theft, friendly fraud, triangulation, and clean fraud. Attackers often exploit vulnerabilities in payment systems to steal credit card information1.
2. **Misconfigurations of Web Applications**: Poorly configured web applications can expose sensitive data and create entry points for attackers.
3. **Distributed Denial of Service (DDoS) Attacks**: These attacks overwhelm servers with traffic, causing service disruptions.
4. **Bad Bots**: Automated bots can exploit vulnerabilities to scrape data, perform credential stuffing attacks, or carry out other malicious activities.
5. **Customer Journey Hijacking**: Attackers can intercept and manipulate the customer journey, leading to unauthorized transactions or data breaches.
6. **E-skimming**: This involves stealing credit card information from online payment forms.

Email Applications

1. **Phishing**: Deceptive emails trick users into revealing sensitive information or downloading malicious attachments.

2. **Malware**: Malicious software delivered through email attachments or links can compromise system security.
3. **Spoofing**: Attackers forge sender email addresses to deceive recipients into believing emails are from trusted sources.
4. **Data Leaks**: Vulnerabilities may grant unauthorized access to sensitive information, leading to data breaches.
5. **Credential Theft**: Attackers target users' passwords and accounts, which may contain sensitive and valuable information.
6. **Business Email Compromise (BEC)**: Attackers use compromised email accounts to conduct fraudulent activities, often targeting employees with access to financial systems.

Both e-commerce services and email applications face significant security challenges, but implementing robust security measures can help mitigate these risks.

Ex. No: 6 (A)

Date: 02/09/2024

Aim:

To Write a java program to implement Caesar Cipher

Program:

Result:

Thus, the program has been executed successfully

Ex. No: 6 (B)

Date: 16/09/2024

Aim:

To Write a java program to implement Playfair Cipher

Program:

Result:

Thus, the program has been executed successfully

Ex. No: 6 (C)

Date: 23/09/2024

Aim:

To Write a java program to implement Hill Cipher

Program:

Result:

Thus, the program has been executed successfully

Ex. No: 7

Date: 23/09/2024

Aim:

To Write a java program to implement the DES algorithm.

Program:

Result:

Thus, the program has been executed successfully

Ex. No: 8

Date: 30/09/2024

Aim:

To Write a java program to implement the RSA algorithm.

Program:

Result:

Thus, the program has been executed successfully

Ex. No: 9

Date: 14/10/2024

Aim:

To Write a java program to implement the Diffie-Hellman key exchange algorithm.

Program:

Result:

Thus, the program has been executed successfully