Fill the blank report samples

Business, Company

- What search string would you use with Google to locate a Web server that was offering up a directory listing of the /etc directory, including the passwd file

Web server + directory listing + etc directory + password file

- You are analyzing network traffic and you see the string dXNlcjpwYXNzd29yZA== in a Web request where the client is authenticating with the server. The username from this request is and the password is

- Before you embark on a penetration test, what is the very first thing you want to get?

The very first thing to get before embarking on a penetration test would be information. This could be organization name, structure or systems which will be useful depending on whether the penetration is black box or white box testing.

- What type of scan are you running if you use the following? nmap -sS 192. 168. 0. 0/24

The command runs a scan command on multiple IP addresses or subnet on IPv4.

- What tool would you use to get passwords on a voice over IP network?

- You find the following in Web logs.

POST /scripts/postit. php? p=%3Cscript%3Ealert(document. cookie())%3C %2Fscript%3E

What is going on?

This is a response from a web server to a query from a user’s browser.

Short essay answer:

- Is a vulnerability scanner completely accurate and reliable? Why or why not?

A vulnerability scanner assesses security vulnerabilities across information systems such as networks, host systems, operating systems and other software applications and produces a set of scan results. It may not be accurate but is reliable. A vulnerability scanner helps detect weaknesses depending on the type of system being monitored. It helps identify rogue machines which might jeopardize the whole system or network security. It also helps retain relevant information on devices on a network such as operating systems, patches and configurations and to detect any form of alteration which could be threatening.

The downside of vulnerability systems is that they only give a snapshot at any given time and therefore continuous monitoring must be exercised to get the most out of these systems. They also require human decision in analyzing the data after scanning to determine the response. As such, vulnerability scanners may not be as accurate as we would want them to be, but they are indeed reliable.

- You see someone using the command " nc www. google. com 80". What is it they are trying to do?

The nc or netcat is a network utility used for creating and investigations TCP and UDP connections in a network. It is sometimes used to connect to servers through command rather than through a graphical user interface. This helps to troubleshoot when to verify data sent by a server in response to user commands. The nc can be used to test HTTP connection to a website’s homepage. For instance, if a user types the command “ nc www. google.

com 80”, he is basically trying to retrieve the homepage of Google website.

- Explain clearly, in your own words, what a buffer overflow is.

A buffer overflow is a flaw in computer security whereby a program tends to store more data in a temporary storage known as buffer. Buffers are created to hold a certain amount of data. The excess data spills over to adjacent memory overwriting the original genuine data. Buffer overflow may be accidental due to program errors or could be a security attack by hackers on data integrity. The extra data may contain programs that corrupt user’s files, modify existing data or even gain access to highly classified information.

- You are periodically running vulnerability scans on your Web server. One day it indicates to you that Firefox has a security vulnerability that could allow for a privilege escalation. How concerned are you about this finding? Include your reasoning.

Security vulnerability is a likely indicator of a web-based threat. One would most likely be concerned about cyber-crime in this type of threat. These browser-based threats are devised to infect machines whose users are connected to the internet. This is because deceitful websites that pose as genuine sites can gather personal information like credit cards and social security numbers for identity theft. The do this by spreading concealed spyware and viruses on client machines. The web browsers should therefore be secured.

Multiple choices

- Which of the following technologies are CLIENT side?

JavaScript

HTML

HTTP

PHP

Flash

Perl

- Which of the following technologies are SERVER side?

Java script

HTTP

PHP

Ruby

HTML

References

Siever, Ellen, and Jessica Perry Hekman. Linux in a nutshell, a desktop quick reference. 2nd ed. Beijing: O'Reilly, 1999. Print.

Russell, Deborah, and G. T. Gangemi. Computer security basics. [Rev. ed. Sebastopol, CA: O'Reilly & Associates, 1991. Print.