


TRY HACK ME


Shan246 [0x6]FR

[Get Profile Badge ID](#) [Share Room Badges](#)


[Rooms Complete](#) [Badges](#) [Created Rooms](#) [Yearly Activity](#) [Tickets](#)




Windows Forensi...
Introduction to Windows
Registry Forensics



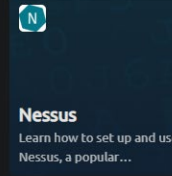
Windows...
In part 1 of the Windows
Fundamentals module, w...




OpenVAS
Learn the basics of threat
and vulnerability...




Yara
Learn the applications and
language that is Yara for...



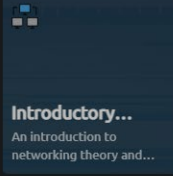
Nessus
Learn how to set up and use
Nessus, a popular...



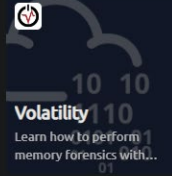
Tutorial 110
Learn how to use a
TryHackMe room to start...



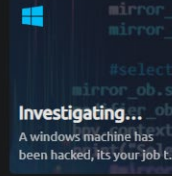
Attacktive...
99% of Corporate networks
run off of AD. But can you...



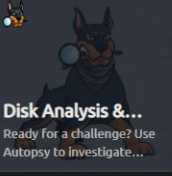
Introductory...
An introduction to
networking theory and...




Volatility 110
Learn how to perform
memory forensics with...




Investigating...
A windows machine has
been hacked, its your job E...



Disk Analysis &...
Ready for a challenge? Use
Autopsy to investigate...



MAL: Malware...
The start of a series of
rooms covering Malware...



Basic Malware RE
This room aims towards
helping everyone learn...

Contents

CYBER DEFENCE	3
CYBER DEFENSE INTRODUCTION	3
Introductory Networking	3
Windows Fundamentals 1	7
THREAT AND VULNERABILITY MANAGEMENT	9
NESSUS	9
YARA	11
OpenVAS	13
THREAT EMULATION	14
Attacktive Directory	14
INCIDENT RESPONSE AND FORENSICS	17
Investigating Windows	17
Windows Forensics 1	18
MALWARE ANALYSIS	21
MAL: Malware Introductory	21
Basic Malware RE	24

CYBER DEFENCE

CYBER DEFENSE INTRODUCTION

Introductory Networking

9059 **Introductory Networking** An introduction to networking theory and basic networking tools [Start AttackBox](#) [Help](#)

100%

- Task 1 Introduction
- Task 2 The OSI Model: An Overview
- Task 3 Encapsulation
- Task 4 The TCP/IP Model
- Task 5 **Networking Tools** Ping
- Task 6 **Networking Tools** Traceroute
- Task 7 **Networking Tools** WHOIS
- Task 8 **Networking Tools** Dig
- Task 9 Further Reading

TASK 2:

Answer the questions below

Which layer would choose to send data over TCP or UDP?

4 [Correct Answer](#)

Which layer checks received packets to make sure that they haven't been corrupted?

2 [Correct Answer](#)

In which layer would data be formatted in preparation for transmission?

2 [Correct Answer](#)

Which layer transmits and receives data?

1 [Correct Answer](#)

Which layer encrypts, compresses, or otherwise transforms the initial data to give it a standardised format?

6 [Correct Answer](#)

Which layer tracks communications between the host and receiving computers?

5 [Correct Answer](#)

Which layer accepts communication requests from applications?

7 [Correct Answer](#)

Which layer handles logical addressing?

3 [Correct Answer](#)

When sending data over TCP, what would you call the "bite-sized" pieces of data?

Segments [Correct Answer](#)

TASK 3

Answer the questions below

How would you refer to data at layer 2 of the encapsulation process (with the OSI model)?

Frames Correct Answer

How would you refer to data at layer 4 of the encapsulation process (with the OSI model), if the UDP protocol has been selected?

Datagrams Correct Answer

What process would a computer perform on a received message?

De-encapsulation Correct Answer

Which is the only layer of the OSI model to add a *trailer* during encapsulation?

Data Link Correct Answer

Does encapsulation provide an extra layer of security (**Aye/Nay**)?

Aye Correct Answer

TASK 4

Answer the questions below

Which model was introduced first, OSI or TCP/IP?

TCP/IP Correct Answer

Which layer of the TCP/IP model covers the functionality of the Transport layer of the OSI model (**Full Name**)?

Transport Correct Answer

Which layer of the TCP/IP model covers the functionality of the Session layer of the OSI model (**Full Name**)?

Application Correct Answer

The Network Interface layer of the TCP/IP model covers the functionality of two layers in the OSI model. These layers are Data Link, and?... (**Full Name**)?

Physical Correct Answer

Which layer of the TCP/IP model handles the functionality of the OSI network layer?

Internet Correct Answer

What kind of protocol is TCP?

Connection-based Correct Answer Hint

What is SYN short for?

Synchronise Correct Answer Hint

What is the second step of the three way handshake?

SYN/ACK Correct Answer

What is the short name for the "Acknowledgement" segment in the three-way handshake?

ACK Correct Answer

TASK 5

Answer the questions below

What command would you use to ping the `bbc.co.uk` website?

Correct Answer

Ping `muirlandoracle.co.uk`
What is the IPv4 address?

Correct Answer Hint

What switch lets you change the interval of sent ping requests?

Correct Answer Hint

What switch would allow you to restrict requests to IPv4?

Correct Answer

What switch would give you a more verbose output?

Correct Answer

TASK 6

Answer the questions below

Use traceroute on `tryhackme.com`
Can you see the path your request has taken?

Question Done

What switch would you use to specify an interface when using Traceroute?

Correct Answer Hint

What switch would you use if you wanted to use TCP SYN requests when tracing the route?

Correct Answer

[Lateral Thinking] Which layer of the TCP/IP model will traceroute run on by default (Windows)?

Correct Answer

TASK 7

Answer the questions below

Perform a whois search on `facebook.com`

Question Done

What is the registrant postal code for facebook.com?

Correct Answer

When was the facebook.com domain first registered (Format: DD/MM/YYYY)?

Correct Answer

Perform a whois search on `microsoft.com`

(Note: If you fail to read the above instruction and consequently get the wrong answer for the next question, don't expect a helpful response if you report it as a bug...)

Question Done

Which city is the registrant based in?

Correct Answer

[OSINT] What is the name of the golf course that is near the registrant address for microsoft.com?

Correct Answer

What is the registered Tech Email for microsoft.com?

Correct Answer

TASK 8

Answer the questions below

What is DNS short for?

Domain Name System

Correct Answer

What is the first type of DNS server your computer would query when you search for a domain?

Recursive

Correct Answer

What type of DNS server contains records specific to domain extensions (i.e. *.com*, *.co.uk**, etc)*? Use the long version of the name.

Top-Level Domain

Correct Answer

Where is the very first place your computer would look to find the IP address of a domain?

Local Cache

Correct Answer

[Research] Google runs two public DNS servers. One of them can be queried with the IP 8.8.8.8, what is the IP address of the other one?

8.8.4.4



Correct Answer

If a DNS query has a TTL of 24 hours, what number would the dig query show?

86400

Correct Answer

Windows Fundamentals 1



Windows Fundamentals 1

In part 1 of the Windows Fundamentals module, we'll start our journey learning about the Windows desktop, the NTFS file system, UAC, the Control Panel, and more...

Start AttackBox Help

2074

100%

Task 1 Introduction to Windows

Task 2 Windows Editions

Task 3 The Desktop (GUI)

Task 4 The File System

Task 5 The Windows\System32 Folders

Task 6 User Accounts, Profiles, and Permissions

Task 7 User Account Control

Task 8 Settings and the Control Panel

Task 9 Task Manager

Task 10 Conclusion

TASK 2

Answer the questions below

What encryption can you enable on Pro that you can't enable in Home?

BitLocker

Correct Answer

TASK 3

Answer the questions below

Which selection will hide/disable the Search box?

Hidden

Correct Answer

Which selection will hide/disable the Task View button?

Show Task View button

Correct Answer

Besides Clock and Network, what other icon is visible in the Notification Area?

Action Center

Correct Answer

Hint

TASK 4

Answer the questions below

What is the meaning of NTFS?

New Technology File System

Correct Answer

TASK 5

Answer the questions below

What is the system variable for the Windows folder?

Correct Answer

TASK 6

Answer the questions below

What is the name of the other user account?

Correct Answer

What groups is this user a member of?

Correct Answer

What built-in account is for guest access to the computer?

Correct Answer

What is the account status?

Correct Answer

TASK 7

Answer the questions below

What does UAC mean?

Correct Answer

TASK 8

Answer the questions below

In the Control Panel, change the view to **Small icons**. What is the last setting in the Control Panel view?

Correct Answer

TASK 9

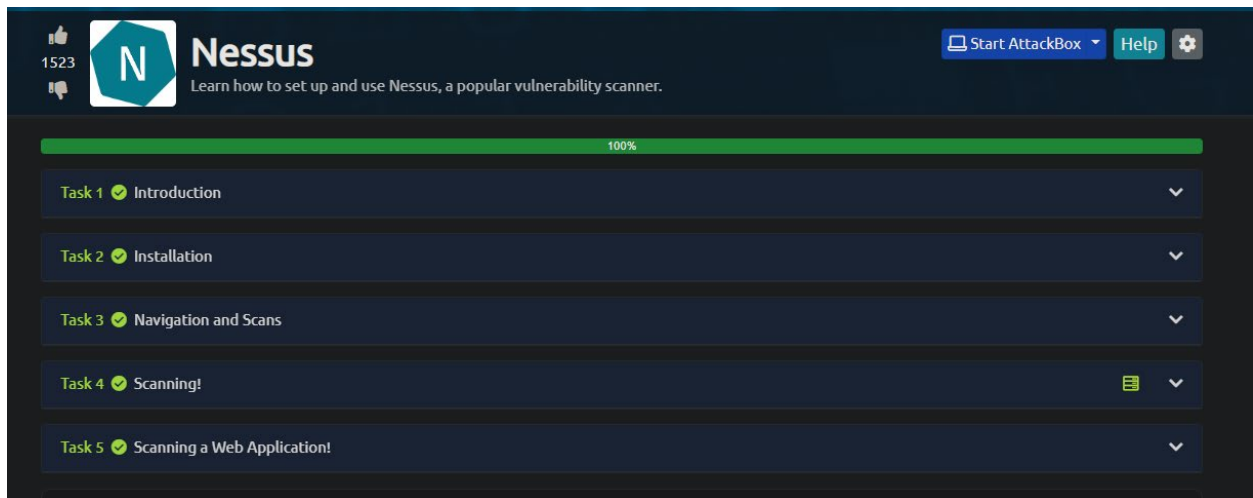
Answer the questions below

What is the keyboard shortcut to open Task Manager?

Correct Answer

THREAT AND VULNERABILITY MANAGEMENT

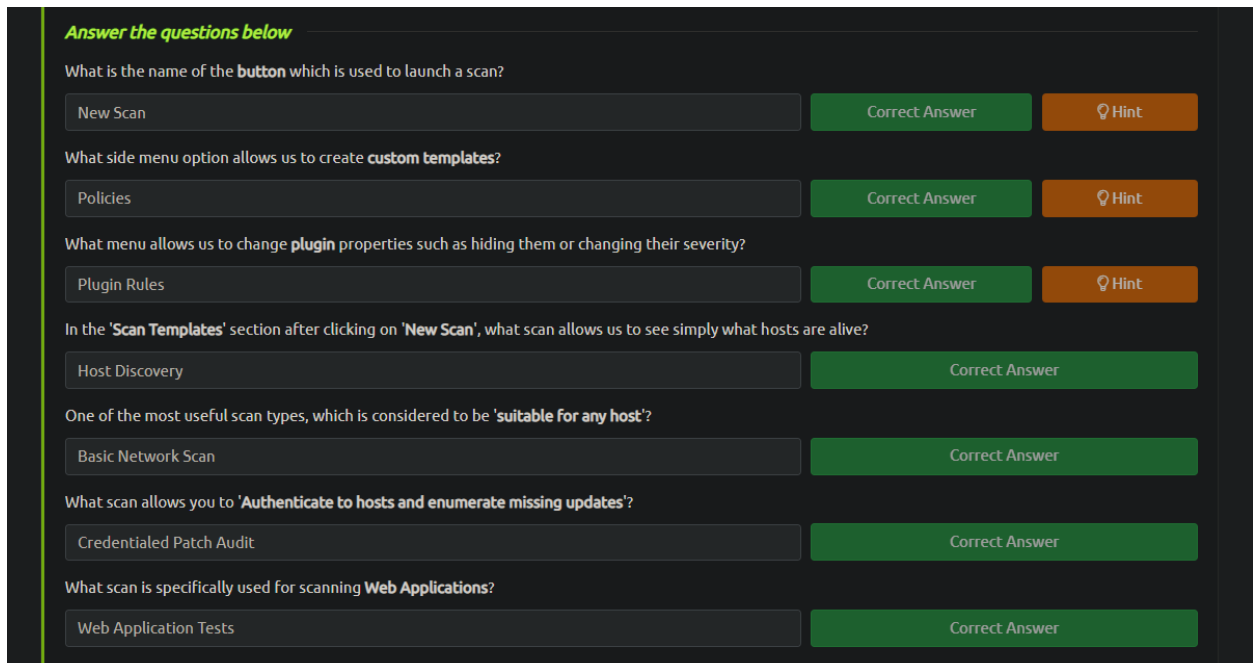
NESSUS



The screenshot shows the Nessus user interface. At the top, there is a header with the Nessus logo, a user profile icon with the number 1523, and buttons for 'Start AttackBox' and 'Help'. Below the header is a green progress bar indicating 100% completion. Underneath the progress bar is a list of five tasks, each with a green checkmark icon and a dropdown arrow:

- Task 1 Introduction
- Task 2 Installation
- Task 3 Navigation and Scans
- Task 4 Scanning!
- Task 5 Scanning a Web Application!

TASK 3



The screenshot shows the Nessus quiz interface for Task 3. The title is 'Answer the questions below'. There are seven questions, each with a text input field, a 'Correct Answer' button, and a 'Hint' button:

- Question 1: What is the name of the **button** which is used to launch a scan? (Answer: New Scan)
- Question 2: What side menu option allows us to create **custom templates**? (Answer: Policies)
- Question 3: What menu allows us to change **plugin** properties such as hiding them or changing their severity? (Answer: Plugin Rules)
- Question 4: In the '**Scan Templates**' section after clicking on '**New Scan**', what scan allows us to see simply what hosts are alive? (Answer: Host Discovery)
- Question 5: One of the most useful scan types, which is considered to be '**suitable for any host**'? (Answer: Basic Network Scan)
- Question 6: What scan allows you to '**Authenticate to hosts and enumerate missing updates**'? (Answer: Credentialed Patch Audit)
- Question 7: What scan is specifically used for scanning **Web Applications**? (Answer: Web Application Tests)

TASK 4

Create a new 'Basic Network Scan' targeting the deployed VM. What option can we set under 'BASIC' (on the left) to set a time for this scan to run? This can be very useful when network congestion is an issue.

Schedule Correct Answer

Under 'DISCOVERY' (on the left) set the 'Scan Type' to cover ports 1-65535. What is this type called?

Port scan (all ports) Correct Answer

What 'Scan Type' can we change to under 'ADVANCED' for lower bandwidth connection?

Scan low bandwidth links Correct Answer

With these options set, launch the scan.

No answer needed Question Done

After the scan completes, which 'Vulnerability' in the 'Port scanners' family can we view the details of to see the open ports on this host?

Nessus SYN scanner Correct Answer

What Apache HTTP Server Version is reported by Nessus?

2.4.99 Correct Answer Hint

TASK 5

Answer the questions below

What is the plugin id of the plugin that determines the HTTP server type and version?

10107 Correct Answer Hint

What authentication page is discovered by the scanner that transmits credentials in cleartext?

login.php Correct Answer Hint

What is the file extension of the config backup?

.bak Correct Answer Hint


Which directory contains example documents? (This will be in a php directory)

/external/phpids/0.6/docs/examples/ Correct Answer Hint

What vulnerability is this application susceptible to that is associated with X-Frame-Options?


Clickjacking Correct Answer Hint

YARA





Yara


Learn the applications and language that is Yara for everything threat intelligence, forensics, and threat hunting!



[Start AttackBox](#) [Help](#) 


100%


Task 1  Introduction


Task 2  What is Yara?


Task 3  Installing Yara (Ubuntu/Debian & Windows)


Task 4  Deploy 


Task 5  Introduction to Yara Rules


Task 6  Expanding on Yara Rules


Task 7  Yara Modules

Task 8  Other tools and Yara

Task 9  Using LOKI and its Yara rule set

Task 10  Creating Yara rules with yarGen

Task 11  Valhalla

Task 12  Conclusion

TASK 9

Answer the questions below

Scan file 1. Does Loki detect this file as suspicious/malicious or benign?

Suspicious

Correct Answer

What Yara rule did it match on?

webshell_metasploit

Correct Answer

What does Loki classify this file as?

Web Shell

Correct Answer

Hint

Based on the output, what string within the Yara rule did it match on?

Str1

Correct Answer

What is the name and version of this hack tool?

b374k 2.2

Correct Answer

Hint

Inspect the actual Yara file that flagged file 1. Within this rule, how many strings are there to flag this file?

1

Correct Answer

Hint

Scan file 2. Does Loki detect this file as suspicious/malicious or benign?

Benign

Correct Answer

Inspect file 2. What is the name and version of this web shell?

b374k 3.2.3

Correct Answer

Hint

TASK 10

Answer the questions below

From within the root of the suspicious files directory, what command would you run to test Yara and your Yara rule against file 2?

Correct Answer 💡 Hint

Did Yara rule flag file 2? (Yay/Nay)

Correct Answer

Copy the Yara rule you created into the Loki signatures directory.

Question Done

Test the Yara rule with Loki, does it flag file 2? (Yay/Nay)

Correct Answer

What is the name of the variable for the string that it matched on?

Correct Answer 💡 Hint

Inspect the Yara rule, how many strings were generated?

Correct Answer

One of the conditions to match on the Yara rule specifies file size. The file has to be less than what amount?

Correct Answer

TASK 11

Answer the questions below

Enter the SHA256 hash of file 1 into Valhalla. Is this file attributed to an APT group? (Yay/Nay)

Correct Answer

Do the same for file 2. What is the name of the first Yara rule to detect file 2?

Correct Answer

Examine the information for file 2 from Virus Total (VT). The Yara Signature Match is from what scanner?

Correct Answer 💡 Hint

Enter the SHA256 hash of file 2 into Virus Total. Did every AV detect this as malicious? (Yay/Nay)

Correct Answer

Besides .PHP, what other extension is recorded for this file?

Correct Answer

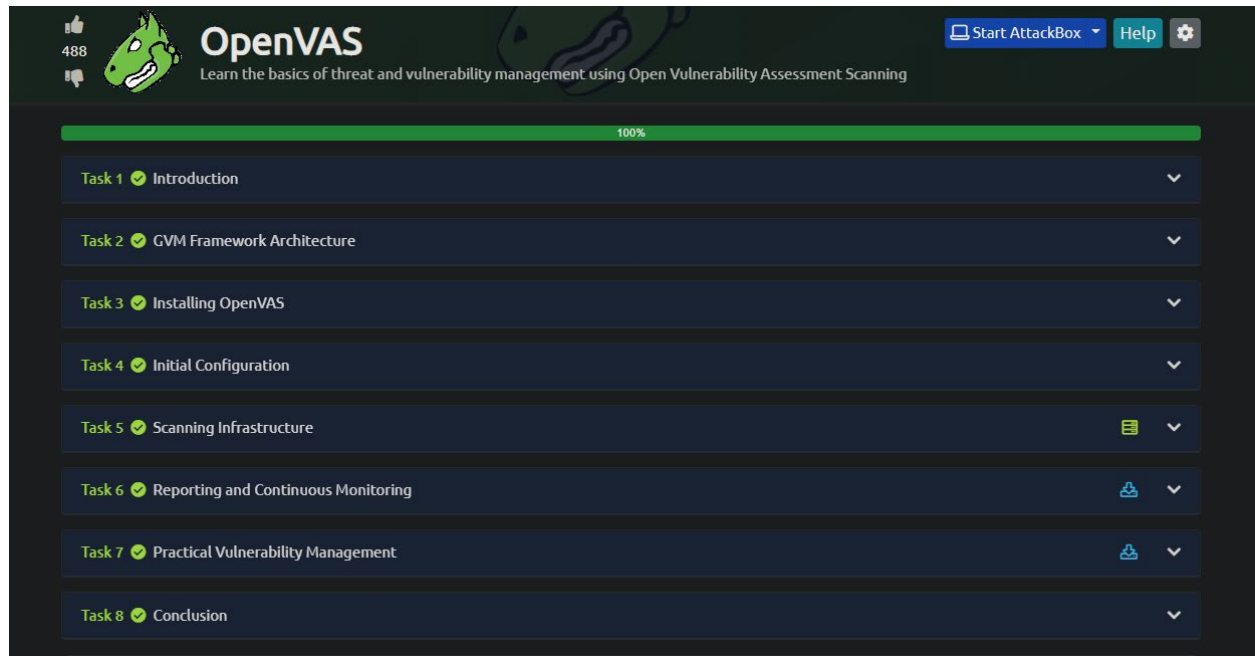
What JavaScript library is used by file 2?

Correct Answer 💡 Hint

Is this Yara rule in the default Yara file Loki uses to detect these type of hack tools? (Yay/Nay)

Correct Answer 💡 Hint

OpenVAS



The image shows the OpenVAS course progress bar. At the top, there is a green progress bar indicating 100% completion. Below it, a list of tasks is shown, each with a green checkmark indicating completion. The tasks are: Task 1 Introduction, Task 2 GVM Framework Architecture, Task 3 Installing OpenVAS, Task 4 Initial Configuration, Task 5 Scanning Infrastructure, Task 6 Reporting and Continuous Monitoring, Task 7 Practical Vulnerability Management, and Task 8 Conclusion. Each task has a dropdown arrow on the right. The OpenVAS logo and name are at the top left, and the text 'Learn the basics of threat and vulnerability management using Open Vulnerability Assessment Scanning' is at the top right. There are also buttons for 'Start AttackBox', 'Help', and a settings icon.

488

OpenVAS

Learn the basics of threat and vulnerability management using Open Vulnerability Assessment Scanning

Start AttackBox Help

100%

- Task 1 Introduction
- Task 2 GVM Framework Architecture
- Task 3 Installing OpenVAS
- Task 4 Initial Configuration
- Task 5 Scanning Infrastructure
- Task 6 Reporting and Continuous Monitoring
- Task 7 Practical Vulnerability Management
- Task 8 Conclusion

TASK 7



The image shows a list of questions and answers for Task 7. The questions are: 'When did the scan start in Case 001?', 'When did the scan end in Case 001?', 'How many ports are open in Case 001?', 'How many total vulnerabilities were found in Case 001?', 'What is the highest severity vulnerability found? (MSxx-xxx)', 'What is the first affected OS to this vulnerability?', and 'What is the recommended vulnerability detection method?'. The answers are: 'Feb 28, 00:04:46', 'Feb 28, 00:21:02', '3', '5', 'MS17-010', 'Microsoft Windows 10 x32/x64 Edition', and 'Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulneral'. Each answer is followed by a green button labeled 'Correct Answer'.

Answer the questions below

When did the scan start in Case 001?

Feb 28, 00:04:46 Correct Answer

When did the scan end in Case 001?

Feb 28, 00:21:02 Correct Answer

How many ports are open in Case 001?

3 Correct Answer

How many total vulnerabilities were found in Case 001?

5 Correct Answer

What is the highest severity vulnerability found? (MSxx-xxx)

MS17-010 Correct Answer

What is the first affected OS to this vulnerability?

Microsoft Windows 10 x32/x64 Edition Correct Answer

What is the recommended vulnerability detection method?

Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulneral Correct Answer

THREAT EMULATION

Attacktive Directory

A screenshot of the Attacktive Directory task list interface. At the top, a green progress bar shows 100% completion. Below it, a list of eight tasks is displayed, each with a green checkmark icon, a category name, and a title. The tasks are: Task 1 (Intro) Deploy The Machine, Task 2 (Intro) Setup, Task 3 (Enumeration) Welcome to Attacktive Directory, Task 4 (Enumeration) Enumerating Users via Kerberos, Task 5 (Exploitation) Abusing Kerberos, Task 6 (Enumeration) Back to the Basics, Task 7 (Domain Privilege Escalation) Elevating Privileges within the Domain, and Task 8 (Flag Submission) Flag Submission Panel. Each task has a dropdown arrow on the right.

Task	Category	Title
Task 1	Intro	Deploy The Machine
Task 2	Intro	Setup
Task 3	Enumeration	Welcome to Attacktive Directory
Task 4	Enumeration	Enumerating Users via Kerberos
Task 5	Exploitation	Abusing Kerberos
Task 6	Enumeration	Back to the Basics
Task 7	Domain Privilege Escalation	Elevating Privileges within the Domain
Task 8	Flag Submission	Flag Submission Panel

TASK 3

A screenshot of the TASK 3 quiz interface. It features a green header with the text "Answer the questions below". Below this, there are three questions, each with a text input field, a "Correct Answer" button, and a "Hint" button. The questions are: "What tool will allow us to enumerate port 139/445?" (answer: enum4linux), "What is the NetBIOS-Domain Name of the machine?" (answer: THM-AD), and "What invalid TLD do people commonly use for their Active Directory Domain?" (answer: .local).

Answer the questions below

What tool will allow us to enumerate port 139/445?
enum4linux Correct Answer

What is the NetBIOS-Domain Name of the machine?
THM-AD Correct Answer

What invalid TLD do people commonly use for their Active Directory Domain?
.local Correct Answer Hint

TASK 4

A screenshot of the TASK 4 quiz interface. It features a green header with the text "Answer the questions below". Below this, there are three questions, each with a text input field, a "Correct Answer" button, and a "Hint" button. The questions are: "What command within Kerbrute will allow us to enumerate valid usernames?" (answer: userenum), "What notable account is discovered? (These should jump out at you)" (answer: svc-admin), and "What is the other notable account is discovered? (These should jump out at you)" (answer: backup).

Answer the questions below

What command within Kerbrute will allow us to enumerate valid usernames?
userenum Correct Answer Hint

What notable account is discovered? (These should jump out at you)
svc-admin Correct Answer

What is the other notable account is discovered? (These should jump out at you)
backup Correct Answer

TASK 5

Answer the questions below

We have two user accounts that we could potentially query a ticket from. Which user account can you query a ticket from with no password?

Correct Answer

Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Specify the full name)

Correct Answer Hint

What mode is the hash?

Correct Answer

Now crack the hash with the modified password list provided, what is the user accounts password?

Correct Answer

TASK 6

Answer the questions below

What utility can we use to map remote SMB shares?

Correct Answer Hint

Which option will list shares?

Correct Answer Hint

How many remote shares is the server listing?

Correct Answer

There is one particular share that we have access to that contains a text file. Which share is it?

Correct Answer

What is the content of the file?

Correct Answer Hint

Decoding the contents of the file, what is the full contents?

Correct Answer

TASK 7

Answer the questions below

What method allowed us to dump NTDS.DIT?

Correct Answer Hint

What is the Administrators NTLM hash?

Correct Answer

What method of attack could allow us to authenticate as the user without the password?

Correct Answer

Using a tool called Evil-WinRM what option will allow us to use a hash?

Correct Answer Hint

TASK 8

Answer the questions below

svc-admin	<input data-bbox="264 331 987 365" type="text" value="TryHackMe{K3rb3r0s_Pr3_4uth}"/>	<input data-bbox="997 331 1377 365" type="button" value="Correct Answer"/>
backup	<input data-bbox="264 415 987 449" type="text" value="TryHackMe{B4ckM3Up5c0tty!}"/>	<input data-bbox="997 415 1377 449" type="button" value="Correct Answer"/>
Administrator	<input data-bbox="264 499 987 533" type="text" value="TryHackMe{4ctiveD1rectoryM4st3r}"/>	<input data-bbox="997 499 1377 533" type="button" value="Correct Answer"/>

INCIDENT RESPONSE AND FORENSICS

Investigating Windows

Answer the questions below

Whats the version and year of the windows machine?

Windows Server 2016

Correct Answer

Which user logged in last?

Administrator

Correct Answer

Hint

When did John log onto the system last?

Answer format: MM/DD/YYYY H:MM:SS AM/PM

03/02/2019 5:48:32 PM

Correct Answer

Hint

What IP does the system connect to when it first starts?

10.34.2.3

Correct Answer

What two accounts had administrative privileges (other than the Administrator user)?

Answer format: username1, username2

Jenny, Guest

Correct Answer

Whats the name of the scheduled task that is malicious.

Clean file system

Correct Answer

What file was the task trying to run daily?

nc.ps1

Correct Answer

What port did this file listen locally for?

1348

Correct Answer

When did Jenny last logon?

Never

Correct Answer

At what date did the compromise take place?

Answer format: MM/DD/YYYY

03/02/2019

Correct Answer

At what time did Windows first assign special privileges to a new logon?

Answer format: MM/DD/YYYY HH:MM:SS AM/PM

03/02/2019 4:04:49 PM

Correct Answer

Hint

What tool was used to get Windows passwords?

Mimikatz

Correct Answer

What was the attackers external control and command servers IP?

76.32.97.132

Correct Answer

What was the extension name of the shell uploaded via the servers website?

.jsp

Correct Answer

What was the last port the attacker opened?

1337

Correct Answer

Hint

Check for DNS poisoning, what site was targeted?

google.com

Correct Answer

Windows Forensics 1

468 **Windows Forensics 1**
Introduction to Windows Registry Forensics

Start AttackBox Help

100%

- Task 1 Introduction to Windows Forensics
- Task 2 Windows Registry and Forensics
- Task 3 Accessing registry hives offline
- Task 4 Data Acquisition
- Task 5 Exploring Windows Registry
- Task 6 System Information and System Accounts
- Task 7 Usage or knowledge of files/folders
- Task 8 Evidence of Execution
- Task 9 External Devices/USB device forensics
- Task 10 Hands-on Challenge
- Task 11 Conclusion

TASK 1

Answer the questions below

What is the most used Desktop Operating System right now?

Microsoft Windows

TASK 2

Answer the questions below

What is the short Form for HKEY_LOCAL_MACHINE?

HKLM

TASK 3

Answer the questions below

What is the path for the five main registry hives, DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM?

C:\Windows\System32\Config

What is the path for the AmCache hive?

C:\Windows\AppCompat\Programs\Amcache.hve

TASK 6

Answer the questions below

What is the Current Build Number of the machine whose data is being investigated?

19044

Correct Answer

Hint

Which ControlSet contains the last known good configuration?

1

Correct Answer

What is the Computer Name of the computer?

THM-4n6

Correct Answer

What is the value of the TimeZoneKeyName?

Pakistan Standard Time

Correct Answer

What is the DHCP IP address

192.168.100.58

Correct Answer

What is the RID of the Guest User account?

501

Correct Answer

Hint

TASK 7

Answer the questions below

When was EZtools opened?

2021-12-01 13:00:34

Correct Answer

Hint

At what time was My Computer last interacted with?

2021-12-01 13:06:47

Correct Answer

Hint

What is the Absolute Path of the file opened using notepad.exe?

C:\Program Files\Amazon\Ec2ConfigService\Settings

Correct Answer

When was this file opened?

2021-11-30 10:56:19

Correct Answer

Hint

TASK 8

Answer the questions below

How many times was the File Explorer launched?

26

Correct Answer

Hint

What is another name for ShimCache?

AppCompatCache

Correct Answer

Which of the artifacts also saves SHA1 hashes of the executed programs?

AmCache

Correct Answer

Which of the artifacts saves the full path of the executed programs?

BAM/DAM

Correct Answer

TASK 9

Answer the questions below

What is the serial number of the device from the manufacturer 'Kingston'?

1C6f654E59A3B0C179D366AE&0

Correct Answer

What is the name of this device?

Kingston Data Traveler 2.0 USB Device

Correct Answer

What is the Friendly name of the device from the manufacturer 'Kingston'?

USB

Correct Answer

TASK 10

Answer the questions below

How many user created accounts are present on the system?

3

Correct Answer

Hint

What is the username of the account that has never been logged in?

thm-user2

Correct Answer

Hint

What's the password hint for the user THM-4n6?

count

Correct Answer

Hint

When was the File 'Changelog.txt' accessed?

2021-11-21 18:18:48

Correct Answer

Hint

What is the complete path from where the python 3.8.2 installer was run?

Z:\setups\python-3.8.2.exe

Correct Answer

Hint

When was the USB device with the friendly name 'USB' last connected?


2021-11-24 18:40:06


Correct Answer

Hint

MALWARE ANALYSIS

MAL: Malware Introductory


1245


















MAL: Malware Introductory

The start of a series of rooms covering Malware Analysis...

Start AttackBox Help

100%

- Task 1  What is the Purpose of Malware Analysis?
- Task 2  Understanding Malware Campaigns
- Task 3  Identifying if a Malware Attack has Happened
- Task 4  Static Vs. Dynamic Analysis
- Task 5  Discussion of Provided Tools & Their Uses
- Task 6  Connecting to the Windows Analysis Environment (Deploy) 
- Task 7  Obtaining MD5 Checksums of Provided Files
- Task 8  Now lets see if the MD5 Checksums have been analysed before
- Task 9  Identifying if the Executables are obfuscated / packed
- Task 10  What is Obfuscation / Packing?
- Task 11  Visualising the Differences Between Packed & Non-Packed Code
- Task 12  Introduction to Strings
- Task 13  Introduction to Imports
- Task 14  Practical Summary

TASK 2

Answer the questions below

What is the famous example of a targeted attack-esque Malware that targeted Iran?

Stuxnet

Correct Answer

What is the name of the Ransomware that used the Eternalblue exploit in a "Mass Campaign" attack?

Wannacry

Correct Answer

TASK 3

Answer the questions below

Name the first essential step of a Malware Attack?

Delivery

Correct Answer

Now name the second essential step of a Malware Attack?

Execution

Correct Answer

What type of signature is used to classify remnants of infection on a host?

Host-Based Signatures

Correct Answer

Hint

What is the name of the other classification of signature used after a Malware attack?

Network-Based Signatures

Correct Answer

Hint

TASK 7

Answer the questions below

The MD5 Checksum of aws.exe

D2778164EF643BA8F44CC202EC7EF157

Correct Answer

The MD5 Checksum of Netlogo.exe

59CB421172A89E1E16C11A428326952C

Correct Answer

The MD5 Checksum of vlc.exe

5416BE1B8B04B1681CB39CF0E2CAAD9F

Correct Answer

TASK 8

Answer the questions below

Does Virustotal report this MD5 Checksum / file aws.exe as malicious? (Yay/Nay)

Nay

Correct Answer

Does Virustotal report this MD5 Checksum / file Netlogo.exe as malicious? (Yay/Nay)

Nay

Correct Answer

Does Virustotal report this MD5 Checksum / file vlc.exe as malicious? (Yay/Nay)

Nay

Correct Answer

TASK 9

Answer the questions below

What does PeID propose 1DE9176AD682FF.dll being packed with?

Microsoft Visual C++ 6.0 DLL

Correct Answer

Hint

What does PeID propose AD29AA1B.bin being packed with?

Microsoft Visual C++ 6.0

Correct Answer

TASK 10

Answer the questions below

What packer does PeID report file "6F431F46547DB2628" to be packed with?

TASK 12

Answer the questions below

What is the URL that is outputted after using "strings"

How many **unique** "Imports" are there?

TASK 13

Answer the questions below

How many references are there to the library "msi" in the "Imports" tab of IDA Freeware for "install.exe"?

TASK 14

Answer the questions below

What is the MD5 Checksum of the file?

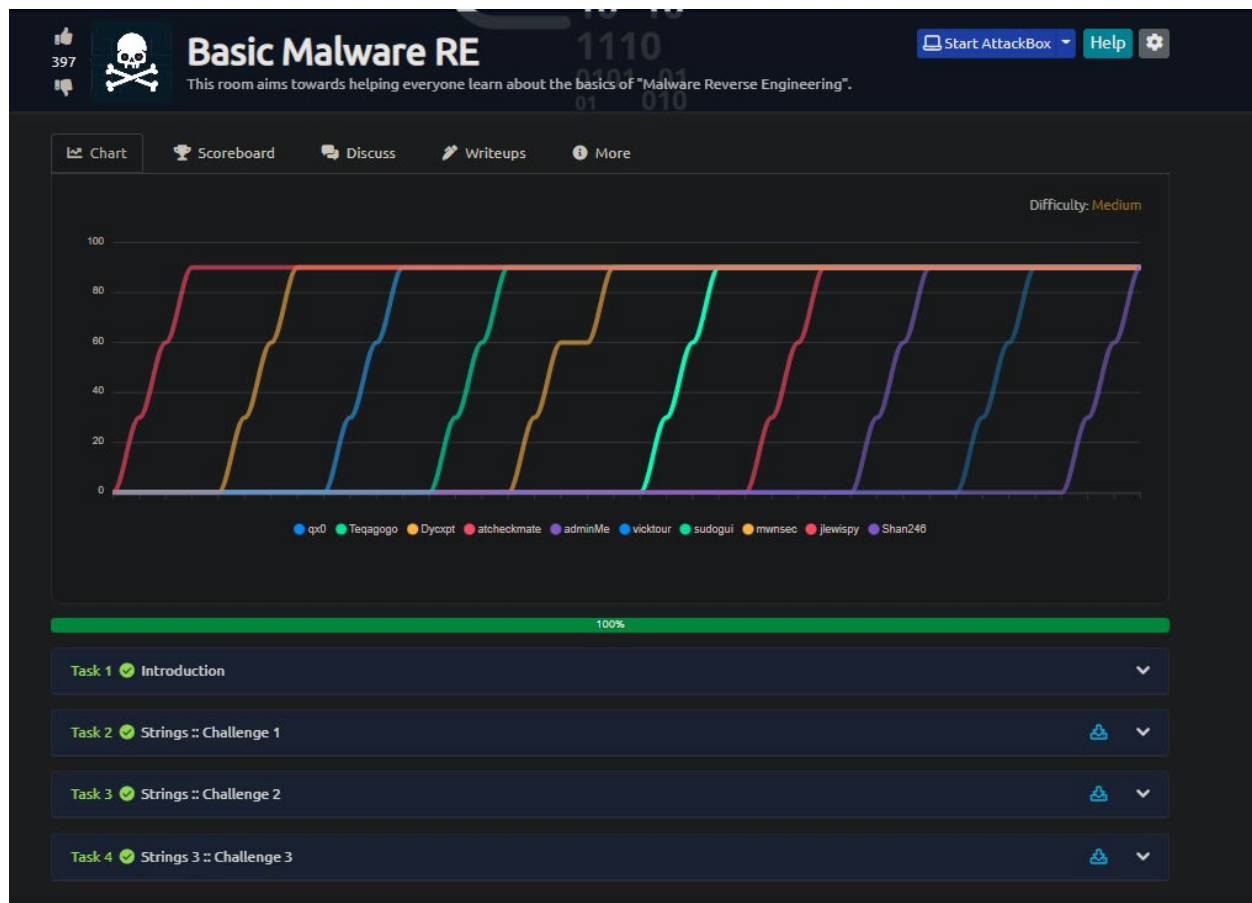
Does Virustotal report this file as malicious? (Yay/Nay)

Output the strings using Sysinternals "strings" tool.

What is the last string outputted?

What is the output of PeID when trying to detect what packer is used by the file?

Basic Malware RE



TASK 2

Answer the questions below

What is the flag of which that MD5 gets generated?

Correct Answer

TASK 3

Answer the questions below

What is the flag of which that MD5 gets generated?

Correct Answer

TASK 4

Answer the questions below

What is the flag of which that MD5 gets generated?

Correct Answer