Question

Answered step-by-step

Jane is a hacker intent on breaking into the XYZ Corporation....

Jane is a hacker intent on breaking into the XYZ Corporation. She...

Jane is a hacker intent on breaking into the XYZ Corporation. She uses a variety of passive reconnaissance techniques and gathers extensive information about the company. Jane finds out what model routers are being used from network administrator questions/comments in user groups. She finds a complete list of the IT staff and their phone numbers from a personnel directory on the company website. She also was able to find out what services are running by using a port scan.
From this scenario, consider the following questions:
1. What reasonable steps could the company have taken to prevent Jane from finding out about company hardware, like router models?
2. What steps should the company take to prevent or at least reduce the efficacy of port scans?

Computer Science | Engineering & Technology | Networking | CIDM 6340

Answer & Explanation

Solved by verified expert

Question 1
Reconnaissance in the Passive Mode
Passive reconnaissance is a method of gathering information about computers and networks without talking with them. The word comes from the military, which conducts passive reconnaissance before starting on a mission to acquire intelligence. Rather of assaulting straight immediately, they gather the knowledge they need to guide their operations.
Passive Reconnaissance Techniques
Wireshark
Any ethical hacker should have this network traffic analysis tool. It allows penetration testers to learn more about the target network. They can listen in on specific traffic and evaluate it by matching IP addresses to their owners and determining the flow's principal goal.
Google
Google can give crucial information about a certain target. Hackers might use it to learn more about a firm. They can look at its employment website and use extensive descriptions of job criteria to locate the systems in their networks. Hackers who know how to use Google Dorking to find files that aren't meant for public consumption may find them.
Shodan
This tool may be used as a search engine for any Internet-connected devices. Because of the widespread use of the Internet of Things (IoT), many businesses and people may unwittingly expose themselves via smart gadgets. Shodan allows hackers to search the Internet for unsecured devices.
The majority of IoT devices simply offer minimal security. Hackers may rapidly discover the networks to which these devices are linked and potentially utilize them as entry points for future assaults.

Stopping an attacker from doing passive reconnaissance successfully
As much code, network information, users, and IPs as possible should be kept secret.
Ensure that the packages in the repository are up to date.
Use lengthy passwords and update them frequently.
Ensure that public-facing code and endpoints are not vulnerable and that some kind of authentication is required.
To protect API and security keys from being exposed to the public, use key vaults or secret managers.

Some protocols are susceptible to sniffing
Sniffing is possible using the following protocols:
HTTP, Telnet, srlogin, sPOP, NNTP, FTP, IMAP and SMTP
Use HTTPS and other secure protocols

Engineers doing passive reconnaissance on their systems to see what they can uncover is the greatest approach to avoid sensitive information from being disclosed. Domains, keys, and IP addresses may all be regenerated and made private if they find something they don't want to be public. Passive reconnaissance is difficult to avoid, but frequent self-reconnaissance can detect possible flaws and repair

them before they become major issues.

Other methods may include:

Networks and functions should be segmented and segmented.

The complete infrastructure layout, including segmentation and isolation, must be considered by security architects. An important security strategy for preventing an adversary from distributing exploits or moving laterally throughout an internal network is proper network segmentation. Intruders might use a poorly segmented network to take control of vital equipment or obtain access to sensitive data and intellectual property. Segregation divides network segments into groups depending on their roles and functions. Malicious events can be contained in a securely segmented network, decreasing the effect of intruders if they get a foothold.

Separation of Sensitive Information on a Physical Level

Local Area Network segments can be separated using traditional network equipment such as routers. Organizations can utilize routers to define boundaries across networks, expand the number of broadcast domains, and filter users' broadcast data effectively. These boundaries can be used to contain security breaches by confining traffic to distinct segments and even shutting down portions of the network during an incursion, limiting adversary access.

Sensitive Data is Virtually Separated

As technology advances, new solutions for improving information technology efficiency and network security measures are developed. The logical isolation of networks on the same physical network is known as virtual separation. Virtual segmentation employs the same design ideas as physical segmentation but does not necessitate the purchase of extra hardware. Existing technology can be utilized to keep an intruder from breaking into other parts of the internal network.

Reduce the number of unnecessary lateral communications.

Allowing unfiltered peer-to-peer connections, including workstation-to-workstation interactions, exposes major vulnerabilities and makes it easy for a network intruder to propagate their access to other computers. Unfiltered lateral communications allow an intruder to construct backdoors throughout the network after they have established an effective beachhead within the network. Backdoors aid attacker persistence within the network while hindering defenders' attempts to confine and eliminate the intruder.

Network Devices Should Be Hardened

Protecting networking devices using secure settings is a key technique to improve network infrastructure security. Administrators may get advice from government agencies, organizations, and manufacturers on how to harden network equipment, including benchmarks and best practices. The following ideas should be implemented in combination with laws, regulations, site security policies, standards, and industry best practices by administrators.

Infrastructure Devices with Secure Access

Users can be granted administrative rights to get access to resources that aren't broadly available. Because hackers might use administrative rights that are wrongly allowed, provided broadly, or not rigorously checked, limiting administrative privileges for infrastructure devices is critical to security. Adversaries can traverse a network, increase access, and seize complete control of the infrastructure backbone using compromised privileges. Implementing safe access policies and processes can help organizations prevent unwanted infrastructure access.

Question 2

How to reduce the efficacy of port scans

Scanning Attacks on Ports

Hackers can find any weaknesses by scanning the ports of a machine. The hacker writes a software that delivers a single message to each of the ports at a time. They can figure out what you're doing with the port this way.

The best defense, as is frequently the case with computer security, is a solid offense. Your network system will be subject to port scans as long as you have a publicly accessible server. However, there are a few things you may do to mitigate your flaws:
Install a Firewall: A firewall can help protect your private network from unauthorized access. It is in charge of the exposed ports and their visibility. A port scan in process can potentially be detected and stopped down by firewalls.
TCP Wrappers: Administrators can use TCP wrappers to allow or refuse access to servers based on IP addresses or domain names.
Find Network Holes: Run your own internal port check to see if there are any ports open that aren't needed. Check your system on a regular basis to see if there are any current vulnerabilities that might be exploited.

Step-by-step explanation

references
https://docs.rackspace.com/blog/packet-sniffers-and-how-you-protect-yourself/
https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0204507

Is this answer helpful? Helpful Unhelpful

Report this answer

Add to library

Related Answered Questions

Q: QUESTION 2 The Malaysian Private Entities Reporting Standards (MPERS) issued by Malaysian Accounting Standards Board (MA

Q: ACCOUNTING PERIOD 1/7/2020 - 30/6/2021. Silver Tech Bhd is a local manufacturing company specialising in computer and te

Q: 1. Below are details on building as at 1 July 2020: Particular Revalued amount (RM)

Q: Tax income rate is 24% Explain accounting treatment and determine journal entry(show calculation). QUESTION 1 Silver T

Q: In this case study, we will consider a network administrator for a small, family-oriented video store. The store is not

See more

Can't find your question?

Ask a new question

We have related textbook solutions for you!

This textbook contains questions and solutions related to the question you are viewing.

Chapter 2 / Exercise 01

Management of Information Security

Mattord/Whitman

Expert Verified

View Solutions

Browse all Textbook Solutions

Related Course Resources

CIDM 6305

West Texas A&M University

268 Documents

142 Question & Answers

DEV 102

Bucharest Academy of Econ...

158 Documents

We