BruteForcing
OF
Virtual Network Computing Authentication

Jason Spencer

Academy

Virtual Networking Computing

VNC or Virtual Network Computing is a graphical desktop-sharing system. It uses Remote Frame Buffer (RFB) protocol to remotely control another computer. RFB is a simple protocol for remote access to graphical user interfaces. The user sits on the client side with the keyboard mouse and visual screen. The endpoint where changes to the framebuffer originate (i.e., the windowing system and applications) is known as the RFB server. RFB is a ”thin client” protocol. The emphasis in the design of the RFB protocol is to make very few requirements of the client.

Multiple clients may connect to a VNC server at the same time. Popular uses for this technology include remote technical support and accessing files on one's work computer from one's home computer, or vice versa.If a client disconnects from a given server and subsequently reconnects to that same server, the state of the user interface is preserved. Furthermore, a different client endpoint can be used to connect to the same RFB server. At the new endpoint, the user will see exactly the same graphical user interface as at the original endpoint.

VNC client contacts the server on TCP port 5900. On systems with multiple VNC servers, server N typically listens on port 5900+N.

There are 3 security types that VNCBruter will deal with Invalid, None, and VNC Authentication. There are other security types, however they are not publicly documented. If the security type is None, no authentication is needed and the client and server can begin to communicate.If VNC Authentication is the chosen security type, the server sends a random 16-byte challenge. The client then encrypts the challenge with DES, using a password supplied by the user as the key. To form the key, the password is truncated to 8 characters, or padded with null bytes on the right of the final character. The client then sends the resulting 16-byte response.

Vulnerabilities that exist

There are two know CVE recorded vulnerabilities associated with VNC.

CVE-2006-2369 - with which two metasploit modules have been modeled after, realvnc_41_bypass and vnc_none_auth. This vulnerability states that VNC 4.1 and VNC 4.1.1, authentication can be bypassed if the security type is set to None, even if that type was not specified by the server.

CVE-2004-1750 - which states that attackers can cause a denial of service to VNC 4.0 and earlier with a large amount of requests to port 5900.

Programs that brute force VNC

Password Attack- Metasploit auxiliary module called vnc_login. This module will test a VNC server on a range of machines and report successful logins. Currently, it supports RFB protocol version 3.3, 3.7, 3.8 and 4.001 using the VNC challenge-response authentication method.

VNCPwn this is a brute forcing tool developed in python. It attempts to brute-force a machine and if a successful login is achieved it will run a ducky script on that machine.

Nrack is also a popular password-cracking tool for cracking network authentications. It can perform multiple other attacks other than brute-forcing attacks, however for VNCs sake it only performs bruteforcing attacks.

Crowbar (formally known as Levye) is a brute forcing tool that can be used OpenVPN, SSH, RDP, and VNC. VNC brutefrocing can be done by setting the ‘b‘ flag to ‘vnc’.

vnc_login, VNCPwn and Nrack all attempt to brute force VNC authentication in a similar fashion to VNCBruter, however Crowbar attempts to brute force VNC key authentication.

What does *vncbruter.py* do?

VNCBruter pulls imports VNC.py ceated by Hegusung. This class has the ability to detect the security type of a connect to a VNC server and connect to a vnc server. VNCBruter uses this - it first looks for the type of security, then having chosen either non or VNC authentication attempts to connect to the server with a given password. The program is set to run through every password for every IP address and port number. For each check it prints a success or failure message.

Figure 1: Testing passwords

At the end of the program it clears the screen and prints out all the valid results.

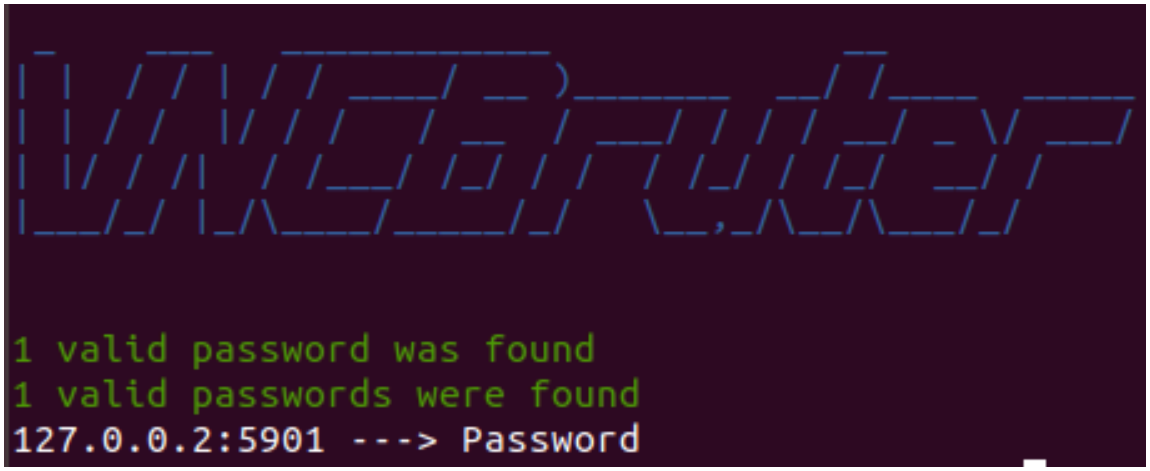

Figure 2: Successful password result

The code allows for a single target and a single password. Multiple targets with multiple passwords, or any other combination of password IP addresses and ports.

```
    parser.add_argument('--pass', dest='pass_file',
                        help='Specify a password to be tested. ')
    parser.add_argument('-P', dest='P_file',
                        help='Specify a file of passwords to be tested. Reads a CSV file
    that contains passwords, one per line')
    parser.add_argument('-l', dest='ip',
                        help='Specify the target and ports to attack (eg 127.0.0.1,5900)'
    )
    parser.add_argument('-p', dest='port',default=5900,
                        help='Specify the ports of the vnc server')
    parser.add_argument('-lL','--targets', dest='target',
                        help='Specify a file with targets to attack. Reads a CSV file
    that contains targets and ports, one per line (eg 127.0.0.1,5900)')
    parser.add_argument('-t', help='timeout', nargs='?', default=15, type=int, dest='
    timeout')
    parser.add_argument('-O',dest='outputfile', help='Destination of the outputfile')
```

Listing 1: Argument parser for VNCBruter

The program itself boils down to one line, vnc.connect(target_IP,target_port,password), the rest of the program makes it verbose and allows for multiple connect attempts.

If the ‘O‘ flag is set, the program will write out to the specified file in both File_Name.txt and File_Name.json format otherwise the program will write out to stdout.

References

https://tools.ietf.org/html/rfc6143

https://www.hackingarticles.in/vnc-penetration-testing/

https://securityonline.info/crowbar-openvpnrdpsshvnc-brute-forcing/

https://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/gref

https://www.cvedetails.com/vulnerability-list/vendor_id-2418/VNC.html

https://github.com/hegusung/VNCPwn