19: Assisted Lab: Analyzing Exploit Code

PenTest+ (Exam PT0-002)

10/10

Congratulations, you passed!

Duration: 11 minutes, 4 seconds

☑ What is the CVE number for this vulnerability? *Score: 1*

CVE-2011-2523

Correct

☑ When was this CVE published? *Score: 1*

● 11/27/2019
○ 11/27/2011
○ 11/27/2021
○ 11/27/2013

Correct

☑ What is the severity base score (number only) does this vulnerability have? *Score: 1*

9.8

Correct

☑ What language was the exploit script written in? *Score: 1*

● Python
○ Bash
○ Ruby
○ Perl

Correct

☑ What libraries are being imported into this script? *Score: 1*

○ Telnet
○ argparse

○ signal, SIGINT
○ exit
● All of the above

Correct

☑ What value does the variable named user hold? (Hint: Type it in exactly as shown including quotation marks) *Score: 1*

"USER nergal:)"

Correct

☑ Which of the following folder is NOT listed in the modules directory from the last command? *Score: 1*

○ auxiliary
○ exploits
○ payloads
● scripts
○ All of the above
○ None of the above

Correct

☑ Which organization represents the standards for Cyber security and related topics? *Score: 1*

○ NASA
○ NSA
○ /usr/share/
● NIST

Correct

☑ Which organizations were not part of the original RFC? *Score: 1*

□ NIST
□ Exploit DN
□ NASA
☑ All of the above
□ None of the above

Correct

☑ Which of the sites used in this lab directly provides code samples for vulnerabilities? *Score: 1*

○ nist.gov
● exploit-db.com
○ Both of them

○ Neither of them

Correct

☑ What is the port number for the backdoor port once you have attempted to login using the ':)' characters? *Score: 0*

○ 6100
● 6200
○ 6300
○ All of the above
○ None of the above

You are correct!