Exam Report: 4.2.10 Practice Questions

Date: 5/2/2020 5:16:42 pm
Time Spent: 7:48

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 60%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following services is most targeted during the reconnaissance phase of a hacking attack?

- DHCP
- DoS
- DNS
- TLS

Explanation

The DNS service is one of the most popular internet services targeted during the reconnaissance phase.

The DHCP service is usually attacked during the gaining access stage.

TLS is a cryptographic protocol, not a service targeted during the reconnaissance phase of a hacking attack.

DoS, or denial-of-service, is a type of attack that prevents legitimate users from accessing computer systems, not a service targeted during the reconnaissance phase of an attack.

References

TestOut Ethical Hacker Pro - 4.2 Reconnaissance Countermeasures
[e_reconcounter_eh1.exam.xml Q_RECON_COUNTERMEASURES_DNS_01_EH1]

Question 2: Correct

Dan wants to implement reconnaissance countermeasures to help protect his DNS service. Which of the following actions should he take?

- Install patches against known vulnerabilities and clean up out-of-date zones, files, users, and groups.
- Limit the sharing of critical information in press releases, annual reports, product catalogs, or marketing materials.
- Review company websites to see what type of sensitive information is being shared.
- Implement policies that restrict the sharing of sensitive company information on employees' personal social media pages.

Explanation

Installing patches against known vulnerabilities and cleaning up out-of-date zones, files, users, and groups are good DNS reconnaissance countermeasures.

Reviewing company websites to see what type of information is being shared about sensitive information is conforming to an internet information sharing policy.

Implementing policies that restrict the sharing of sensitive company information on employees' personal social media pages is conforming to an employee social media information sharing policy.
Limiting the sharing of critical information in press releases, annual reports, product catalogs, and marketing materials is conforming to a printed materials information sharing policy.

References

TestOut Ethical Hacker Pro - 4.2 Reconnaissance Countermeasures
[e_reconcounter_eh1.exam.xml Q_RECON_COUNTERMEASURES_DNS_02_EH1]

Question 3: Incorrect

Julie configures two DNS servers, one internal and one external, with authoritative zones for the corpnet.xyz domain. One DNS server directs external clients to an external server. The other DNS server directs internal clients to an internal server. Which of the following DNS countermeasures is she implementing?

- Split DNS
- Proxy server
- Information sharing policy
- ~~DNS propagation~~

Explanation

A split DNS is implemented with two DNS servers configured to be authoritative for the same domain, one on the external network and one on the internal network.

A proxy server is an intermediary server that separates end users from the websites they browse and is not a DNS countermeasure.

A DNS propagation is a process used by DNS servers when a DNS record changes and is not a DNS countermeasure.

An information sharing policy is a reconnaissance countermeasure but is not a DNS countermeasure.

References

TestOut Ethical Hacker Pro - 4.2 Reconnaissance Countermeasures
[e_reconcounter_eh1.exam.xml Q_RECON_COUNTERMEASURES_DNS_03_EH1]

Question 4: Incorrect

Which of the following information sharing policies addresses the sharing of critical information in press releases, annual reports, product catalogs, and marketing materials?

- ~~A company social media policy~~
- An internet policy
- An employee social media policy
- A printed materials policy

Explanation

A printed material information sharing policy would limit the sharing of critical information in press releases, annual reports, product catalogs, and marketing materials.

An internet information sharing policy would require a review of company websites to see what type of information is being shared about sensitive information.

A company social media information sharing policy would provide guidelines regarding the types of posts that are made to the company's social media site.

An employee social media information sharing policy would restrict the sharing of sensitive company information on an employee's personal social media page. This could include product information, customer or vendor information, employee information, or even pictures of the organization.

References

TestOut Ethical Hacker Pro - 4.2 Reconnaissance Countermeasures
[e_reconcounter_eh1.exam.xml Q_RECON_COUNTERMEASURES_INFO_SHARING_01_EH1]

Question 5: Correct

John, a security specialist, conducted a review of the company's website. He discovered that sensitive company information was publicly available. Which of the following information sharing policies did he discover were being violated?

- A company social media policy
- A printed materials policy
- An employee social media policy
- An internet policy

Explanation

An internet information sharing policy would require a review of company websites to see what type of information is being shared about sensitive information.

A company's social media information sharing policy would provide guidelines regarding the types of posts that are made to the company's social media site.

An employee's social media information sharing policy would restrict the sharing of sensitive company information on an employee's personal social media page. This could include product information, customer or vendor information, employee information, or even pictures of the organization.

A printed material information sharing policy would limit the sharing of critical information in press releases, annual reports, product catalogs, or marketing materials.

References

TestOut Ethical Hacker Pro - 4.2 Reconnaissance Countermeasures
[e_reconcounter_eh1.exam.xml Q_RECON_COUNTERMEASURES_INFO_SHARING_02_EH1]