```
8 - Search output
9 - Exit
9
... Date collection log: ...
... Script ended on: Sat May 17 11:45:47 EDT 2025 ...

┌──(kali㉿kali)-[~/Desktop/Penetration Testing]
└─$ sudo ./project3.1.sh
... MENU ...
... Network Address: None     ...
... Output Directory Name: None     ...
... Password list: Default - rockyou     ...
... type the number to execute: ...
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Address
4 - Change output directory name
5 - Basic scan (TCP, UDP, services versions, weak passwords)
6 - Full scan (NSE, weak passwords, vulnerability analysis)
7 - Password list options
8 - Search output
9 - Exit
3
Please type a network address, for example 127.0.0.11
127.0.1.1
Default output directory name is "127.0.1.1_output". would you like to change it? (Y/N)
n
... MENU ...
... Network Address: 127.0.1.1     ...
... Output Directory Name: 127.0.1.1_output     ...
... Password list: Default - rockyou     ...
... type the number to execute: ...
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Address
4 - Change output directory name
5 - Basic scan (TCP, UDP, services versions, weak passwords)
6 - Full scan (NSE, weak passwords, vulnerability analysis)
7 - Password list options
8 - Search output
9 - Exit
4
Please insert your preferred name for the directory:
metasploit output
... MENU ...
... Network Address: 127.0.1.1     ...
... Output Directory Name: metasploit output     ...
... Password list: Default - rockyou     ...
... type the number to execute: ...
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Address
4 - Change output directory name
5 - Basic scan (TCP, UDP, services versions, weak passwords)
6 - Full scan (NSE, weak passwords, vulnerability analysis)
7 - Password list options
8 - Search output
9 - Exit
```

1

2

3

4

5

6

PENETRATION TESTING | PROJECT: VULNER

Project Structure

1. Getting the User Input

1.1 Get from the user a network to scan.
1.2 Get from the user a name for the output directory.
1.3 Allow the user to choose '**Basic**' or '**Full**'.
1.3.1 **Basic:** scans the network for TCP and UDP, including the service version and weak passwords.
1.3.2 **Full:** include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.
1.4 Make sure the input is valid.

2. Weak Credentials

2.1 Look for weak passwords used in the network for login services.
2.1.1 Have a built-in password.lst to check for weak passwords.
2.1.2 Allow the user to supply their own password list.
2.2 Login services to check include: SSH, RDP, FTP, and TELNET.

3. Mapping Vulnerabilities

3.1 Mapping vulnerabilities should only take place if **Full** was chosen.
3.2 Display potential vulnerabilities via NSE and Searchsploit.

4. Log Results

4.1 During each stage, display the stage in the terminal.
4.2 At the end, show the user the found information.
4.3 Allow the user to search inside the results.
4.4 Allow to save all results into a Zip file.

5. Creativity

General

- Suggested tools: Nmap, Hydra, Medusa, Searchsploit.
- Everything other than the user input should be automated.
- Use functions.

Comments

Use comments in your code to explain what you did.
If you are using code from the internet, add credit and links.
In the script, write the student's name and code, the class code, and the lecturer's name.

```
# 1.3 + 1.3.1 Basic scan (TCP, UDP, Service versions, trying weak passwords)
# 4.4 Option to zip results
BasicScn() {
    local masscan_file nmout outfile hosts host \
          tcp_ports udp_ports portspec zip_file choice

    # 0. Prepare output file
    [[ ! -d "$OUTPUT" ]] && mkdir -p "$OUTPUT"
    outfile="$OUTPUT/${NTADR}_basic.txt"
    : > "$outfile"
    echo "Basic scan results for network $NTADR" >> "$outfile"

    # 1. Fast TCP+UDP discovery with masscan
    masscan_file="$OUTPUT/${NTADR}_masscan.txt"
    echo -e "\e[95m... Performing fast TCP+UDP discovery on $NTADR with masscan ...\e[0m"
    log_message "Starting masscan on $NTADR"
    sudo masscan "$NTADR" -p1-1000,U:1-1000 --rate=1000 -oL "$masscan_file"

    # 2. Parse Masscan for unique hosts
    hosts=( $(awk '$1=="open" {print $4}' "$masscan_file" | sort -u) )
    if [[ ${#hosts[@]} -eq 0 ]]; then
        echo -e "\e[91m... No hosts with open ports found in $NTADR ...\e[0m"
        return
    fi
    echo -e "\e[95m... Hosts with open ports: ${hosts[*]} ...\e[0m"
    log_message "Hosts discovered via masscan: ${hosts[*]}"

    # 3. Deeper Nmap + Hydra per host
    for host in "${hosts[@]}"; do
        echo -e "\e[95m... Starting deeper scan on $host ...\e[0m"
        log_message "Nmap version scan on $host"
        echo "Host: $host" >> "$outfile"

        # build port lists
        tcp_ports=$(awk -v h="$host" '$1=="open" && $4==h && $2=="tcp" {print $3}' \
                    "$masscan_file" | paste -sd, -)
        udp_ports=$(awk -v h="$host" '$1=="open" && $4==h && $2=="udp" {print $3}' \
                    "$masscan_file" | paste -sd, -)

        portspec=""
        [[ -n "$tcp_ports" ]] && portspec="$tcp_ports"
        [[ -n "$udp_ports" ]] && portspec+="${portspec:+,}U:$udp_ports"

        if [[ -z "$portspec" ]]; then
            echo -e "\e[91m... No open ports on $host ...\e[0m"
            echo "No open ports on $host" >> "$outfile"
            continue
        fi

        nmout=$(mktemp)
        nmap -sTU -sV -p"$portspec" "$host" -oG "$nmout"
        log_message "Nmap output for $host saved to $nmout"

        # parse Nmap results
        grep '/open/' "$nmout" \
          | sed -e 's/.*Ports: //' -e 's/, /\n/g' \
          | while IFS= read -r entry; do
              IFS='/' read -r port _ proto _ service _ version <<<"$entry"

              # record service presence (no version echo)
              echo "Found $service on port $port/$proto" >> "$outfile"

              if [[ "$proto" == "tcp" ]]; then
                  echo -e "\e[95m... Trying login on $service/$port ...\e[0m"
                  hydra -C "$PWLDir" -s "$port" "$service"://"$host" \
                        -f -o "${nmout}_hydra" &>/dev/null

                  if [ -s "${nmout}_hydra" ]; then
                      while read -r cred; do
                          echo -e "\e[95m... SUCCESS: $service/$port [] $cred\e[0m"
                          echo "[$service @ $port] SUCCESS: $cred" >> "$outfile"
                      done < "${nmout}_hydra"
                      log_message "Valid credentials for $service on $port of $host"
                  else
                      echo -e "\e[91m... FAIL: no valid creds for $service/$port\e[0m"
                      echo "[$service @ $port] FAIL: no valid credentials" >> "$outfile"
                  fi
                  rm -f "${nmout}_hydra"
              fi
          done

        rm -f "$nmout"
        echo >> "$outfile"
    done
```

```
... Performing fast TCP+UDP discovery on 192.168.132.132 with masscan ...
./project3.2.sh: line 15: /var/log/project3.log: Permission denied
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-05-23 18:35:05 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [2000 ports/host]
... Hosts with open ports: 192.168.132.132 ...
./project3.2.sh: line 15: /var/log/project3.log: Permission denied
... Starting deeper scan on 192.168.132.132 ...
./project3.2.sh: line 15: /var/log/project3.log: Permission denied
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 14:35 EDT
WARNING: Duplicate port number(s) specified.  Are you alert enough to be using Nmap?  Ha
ve some coffee or Jolt(tm).
Nmap scan report for 192.168.132.132
Host is up (0.0017s latency).

PORT    STATE  SERVICE      VERSION
21/tcp  open   ftp          vsftpd 2.3.4
22/tcp  open   ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp  open   telnet       Linux telnetd
25/tcp  open   smtp         Postfix smtpd
53/tcp  open   domain       ISC BIND 9.4.2
80/tcp  open   http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open   rpcbind      2 (RPC #100000)
139/tcp open   netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open   netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open   exec         netkit-rsh rexecd
513/tcp open   login        OpenBSD or Solaris rlogind
514/tcp open   tcpwrapped
21/udp  closed ftp
22/udp  closed ssh
23/udp  closed telnet
25/udp  closed smtp
53/udp  open   domain       ISC BIND 9.4.2
80/udp  closed http
111/udp open   rpcbind      2 (RPC #100000)
137/udp open   netbios-ns   Microsoft Windows netbios-ns (workgroup: WORKGROUP)
139/udp closed netbios-ssn
445/udp closed microsoft-ds
512/udp closed biff
513/udp closed who
514/udp closed syslog
MAC Address: 00:0C:29:71:CA:8D (VMware)
Service Info: Hosts:  metasploitable.localdomain, METASPLOITABLE; OSs: Unix, Linux, Wind
ows; CPE: cpe:/o:linux:linux_kernel, cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.87 seconds
./project3.2.sh: line 15: /var/log/project3.log: Permission denied
... Trying login on ftp/21 ...
... FAIL: no valid creds for ftp/21
... Trying login on ssh/22 ...
... FAIL: no valid creds for ssh/22
... Trying login on telnet/23 ...
... FAIL: no valid creds for telnet/23
... Trying login on smtp/25 ...
... FAIL: no valid creds for smtp/25
... Trying login on domain/53 ...
... FAIL: no valid creds for domain/53
... Trying login on http/80 ...
... FAIL: no valid creds for http/80
... Trying login on rpcbind/111 ...
... FAIL: no valid creds for rpcbind/111
... Trying login on netbios-ssn/139 ...
... FAIL: no valid creds for netbios-ssn/139
... Trying login on netbios-ssn/445 ...
... FAIL: no valid creds for netbios-ssn/445
... Trying login on exec/512 ...
... FAIL: no valid creds for exec/512
... Trying login on login/513 ...
... FAIL: no valid creds for login/513
... Trying login on tcpwrapped/514 ...
```

1

2

3

4

5

6

PENETRATION TESTING | PROJECT: VULNER

Project Structure

1. Getting the User Input

- 1.1 Get from the user a network to scan.
- 1.2 Get from the user a name for the output directory.
- 1.3 Allow the user to choose **'Basic'** or **'Full'**.
- 1.3.1 **Basic:** scans the network for TCP and UDP, including the service version and weak passwords.
- 1.3.2 **Full:** include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.
- 1.4 Make sure the input is valid.

2. Weak Credentials

- 2.1 Look for weak passwords used in the network for login services.
- 2.1.1 Have a built-in password.lst to check for weak passwords.
- 2.1.2 Allow the user to supply their own password list.
- 2.2 Login services to check include: SSH, RDP, FTP, and TELNET.

3. Mapping Vulnerabilities

- 3.1 Mapping vulnerabilities should only take place if **Full** was chosen.
- 3.2 Display potential vulnerabilities via NSE and Searchsploit.

4. Log Results

- 4.1 During each stage, display the stage in the terminal.
- 4.2 At the end, show the user the found information.
- 4.3 Allow the user to search inside the results.
- 4.4 Allow to save all results into a Zip file.

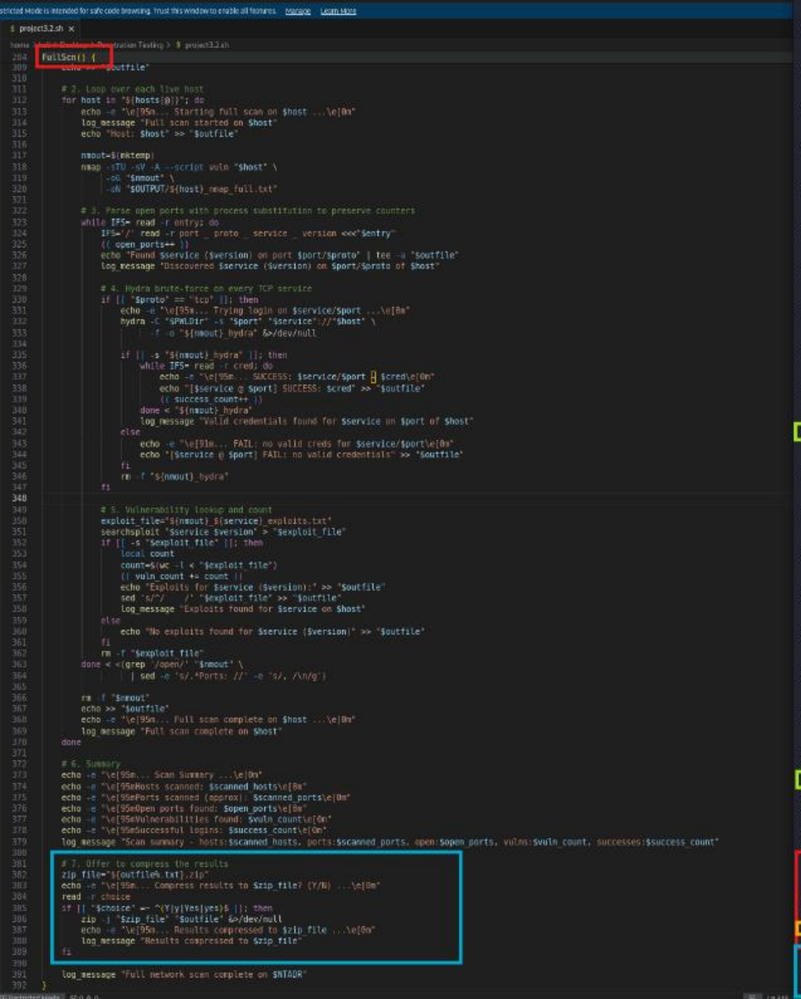
5. Creativity

General

- Suggested tools: Nmap, Hydra, Medusa, Searchsploit.
- Everything other than the user input should be automated.
- Use functions.

Comments

Use comments in your code to explain what you did.
If you are using code from the internet, add credit and links.
In the script, write the student's name and code, the class code, and the lecturer's name.



```
File  Actions  Edit  View  Help
Found http (Apache httpd 2.2.8 ((Ubuntu) DAV/2)) on port 80/tcp
... Trying login on http/80 ...
... FAIL: no valid creds for http/80
Found rpcbind (2 (RPC #100000)) on port 111/tcp
... Trying login on rpcbind/111 ...
... FAIL: no valid creds for rpcbind/111
Found netbios-ssn (Samba smbd 3.X - 4.X (workgroup: WORKGROUP)) on port 139/tcp
... Trying login on netbios-ssn/139 ...
... FAIL: no valid creds for netbios-ssn/139
Found netbios-ssn (Samba smbd 3.X - 4.X (workgroup: WORKGROUP)) on port 445/tcp
... Trying login on netbios-ssn/445 ...
... FAIL: no valid creds for netbios-ssn/445
Found exec (netkit-rsh rexecd) on port 512/tcp
... Trying login on exec/512 ...
... FAIL: no valid creds for exec/512
Found login (OpenBSD or Solaris rlogind) on port 513/tcp
... Trying login on login/513 ...
... FAIL: no valid creds for login/513
Found tcpwrapped () on port 514/tcp
... Trying login on tcpwrapped/514 ...
... FAIL: no valid creds for tcpwrapped/514
Found java-rmi (GNU Classpath grmiregistry) on port 1099/tcp
... Trying login on java-rmi/1099 ...
... FAIL: no valid creds for java-rmi/1099
Found bindshell (Metasploitable root shell) on port 1524/tcp
... Trying login on bindshell/1524 ...
... FAIL: no valid creds for bindshell/1524
Found nfs (2-4 (RPC #100003)) on port 2049/tcp
... Trying login on nfs/2049 ...
... FAIL: no valid creds for nfs/2049
Found ftp (ProFTPD 1.3.1) on port 2121/tcp
... Trying login on ftp/2121 ...
... FAIL: no valid creds for ftp/2121
Found mysql (MySQL 5.0.51a-3ubuntu5) on port 3306/tcp
... Trying login on mysql/3306 ...
... FAIL: no valid creds for mysql/3306
Found postgresql (PostgreSQL DB 8.3.0 - 8.3.7) on port 5432/tcp
... Trying login on postgresql/5432 ...
... FAIL: no valid creds for postgresql/5432
Found vnc (VNC (protocol 3.3)) on port 5900/tcp
... Trying login on vnc/5900 ...
... FAIL: no valid creds for vnc/5900
Found X11 ((access denied)) on port 6000/tcp
... Trying login on X11/6000 ...
... FAIL: no valid creds for X11/6000
Found irc (UnrealIRCd) on port 6667/tcp
... Trying login on irc/6667 ...
... FAIL: no valid creds for irc/6667
Found ajp13 (Apache Jserv (Protocol v1.3)) on port 8009/tcp
... Trying login on ajp13/8009 ...
... FAIL: no valid creds for ajp13/8009
Found http (Apache Tomcat|Coyote JSP engine 1.1) on port 8180/tcp
... Trying login on http/8180 ...
... FAIL: no valid creds for http/8180
Found domain (ISC BIND 9.4.2) on port 53/udp
Found dhcpc () on port 68/udp
Found tftp () on port 69/udp
Found rpcbind (2 (RPC #100000)) on port 111/udp
Found netbios-ns (Microsoft Windows netbios-ns (workgroup: WORKGROUP)) on port 137/udp
Found netbios-dgm () on port 138/udp
Found nfs (2-4 (RPC #100003)/   Ignored State: closed (1970)    OS: Linux 2.6.9 - 2.6.33
Seq Index: 203  IP ID Seq: All zeros) on port 2049/udp
... Full scan complete on 192.168.132.132 ...
... Scan Summary ...
Hosts scanned: 1
Ports scanned (approx): 3000
Open ports found: 70
Vulnerabilities found: 200
Successful logins: 0
... Compress results to 192.168.132.132_output/192.168.132.132_full.zip? (Y/N) ...
y
... Results compressed to 192.168.132.132_output/192.168.132.132_full.zip ...
```

1

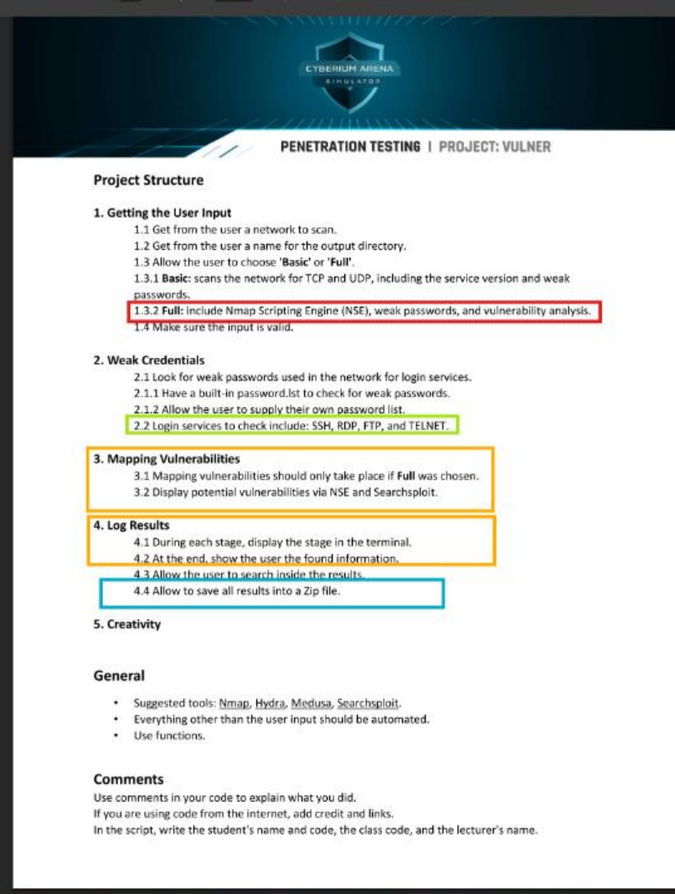
2

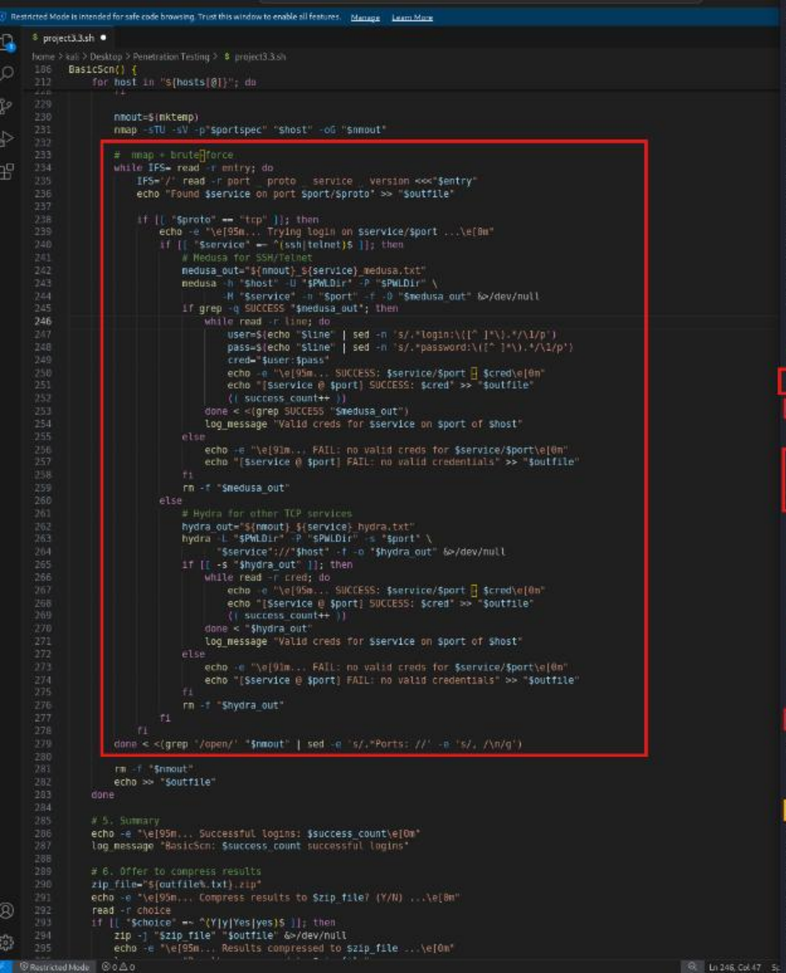
3

4

5

6





```
Restricted Mode is intended for safe code browsing. Trust this window to enable all features.  Manage  Learn More

$ project3.3.sh ●

home > kali > Desktop > Penetration Testing > $ project3.3.sh

BasicScn() {
    for host in "${hosts[@]}"; do

        nmout=$(mktemp)
        nmap -sTU -sV -p"$portspec" "$host" -oG "$nmout"

        #  nmap + brute force
        while IFS= read -r entry; do
            IFS=' ' read -r port  proto  service  version <<<"$entry"
            echo "Found $service on port $port/$proto" >> "$outfile"

            if [[ "$proto" == "tcp" ]]; then
                echo -e "\e[95m... Trying login on $service/$port ...\e[0m"
                if [[ "$service" =~ ^(ssh|telnet)$ ]]; then
                    # Medusa for SSH/Telnet
                    medusa_out="${nmout}_${service}_medusa.txt"
                    medusa -h "$host" -U "$PWLDir" -P "$PWLDir" \
                           -M "$service" -n "$port" -f -0 "$medusa_out" &>/dev/null
                    if grep -q SUCCESS "$medusa_out"; then
                        while read -r line; do
                            user=$(echo "$line" | sed -n 's/.*login:\([^ ]*\).*/\1/p')
                            pass=$(echo "$line" | sed -n 's/.*password:\([^ ]*\).*/\1/p')
                            cred="$user:$pass"
                            echo -e "\e[95m... SUCCESS: $service/$port $cred\e[0m"
                            echo "[$service @ $port] SUCCESS: $cred" >> "$outfile"
                            (( success_count++ ))
                        done < <(grep SUCCESS "$medusa_out")
                        log_message "Valid creds for $service on $port of $host"
                    else
                        echo -e "\e[91m... FAIL: no valid creds for $service/$port\e[0m"
                        echo "[$service @ $port] FAIL: no valid credentials" >> "$outfile"
                    fi
                    rm -f "$medusa_out"
                else
                    # Hydra for other TCP services
                    hydra_out="${nmout}_${service}_hydra.txt"
                    hydra -L "$PWLDir" -P "$PWLDir" -s "$port" \
                          "$service"://"$host" -f -o "$hydra_out" &>/dev/null
                    if [[ -s "$hydra_out" ]]; then
                        while read -r cred; do
                            echo -e "\e[95m... SUCCESS: $service/$port $cred\e[0m"
                            echo "[$service @ $port] SUCCESS: $cred" >> "$outfile"
                            (( success_count++ ))
                        done < "$hydra_out"
                        log_message "Valid creds for $service on $port of $host"
                    else
                        echo -e "\e[91m... FAIL: no valid creds for $service/$port\e[0m"
                        echo "[$service @ $port] FAIL: no valid credentials" >> "$outfile"
                    fi
                    rm -f "$hydra_out"
                fi
            fi
        done < <(grep '/open/' "$nmout" | sed -e 's/,*Ports: //' -e 's/, /\n/g')

        rm -f "$nmout"
        echo >> "$outfile"
    done

    # 5. Summary
    echo -e "\e[95m... Successful logins: $success_count\e[0m"
    log_message "BasicScn: $success_count successful logins"

    # 6. Offer to compress results
    zip_file="${outfile%.txt}.zip"
    echo -e "\e[95m... Compress results to $zip_file? (Y/N) ...\e[0m"
    read -r choice
    if [[ "$choice" =~ ^(Y|y|Yes|yes)$ ]]; then
        zip -j "$zip_file" "$outfile" &>/dev/null
        echo -e "\e[95m... Results compressed to $zip_file ...\e[0m"

Restricted Mode  ⊗ 0 △ 0                                                    Ln 248, Col 47  Sp
```

```
File  Actions  Edit  View  Help
513/tcp open   login       OpenBSD or Solaris rlogind
514/tcp open   tcpwrapped
21/udp  closed ftp
22/udp  closed ssh
23/udp  closed telnet
25/udp  closed smtp
53/udp  open   domain      ISC BIND 9.4.2
80/udp  closed http
111/udp open   rpcbind     2 (RPC #100000)
137/udp open   netbios-ns  Microsoft Windows netbios-ns (workgroup: WORKGROUP)
139/udp closed netbios-ssn
445/udp closed microsoft-ds
512/udp closed biff
513/udp closed who
514/udp closed syslog
MAC Address: 08:0C:29:71:CA:8D (VMware)
Service Info: Hosts:  metasploitable.localdomain, METASPLOITABLE; OSs: Unix, Linux, Wind
ows; CPE: cpe:/o:linux:linux_kernel, cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.87 seconds
... Trying login on ftp/21 ...
... SUCCESS: ftp/21 + # Hydra v9.5 run at 2025-05-28 15:13:52 on 192.168.132.132 ftp (hy
dra -L /home/kali/Desktop/Penetration Testing/Basic_PWList.txt -P /home/kali/Desktop/Pen
etration Testing/Basic_PWList.txt -s 21 -f -o /tmp/tmp.ynltACWpMy_ftp_hydra.txt ftp://19
2.168.132.132)
... SUCCESS: ftp/21 + [21][ftp] host: 192.168.132.132   login: 1111   password: 1234
... Trying login on ssh/22 ...
... SUCCESS: ssh/22 + [
... Trying login on telnet/23 ...
... FAIL: no valid creds for telnet/23
... Trying login on smtp/25 ...
... SUCCESS: smtp/25 + # Hydra v9.5 run at 2025-05-28 15:13:56 on 192.168.132.132 smtp (
hydra -L /home/kali/Desktop/Penetration Testing/Basic_PWList.txt -P /home/kali/Desktop/P
enetration Testing/Basic_PWList.txt -s 25 -f -o /tmp/tmp.ynltACWpMy_smtp_hydra.txt smtp:
//192.168.132.132)
... Trying login on domain/53 ...
... FAIL: no valid creds for domain/53
... Trying login on http/80 ...
... FAIL: no valid creds for http/80
... Trying login on rpcbind/111 ...
... FAIL: no valid creds for rpcbind/111
... Trying login on netbios-ssn/139 ...
... FAIL: no valid creds for netbios-ssn/139
... Trying login on netbios-ssn/445 ...
... FAIL: no valid creds for netbios-ssn/445
... Trying login on exec/512 ...
... FAIL: no valid creds for exec/512
... Trying login on login/513 ...
... FAIL: no valid creds for login/513
... Trying login on tcpwrapped/514 ...
... FAIL: no valid creds for tcpwrapped/514
... Successful logins: 4
... Compress results to 192.168.132.132_output/192.168.132.132_basic.zip? (Y/N) ...
y
... Results compressed to 192.168.132.132_output/192.168.132.132_basic.zip ...
... MENU ...
... Network Address: 192.168.132.132
... Output Directory Name: 192.168.132.132_output
... Password List: Basic
... Type the number to execute:
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Address
4 - Change output directory name
5 - Basic scan (TCP, UDP, services versions, weak passwords)
6 - Full scan (NSE, weak passwords, vulnerability analysis)
7 - Password list options
8 - Search output
9 - Exit
```

1

2

3

4

5

6

PENETRATION TESTING | **PROJECT: VULNER**

Project Structure

1. Getting the User Input

- 1.1 Get from the user a network to scan.
- 1.2 Get from the user a name for the output directory.
- 1.3 Allow the user to choose '**Basic**' or '**Full**'.
- 1.3.1 **Basic:** scans the network for TCP and UDP, including the service version and weak passwords.
- 1.3.2 **Full:** include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.
- 1.4 Make sure the input is valid.

2. Weak Credentials

- 2.1 Look for weak passwords used in the network for login services.
- 2.1.1 Have a built-in password.lst to check for weak passwords.
- 2.1.2 Allow the user to supply their own password list.
- 2.2 Login services to check include: SSH, RDP, FTP, and TELNET.

3. Mapping Vulnerabilities

- 3.1 Mapping vulnerabilities should only take place if **Full** was chosen.
- 3.2 Display potential vulnerabilities via NSE and Searchsploit.

4. Log Results

- 4.1 During each stage, display the stage in the terminal.
- 4.2 At the end, show the user the found information.
- 4.3 Allow the user to search inside the results.
- 4.4 Allow to save all results into a Zip file.

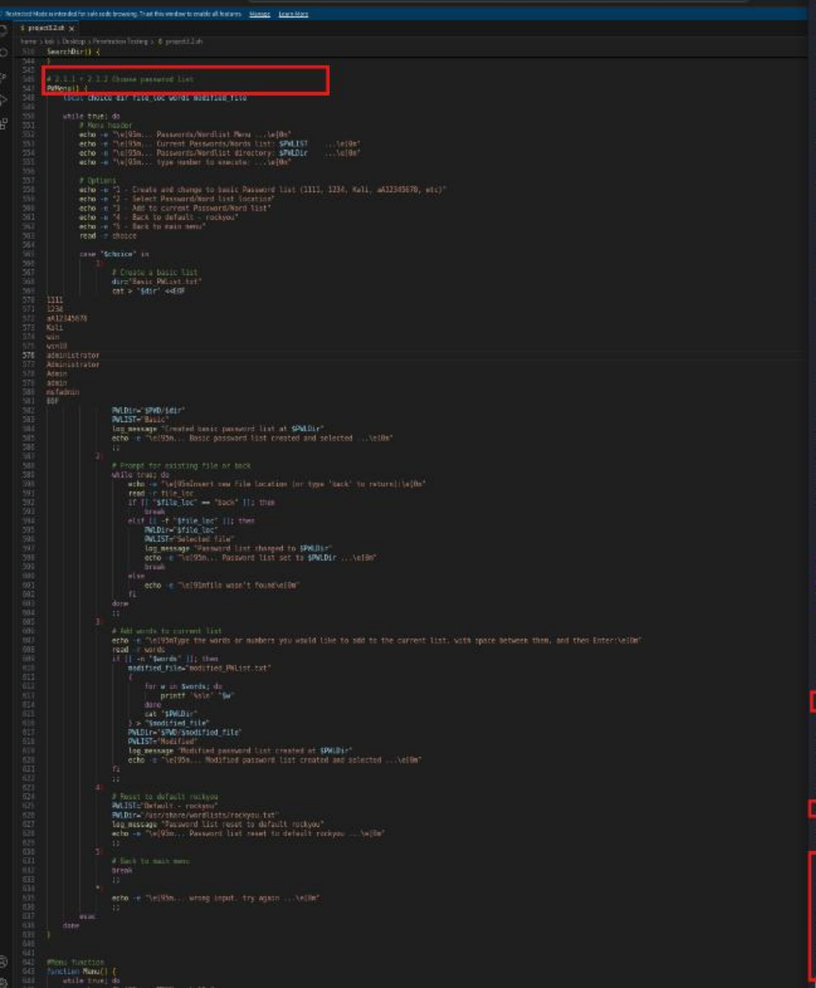
5. Creativity

General

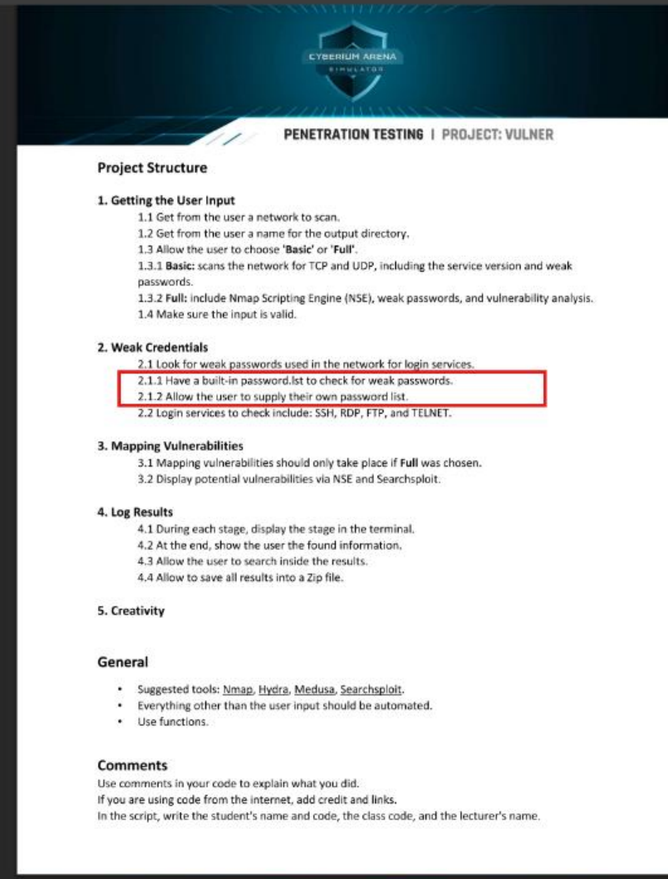
- Suggested tools: Nmap, Hydra, Medusa, Searchsploit.
- Everything other than the user input should be automated.
- Use functions.

Comments

Use comments in your code to explain what you did.
If you are using code from the internet, add credit and links.
In the script, write the student's name and code, the class code, and the lecturer's name.



```
File  Actions  Edit  View  Help
... Trying login on bindshell/1524 ...
... FAIL: no valid creds for bindshell/1524
Found nfs (2-4 (RPC #100003)) on port 2049/tcp
... Trying login on nfs/2049 ...
... FAIL: no valid creds for nfs/2049
Found ftp (ProFTPD 1.3.1) on port 2121/tcp
... Trying login on ftp/2121 ...
... FAIL: no valid creds for ftp/2121
Found mysql (MySQL 5.0.51a-3ubuntu5) on port 3306/tcp
... Trying login on mysql/3306 ...
... FAIL: no valid creds for mysql/3306
Found postgresql (PostgreSQL DB 8.3.0 - 8.3.7) on port 5432/tcp
... Trying login on postgresql/5432 ...
... FAIL: no valid creds for postgresql/5432
Found vnc (VNC (protocol 3.3)) on port 5900/tcp
... Trying login on vnc/5900 ...
... FAIL: no valid creds for vnc/5900
Found X11 ((access denied)) on port 6000/tcp
... Trying login on X11/6000 ...
... FAIL: no valid creds for X11/6000
Found irc (UnrealIRCd) on port 6667/tcp
... Trying login on irc/6667 ...
... FAIL: no valid creds for irc/6667
Found ajp13 (Apache Jserv (Protocol v1.3)) on port 8009/tcp
... Trying login on ajp13/8009 ...
... FAIL: no valid creds for ajp13/8009
Found http (Apache Tomcat|Coyote JSP engine 1.1) on port 8180/tcp
... Trying login on http/8180 ...
... FAIL: no valid creds for http/8180
Found domain (ISC BIND 9.4.2) on port 53/udp
Found dhcpc () on port 68/udp
Found tftp () on port 69/udp
Found rpcbind (2 (RPC #100000)) on port 111/udp
Found netbios-ns (Microsoft Windows netbios-ns (workgroup: WORKGROUP)) on port 137/udp
Found netbios-dgm () on port 138/udp
Found nfs (2-4 (RPC #100003)/   Ignored State: closed (1970)    OS: Linux 2.6.9 - 2.6.33
Seq Index: 203  IP ID Seq: All zeros) on port 2049/udp
... Full scan complete on 192.168.132.132 ...
... Scan Summary ...
Hosts scanned: 1
Ports scanned (approx): 2089
Open ports found: 30
Vulnerabilities found: 208
Successful logins: 0
... Compress results to 192.168.132.132_output/192.168.132.132_full.zip? (Y/N) ...
y
... Results compressed to 192.168.132.132_output/192.168.132.132_full.zip ...
... MENU ...
... Network Address: 192.168.132.132    ...
... Output directory Name: 192.168.132.132_output    ...
... Password list: Default - rockyou    ...
... Type the number to execute: ...
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Address
4 - Change output directory name
5 - Basic scan (TCP, UDP, services versions, weak passwords)
6 - Full scan (NSE, weak passwords, vulnerability analysis)
7 - Password list options
8 - Search output
9 - Exit
7
... Passwords/Wordlist Menu ...
... Current Passwords/Words list: Default - rockyou    ...
... Passwords/Wordlist directory: /usr/share/wordlists/rockyou.txt    ...
... type number to execute: ...
1 - Create and change to basic Password list (1111, 1234, Kali, aA12345678, etc)
2 - Select Password/Word list location
3 - Add to current Password/Word list
4 - Back to default - rockyou
5 - Back to main menu
```



CYBERIUM ARENA
SIMULATOR

PENETRATION TESTING | PROJECT: VULNER

Project Structure

1. Getting the User Input

- 1.1 Get from the user a network to scan.
- 1.2 Get from the user a name for the output directory.
- 1.3 Allow the user to choose **'Basic'** or **'Full'**.
- 1.3.1 **Basic:** scans the network for TCP and UDP, including the service version and weak passwords.
- 1.3.2 **Full:** include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.
- 1.4 Make sure the input is valid.

2. Weak Credentials

- 2.1 Look for weak passwords used in the network for login services.
- 2.1.1 Have a built-in password.lst to check for weak passwords.
- 2.1.2 Allow the user to supply their own password list.
- 2.2 Login services to check include: SSH, RDP, FTP, and TELNET.

3. Mapping Vulnerabilities

- 3.1 Mapping vulnerabilities should only take place if **Full** was chosen.
- 3.2 Display potential vulnerabilities via NSE and Searchsploit.

4. Log Results

- 4.1 During each stage, display the stage in the terminal.
- 4.2 At the end, show the user the found information.
- 4.3 Allow the user to search inside the results.
- 4.4 Allow to save all results into a Zip file.

5. Creativity

General

- Suggested tools: Nmap, Hydra, Medusa, Searchsploit.
- Everything other than the user input should be automated.
- Use functions.

Comments

Use comments in your code to explain what you did.
If you are using code from the internet, add credit and links.
In the script, write the student's name and code, the class code, and the lecturer's name.

```
# > /dev/null 2>&1

    # Proceed with the appropriate function based on OS type.
    if [[ "$os_type" == "Linux" ]]; then
        echo -e "\e[95m Linux OS detected via brute-force credentials!\e[0m"
        getInfoL "$found_user" "$ip" "$found_pass"
    elif [[ "$os_type" == "Windows" ]]; then
        echo -e "\e[95m Windows OS detected via brute-force credentials!\e[0m"
        getInfoW "$found_user" "$ip" "$found_pass"
    else
        echo -e "\e[31m Unknown OS detected via brute-force credentials. Exiting.\e[0m"
        log_message "Brute-force login succeeded on $ip but OS detection failed."
        rm -f "$temp_pwd_file" "$hydra_output_file"
        return 1
    fi

    # Clean up temporary files.
    rm -f "$temp_pwd_file" "$hydra_output_file"
}

# 4.3 Allow the user to search inside the resaults
SearchDir() {
    local search results

    # 1. Check if OUTPUT was set
    if [[ "$OUTPUT" == "None" ]]; then
        echo -e "\e[91m... No output directory name was selected ...\e[0m"
        return
    fi

    # 2. Check that the directory exists
    if [[ ! -d "$OUTPUT" ]]; then
        echo -e "\e[91m... Selected output directory \"$OUTPUT\" does not exist ...\e[0m"
        return
    fi

    # 2b. Check if it contains any files
    if [[ -z "$(ls -A "$OUTPUT")" ]]; then
        echo -e "\e[91m... Selected output directory is empty ...\e[0m"
        return
    fi

    # 3. Ask for the search term
    echo -e "\e[95m... Type your search: ...\e[0m"
    read -r search

    # Perform the search
    results=$(grep -R -n --color=always "$search" "$OUTPUT")

    if [[ -z "$results" ]]; then
        echo -e "\e[95m... No results found for \"$search\" ...\e[0m"
    else
        echo -e "\e[95m... Results for \"$search\": ...\e[0m"
        echo "$results"
    fi
}

# 2.1.1 + 2.1.2 Choose password list
PWMenu() {
    local choice dir file_loc words modified_file

    while true; do
        # Menu header
        echo -e "\e[95m... Passwords/Wordlist Menu ...\e[0m"
        echo -e "\e[95m... Current Passwords/Words list: $PWLIST    ...\e[0m"
        echo -e "\e[95m... Passwords/Wordlist directory: $PWLDir    ...\e[0m"
        echo -e "\e[95m... type number to execute: ...\e[0m"

        # Options
        echo -e "1 - Create and change to basic Password list (1111, 1234, Kali, aA12345678, etc)"
```

```
... Output Directory Name: 192.168.132.132_output     ...
... Password list: Default - rockyou     ...
... type the number to execute: ...
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Address
4 - Change output directory name
5 - Basic scan (TCP, UDP, services versions, weak passwords)
6 - Full scan (NSE, weak passwords, vulnerability analysis)
7 - Password list options
8 - Search output
9 - Exit
3
Please type a network address, for example 127.0.0.11
23
Invalid address - please try again. For example: 127.0.0.11
Please type a network address, for example 127.0.0.11
192.168.132.132
Default output directory name is "192.168.132.132_output". would you like to change it? (Y/N)
n
... MENU ...
... Network Address: 192.168.132.132     ...
... Output Directory Name: 192.168.132.132_output     ...
... Password list: Default - rockyou     ...
... type the number to execute: ...
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Address
4 - Change output directory name
5 - Basic scan (TCP, UDP, services versions, weak passwords)
6 - Full scan (NSE, weak passwords, vulnerability analysis)
7 - Password list options
8 - Search output
9 - Exit
ttt
... wrong number, try again ...
... MENU ...
... Network Address: 192.168.132.132     ...
... Output Directory Name: 192.168.132.132_output     ...
... Password list: Default - rockyou     ...
... type the number to execute: ...
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Address
4 - Change output directory name
5 - Basic scan (TCP, UDP, services versions, weak passwords)
6 - Full scan (NSE, weak passwords, vulnerability analysis)
7 - Password list options
8 - Search output
9 - Exit
8
... Type your search: ...
open
... Results for "open": ...
192.168.132.132_output/192.168.132.132_nmap_full.txt:6:21/tcp   open          ftp
  vsftpd 2.3.4
192.168.132.132_output/192.168.132.132_nmap_full.txt:28:22/tcp   open          ssh
   OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
192.168.132.132_output/192.168.132.132_nmap_full.txt:30:|   cpe:/a:openbsd:openssh:4.7p1
:
192.168.132.132_output/192.168.132.132_nmap_full.txt:145:23/tcp   open          telnet
   Linux telnetd
192.168.132.132_output/192.168.132.132_nmap_full.txt:146:25/tcp   open          smtp
   Postfix smtpd
192.168.132.132_output/192.168.132.132_nmap_full.txt:224:|_      https://www.openssl.org
/~bodo/ssl-poodle.pdf
192.168.132.132_output/192.168.132.132_nmap_full.txt:226:53/tcp   open          domain
   ISC BIND 9.4.2
192.168.132.132_output/192.168.132.132_nmap_full.txt:315:80/tcp   open          http
   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
192.168.132.132_output/192.168.132.132_nmap_full.txt:321:|       Slowloris tries to keep
```


1


2


3


4


5


6

PENETRATION TESTING | PROJECT: VULNER

Project Structure

1. Getting the User Input

1.1 Get from the user a network to scan.
1.2 Get from the user a name for the output directory.
1.3 Allow the user to choose '**Basic**' or '**Full**'.
1.3.1 **Basic:** scans the network for TCP and UDP, including the service version and weak passwords.
1.3.2 **Full:** include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.
1.4 Make sure the input is valid.

2. Weak Credentials

2.1 Look for weak passwords used in the network for login services.
2.1.1 Have a built-in password.lst to check for weak passwords.
2.1.2 Allow the user to supply their own password list.
2.2 Login services to check include: SSH, RDP, FTP, and TELNET.

3. Mapping Vulnerabilities

3.1 Mapping vulnerabilities should only take place if **Full** was chosen.
3.2 Display potential vulnerabilities via NSE and Searchsploit.

4. Log Results

4.1 During each stage, display the stage in the terminal.
4.2 At the end, show the user the found information.
4.3 Allow the user to search inside the results.
4.4 Allow to save all results into a Zip file.

5. Creativity

General

- Suggested tools: Nmap, Hydra, Medusa, Searchsploit.
- Everything other than the user input should be automated.
- Use functions.

Comments

Use comments in your code to explain what you did.
If you are using code from the internet, add credit and links.
In the script, write the student's name and code, the class code, and the lecturer's name.