

PenTest 1

ROOM A

GROUPNAME

Members

ID	Name	Role
XXX		Leader
YYY	Timothy Yap	Member
ZZZ	Ian Chai	Member
AAA	YPWong	Member

Steps: (example) Recon and Enumeration

You should divide your report into 4 sections in general:

- 1) Recon and Enumeration (Where you gather data)
- 2) Initial Foothold (where you gain the first reverse shell)
- 3) Horizontal Privilege Escalation (If any, if you pivot to other users)
- 4) Root Privilege Escalation (final step, rooting)

For each section do the following:



(frame your images with borders)

Members Involved: JJChin, Timothy

Tools used: Nmap/Gobuster/WPScan etc

Thought Process and Methodology and Attempts:

JJChin recognised that the string is a base64 code with the '==' ending. Prior to the link being released, JJChin was already aware that Cyberchef could be used to decode base64 strings. Therefore he first attempted

JJChin copied the string to Cyberchef, and the magic wand output revealed the flag.

Input

VGlhIGZsYWwgaXlmgbmV4YXtCYXNpY18xfQ==

From Base64 will produce
"The flag is
nexa{Basic_1}"

Output

VGlhIGZsYWwgaXlmgbmV4YXtCYXNpY18xfQ==

Later Timothy verified the string was correct using the asciitohex alternative. However, he made a mistake of pasting to the wrong textbox which was the ASCII/ANSI textbox.

ASCII to Hex

...and other free text conversion tools

Text (ASCII / ANSI)

VGlhIGZsYWwgaXlmgbmV4YXtCYXNpY18xfQ==

Convert Highlight Text

BASE64

VkdobEhWnNZ2NnYVhNZ2JvJRZVHRDWhOcFxoHhmUT09

Convert Highlight Text

Decimal

86 71 104 108 73 71 90 115 89 87 99 103 97 88 77
103 98 109 86 52 89 88 116 67 89 88 78 112 89 49 56
120 102 81 61 61

Convert Highlight Text

Binary

01010110 01000111 01101000 01101100
01001001 01000111 01011010 01110011
01011001 01010111 01100011 01100111
01100001 01011000 01001101 01100111
01100010 01101101 01010110 00110100
01011001 01011000 01110100 01000011
01011001 01011000 01001110 01110000
01011001 00110001 00111000 01111000

Convert Highlight Text

Hexadecimal

56 47 68 6c 49 47 5a 73 59 57 63 67 61 58 4d 67 62
6d 56 34 59 58 74 43 59 58 4e 70 59 31 38 78 66 51
3d 3d

Convert Highlight Text

ROT13

ITuyVTMfljptrnk2toz4LkgPLKAcL18ksD==

Convert Highlight Text

Upon double check, he repasted the string to Base64 textbox and managed to convert and verify the flag successfully.

ASCII to Hex

...and other free text conversion tools

The screenshot shows a web interface for text conversion. It has three main sections: 'Text (ASCII / ANSI)' at the top, 'BASE64' in the middle left, and 'Decimal' in the middle right. The 'Text' section contains the input 'The flag is nexa{Basic_1}' and buttons for 'Convert' and 'Highlight Text'. The 'BASE64' section contains the output 'VGhlIGZsYWcgaXMgbmV4YXtCYXNpY18xfQ==' and similar buttons. The 'Decimal' section shows the hex values '84 104 101 32' and '101 120 97 123' with a 'Convert' button.

Final Result: (if you did not manage to solve, just mention you moved on to other questions)

Upon verification of the flag, Timothy placed the flag into the TryHackMe site and got the confirmation.

The screenshot shows a challenge page titled 'Basic 1' with a difficulty of '10'. It includes a 'crypto' tag and the instruction 'Please decode this :'. The encoded text is 'VGhlIGZsYWcgaXMgbmV4YXtCYXNpY18xfQ=='. A hint is provided with the link 'https://www.asciitohex.com/'. A message states 'You already solved this'. At the bottom, there is a text input field containing the flag 'nexa{Basic_1}' and a 'Submit' button.

Use a new page for a new Step

Category:

Question:

Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	Name	Contribution	Signatures
XXX	JJChin	Did the recon. Discovered the exploit to root.	
YYY	Timothy Yap	Figured out the exploit for initial foothold.	
ZZZ	Ian Chai	Tried Exploit alternatives B and C but didn't work. Did most of the writing after compiling findings.	
AAA	YPWong	Pivoted from User A to User B. Coke and instant noodles supplier.	

NOTE: IT IS IMPORTANT EACH MEMBER CONTRIBUTES IN SOME WAY AND ALL MEMBERS MUST SIGN TO ACKNOWLEDGE THE CONTRIBUTIONS! DO NOT GIVE FREELoadERS THE FLAGS AS THEY DON'T DESERVE THE MARKS. DO NOT SHARE THE FLAGS WITH OTHER GROUPS AS WELL!

Attach the video link at the end of the report:

VIDEO LINK: <https://www.youtube.com/asdkljaklsjds>