Introductory Researching

A brief introduction to research skills for pentesting.

Task 2 Example Research Question

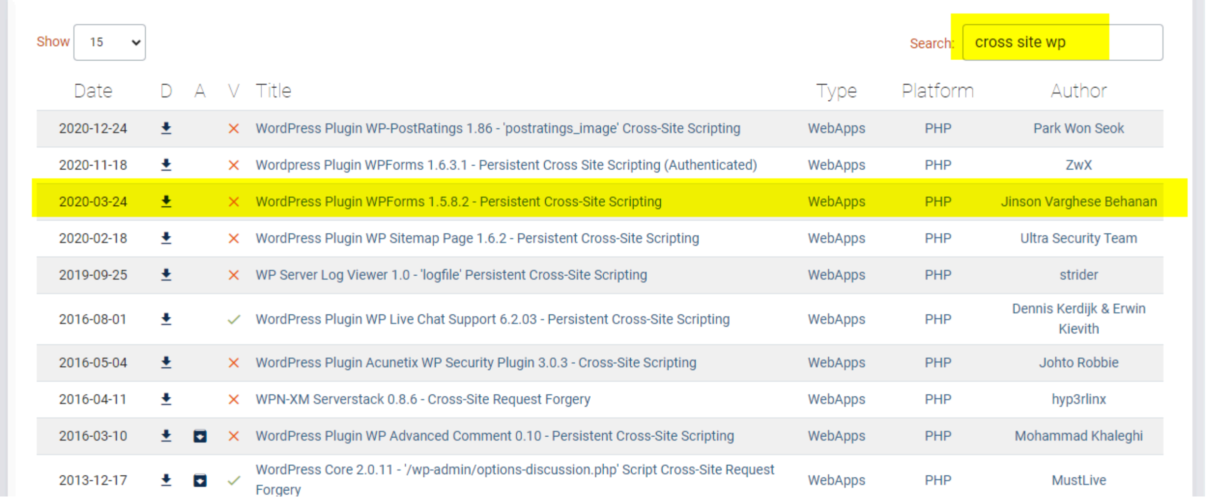
Question	**Answer**
In the Burp Suite Program that ships with Kali Linux, what mode would you use to manually send a request (often repeating a captured request numerous times)?	repeater
What hash format are modern Windows login passwords stored in?	NTLM
What are automated tasks called in Linux?	Cron jobs
What number base could you use as a shorthand for base 2 (binary)?	base 16
If a password hash starts with 6, what format is it (Unix variant)?	SHA512 crypt

Task 3 Vulnerability Searching

What is the CVE for the 2020 Cross-Site Scripting (XSS) vulnerability found in WPForms?

On **exploitdb**, i searched for “cross site wp”, specifically looked for those in 2020

Answer: CVE-2020-10385



Show 15

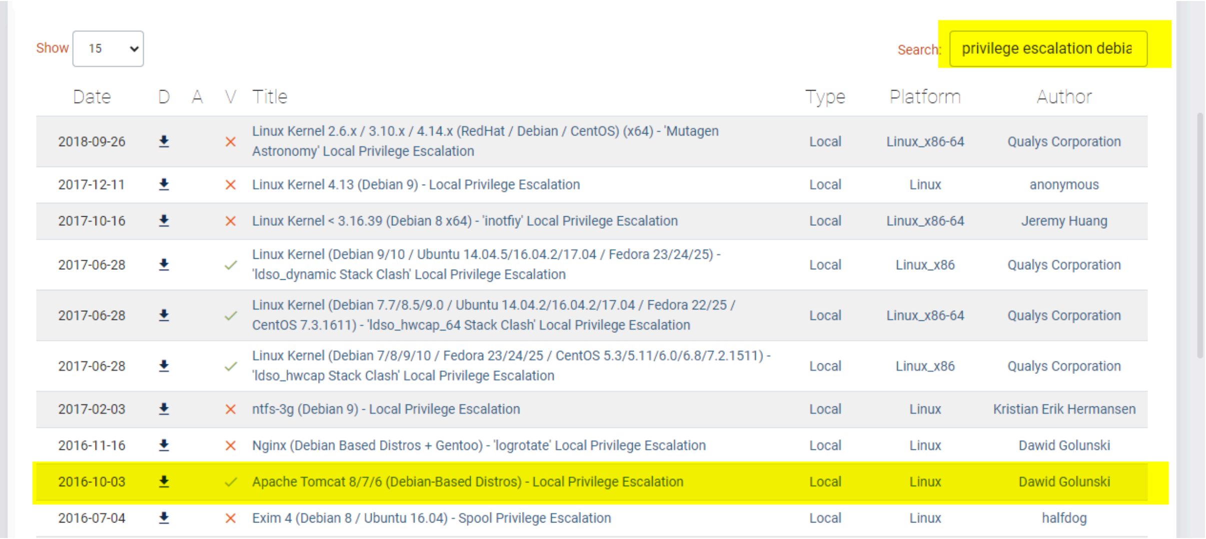
Search: cross site wp

Date	D	A	V	Title	Type	Platform	Author
2020-12-24	⬇		✗	WordPress Plugin WP-PostRatings 1.86 - 'postratings_image' Cross-Site Scripting	WebApps	PHP	Park Won Seok
2020-11-18	⬇		✗	Wordpress Plugin WPForms 1.6.3.1 - Persistent Cross Site Scripting (Authenticated)	WebApps	PHP	ZwX
2020-03-24	⬇		✗	WordPress Plugin WPForms 1.5.8.2 - Persistent Cross-Site Scripting	WebApps	PHP	Jinson Varghese Behanan
2020-02-18	⬇		✗	WordPress Plugin WP Sitemap Page 1.6.2 - Persistent Cross-Site Scripting	WebApps	PHP	Ultra Security Team
2019-09-25	⬇		✗	WP Server Log Viewer 1.0 - 'logfile' Persistent Cross-Site Scripting	WebApps	PHP	strider
2016-08-01	⬇		✓	WordPress Plugin WP Live Chat Support 6.2.03 - Persistent Cross-Site Scripting	WebApps	PHP	Dennis Kerdijk & Erwin Kievith
2016-05-04	⬇		✗	WordPress Plugin Acunetix WP Security Plugin 3.0.3 - Cross-Site Scripting	WebApps	PHP	Johto Robbie
2016-04-11	⬇		✗	WPN-XM Serverstack 0.8.6 - Cross-Site Request Forgery	WebApps	PHP	hyp3rlinx
2016-03-10	⬇	▣	✗	WordPress Plugin WP Advanced Comment 0.10 - Persistent Cross-Site Scripting	WebApps	PHP	Mohammad Khaleghi
2013-12-17	⬇	▣	✓	WordPress Core 2.0.11 - '/wp-admin/options-discussion.php' Script Cross-Site Request Forgery	WebApps	PHP	MustLive

There was a Local Privilege Escalation vulnerability found in the *Debian* version of Apache Tomcat, back in 2016. What's the CVE for this vulnerability?

I searched for privilege escalation debian, specifically looked for those in 2016

Answer: **CVE-2016-1240**



Show 15

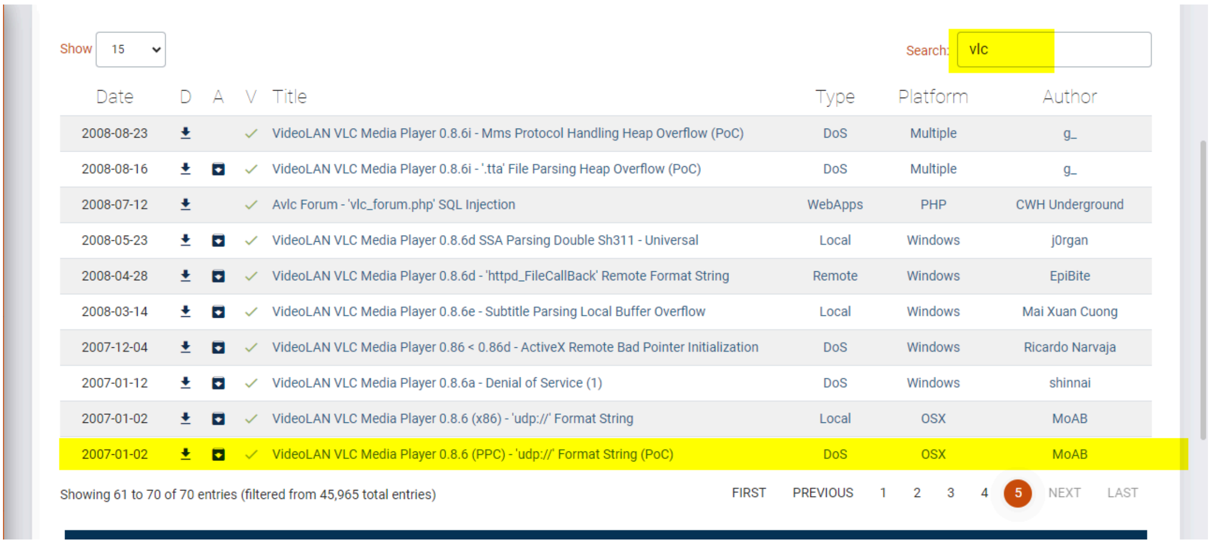
Search: privilege escalation debia

Date	D	A	V	Title	Type	Platform	Author
2018-09-26	⬇		✗	Linux Kernel 2.6.x / 3.10.x / 4.14.x (RedHat / Debian / CentOS) (x64) - 'Mutagen Astronomy' Local Privilege Escalation	Local	Linux_x86-64	Qualys Corporation
2017-12-11	⬇		✗	Linux Kernel 4.13 (Debian 9) - Local Privilege Escalation	Local	Linux	anonymous
2017-10-16	⬇		✗	Linux Kernel < 3.16.39 (Debian 8 x64) - 'inotfiy' Local Privilege Escalation	Local	Linux_x86-64	Jeremy Huang
2017-06-28	⬇		✓	Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'ldso_dynamic Stack Clash' Local Privilege Escalation	Local	Linux_x86	Qualys Corporation
2017-06-28	⬇		✓	Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / CentOS 7.3.1611) - 'ldso_hwcap_64 Stack Clash' Local Privilege Escalation	Local	Linux_x86-64	Qualys Corporation
2017-06-28	⬇		✓	Linux Kernel (Debian 7/8/9/10 / Fedora 23/24/25 / CentOS 5.3/5.11/6.0/6.8/7.2.1511) - 'ldso_hwcap Stack Clash' Local Privilege Escalation	Local	Linux_x86	Qualys Corporation
2017-02-03	⬇		✗	ntfs-3g (Debian 9) - Local Privilege Escalation	Local	Linux	Kristian Erik Hermansen
2016-11-16	⬇		✗	Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Privilege Escalation	Local	Linux	Dawid Golunski
2016-10-03	⬇		✓	Apache Tomcat 8/7/6 (Debian-Based Distros) - Local Privilege Escalation	Local	Linux	Dawid Golunski
2016-07-04	⬇		✗	Exim 4 (Debian 8 / Ubuntu 16.04) - Spool Privilege Escalation	Local	Linux	halfdog

What is the very first CVE found in the VLC media player?

I searched for “vlc”, moved to the last set of vulnerabilities

Answer: **CVE-2007-0017**



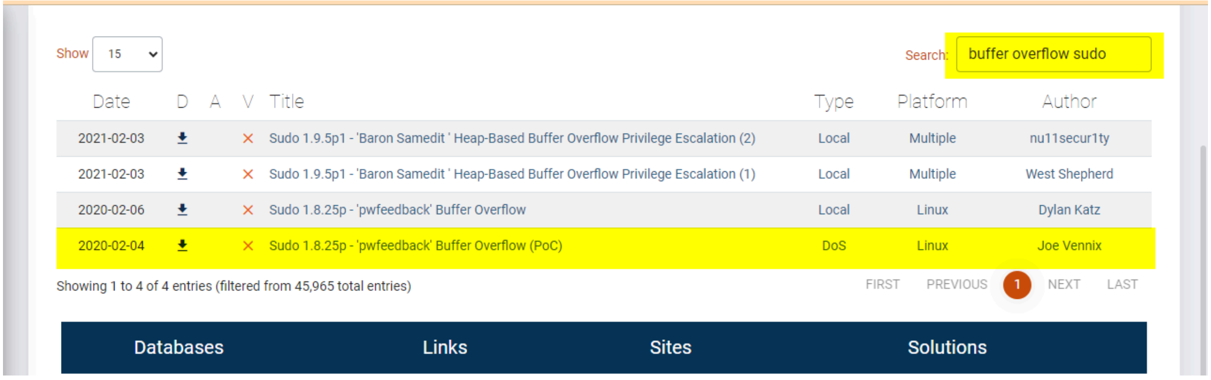
Date	D	A	V	Title	Type	Platform	Author
2008-08-23	⬇		✓	VideoLAN VLC Media Player 0.8.6i - Mms Protocol Handling Heap Overflow (PoC)	DoS	Multiple	g_
2008-08-16	⬇	▣	✓	VideoLAN VLC Media Player 0.8.6i - '.tta' File Parsing Heap Overflow (PoC)	DoS	Multiple	g_
2008-07-12	⬇		✓	Avlc Forum - 'vlc_forum.php' SQL Injection	WebApps	PHP	CWH Underground
2008-05-23	⬇	▣	✓	VideoLAN VLC Media Player 0.8.6d SSA Parsing Double Sh311 - Universal	Local	Windows	j0rgan
2008-04-28	⬇	▣	✓	VideoLAN VLC Media Player 0.8.6d - 'httpd_FileCallBack' Remote Format String	Remote	Windows	EpiBite
2008-03-14	⬇	▣	✓	VideoLAN VLC Media Player 0.8.6e - Subtitle Parsing Local Buffer Overflow	Local	Windows	Mai Xuan Cuong
2007-12-04	⬇	▣	✓	VideoLAN VLC Media Player 0.86 < 0.86d - ActiveX Remote Bad Pointer Initialization	DoS	Windows	Ricardo Narvaja
2007-01-12	⬇	▣	✓	VideoLAN VLC Media Player 0.8.6a - Denial of Service (1)	DoS	Windows	shinnai
2007-01-02	⬇	▣	✓	VideoLAN VLC Media Player 0.8.6 (x86) - 'udp://' Format String	Local	OSX	MoAB
2007-01-02	⬇	▣	✓	VideoLAN VLC Media Player 0.8.6 (PPC) - 'udp://' Format String (PoC)	DoS	OSX	MoAB

Showing 61 to 70 of 70 entries (filtered from 45,965 total entries)

If you wanted to exploit a 2020 buffer overflow in the sudo program, which CVE would you use?

I searched for “buffer overflow sudo”, looked at the one in 2020

Answer: CVE-2019-18634



Date	D	A	V	Title	Type	Platform	Author
2021-02-03	⬇		✗	Sudo 1.9.5p1 - 'Baron Samedit ' Heap-Based Buffer Overflow Privilege Escalation (2)	Local	Multiple	nu11secur1ty
2021-02-03	⬇		✗	Sudo 1.9.5p1 - 'Baron Samedit ' Heap-Based Buffer Overflow Privilege Escalation (1)	Local	Multiple	West Shepherd
2020-02-06	⬇		✗	Sudo 1.8.25p - 'pwfeedback' Buffer Overflow	Local	Linux	Dylan Katz
2020-02-04	⬇		✗	Sudo 1.8.25p - 'pwfeedback' Buffer Overflow (PoC)	DoS	Linux	Joe Vennix

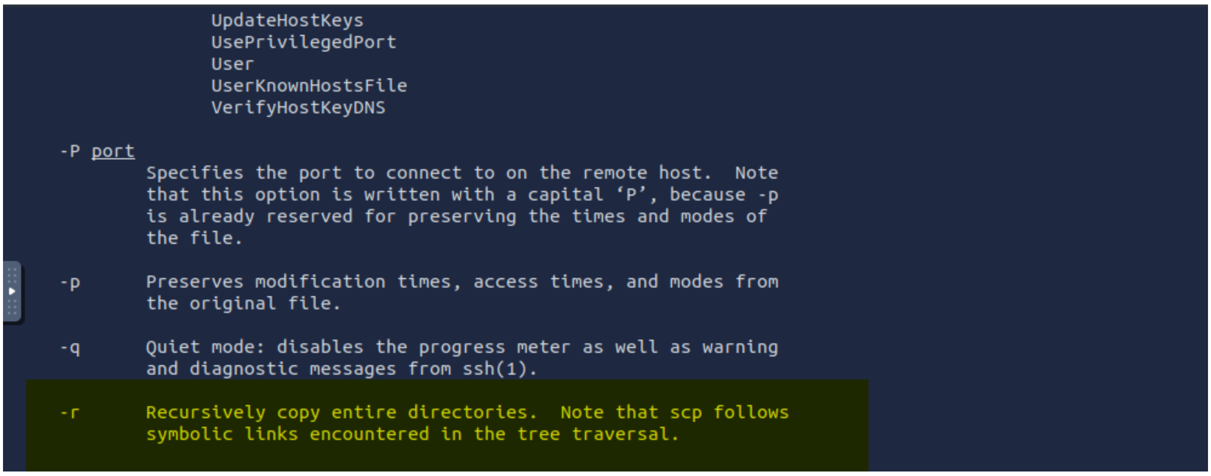
Showing 1 to 4 of 4 entries (filtered from 45,965 total entries)

Task 4 Manual Pages

SCP is a tool used to copy files from one computer to another. *What switch would you use to copy an entire directory?*

On my terminal, i checked the manual page for scp

Command: man scp
Answer: -r



```
                   UpdateHostKeys
                   UsePrivilegedPort
                   User
                   UserKnownHostsFile
                   VerifyHostKeyDNS

     -P port
             Specifies the port to connect to on the remote host.  Note
             that this option is written with a capital ‘P’, because -p
             is already reserved for preserving the times and modes of
             the file.

     -p      Preserves modification times, access times, and modes from
             the original file.

     -q      Quiet mode: disables the progress meter as well as warning
             and diagnostic messages from ssh(1).

     -r      Recursively copy entire directories.  Note that scp follows
             symbolic links encountered in the tree traversal.
```

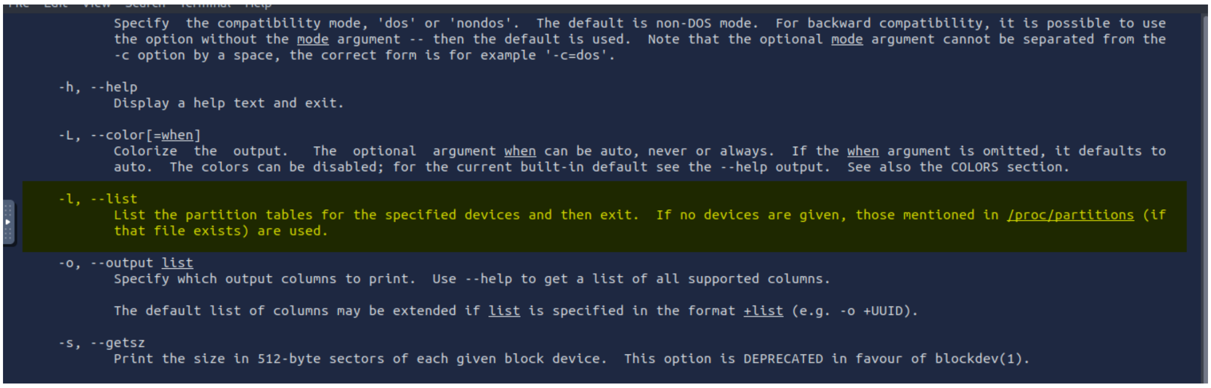
fdisk is a command used to view and alter the partitioning scheme used on your hard drive.

What switch would you use to list the current partitions?

On my terminal, i checked the manual page for fdisk

Command: man fdisk

Answer: -l



```
              Specify  the compatibility mode, 'dos' or 'nondos'.  The default is non-DOS mode.  For backward compatibility, it is possible to use
              the option without the mode argument -- then the default is used.  Note that the optional mode argument cannot be separated from the
              -c option by a space, the correct form is for example '-c=dos'.

       -h, --help
              Display a help text and exit.

       -L, --color[=when]
              Colorize  the  output.   The  optional  argument when can be auto, never or always.  If the when argument is omitted, it defaults to
              auto.  The colors can be disabled; for the current built-in default see the --help output.  See also the COLORS section.

       -l, --list
              List the partition tables for the specified devices and then exit.  If no devices are given, those mentioned in /proc/partitions (if
              that file exists) are used.

       -o, --output list
              Specify which output columns to print.  Use --help to get a list of all supported columns.

              The default list of columns may be extended if list is specified in the format +list (e.g. -o +UUID).

       -s, --getsz
              Print the size in 512-byte sectors of each given block device.  This option is DEPRECATED in favour of blockdev(1).
```

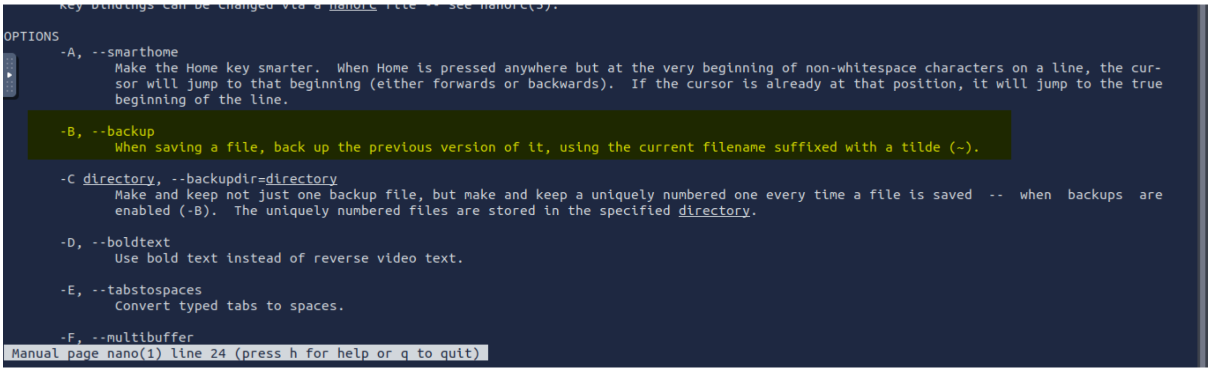
nano is an easy-to-use text editor for Linux. There are arguably better editors (Vim, being the obvious choice); however, nano is a great one to start with.

What switch would you use to make a backup when opening a file with nano?

On my terminal, i checked the manual page for nano

Command: man nano

Answer: -B



```
       key bindings can be changed via a nanorc file -- see nanorc(5).

OPTIONS
       -A, --smarthome
              Make the Home key smarter.  When Home is pressed anywhere but at the very beginning of non-whitespace characters on a line, the cur-
              sor will jump to that beginning (either forwards or backwards).  If the cursor is already at that position, it will jump to the true
              beginning of the line.

       -B, --backup
              When saving a file, back up the previous version of it, using the current filename suffixed with a tilde (~).

       -C directory, --backupdir=directory
              Make and keep not just one backup file, but make and keep a uniquely numbered one every time a file is saved  --  when  backups  are
              enabled (-B).  The uniquely numbered files are stored in the specified directory.

       -D, --boldtext
              Use bold text instead of reverse video text.

       -E, --tabstospaces
              Convert typed tabs to spaces.

       -F, --multibuffer
 Manual page nano(1) line 24 (press h for help or q to quit)
```

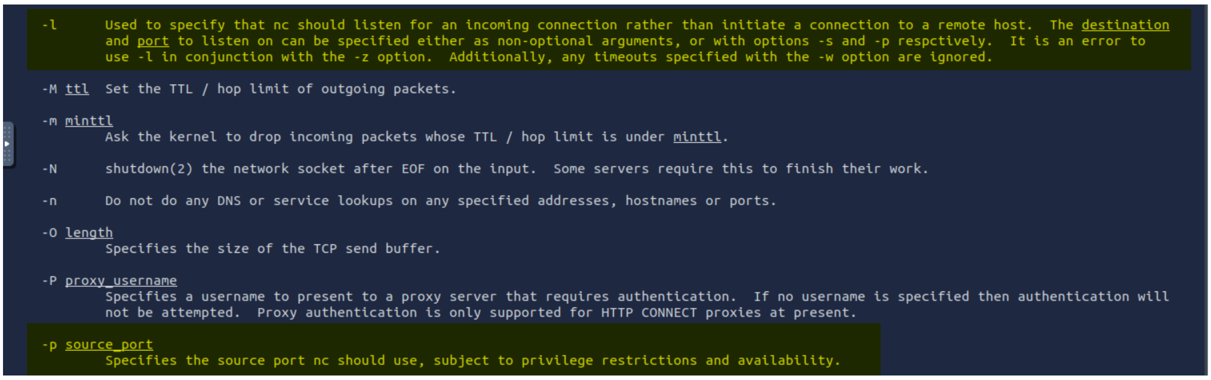
Netcat is a basic tool used to manually send and receive network requests.
What command would you use to start netcat in listen mode, using port 12345?

On my terminal, i checked the manual page for netcat

Command: man netcat

Sample: nc -l -p port [-options] [hostname] [port]

Answer: nc -l -p 12345



```
     -l      Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host.  The destination
             and port to listen on can be specified either as non-optional arguments, or with options -s and -p respctively.  It is an error to
             use -l in conjunction with the -z option.  Additionally, any timeouts specified with the -w option are ignored.

     -M ttl  Set the TTL / hop limit of outgoing packets.

     -m minttl
             Ask the kernel to drop incoming packets whose TTL / hop limit is under minttl.

     -N      shutdown(2) the network socket after EOF on the input.  Some servers require this to finish their work.

     -n      Do not do any DNS or service lookups on any specified addresses, hostnames or ports.

     -O length
             Specifies the size of the TCP send buffer.

     -P proxy_username
             Specifies a username to present to a proxy server that requires authentication.  If no username is specified then authentication will
             not be attempted.  Proxy authentication is only supported for HTTP CONNECT proxies at present.

     -p source_port
             Specifies the source port nc should use, subject to privilege restrictions and availability.
```

END!!!