Vendor:EC-COUNCIL

Exam Code:312-50V12

Exam Name: Certified Ethical Hacker Exam (CEHv12)

Version: Demo

QUESTION 1

Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

A. msfpayload

B. msfcli

C. msfd

D. msfencode

Correct Answer: D

https://www.offensive-security.com/metasploit-unleashed/msfencode/ One of the best ways to avoid being stopped by antivirus software is to encode our payload with msfencode. Msfencode is a useful tool that alters the code in an executable so that it looks different to antivirus software but will still run the same way. Much as the binary attachment in email is encoded in Base64, msfencode encodes the original executable in a new binary. Then, when the executable is run, msfencode decodes the original code into memory and exe-cutes it.

QUESTION 2

A. Compound SQLi

B. Blind SQLi

C. Classic SQLi

D. DMS-specific SQLi

Correct Answer: B

https://en.wikipedia.org/wiki/SQL_injection#Blind_SQL_injection Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack has traditionally been considered time-intensive because a new statement needed to be crafted for each bit recovered, and depending on its structure, the attack may consist of many unsuccessful requests. Recent advancements have allowed each request to recover multiple bits, with no unsuccessful requests, allowing for more consistent and efficient extraction.

QUESTION 3

Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus

B. Multipart virus

C. Macro virus

D. Stealth virus

Correct Answer: C

A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread. (Wikipedia) NB: The virus Melissa is a well-known macro virus we could find attached to word documents.

QUESTION 4

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.

What command is used to determine if the entry is present in DNS cache?

A. nslookup -fullrecursive update.antivirus.com

B. dnsnooping -rt update.antivirus.com

C. nslookup -norecursive update.antivirus.com

D. dns --snoop update.antivirus.com

Correct Answer: C

QUESTION 5

Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

A. Presentation tier

B. Application Layer

C. Logic tier

D. Data tier

Correct Answer: C

QUESTION 6

Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open pons and running services on systems connected to the organization\\'s OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

A. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p

B. nmap -Pn -sU -p 44818 --script enip-info

C. nmap -Pn -sT -p 46824

D. nmap -Pn -sT -p 102 --script s7-info

Correct Answer: B

https://nmap.org/nsedoc/scripts/enip-info.html Example Usage enip-info:

-nmap --script enip-info -sU -p 44818

This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command

that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.

This script was written based of information collected by using the the Wireshark dissector for CIP, and EtherNet/IP, The original information was collected by running a modified version of the ethernetip.py script (https://github.com/

paperwork/pyenip)

QUESTION 7

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

A. Data items and vulnerability scanning

B. Interviewing employees and network engineers

C. Reviewing the firewalls configuration

D. Source code review

Correct Answer: A

QUESTION 8

Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time Information.

Which of the following techniques is employed by Susan?

A. web shells

B. Webhooks

C. REST API

D. SOAP API

Correct Answer: B

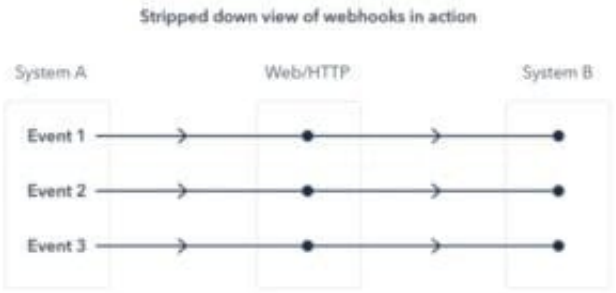
Webhooks are one of a few ways internet applications will communicate with one another.

It allows you to send real-time data from one application to another whenever a given event happens.

For example, let\\'s say you\\'ve created an application using the Foursquare API that tracks when people check into your restaurant. You ideally wish to be able to greet customers by name and provide a complimentary drink when they check

in. What a webhook will is notify you any time someone checks in, therefore you\\'d be able to run any processes that you simply had in your application once this event is triggered. The data is then sent over the web from the application

wherever the event originally occurred, to the receiving application that handles the data.



Here\\'s a visual representation of what that looks like:

A webhook url is provided by the receiving application, and acts as a phone number that the other application will call once an event happens. Only it\\'s more complicated than a phone number, because data about the event is shipped

Here\\'s an example of what a webhook url looks like with the payload it\\'s carrying:

What are Webhooks? Webhooks are user-defined HTTP callback or push APIs that are raised based on events triggered, such as comment received on a post and pushing code to the registry. A webhook allows an application to update other applications with the latest information. Once invoked, it supplies data to the other applications, which means that users instantly receive real-time information. Webhooks are sometimes called "Reverse APIs" as they provide what is required for API specification, and the developer should create an API to use a webhook. A webhook is an API concept that is also used to send text messages and notifications to mobile numbers or email addresses from an application when a specific event is triggered. For instance, if you search for something in the online store and the required item is out of stock, you click on the "Notify me" bar to get an alert from the application when that item is available for purchase. These notifications from the applications are usually sent through webhooks.

QUESTION 9

Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?

A. Rootkit

B. Trojan

C. Worm

D. Adware

Correct Answer: C

QUESTION 10

Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

A. Take over the session

B. Reverse sequence prediction

C. Guess the sequence numbers

D. Take one of the parties offline

Correct Answer: C

QUESTION 11

Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility. Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?

A. wash

B. ntptrace

C. macof

D. net View

Correct Answer: A

QUESTION 12

Which of the following is an extremely common IDS evasion technique in the web world?

A. Spyware

B. Subnetting

C. Unicode Characters

D. Port Knocking

Correct Answer: C