The Cybersecurity Cheat Sheet: Essentials Every IT Professional Should Know

KANSAS KEYNOTE

APRIL 25,2025

Jay Ferron

CDPSE, CEH, CHFI, C)PTE, CWSP, CISSP, CRISC, CVEi, MCITP, MCSE, MCT, MVP, NSA-IAM...

blog.mir.net

jay@ferron.com

Common Threats to Digital Security

Malware Threats

Malware consists of harmful software designed to infiltrate and damage systems, making it essential to have strong protection measures.

Phishing Attacks

Phishing attacks deceive users into providing sensitive information by masquerading as trustworthy entities via emails or websites.

Ransomware Risks

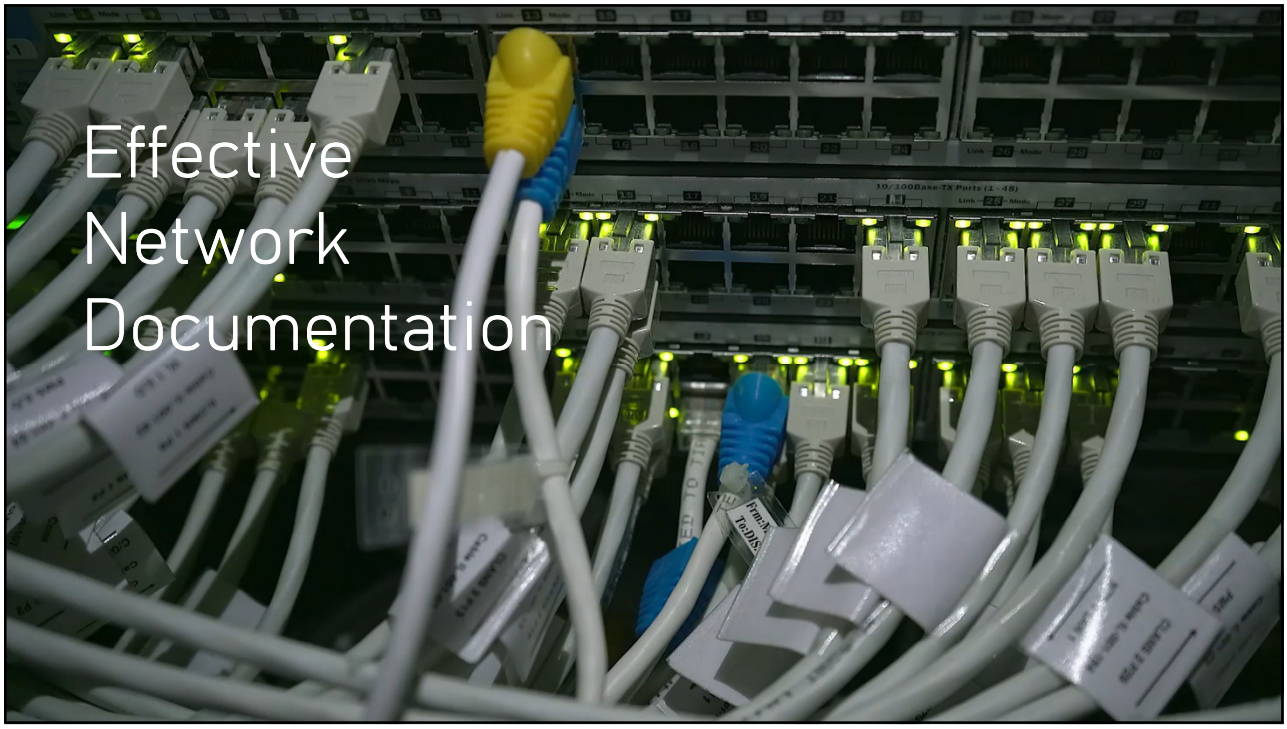
Ransomware is a type of malware that locks users out of their systems until a ransom is paid, posing significant threats to data security.

Unauthorized Access

Unauthorized access refers to individuals gaining access to systems or data without permission, highlighting the importance of robust security measures.

Can you tell me ?

- What computers are on your network ?
- What ports are open ?
- What operating systems are in use ?
- What devices are on your network ?
- What application are running ?
- What is your normal traffic levels ?



Importance of Network Documentation

Overview of IT Environment

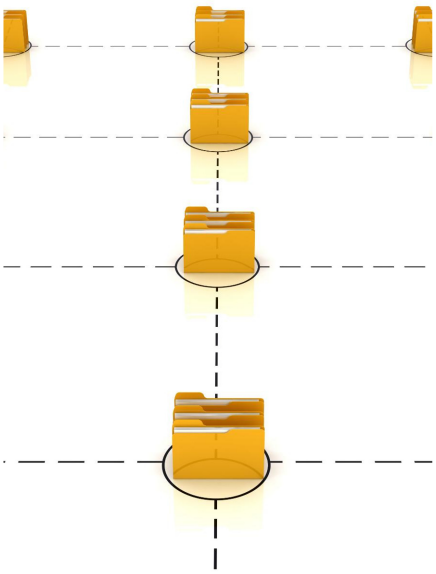
Effective network documentation offers a comprehensive overview of the IT environment, aiding in system management and understanding.

Troubleshooting and Audits

Well-maintained documentation is essential for troubleshooting issues and conducting compliance audits efficiently.

Security Assessments

Network documentation plays a key role in security assessments by providing crucial insights into the network architecture and vulnerabilities.



Tools for Network Mapping and Documentation

Microsoft Visio

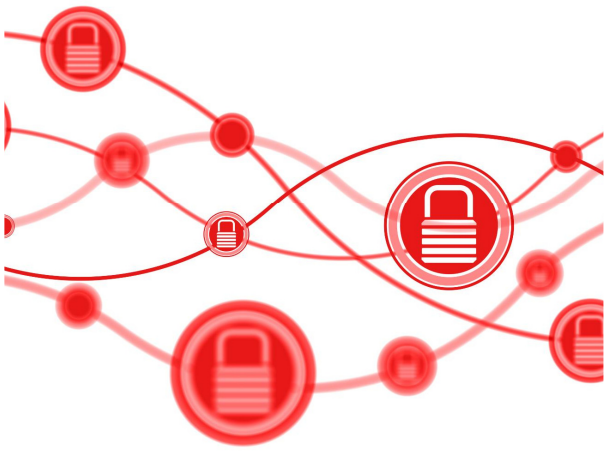
Microsoft Visio is a powerful tool for creating detailed network diagrams, allowing users to visualize complex network structures.

Lucidchart

Lucidchart is a web-based diagramming application that enables easy collaboration for network mapping and documentation.

SolarWinds Network Topology Mapper

SolarWinds Network Topology Mapper automates the creation of network diagrams, ensuring documentation remains current and accurate.



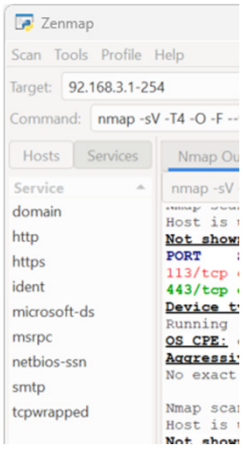
Maintaining and Updating Network Documentation

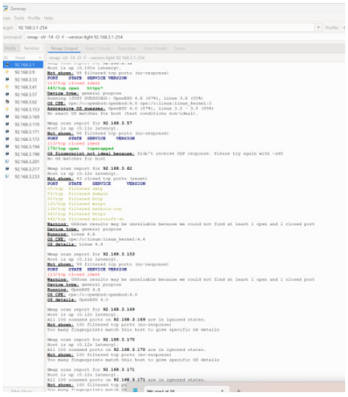
Importance of Regular Updates

Regularly updating network documentation is crucial for maintaining accuracy in IT infrastructure and ensuring operational efficiency.

Routine Review Process

Establishing a routine review process helps ensure that all documentation remains accurate and relevant over time.





NMAP – *Nmap* is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Introduction to Firewall Tools

Function of Firewalls

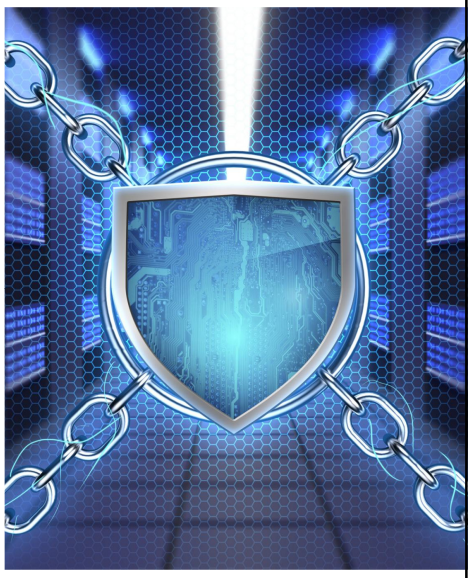
Firewalls serve as barriers between trusted and untrusted networks, controlling the flow of traffic and blocking unauthorized access.

Types of Firewalls

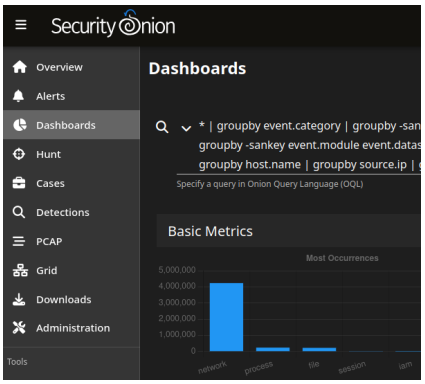
There are various types of firewalls, including hardware and software options, each serving different security needs.

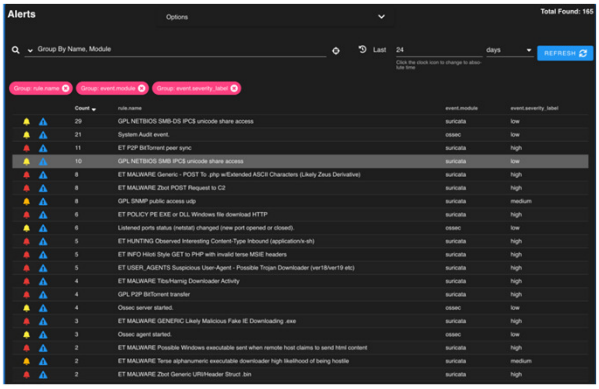
Importance of Firewalls

Understanding firewalls is crucial for network security, as they protect sensitive data from unauthorized access and cyber threats.



Router / Firewall Security Onion (virtual or physical)





Securing Your Network with Public Domain Tools

Enhanced Network Security

Public domain tools enhance your network security by providing additional layers of protection and monitoring capabilities.

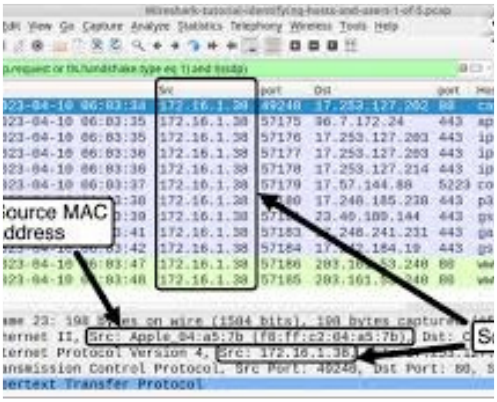
Traffic Monitoring

These tools help in monitoring network traffic for unusual activities that could indicate a security breach.

Preventing Unauthorized Access

Public domain tools play a crucial role in preventing unauthorized access to your network, ensuring data safety.

Network Monitoring – Packet Sniffer



Wireshark is a free and open-source network protocol analyzer, or "packet sniffer," that allows users to capture and analyze network traffic, helping troubleshoot network issues, examine security problems, and understand network protocols

Open-Source Vulnerability Scanners

Cost-Effective Security

Open-source vulnerability scanners allow users to identify network vulnerabilities without incurring costs, making security accessible to everyone.

Powerful Scanning Capabilities

These scanners provide robust functionalities for detecting potential weaknesses in various network environments, enhancing overall security.

Community Support and Development

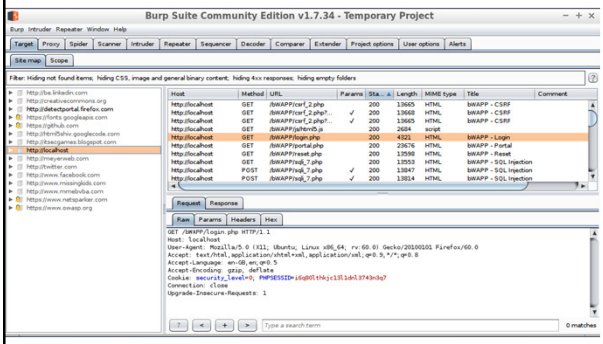
Being open-source, these scanners benefit from continuous community support and development, ensuring they remain effective against evolving threats.

Scanners

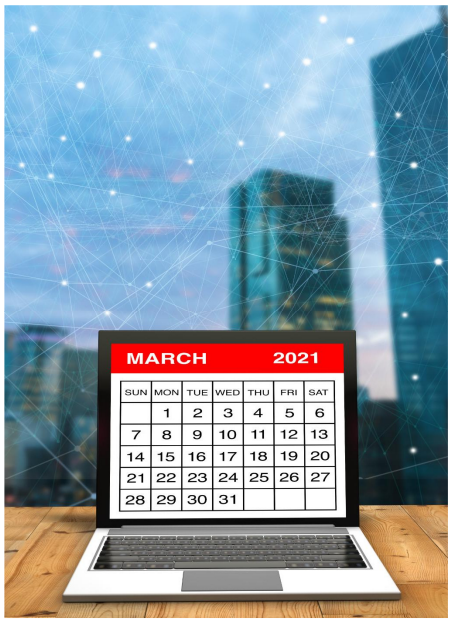
Greenbone – OpenVAS

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.
The scanner obtains the tests for detecting vulnerabilities from a feed that has a long history and daily updates.

Burp Suite



•Burp Suite is a widely used, comprehensive toolkit for web application security testing, offering both manual and automated tools to identify vulnerabilities. It's known for its proxy, history, and vulnerability scanner, and comes in Community Edition (free) and Professional Edition (paid) versions.



Patch Management Techniques

Regular Patch Schedule

Establishing a regular patch management schedule ensures timely updates for software and systems.

Close Vulnerabilities

Timely updates help close vulnerabilities in software, reducing the risk of exploitation.

Protection Against Exploits

Regular patching protects systems against exploits and enhances overall cybersecurity posture.

SNORT

•Snort is a free, open-source network intrusion detection system (IDS) and intrusion prevention system (IPS) that analyzes network traffic for suspicious activity, offering real-time traffic analysis, protocol analysis, and content matching to detect and prevent various attacks.

Implementing Penetration Testing

Regular Testing Schedule

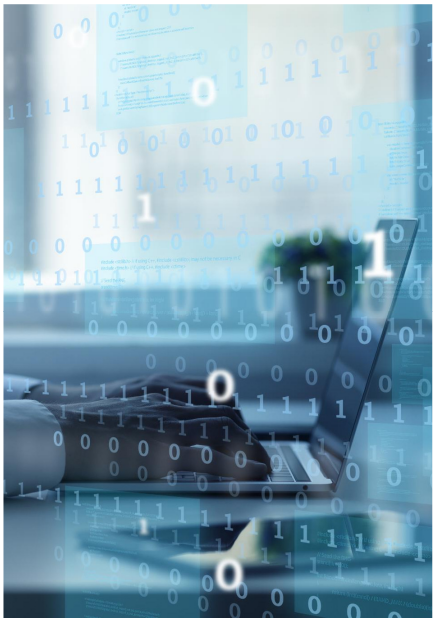
Establish a regular schedule for penetration testing to ensure systems remain secure and vulnerabilities are identified promptly.

Identify System Weaknesses

Penetration testing helps organizations identify weaknesses within their systems, allowing for timely remediation of vulnerabilities.

Proactive Security Measure

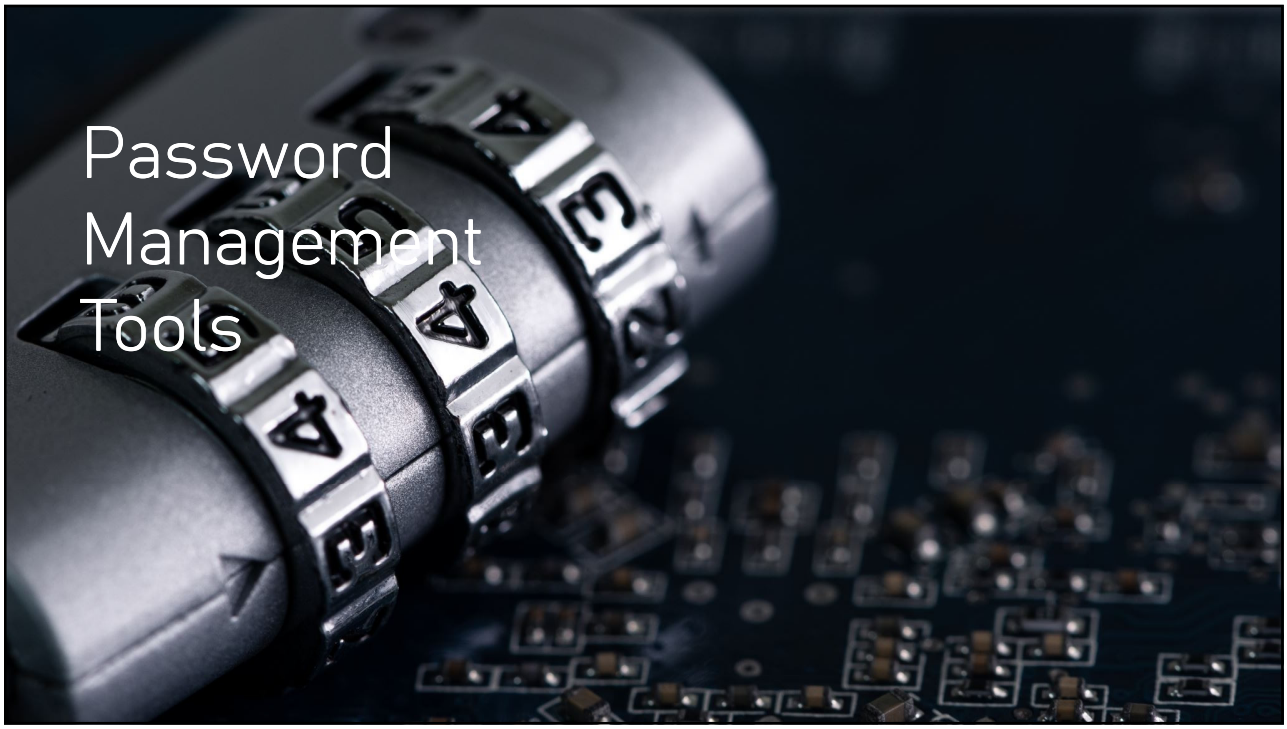
Implementing penetration testing as a proactive measure prevents potential exploitation of vulnerabilities by malicious actors.



Linux Security Tools

Kali Linux

Parrott Linux



Importance of Strong Passwords

First Line of Defense

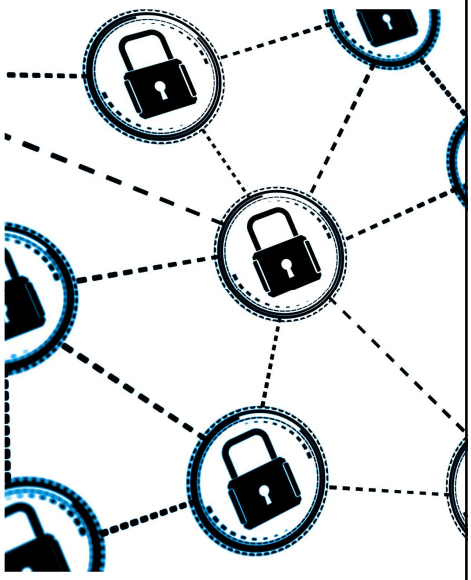
Strong passwords serve as the primary barrier against unauthorized access to personal information and accounts.

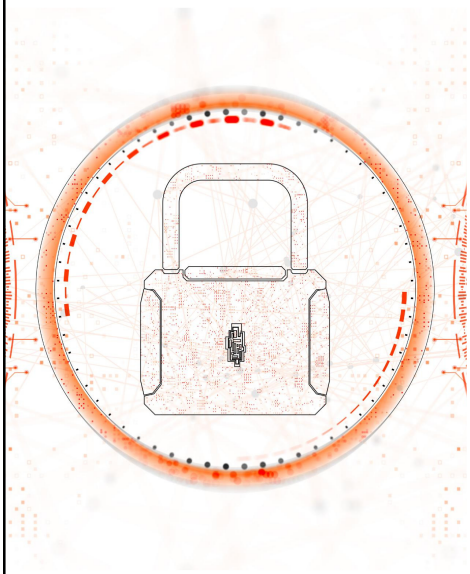
Unique Passwords

Using unique passwords for different accounts reduces the risk of multiple accounts being compromised at once.

Complex Passwords

Complex passwords that mix letters, numbers, and symbols are harder to guess and significantly increase security.





Ensuring Password Security and Management

Regular Password Updates

Regularly updating passwords is essential for maintaining strong security and protecting sensitive information from unauthorized access.

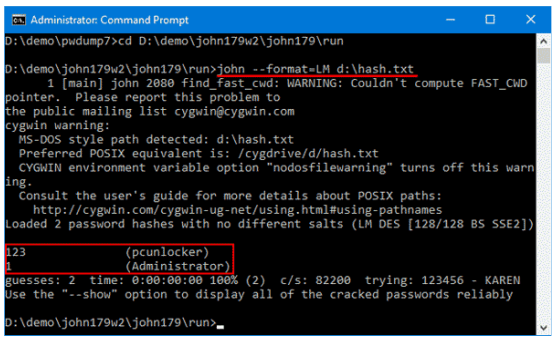
Two-Factor Authentication

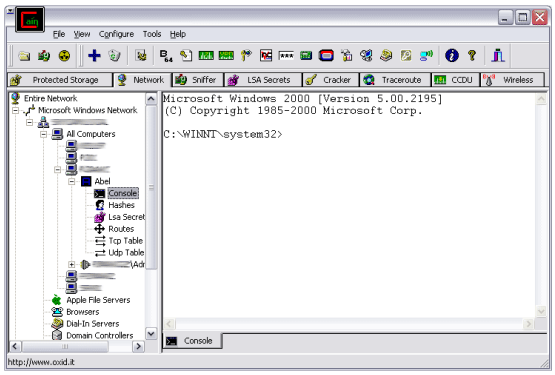
Implementing two-factor authentication adds an extra layer of security, making unauthorized access significantly harder.

Using Password Managers

Password managers simplify password creation and storage, allowing users to generate strong, unique passwords without hassle.

Password Testing Tools





Continuous Improvement and Monitoring

Establishing Processes

It's essential to set up clear processes for the ongoing improvement of security practices. This helps in adapting to new challenges.

Regular Reviews

Conduct regular reviews of existing security strategies to ensure they remain effective against emerging threats.

Learning from Threats

Update security practices based on lessons learned from previous incidents and emerging threat landscapes.

Keeping Software Updated

Importance of Updates

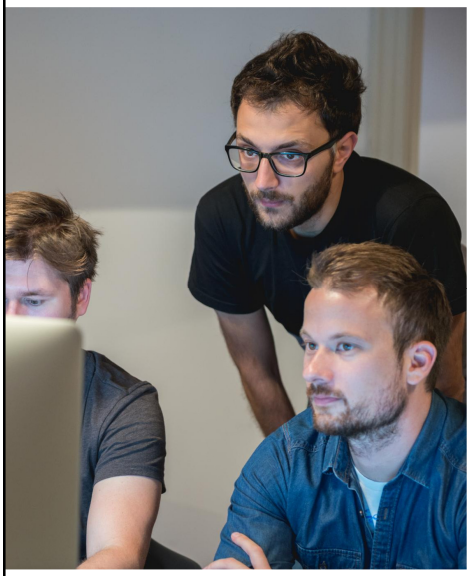
Regular software updates are crucial for maintaining security and functionality, ensuring that systems run smoothly.

Security Patches

Updates often include security patches that address vulnerabilities, protecting users from potential threats and cyber attacks.

Minimizing Cyber Threats

Keeping software updated significantly reduces the risk of cyber threats, ensuring data and privacy are safeguarded.



Educating Users on Cybersecurity

Importance of Cybersecurity Education

Educating users about cybersecurity is essential to protect sensitive information and prevent data breaches.

Recognizing Cyber Threats

Training enables users to identify potential cybersecurity threats, such as phishing and malware attacks, effectively.

Responding to Risks

Ongoing training equips users with the skills to respond promptly and appropriately to cybersecurity incidents.

Definition and Importance of Patch Management

What is Patch Management?

Patch management is the process of managing updates for software and systems to ensure their security and efficiency.

Mitigating Vulnerabilities

Effective patch management helps mitigate vulnerabilities in software, reducing the risk of security breaches.

Enhancing Security

Regularly applying patches is crucial for enhancing overall system security and maintaining a secure environment.

Tools for Automated Patch Management

Streamlining Updates

Automated patch management tools simplify the update process, minimizing manual intervention and reducing the risk of outdated systems.

Security Fixes

These tools ensure that systems remain secure by applying the latest security fixes promptly to safeguard against vulnerabilities.

Examples of Tools

Popular automated patch management tools include Microsoft WSUS and ManageEngine Patch Manager, each offering unique features.

Best Practices for Effective Patch Management

Vulnerability Assessment

Regularly assessing vulnerabilities is critical to identify security gaps and prioritize patching efforts effectively.

Patch Management Schedule

Setting up a patch management schedule ensures timely updates and minimizes the risk of security threats.

Testing Patches

Testing patches before deployment helps to prevent potential disruptions to systems and ensures compatibility.

Accurate Documentation

Maintaining accurate documentation of applied patches is essential for tracking changes and compliance purposes.

Penetration Testing Techniques

Overview of Penetration Testing

Purpose of Penetration Testing

Penetration testing aims to simulate cyber attacks to assess the security of a system effectively.

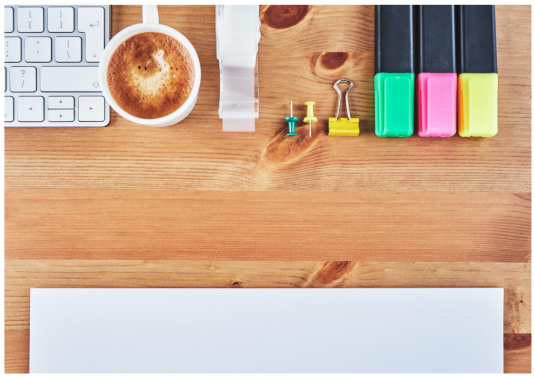
Identifying Vulnerabilities

This process helps organizations uncover vulnerabilities before malicious actors have the opportunity to exploit them.

Security Posture Evaluation

Penetration testing provides a comprehensive evaluation of the organization's security posture against potential threats.

Tools Used for Penetration Testing



Metasploit Framework

Metasploit is a powerful penetration testing tool that allows security professionals to find and exploit vulnerabilities in systems.

Nmap Scanning Tool

Nmap is widely used for network exploration and security auditing, helping identify hosts and services on a network.

Burp Suite for Web Security

Burp Suite is an integrated platform used for testing web application security, providing various tools for attackers and defenders.

Wireshark Packet Analyzer

Wireshark is a network protocol analyzer that enables penetration testers to capture and analyze network packets in real-time.

Steps and Methodologies in Penetration Testing

Planning Phase

The planning phase involves defining the scope and objectives of the penetration test to ensure alignment with business needs.

Scanning Phase

During the scanning phase, tools are used to identify vulnerabilities and gather information about the target system.

Gaining Access

This phase focuses on exploiting identified vulnerabilities to gain unauthorized access to the system.

Maintaining Access

Maintaining access involves ensuring that the tester can return to the system later for further analysis.

Analysis Phase

The analysis phase concludes the process by documenting findings and providing recommendations for remediation.

Forensic Tools

CAINE (Computer Aided INvestigative Environment) is an **Ubuntu-based GNU/Linux live distribution** created as a project of digital forensics.

Understanding Zero Trust Security

Principles of Zero Trust

Never Trust, Always Verify

Zero Trust emphasizes that no user or device should be trusted by default, reinforcing security protocols continuously.

Authentication and Authorization

Every access request must undergo strict authentication and authorization processes to enhance security measures.

Data Encryption

Regardless of the user or device location, all data transactions should be encrypted to protect sensitive information.

Why Traditional Security Models Are Insufficient

Defined Perimeter Vulnerabilities

Traditional security models depend on a defined perimeter, making them vulnerable to modern threats, especially with remote work.

Rise of Remote Work

The expansion of remote work and cloud services has exposed significant gaps in conventional security approaches.

Zero Trust Approach

Zero Trust security removes the assumption that users within the network are trustworthy, enhancing overall security.

Key Components of Zero Trust

Identity and Access Management

This component ensures that proper authentication controls are in place to manage user identities effectively.

Encryption

Encryption protects sensitive data both in transit and at rest, ensuring it remains secure from unauthorized access.

Network Segmentation

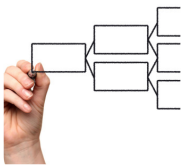
Network segmentation divides the network into smaller, isolated segments to limit unauthorized access and contain breaches.

Continuous Monitoring

Continuous monitoring involves real-time analysis of user activity and network traffic to detect and respond to security threats.

Implementing Conditional Access

Defining Conditional Access Policies



User Roles Specification

Clearly defining user roles is crucial for creating effective conditional access policies. This ensures appropriate access based on responsibilities.

Assessing Risk Levels

Organizations must assess risk levels to tailor access policies appropriately, ensuring that sensitive data is protected.

Compliance Requirements

Incorporating compliance requirements ensures that conditional access policies meet legal and organizational standards for data protection.

Use of Multi-Factor Authentication (MFA)

Enhanced Security Measures

MFA enhances security by requiring multiple forms of verification to access sensitive information.

Password and Smartphone Verification

Combining a password with a smartphone for verification adds an extra layer of security against unauthorized access.

Reduction of Unauthorized Access

The implementation of MFA significantly reduces the risk of unauthorized access to accounts and sensitive data.

Monitoring and Response Based on User Behavior

Importance of User Monitoring

Continuous monitoring of user behavior is essential in a Zero Trust security framework to identify potential threats.

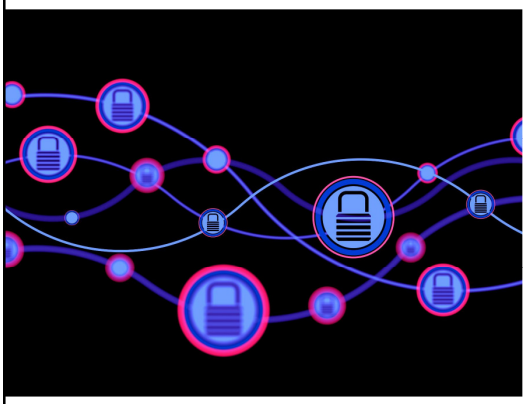
Anomaly Detection

Detecting anomalies in user behavior can trigger alerts and responsive actions, enhancing security measures.

Swift Response Actions

Implementing responsive actions based on detected anomalies helps organizations quickly mitigate potential security breaches.

Setting up Conditional Access Policies



Defining User Roles

Establishing clear user roles is essential for creating effective conditional access policies tailored to different access needs.

Device Type Specifications

Conditional access policies must consider device types to ensure that only secure devices can access sensitive information.

Location-Based Access

Geographical location plays a crucial role in determining access permissions, helping to mitigate risks associated with unauthorized access.

Risk Level Assessment

Evaluating risk levels allows organizations to implement adaptive security measures based on user context and behavior.

Rights Management and Data Protection

Overview of Rights Management

Data Access Control

Rights Management defines who can access specific data, ensuring that only authorized users have the necessary permissions.

Intellectual Property Safeguarding

It is essential for protecting intellectual property rights, preventing unauthorized use or distribution of creative works.

Regulatory Compliance

Rights Management helps organizations comply with legal and regulatory requirements related to data access and usage.

Encrypting Sensitive Data

Importance of Encryption

Encryption protects sensitive data from unauthorized access, ensuring data integrity and confidentiality in organizations.

Data Interception Risks

Without encryption, intercepted data can be easily read by unauthorized users, compromising sensitive information.

Benefits of Encrypting Data

Encrypting data protects against breaches and maintains trust with clients by securing their sensitive information.

Access Control and Permissions Management

Importance of Access Control

Access control is essential for protecting data integrity and preventing unauthorized access to sensitive information.

Least-Privilege Principle

Implementing least-privilege access minimizes exposure of sensitive data by ensuring users have only the permissions necessary for their roles.

Objectives of Using Cybersecurity Tools

Preventing Attacks

Cybersecurity tools are designed to prevent unauthorized access and attacks on systems, ensuring data integrity and safety.

Detecting Vulnerabilities

These tools help identify and assess vulnerabilities within systems, enabling organizations to address weaknesses before they can be exploited.

Responding to Incidents

Effective cybersecurity tools enable swift response to security incidents, minimizing damage and restoring normal operations quickly.

Work toward a Zero Trust design