Stats: 0:02:24 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 75.00% done; ETC: 21:53 (0:00:00 remaining)

Nmap scan report for owasp-juice.shop (81.169.145.156)

Host is up (0.031s latency).

Other addresses for owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::

rDNS record for 81.169.145.156: w9c.rzone.de

PORT STATE SERVICE VERSION

80/tcp open http BigIP

443/tcp open ssl/http Apache httpd 2.4.63 ((Unix))

3000/tcp closed ppp

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port80-TCP:V=7.94SVN%I=7%D=5/7%Time=681BD5BF%P=aarch64-unknown-linux-gn

SF:u%r(GetRequest,218,"HTTP/1\.1\x20302\x20Found\r\nLocation:\x20http://wi

SF:red\.meraki\.com:8090/blocked\.cgi\?blocked_server=81\.169\.145\.156:80

SF:&blocked_url=http%3A%2F%2F81\.169\.145\.156%2F&blocked_categories=bs_02

SF:2\r\nContent-Type:\x20text/html\r\nContent-Length:\x20217\r\nCache-Cont

SF:rol:\x20no-cache\r\nContent-Type:\x20text/html\r\nPragma:\x20no-cache\r

SF:\nExpires:\x200\r\nContinue:\x20close\r\n\r\n<html><body>You\x20are\x20

SF:being\x20<a\x20href='http://wired\.meraki\.com:8090/blocked\.cgi\?block

SF:ed_server=81\.169\.145\.156:80&blocked_url=http%3A%2F%2F81\.169\.14

SF:5\.156%2F&blocked_categories=bs_022'>redirected\.</body></html>

SF:\n")%r(HTTPOptions,218,"HTTP/1\.1\x20302\x20Found\r\nLocation:\x20http:

SF://wired\.meraki\.com:8090/blocked\.cgi\?blocked_server=81\.169\.145\.15

SF:6:80&blocked_url=http%3A%2F%2F81\.169\.145\.156%2F&blocked_categories=b

SF:s_022\r\nContent-Type:\x20text/html\r\nContent-Length:\x20217\r\nCache-

SF:Control:\x20no-cache\r\nContent-Type:\x20text/html\r\nPragma:\x20no-cac

SF:he\r\nExpires:\x200\r\nContinue:\x20close\r\n\r\n<html><body>You\x20are

SF:\x20being\x20<a\x20href='http://wired\.meraki\.com:8090/blocked\.cgi\?b

SF:locked_server=81\.169\.145\.156:80&blocked_url=http%3A%2F%2F81\.169

SF:\.145\.156%2F&blocked_categories=bs_022'>redirected\.</body></h

SF:tml>\n")%r(RTSPRequest,6A,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nServer

SF::\x20BigIP\r\nConnection:\x20close\r\nContent-Length:\x2024\r\n\r\nHTTP

SF:/1\.1\x20400\x20Bad\x20Request")%r(FourOhFourRequest,272,"HTTP/1\.1\x20

SF:302\x20Found\r\nLocation:\x20http://wired\.meraki\.com:8090/blocked\.cg

SF:i\?blocked_server=81\.169\.145\.156:80&blocked_url=http%3A%2F%2F81\.169

SF:\.145\.156%2Fnice%2520ports%252C%2FTri%256Eity\.txt%252ebak&blocked_cat

SF:egories=bs_022\r\nContent-Type:\x20text/html\r\nContent-Length:\x20262\

SF:r\nCache-Control:\x20no-cache\r\nContent-Type:\x20text/html\r\nPragma:\

SF:x20no-cache\r\nExpires:\x200\r\nContinue:\x20close\r\n\r\n<html><body>Y

SF:ou\x20are\x20being\x20<a\x20href='http://wired\.meraki\.com:8090/blocke

SF:d\.cgi\?blocked_server=81\.169\.145\.156:80&blocked_url=http%3A%2F%

SF:2F81\.169\.145\.156%2Fnice%2520ports%252C%2FTri%256Eity\.txt%252ebak&am

SF:p;blocked_categories=bs_022'>redirected\.</body></html>\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 144.46 seconds

┌──[root@parrot]─[/home/user]

└──╼ #

┌──[root@parrot]─[/home/user]

└──╼ #

create a detailed report hitting all of this requirements Criteria Grading Scale

Environment Setup & Tools

The project must demonstrate successful installation and configuration of Parrot OS in VirtualBox with evidence of proper network configuration. Essential ethical hacking tools including Nmap, Wireshark, and Metasploit must be installed and configured with demonstrated functionality. Documentation must include screenshots of tool configurations, network settings, and successful test executions. A secure lab environment must be established with proper isolation. All configurations must include proper documentation and evidence of functionality testing.

1

Complete

0

Incomplete

Information Gathering & Reconnaissance

The project must include execution of passive reconnaissance using OSINT tools with documented methodologies and findings. Network mapping using Nmap must be performed with evidence of proper scan configurations and results analysis. Domain information gathering using theHarvester must be conducted with comprehensive output documentation. A detailed target profile must be created using the standard template with all discovered information properly categorized and analyzed. All reconnaissance activities must be conducted within ethical boundaries with proper documentation

1

Complete

0

Incomplete

Scanning & Enumeration

The project must demonstrate port scanning using multiple Nmap techniques including TCP, UDP, and service scanning with proper scan configurations documented. Service enumeration must be performed on identified services with detailed output analysis. Vulnerability scanning using Nessus Essentials must be executed with proper scope and configuration. All findings must be documented with evidence including scan configurations, raw output, and analysis of results. Documentation must include false positive analysis and verification steps.

1

Complete

0

Incomplete

Vulnerability Analysis

The project must demonstrate the use of 1 port scanning tool and 1 network service enumeration method to identify active services on a system. A vulnerability scan report must be included, documenting at least 3 identified vulnerabilities and an analysis of their risk levels, potential impact, and recommended mitigation strategies.

1

Complete

0

Incomplete

Basic Exploitation

The project must demonstrate basic exploitation skills in a controlled lab environment using Metasploit Framework with proper target verification and scope definition. Exploitation process must be documented step-by-step including tool configurations, execution steps, and results. All activities must follow safety guidelines and ethical considerations with proper documentation. Evidence of proper lab containment and clean-up procedures must be included. A comprehensive report detailing the exploitation process must be provided.

1

Complete

0

Incomplete

Web Application Testing

The project must include basic web application scanning using appropriate tools such as OWASP ZAP and Burp Suite Community Edition with proper scope and configuration. Common web vulnerabilities must be identified and documented following OWASP guidelines. Testing methodology must be documented including tool configurations, test cases, and results. A detailed web application testing report must be created including findings, evidence, and remediation recommendations. All testing must be conducted within defined boundaries with proper documentation.