Pentest Quiz Writeup

[Task 1] Getting better at doing "Google Searches"

Getting better at using "Search Engines" in order to find the right answers in less time is an art. This room is all about quick challenges which most of the n00bs like me already have in mind and don't really require a "Google Search" but for some of the n00bs it is still remained to be learnt!

So these little challenges will be helping you a lot! Have fun!

~/w4tchd0g

#1 Famous port scanner. Can you name it?

nmap

#2 Famous network packet analyzer. Can you name it?

wireshark

#3 Best place to find public exploits?

exploit-db

#4 Best place to find google dorks?

GHDB

#5 Entering enough data to make the application crash!

buffer overflow

#6 I am a security bug but not known to anyone yet?

0day

#7 "Your system has been locked, Pay me the money!"

ransomware

#8 Group of compromised machines connected to a C&C server!

botnet

#9 Name the organization that releases TOP 10 Web and Mobile vulnerabilities?

owasp

#10 Name the famous worm which targeted SCADA environments?

stuxnet

#11 Art of hiding information in other files!

steganography

#12 Converting readable data into unreadable format!

encryption

#13 Name the tool used for reading metadata of images!

exiftool

#14 Famous Web Application Proxy Tool?

burp suite

#15 NSA Reverse Engineering Tool?

ghidra

#16 Famous Open Source Web Application Proxy Tool?

owasp zap