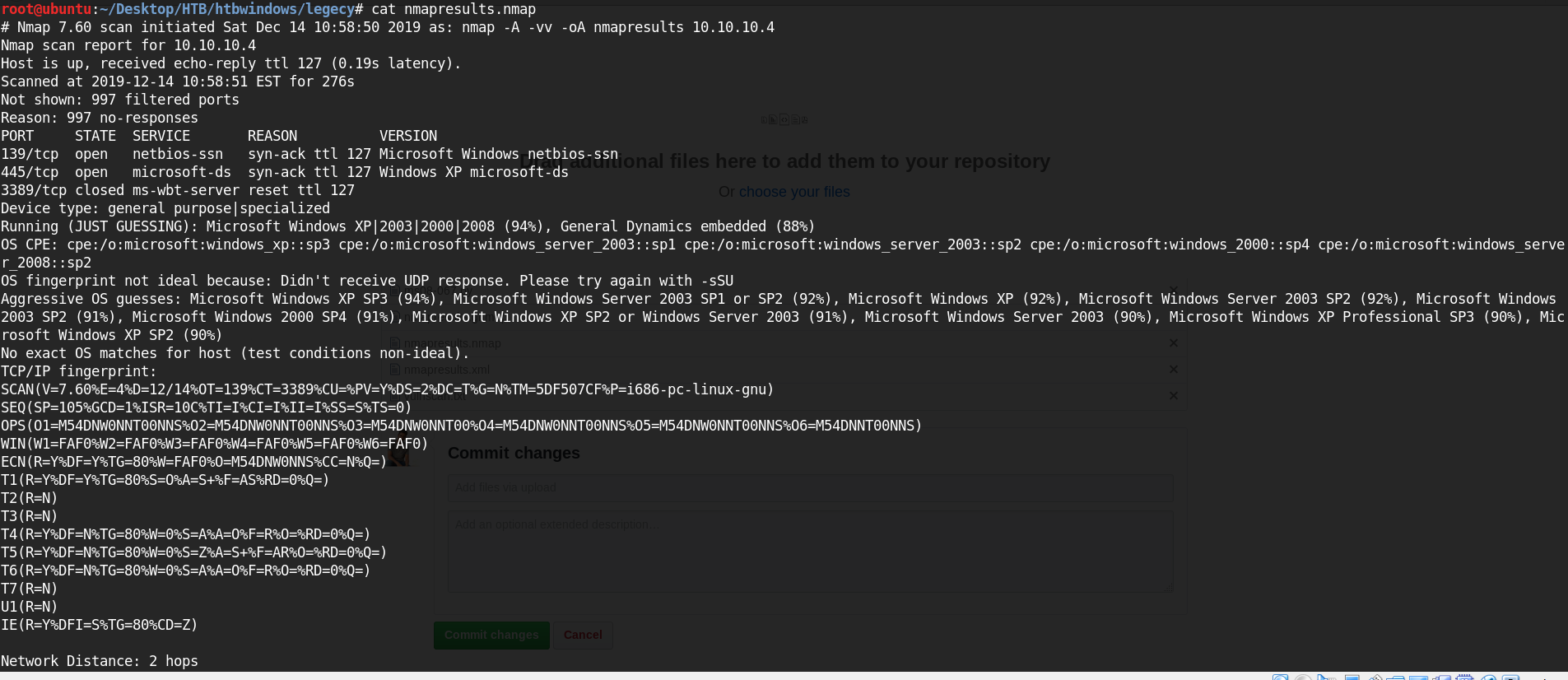
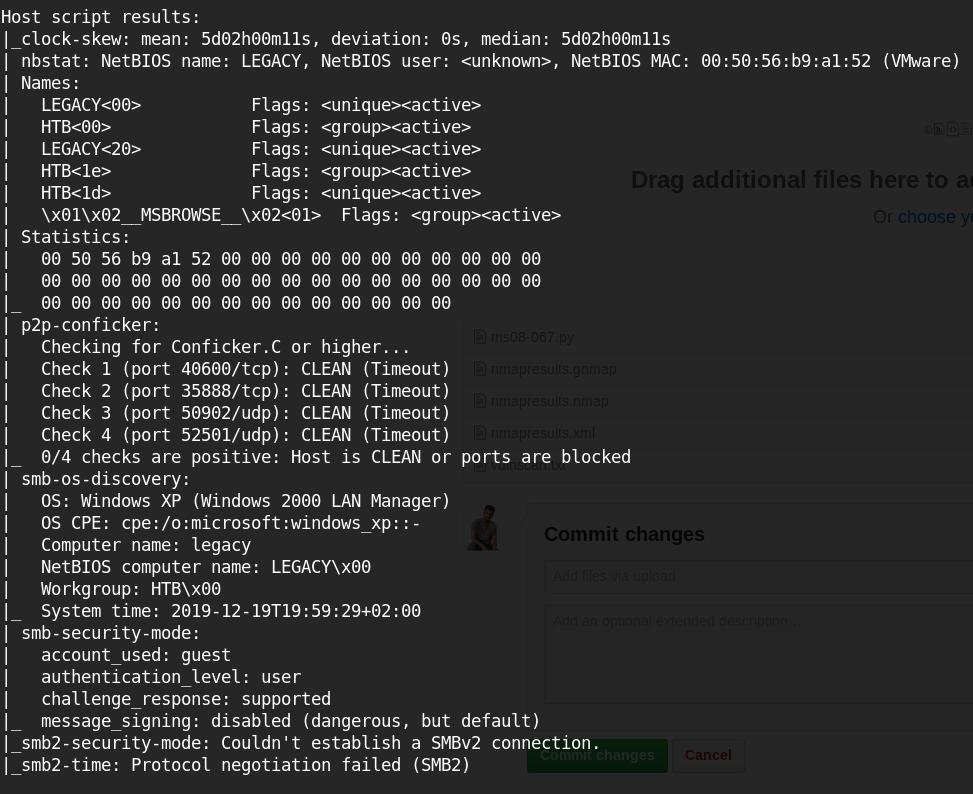
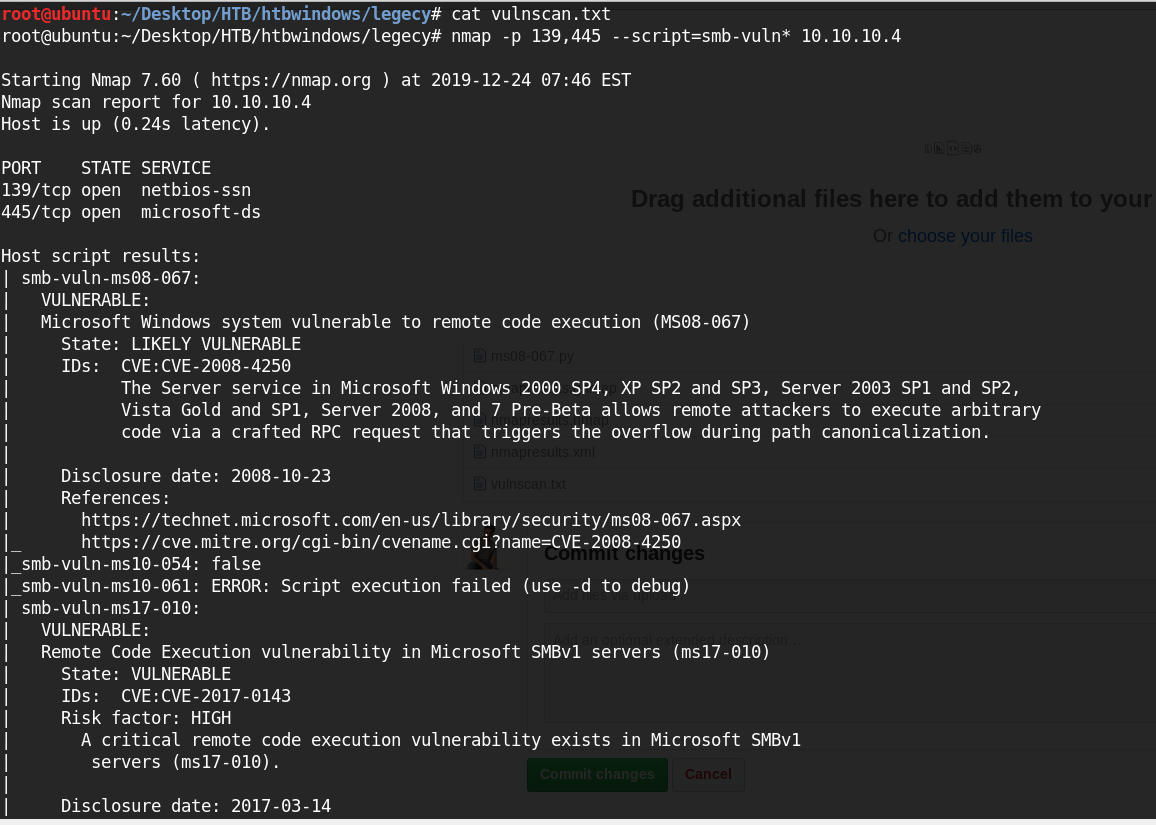
**Legacy HTB Walkthrough:**

Check out the nmap scan results on the folder.





Ran vuln scan for any kernel exploits



﻿

smb-vuln-ms08-067:

| VULNERABLE:

| Microsoft Windows system vulnerable to remote code execution (MS08-067)

| State: LIKELY VULNERABLE

| IDs: CVE:CVE-2008-4250

| The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,

| Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary

| code via a crafted RPC request that triggers the overflow during path canonicalization.

|

| Disclosure date: 2008-10-23

| References:

| https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

|\_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

Download link: <https://raw.githubusercontent.com/jivoi/pentest/master/exploit_win/ms08-067.py>

