**NineTail HTB Write-up**

1. Firstly, I did a Nmap scan for any open ports and their information.

A screenshot of a computer

Description automatically generated

1. Next, I used ldapsearch command to enumerate more about the DNS. I have found that the naming was Ninetail and htb. Hence, I further enumerated and found out the various users in this domain. Additionally, I’ve noted the password security configurations. Finally, I enumerate using crackmapexec via SMB for more information since port 445 is open. I’ve then found out that this OS build has known vulnerabilities.

A computer screen shot of a program

Description automatically generated

A computer screen shot of numbers and letters

Description automatically generated

A computer screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated



1. Since we have found the user for the domain, I need to find a way to retrieve the password. Hence, I created this file based on the information gathered about the password complexity.

A screen shot of a computer

Description automatically generated

1. I used Metasploit to brute force the SMB login as we have the passlist file created previously and the SMB user that has been found from ldapsearch. I did this since port 445 is open too. And it was successful! So, we have the SMB user and SMB password !!

A screen shot of a computer

Description automatically generated

1. I’ve added the target IP address into /etc/hosts to simulate or redirect network traffic to a specific IP address, without modifying DNS records globally. Next, I used rpcdump.py to verify the vulnerability PoC.

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

1. I copied and created a file CVE-2021-1675.py that I found on the internet from Git Hub with the same content. Next, I created a malicious dll file using msfvenom and started an SMB server in another shell using impacket.

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer screen

Description automatically generated

1. I started a new terminal to run the exploit and another terminal to run msfconsole again to start a reverse shell whereby I’ve managed to get a shell. I’ve then used the command whoami to check who’s the current user and it’s the nt authority, which has the highest authority account on a local system! Afterwards, I searched through the directory to look for the user.txt and root.txt for the flags. For the user flag, I searched in the pwnmeow directory, but it doesn’t have the flag there, so I went to look around and found that pwnmeowSvc has the flag!

A screen shot of a computer

Description automatically generated

**A screenshot of a computer

Description automatically generated**

**A screen shot of a computer code

Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

1. There!! The flag is found.