VULN SCANR™

by Keith Tan

PROJECT: VULNER

PENETRATION TESTING

CFC011023 (GROUP 2)

STUDENT: TAN KE HAN KEITH (S9)
TRAINER: TUSHAR

Table of Contents

1. INTRODUCTION **3**

2. SETTING UP TARGET NETWORK **3**

3. BASH SCRIPTING **4**

3.1 Formatting & Introduction 4
3.2 Stage 1: Defining & Investigating Target Network 5
3.3 Stage 2: Nmap & Masscan Target Network 6
3.4 Stage 3: Finding Weak Passwords Used in Target Network (Hydra Bruteforce) 8
3.4.1 Defining Username & Password List *8*
3.4.2 Hydra Bruteforce into Login Services (SSH, RDP, FTP, Telnet) *9*
3.4.3 Save Hydra Bruteforce Results *10*
3.5 Stage 4: Mapping Vulnerabilities – Searchsploit (only for Full Scan Option) 12
3.6 End: All Scans Completed, what will user like to do? 13
3.6.1 Option A: Display Scan Results *13*
3.6.2 Option B: Search within Scan Results *13*
3.6.3 Options C & D: Save Results into ZIP File & Exit Script *14*
3.6.4 Error-Handling *15*

REFERENCES **16**

ANNEX A: BASH SCRIPT **17**

ANNEX B: SCRIPT RESULTS [BASIC SCAN + DEFAULT PASSWORD LIST FOR BRUTEFORCE] **21**

ANNEX C: SCRIPT RESULTS [FULL SCAN + OWN PASSWORD LIST FOR BRUTEFORCE] **25**

SCRIPT FLOW

INTRODUCTION

Welcome Message

STAGE 1

Defining & Investigating Target Network

- Prompt user for Target IP & CIDR
- Host Discovery with Nmap -sn

STAGE 2

Performing Nmap & Masscan on Target Network

- Prompt user for an output directory
- Prompt user to choose **Basic Scan** or **Full Scan**

Basic Scan

- TCP Ports: sudo nmap -sV
- UDP Ports: sudo masscan -pU

Full Scan

- TCP Ports: sudo nmap -sV **-sC**
- UDP Ports: sudo masscan -pU

STAGE 3

Finding Weak Passwords used in Target Network for Login Services (Hydra Bruteforce into SSH, RDP, FTP, Telnet)

- Prompt user for an output directory to save results
- Prompt user for Target Username
- Prompt user to choose Password List

STAGE 4

Mapping Vulnerabilities (SearchSploit)

- searchsploit --nmap <nmap output file>.xml

END

All scans completed. What will user like to do?

(A) Display full scan results.
(B) Search within scan results.
(C) Save results into a ZIP file.
(D) Exit VulnScanr™

VULN SCANR™

1. Introduction

This report documents a Bash scripting project named VulnScanr™, which performs **network** vulnerability scanning and analysis. It guides the user through the following stages:

- Defining and investigating the target network.
- Performing scans using Nmap and Masscan.
- Identifying weak passwords through the use of Hydra brute-forcing.
- Mapping vulnerabilities with Searchsploit and NSE.
- Providing options to view, search within, or save the scan results.

The script automates the above-mentioned tasks, which helps to enhance the efficiency of security professionals in identifying potential vulnerabilities within a particular target network. Please refer to the Script Flow diagram located in the previous page, which illustrates the overall flow of the Bash Script.

2. Setting Up Target Network

The local network was set up and used to test and run the script. Within the local network, a Metasploitable 2 machine was set up with a new account with the username of 'polarbear' and a weak password of '12345678'.

```
msfadmin@metasploitable:~$ sudo adduser polarbear
Adding user `polarbear' ...
Adding new group `polarbear' (1003) ...
Adding new user `polarbear' (1003) with group `polarbear' ...
Creating home directory `/home/polarbear' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for polarbear
Enter the new value, or press ENTER for the default
        Full Name []: polarbear
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [y/N] y
msfadmin@metasploitable:~$ _
```

3. Bash Scripting

3.1 Formatting & Introduction

```
1   #!/bin/bash
2
3   # FORMATTING & INTRODUCTION
4   bold="\033[1m"
5   boldend="\033[0m"
6   echo
7   echo -e "${bold}Welcome to VulnScanr™ by Keith Tan!${boldend}"
8   echo
9   printf "    [?] What is your name? "; read name
10  echo "  [#] Welcome $name!"
11  echo
12
13
14
15
16
```

Line 1 to 11: The script starts off by defining the shebang to inform the machine to interpret the script in Bash. Subsequently, the user is prompted to provide his/her name to create a personalized experience. The script outputs the following results:

```
┌──(kali㉿kali)-[~/projectvulner]
└─$ sudo bash /home/kali/Desktop/vulnscanr.sh

Welcome to VulnScanr™ by Keith Tan!

        [?] What is your name? Not Loi Liang Yang
        [#] Welcome Not Loi Liang Yang!
```

3.2 Stage 1: Defining & Investigating Target Network

The script continues with Stage 1, where the user is prompted to provide valid inputs for the target network address with CIDR notation. Host discovery is then performed to reveal individual hosts.

```
17  # STAGE 1: DEFINING & INVESTIGATING TARGET NETWORK
18  echo -e "${bold}STAGE 1: DEFINING & INVESTIGATING TARGET NETWORK...${boldend}"
19  echo
20
21
22  # Get from User a Network to Scan; List all Hosts in Target Network:
23  IP_regex="^(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])$"
24  CIDR_regex='^([0-2]?[0-9]|3[0-2])$'
25
26  echo "  [?] State the target network you want to scan..."
27  while true; do #prompt user to input target's IP address, then validate it
28      read -p "   [?] Enter an IP Address to scan: " IP_addr
29      if [[ $IP_addr =~ $IP_regex ]]; then
30          break  #exit loop if IP address is valid
31      else
32          echo "  [!] Invalid IP address of $IP_addr, please re-enter a valid IP address."
33      fi
34  done
35
36  while true; do #prompt user to input target's CIDR, then validate it
37      read -p "   [?] Enter the CIDR Notation: /" CIDR
38      if [[ $CIDR =~ $CIDR_regex ]]; then
39          break  #exit loop if CIDR notation is valid
40      else
41          echo "  [!] Invalid CIDR notation of $CIDR, please re-enter a valid CIDR notation."
42      fi
43  done
44
45  echo -e "   ${bold}[@] Your target network is: $IP_addr/$CIDR${boldend}; List of hosts within your target network:"
46
47  # Discover Hosts in Target Network Using 'sudo nmap -sn'
48  readarray -t host_array < <(sudo nmap -sn ${IP_addr}/${CIDR} | grep "report" | awk '{print $(NF)}')
49  for host in "${host_array[@]}"; do
50      echo "      $host"
51  done
52
53
54
55
56
```

Lines 17 to 43: The user is informed that Stage 1 has started, where the target network is defined and the IPv4 addresses of hosts within the target network will be discovered. Subsequently, the user is prompted to specify the target network inclusive of IPv4 address and the CIDR notation. These inputs are then validated against the respective IPv4 and CIDR regex-es. If inputs are invalid, user is re-prompted to provide valid IPv4 and CIDR inputs (using while true loop).

Lines 45 to 51: With the valid target network address obtained, all hosts are discovered within the target network, using sudo nmap -sn. Through text manipulation, the discovered hosts are saved into host_array. Finally, using a for loop, all hosts are displayed onto the terminal for the user.

The script outputs the following results:

```
STAGE 1: DEFINING & INVESTIGATING TARGET NETWORK...

        [?] State the target network you want to scan...
        [?] Enter an IP Address to scan: 192.168.182.129
        [?] Enter the CIDR Notation: /24
        [@] Your target network is: 192.168.182.129/24; List of hosts within your target network:
            192.168.182.1
            192.168.182.2
            192.168.182.129
            192.168.182.254
            192.168.182.135
```

3.3 Stage 2: Nmap & Masscan Target Network

Stage 2 involves prompting the user for the target network's address (with CIDR), as well as performing of host discovery to uncover individual hosts' IPv4 address within the target network.

```
57  # STAGE 2: NMAP & MASSSCAN ON TARGET NETWORK
58  # Prompt User to Specify an Output Directory for Scan Results:
59  echo
60  echo
61  echo -e "${bold}STAGE 2: PERFORMING NMAP & MASSCAN ON TARGET NETWORK...${boldend}"
62  read -p "   [?] Enter an output directory to save your scan: " output_dir
63  echo -e "   ${bold}[@] Your output directory is: $output_dir${boldend}"
64
65
66  # Allow User to choose 'Basic' or 'Full' Scan Mode; Perform Nmap & Masscan:
67  echo "  [?] Choose your preferred Scan Mode:"
68  echo "      (A) Basic Scan: Scan the network for TCP & UDP, including Service Version and Weak Passwords."
69  echo "      (B) Full Scan: Use NSE, Weak Passwords and Vulnerability Analysis."
70  read -r option
71  case $option in
72      A|a) #basic scan mode using 'sudo nmap -sV' & masscan
73          echo "  [#] Basic Scan mode selected. Basic-scanning the network now..."
74          echo "  [#] Scanning TCP Ports: sudo nmap -sV ..."
75          sudo nmap -sV "${IP_addr}/${CIDR}" -oX ${output_dir}/basic_nmap.xml -o ${output_dir}/basic_nmap.txt > /dev/null
            2>&1
76          echo -e "   ${bold}[@] Scan results saved: ${output_dir}/basic_nmap.xml & ${output_dir}/basic_nmap.txt${boldend}"
77          echo "  [#] Scanning UDP Ports: sudo masscan -pU ..."
78          sudo masscan ${IP_addr}/${CIDR} -pU:0-65535 --rate=100000 -oL ${output_dir}/masscan.txt > /dev/null 2>&1
79          echo -e "   ${bold}[@] Scan results saved: ${output_dir}/masscan.txt"
80          echo -e "   ${bold}[@] Basic Scan completed.${boldend}"
81          ;;
82      B|b) #full scan mode using 'sudo nmap -sV -sC' & masscan
83          echo "  [#] Full Scan mode selected. Full-scanning the network now..."
84          echo "  [#] Scanning TCP Ports: sudo nmap -p- -sV -sC ..."
85          sudo nmap -sV -sC "${IP_addr}/${CIDR}" -oX ${output_dir}/full_nmap.xml -o ${output_dir}/full_nmap.txt > /dev/
            null 2>&1
86          echo -e "   ${bold}[@] Scan results saved: ${output_dir}/full_nmap.xml & ${output_dir}/full_nmap.txt${boldend}"
87          echo "  [#] Scanning UDP Ports: sudo masscan -pU ..."
88          sudo masscan ${IP_addr}/${CIDR} -pU:0-65535 --rate=100000 -oL ${output_dir}/masscan.txt > /dev/null 2>&1
89          echo -e "   ${bold}[@] Scan results saved: ${output_dir}/masscan.txt"
90          echo -e "   ${bold}[@] Full Scan completed.${boldend}"
91          ;;
92      *)
93          echo "  [!] Invalid input, please choose either 'A' or 'B'."
94          ;;
95  esac
96
97
98
99
100
```

Lines 57 to 63: The user is informed that Stage 2 has started, where Nmap and Masscans will be performed on the target network. The user is prompted to specify an output directory to save the scan results as the script progresses.

Lines 66 to 95: Through the use of a case, the user is prompted to choose their preferred scan mode – Basic scan or Full scan. Upon the respective scan completions, the user is alerted through terminal.

- Basic scan:
  - Using Nmap, the target network is scanned for open TCP ports, including service versions. Results are saved into the user-specified output directory, as a .txt file. All standard outputs and errors generated from this process are silenced through > /dev/null 2>&1.
  - Using Masscan, the target network is scanned for open UDP ports. Results are saved into the user-specified output directory, as a .txt file. All standard outputs and errors generated from this process are silenced through > /dev/null 2>&1.

- Using hydra bruteforcing into unsecure login services, weak passwords are uncovered. Results are saved into the user-specified output directory, as a .txt file. (will be performed in Stage 3).

- Full scan:
  - Everything in Basic scan are carried out. In addition:
    - Nmap scans are ran using NSEs (-sC flag).
    - Searchsploit is also used to perform vulnerability scans.

The script outputs the following results:

- Basic scan:

```
STAGE 2: PERFORMING NMAP & MASSCAN ON TARGET NETWORK...
        [?] Enter an output directory to save your scan: /home/kali/projectvulner
        [@] Your output directory is: /home/kali/projectvulner
        [?] Choose your preferred Scan Mode:
                (A) Basic Scan: Scan the network for TCP & UDP, including Service Version and Weak Passwords.
                (B) Full Scan: Use NSE, Weak Passwords and Vulnerability Analysis.
A
        [#] Basic Scan mode selected. Basic-scanning the network now...
        [#] Scanning TCP Ports: sudo nmap -sV ...
        [@] Scan results saved: /home/kali/projectvulner/basic_nmap.xml & /home/kali/projectvulner/basic_nmap.txt
        [#] Scanning UDP Ports: sudo masscan -pU ...
        [@] Scan results saved: /home/kali/projectvulner/masscan.txt
        [@] Basic Scan completed.
```

- Full scan:

```
STAGE 2: PERFORMING NMAP & MASSCAN ON TARGET NETWORK...
        [?] Enter an output directory to save your scan: /home/kali/projectvulner
        [@] Your output directory is: /home/kali/projectvulner
        [?] Choose your preferred Scan Mode:
                (A) Basic Scan: Scan the network for TCP & UDP, including Service Version and Weak Passwords.
                (B) Full Scan: Use NSE, Weak Passwords and Vulnerability Analysis.
B
        [#] Full Scan mode selected. Full-scanning the network now...
        [#] Scanning TCP Ports: sudo nmap -p- -sV -sC ...
        [@] Scan results saved: /home/kali/projectvulner/full_nmap.xml & /home/kali/projectvulner/full_nmap.txt
        [#] Scanning UDP Ports: sudo masscan -pU ...
        [@] Scan results saved: /home/kali/projectvulner/masscan.txt
        [@] Full Scan completed.
```

3.4 Stage 3: Finding Weak Passwords Used in Target Network (Hydra Bruteforce)

Stage 3 involves the detection of weak or commonly-used passwords in the target network. Firstly, the user is prompted for his/her desired username to target. Thereafter, the user is prompted for a password list (either to use a default from Seclists or to provide his/her own list). With the username and password list, hydra bruteforcing is conducted on login services – SSH, RDP, FTP, Telnet. Successful login results are displayed to the user, alongside the weak password detected.

3.4.1 Defining Username & Password List

```
101  # STAGE 3: FINDING WEAK PASSWORDS USED IN TARGET NETWORK (USING HYDRA BRUTEFORCING)
102  echo
103  echo
104  echo -e "${bold}STAGE 3: FINDING WEAK PASSWORDS USED IN TARGET NETWORK FOR LOGIN SERVICES...${boldend}"
105  read -p "   [?] What username do you want to target? " username
106
107
108  # Define Password List to Use
109  while true; do #prompt user to define what password list to use
110      echo "  [?] What password list do you want to use on the target? (A) Use default list (B) Supply your list"
111      read -r pw_option
112      case $pw_option in
113          A|a) #using default password list
114              echo "  [#] Using default password list. Downloading password.lst file..."
115              wget -q -O -
                 "https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/10-million-pa
                 ssword-list-top-100.txt" | head -n 20 > "${output_dir}/password.lst"
116              if [ $? -eq 0 ]; then #check if last command (to download default password file) was executed successfully
117                  echo -e "   ${bold}[@] Default password list saved to your output directory as:
                     ${output_dir}/password.lst${boldend}"
118                  break
119              else
120                  echo "  [!] Failed to download the default password file."
121              fi
122              ;;
123          B|b) #using user's own password list
124              read -p "   [?] Using your password list. Please state its file path: " ownpwlist_path
125              if [ -f "$ownpwlist_path" ]; then #check if user specified a file path
126                  echo "  [#] Using custom password list: $ownpwlist_path"
127                  break
128              else
129                  echo "  [!] Error: File not found at $ownpwlist_path"
130              fi
131              ;;
132          *) #error-handling for all other options (deemed invalid)
133              echo "  [!] Invalid input, please choose either 'A' or 'B'."
134              continue #re-prompt user to choose a valid option
135              ;;
136      esac
137  done
138
139
```

Lines 101 to 105: The user is informed that Stage 3 has started, and prompts user for the target username to be used to hydra bruteforce into login services – SSH, RDP, FTP and Telnet.

Lines 108 to 137: Using while true loop and a case, the user is prompted to choose what password list to use for hydra bruteforce. If neither of both options are chosen, the error and handled by re-prompting the user to type a valid option (A) or (B).

- (A) Default Password List: 10-million-password-list-top-100.txt from SecLists is downloaded using wget, and saved to the output directory that was specified by the user earlier. *Note: head -n 20 filters the first 20 passwords from the list, to reduce time taken for faster simulation purposes.*
- (B) Own Password List: The user is prompted to state file path of own password list.

3.4.2 Hydra Bruteforce into Login Services (SSH, RDP, FTP, Telnet)

```
140  # Bruteforce Login Services (SSH, RDP, FTP, Telnet)
141  hydra_login_svcs () {
142      protocol_array=("ssh" "rdp" "ftp" "telnet")
143
144      for protocol in "${protocol_array[@]}"; do #iterate and bruteforce each protocol
145          echo
146          echo -e "   ${bold}[#] Bruteforcing into ${protocol} protocol...${boldend}"
147
148          #bruteforce protocols
149          if [ $pw_option == "A" ] || [ $pw_option == "a" ]; then #if user chose to use default password list...
150              if [ -f "${output_dir}/password.lst" ]; then #if default password list has been downloaded...
151                  for host in "${host_array[@]}"; do #hydra bruteforce into all hosts
152                      hydra -l $username -P "${output_dir}/password.lst" "$host" ${protocol} -o ${output_dir}/${protocol}
                         _hydra.txt > /dev/null 2>&1
153                  done
154              else
155                  echo "  [!] Error: ${output_dir}/password.lst does not exist."
156              fi
157          else
158              if [ -f "$ownpwlist_path" ]; then #if user chose to use own password list...
159                  for host in "${host_array[@]}"; do #hydra bruteforce into all hosts
160                      hydra -l $username -P "$ownpwlist_path" "$host" ${protocol} -o ${output_dir}/${protocol}_hydra.txt >
                          /dev/null 2>&1
161                  done
162              else
163                  echo "  [!] Error: $ownpwlist_path does not exist."
164              fi
165          fi
166
167          #check if logins are successful:
168          if grep -iq "password:" "${output_dir}/${protocol}_hydra.txt"; then #if the hydra output file contains string
             'password:'...
169              pw_found=$(grep -o 'password: .*' ${output_dir}/${protocol}_hydra.txt | cut -d' ' -f2)
170              echo -e "   ${bold}[!] Bruteforce successful. Weak password found: $pw_found${boldend}" #echo to user in
                 terminal
171              echo "[!] Bruteforce successful. Weak password found: $pw_found" >> ${output_dir}/${protocol}_hydra.txt
                 #add to output file
172          else
173              echo "  [@] Bruteforce completed. No weak passwords were detected." #echo to user in terminal
174              echo "[@] Bruteforce completed. No weak passwords were detected." >> ${output_dir}/${protocol}_hydra.txt
                 #add to output file
175          fi
176      done
177
```

Lines 140 to 142: The function hydra_login_svcs() is defined to execute the multiple hydra bruteforcing into SSH, RDP, FTP and Telnet servers of every host within the target network. A new array protocol_array is defined to store the string names of each target server.

Lines 144 to 146: Using a for loop on protocol_array, the script is set up to progressively hydra bruteforce logins into each of the 4 servers.

Lines 148 to 165: If user chose to use a default password list and if the default password list had indeed been downloaded and saved to the user-specified output directory, run a for loop across the host_array, to iterate across all discovered hosts within the target network, and hydra bruteforce into each of them. Save the results into respective output files, within the user-specified output directory. Silence the standard outputs and standard errors from the hydra process, by using > /dev/null 2>&1. If the default password cannot be found, error-handle.

Lines 167 to 176: This section checks if any hydra bruteforce logins are successful, by using grep -iq for the string "password:" within the respective hydra output files. For each hydra bruteforce into each protocol, if the string "password:" exists, alert the user and display the

weak password found onto the terminal. If that string does not exist, alert the user that no weak passwords are detected.

3.4.3 Save Hydra Bruteforce Results

```
178     echo -e "${bold}FULL HYDRA SCAN RESULTS FOR SSH, RDP, FTP, TELNET:${boldend}" >> ${output_dir}/full_hydra.txt #make
        new file to store all hydra results
179     for protocol in "${protocol_array[@]}"; do #save all output files into a new singular file
180         cat ${output_dir}/${protocol}_hydra.txt >> ${output_dir}/full_hydra.txt
181         sudo rm ${output_dir}/${protocol}_hydra.txt #delete the individual files
182     done
183 }
184 hydra_login_svcs
185
186
187
188
189
```

Lines 178 to 184: With all hydra bruteforcing into each protocol completed at this juncture, create a new file called full_hydra.txt, to compile and store all hydra bruteforcing results into this singular file.

The script outputs the following results:

- Default Password List used:

```
STAGE 3: FINDING WEAK PASSWORDS USED IN TARGET NETWORK FOR LOGIN SERVICES ...
        [?] What username do you want to target? polarbear
        [?] What password list do you want to use on the target? (A) Use default list (B) Supply your list
A
        [#] Using default password list. Downloading password.lst file ...
        [@] Default password list saved to your output directory as: /home/kali/projectvulner/password.lst

        [#] Bruteforcing into ssh protocol ...
        [@] Bruteforce completed. No weak passwords were detected.

        [#] Bruteforcing into rdp protocol ...
        [@] Bruteforce completed. No weak passwords were detected.

        [#] Bruteforcing into ftp protocol ...
        [!] Bruteforce successful. Weak password found: 12345678

        [#] Bruteforcing into telnet protocol ...
        [!] Bruteforce successful. Weak password found: 12345678
```

- Own Password List used:

```
STAGE 3: FINDING WEAK PASSWORDS USED IN TARGET NETWORK FOR LOGIN SERVICES ...
        [?] What username do you want to target? polarbear
        [?] What password list do you want to use on the target? (A) Use default list (B) Supply your list
B
        [?] Using your password list. Please state its file path: /home/kali/Desktop/myprivatedir/myownpwlist.txt
        [#] Using custom password list: /home/kali/Desktop/myprivatedir/myownpwlist.txt

        [#] Bruteforcing into ssh protocol ...
        [@] Bruteforce completed. No weak passwords were detected.

        [#] Bruteforcing into rdp protocol ...
        [@] Bruteforce completed. No weak passwords were detected.

        [#] Bruteforcing into ftp protocol ...
        [!] Bruteforce successful. Weak password found: 12345678

        [#] Bruteforcing into telnet protocol ...
        [@] Bruteforce completed. No weak passwords were detected.
```

Referring to the above-shown outputs for hydra bruteforcing, it is noteworthy that when hydra is used to bruteforce into a Telnet server, the results are found to be generally inconsistent or unstable.

Therefore, it may be more meaningful to pair hydra with other bruteforcing methods, such as medusa or msfconsole's auxiliary module use auxiliary/scanner/telnet/telnet_login.

3.5 Stage 4: Mapping Vulnerabilities – Searchsploit (only for Full Scan Option)

Upon completion of hydra bruteforcing in Stage 3, the script progresses on to Stage 4, which entails the mapping of vulnerabilities on the target network, using SearchSploit (YouTube, 2022).

```
190  # STAGE 4: MAPPING VULNERABILITIES WITH SEARCHSPLOIT
191  echo
192  map_vulns () { #map vulnerabilities using
193      if [ $option == "B" ] || [ $option == "b" ]; then #if user chose to do full scan...
194          echo -e "${bold}STAGE 4: MAPPING VULNERABILITIES WITH SEARCHSPLOIT...${boldend}"
195          echo -e "${bold}POTENTIAL VULNERABILITIES:${boldend}" >> ${output_dir}/potential_vulns.txt #add title to
             potential vulns file
196          searchsploit -u > /dev/null 2>&1 #update searchsploit offline database
197          searchsploit --nmap ${output_dir}/full_nmap.xml >> ${output_dir}/potential_vulns.txt 2>&1 #checks all results
             in Nmap's full scan .xml output file with service version
198          echo -e "   ${bold}[@] Vulnerabilities mapped and saved to ${output_dir}/potential_vulns.txt${bold}" #echo to
             user in terminal where the results are saved
199      fi
200  }
201  map_vulns
202
203
204
205
206
```

Lines 190 to 192: A new function map_vulns() is defined to store commands that map vulnerabilities on the target network.

Lines 193 to 201: If the user chose to do a Full scan (back in Stage 2), vulnerabilities will be mapped. A new file potential_vulns.txt is created and stored within the user-specified output directory, and appended with a title. Next, the command searchsploit -u updates the offline database of SearchSploit, with the standard outputs and errors suppressed by > /dev/null 2>&1. Thereafter, searchsploit --nmap <nmap .xml file> checks the nmap scan results and maps all potential vulnerabilities, results are saved to potential_vulns.txt (O'Reilly, 2024).

The script outputs the following results:

```
STAGE 4: MAPPING VULNERABILITIES WITH SEARCHSPLOIT ...
        [@] Vulnerabilities mapped and saved to /home/kali/projectvulner/potential_vulns.txt
```

Upon further research, it was learned that by using SearchSploit to scan Nmap .xml files, many false positive vulnerabilities will be displayed (YouTube, 2021).

3.6 End: All Scans Completed, what will user like to do?

At this juncture, all scans are completed. The script prompts the user to choose 4 options on what to do with the scan results.

3.6.1 Option A: Display Scan Results

If user chooses Option A, all results from the user-specified output directory are printed out using cat. This includes the Nmap, Masscan and hydra results. If user had chosen Full scan in Stage 2, this means that vulnerabilities have been mapped and therefore, potential_vulns.txt will also be printed out.

```
# END: ALL VulnScanr™ SCANS COMPLETED - LOGGING
workwith_results () {
    echo
    echo
    echo -e "${bold}END: ALL VulnScanr™ SCANS COMPLETED.${boldend}"
    while true; do
        echo "  [?] What would you like to do?:"
        echo "      (A) Display full scan results."
        echo "      (B) Search within scan results."
        echo "      (C) Save results into a ZIP File."
        echo "      (D) Exit VulnScanr™"
        read -r results_option
        case $results_option in
            A|a) #display full scan results
                echo
                echo "  [#] Displaying full scan results:"
                cd $output_dir
                echo -e "${bold}NMAP & MASSCAN RESULTS:${boldend}"
                cat *nmap.txt
                cat masscan.txt
                cat full_hydra.txt
                if [ $option == "B" ] || [ $option == "b" ]; then
                    cat potential_vulns.txt
                fi
                echo -e "   ${bold}[@] Full scan results displayed.${boldend}"
                echo
                ;;
```

For option A, please refer to Annexes B and C to see the full outputs.

3.6.2 Option B: Search within Scan Results

If user chooses Option B, the user is prompted for their search string, and results are stored in search_str. All results in the user-specified output directory are printed out and filtered for search_str, using cat * | grep -i.

```
            B|b) #search string in scan results
                echo
                read -p "   [?] Searching within scan results. Please specify your search string: " search_str
                echo "  [#] Search Results:"
                cd $output_dir
                cat * | grep -i "$search_str"
                echo -e "   ${bold}[@] Search for "$search_str" is completed.${boldend}"
                echo
                ;;
```

For option B, the script outputs the following results. In this example, an attempt was made to search for the string 'password:', which is a typical string that hydra bruteforce prints for every successful login. Essentially, this command reveals the weak password(s):

```
        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
B

        [?] Searching within scan results. Please specify your search string: password:
        [#] Search Results:
[21][ftp] host: 192.168.182.129   login: polarbear   password: 12345678
[23][telnet] host: 192.168.182.129   login: polarbear   password: 12345678
        [@] Search for password: is completed.

        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
```

3.6.3 Options C & D: Save Results into ZIP File & Exit Script

If user chooses Option C, the user is prompted to specify a file name for a new .zip file, to which all scan results will be saved into. Firstly, sudo cp -r recursively copies the output directory and its inner contents, and pastes it into /home/kali. Thereafter, the file is zipped using zip -j -r. Once zipped, the user is informed of the file destination. The user can then choose Option D to exit the script.

```
            C|c) #save scan results into ZIP file
                echo
                read -p "   [?] Saving scan results into ZIP File. Please specify your desired file name (without file extension): " zip_filename
                sudo cp -r $output_dir /home/kali/${zip_filename}
                sudo zip -j -r /home/kali/${zip_filename}.zip /home/kali/${zip_filename}
                echo -e "   ${bold}[@] Scan results are zipped into new file at: /home/kali/${zip_filename}.zip"
                echo
                ;;
            D|d) #exit script
                echo "  [#] Exiting VulnScanr™..."
                exit
                ;;
```

For options C and D, the script outputs the following results:

- Basic scan:

```
        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
C

        [?] Saving scan results into ZIP File. Please specify your desired file name (without file extension): basicresultsvuln
  adding: masscan.txt (deflated 63%)
  adding: password.lst (deflated 34%)
  adding: basic_nmap.xml (deflated 87%)
  adding: basic_nmap.txt (deflated 58%)
  adding: full_hydra.txt (deflated 87%)
        [@] Scan results are zipped into new file at: /home/kali/basicresultsvuln.zip

        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
D
        [#] Exiting VulnScanr™...
```

```
┌──(kali㉿kali)-[~/projectvulner]
└─$ cd && ls
basicresultsvuln     Desktop   go         impacket                    Pictures       Responder    TheFatRat    zphisher-master
basicresultsvuln.zip Documents gobuster   mongodb-linux-x86_64-3.4.7  projectvulner  resultsvuln  Videos
beef                 Downloads home       Music                       Public         Templates    webseclab9

┌──(kali㉿kali)-[~]
└─$ unzip basicresultsvuln.zip
Archive:  basicresultsvuln.zip
  inflating: masscan.txt
  inflating: password.lst
  inflating: basic_nmap.xml
  inflating: basic_nmap.txt
  inflating: full_hydra.txt

┌──(kali㉿kali)-[~]
└─$ ls
basic_nmap.txt       beef      full_hydra.txt  impacket                    password.lst   Responder    Videos
basic_nmap.xml       Desktop   go              masscan.txt                 Pictures       resultsvuln  webseclab9
basicresultsvuln     Documents gobuster        mongodb-linux-x86_64-3.4.7  projectvulner  Templates    zphisher-master
basicresultsvuln.zip Downloads home            Music                       Public         TheFatRat

┌──(kali㉿kali)-[~]
└─$
```

- Full scan:

```
        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
C

        [?] Saving scan results into ZIP File. Please specify your desired file name (without file extension): resultsvuln
  adding: masscan.txt (deflated 54%)
  adding: potential_vulns.txt (deflated 77%)
  adding: full_nmap.xml (deflated 82%)
  adding: full_nmap.txt (deflated 58%)
  adding: full_hydra.txt (deflated 87%)
        [@] Scan results are zipped into new file at: /home/kali/resultsvuln.zip
```

```
        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
D
        [#] Exiting VulnScanr™...

┌──(kali㉿kali)-[~/projectvulner]
└─$ cd

┌──(kali㉿kali)-[~]
└─$ ls
beef       Downloads  home                       Music          Public       resultsvuln.zip  Videos
Desktop    go         impacket                   Pictures       Responder    Templates        webseclab9
Documents  gobuster   mongodb-linux-x86_64-3.4.7 projectvulner  resultsvuln  TheFatRat        zphisher-master

┌──(kali㉿kali)-[~]
└─$ sudo bash /home/kali/Desktop/vulnscanr.sh
[sudo] password for kali:
sudo: a password is required

┌──(kali㉿kali)-[~]
└─$ unzip resultsvuln.zip
Archive:  resultsvuln.zip
  inflating: masscan.txt
  inflating: potential_vulns.txt
  inflating: full_nmap.xml
  inflating: full_nmap.txt
  inflating: full_hydra.txt

┌──(kali㉿kali)-[~]
└─$ ls
beef       full_hydra.txt  gobuster     mongodb-linux-x86_64-3.4.7  projectvulner  resultsvuln.zip  webseclab9
Desktop    full_nmap.txt   home         Music                       Public         Templates        zphisher-master
Documents  full_nmap.xml   impacket     Pictures                    Responder      TheFatRat
Downloads  go              masscan.txt  potential_vulns.txt         resultsvuln    Videos

┌──(kali㉿kali)-[~]
└─$
```

3.6.4 Error-Handling

If an invalid input is keyed, the user is alerted. The command continue will re-prompt the user to provide a valid input.

```
            *) #error-handling
                echo "  [!] Invalid input, please choose either 'A', 'B', 'C' or 'D'."
                echo
                continue
                ;;
        esac
    done
}
workwith_results
```

References

YouTube. (2021). Vulnerability Scanning With SearchSploit+NMAP | How to do Vulnerability Scanning | Kali linux https://www.youtube.com/watch?v=zE28eTxYo5Q (Accessed: 9 March, 2024)

YouTube. (2022). SearchSploit Guide | Finding Exploits | Kali Linux https://www.youtube.com/watch?v=nx3Uz9zNrWQ (Accessed: 10 March, 2024)

O'Reilly. (2024). Understanding search options in searchsploit https://www.oreilly.com/library/view/kali-linux-cookbook/9781784390303/a8146441-a9a9-421e-94da-b5ecf4357a45.xhtml (Accessed: 10 March, 2024)

Annex A: Bash Script

```bash
#!/bin/bash

# FORMATTING & INTRODUCTION
bold="\033[1m"
boldend="\033[0m"
echo
echo -e "${bold}Welcome to VulnScanr™ by Keith Tan!${boldend}"
echo
printf "    [?] What is your name? "; read name
echo "  [#] Welcome $name!"
echo




# STAGE 1: DEFINING & INVESTIGATING TARGET NETWORK
echo -e "${bold}STAGE 1: DEFINING & INVESTIGATING TARGET NETWORK...${boldend}"
echo


# Get from User a Network to Scan; List all Hosts in Target Network:
IP_regex="^(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])$"
CIDR_regex='^([0-2]?[0-9]|3[0-2])$'

echo "  [?] State the target network you want to scan..."
while true; do #prompt user to input target's IP address, then validate it
    read -p "   [?] Enter an IP Address to scan: " IP_addr
    if [[ $IP_addr =~ $IP_regex ]]; then
        break  #exit loop if IP address is valid
    else
        echo "  [!] Invalid IP address of $IP_addr, please re-enter a valid IP address."
    fi
done

while true; do #prompt user to input target's CIDR, then validate it
    read -p "   [?] Enter the CIDR Notation: /" CIDR
    if [[ $CIDR =~ $CIDR_regex ]]; then
        break  #exit loop if CIDR notation is valid
    else
        echo "  [!] Invalid CIDR notation of $CIDR, please re-enter a valid CIDR notation."
    fi
done

echo -e "   ${bold}[@] Your target network is: $IP_addr/$CIDR${boldend}; List of hosts within your target network:"

# Discover Hosts in Target Network Using 'sudo nmap -sn'
readarray -t host_array < <(sudo nmap -sn ${IP_addr}/${CIDR} | grep "report" | awk '{print $(NF)}')
for host in "${host_array[@]}"; do
    echo "      $host"
done
```

```
# STAGE 2: NMAP & MASSSCAN ON TARGET NETWORK
# Prompt User to Specify an Output Directory for Scan Results:
echo
echo
echo -e "${bold}STAGE 2: PERFORMING NMAP & MASSCAN ON TARGET NETWORK...${boldend}"
read -p "   [?] Enter an output directory to save your scan: " output_dir
echo -e "   ${bold}[@] Your output directory is: $output_dir${boldend}"


# Allow User to choose 'Basic' or 'Full' Scan Mode; Perform Nmap & Masscan:
echo "  [?] Choose your preferred Scan Mode:"
echo "      (A) Basic Scan: Scan the network for TCP & UDP, including Service Version and Weak Passwords."
echo "      (B) Full Scan: Use NSE, Weak Passwords and Vulnerability Analysis."
read -r option
case $option in
    A|a) #basic scan mode using 'sudo nmap -sV' & masscan
        echo "  [#] Basic Scan mode selected. Basic-scanning the network now..."
        echo "  [#] Scanning TCP Ports: sudo nmap -sV ..."
        sudo nmap -sV "${IP_addr}/${CIDR}" -oX ${output_dir}/basic_nmap.xml -o ${output_dir}/basic_nmap.txt > /dev/null 2>&1
        echo -e "   ${bold}[@] Scan results saved: ${output_dir}/basic_nmap.xml & ${output_dir}/basic_nmap.txt${boldend}"
        echo "  [#] Scanning UDP Ports: sudo masscan -pU ..."
        sudo masscan ${IP_addr}/${CIDR} -pU:0-65535 --rate=100000 -oL ${output_dir}/masscan.txt > /dev/null 2>&1
        echo -e "   ${bold}[@] Scan results saved: ${output_dir}/masscan.txt"
        echo -e "   ${bold}[@] Basic Scan completed.${boldend}"
        ;;
    B|b) #full scan mode using 'sudo nmap -sV -sC' & masscan
        echo "  [#] Full Scan mode selected. Full-scanning the network now..."
        echo "  [#] Scanning TCP Ports: sudo nmap -p- -sV -sC ..."
        sudo nmap -sV -sC "${IP_addr}/${CIDR}" -oX ${output_dir}/full_nmap.xml -o ${output_dir}/full_nmap.txt > /dev/null 2>&1
        echo -e "   ${bold}[@] Scan results saved: ${output_dir}/full_nmap.xml & ${output_dir}/full_nmap.txt${boldend}"
        echo "  [#] Scanning UDP Ports: sudo masscan -pU ..."
        sudo masscan ${IP_addr}/${CIDR} -pU:0-65535 --rate=100000 -oL ${output_dir}/masscan.txt > /dev/null 2>&1
        echo -e "   ${bold}[@] Scan results saved: ${output_dir}/masscan.txt"
        echo -e "   ${bold}[@] Full Scan completed.${boldend}"
        ;;
    *)
        echo "  [!] Invalid input, please choose either 'A' or 'B'."
        ;;
esac
```

```
# STAGE 3: FINDING WEAK PASSWORDS USED IN TARGET NETWORK (USING HYDRA BRUTEFORCING)
echo
echo
echo -e "${bold}STAGE 3: FINDING WEAK PASSWORDS USED IN TARGET NETWORK FOR LOGIN SERVICES...${boldend}"
read -p "   [?] What username do you want to target? " username


# Define Password List to Use
while true; do #prompt user to define what password list to use
    echo "  [?] What password list do you want to use on the target? (A) Use default list (B) Supply your list"
    read -r pw_option
    case $pw_option in
        A|a) #using default password list
            echo "  [#] Using default password list. Downloading password.lst file..."
            wget -q -O - "https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/10-million-password-list-top-100.txt" | head -n 20 > "${output_dir}/password.lst"
            if [ $? -eq 0 ]; then #check if last command (to download default password file) was executed successfully
                echo -e "   ${bold}[@] Default password list saved to your output directory as: ${output_dir}/password.lst${boldend}"
                break
            else
                echo "  [!] Failed to download the default password file."
            fi
            ;;
        B|b) #using user's own password list
            read -p "   [?] Using your password list. Please state its file path: " ownpwlist_path
            if [ -f "$ownpwlist_path" ]; then #check if user specified a file path
                echo "  [#] Using custom password list: $ownpwlist_path"
                break
            else
                echo "  [!] Error: File not found at $ownpwlist_path"
            fi
            ;;
        *) #error-handling for all other options (deemed invalid)
            echo "  [!] Invalid input, please choose either 'A' or 'B'."
            continue #re-prompt user to choose a valid option
            ;;
    esac
done
```

```
# Bruteforce Login Services (SSH, RDP, FTP, Telnet)
hydra_login_svcs () {
    protocol_array=("ssh" "rdp" "ftp" "telnet")

    for protocol in "${protocol_array[@]}"; do #iterate and bruteforce each protocol
        echo
        echo -e "   ${bold}[#] Bruteforcing into ${protocol} protocol...${boldend}"

        #bruteforce protocols
        if [ $pw_option == "A" ] || [ $pw_option == "a" ]; then #if user chose to use default password list...
            if [ -f "${output_dir}/password.lst" ]; then #if default password list has been downloaded...
                for host in "${host_array[@]}"; do #hydra bruteforce into all hosts
                    hydra -l $username -P "${output_dir}/password.lst" "$host" ${protocol} -o ${output_dir}/${protocol}_hydra.txt > /dev/null 2>&1
                done
            else
                echo "  [!] Error: ${output_dir}/password.lst does not exist."
            fi
        else
            if [ -f "$ownpwlist_path" ]; then #if user chose to use own password list...
                for host in "${host_array[@]}"; do #hydra bruteforce into all hosts
                    hydra -l $username -P "$ownpwlist_path" "$host" ${protocol} -o ${output_dir}/${protocol}_hydra.txt > /dev/null 2>&1
                done
            else
                echo "  [!] Error: $ownpwlist_path does not exist."
            fi
        fi

        #check if logins are successful:
        if grep -iq "password:" "${output_dir}/${protocol}_hydra.txt"; then #if the hydra output file contains string 'password:'...
            pw_found=$(grep -o 'password: .*' ${output_dir}/${protocol}_hydra.txt | cut -d' ' -f2)
            echo -e "   ${bold}[!] Bruteforce successful. Weak password found: $pw_found${boldend}" #echo to user in terminal
            echo "[!] Bruteforce successful. Weak password found: $pw_found" >> ${output_dir}/${protocol}_hydra.txt #add to output file
        else
            echo "  [@] Bruteforce completed. No weak passwords were detected." #echo to user in terminal
            echo "[@] Bruteforce completed. No weak passwords were detected." >> ${output_dir}/${protocol}_hydra.txt #add to output file
        fi
    done

    echo -e "${bold}FULL HYDRA SCAN RESULTS FOR SSH, RDP, FTP, TELNET:${boldend}" >> ${output_dir}/full_hydra.txt #make new file to store all hydra results
    for protocol in "${protocol_array[@]}"; do #save all output files into a new singular file
        cat ${output_dir}/${protocol}_hydra.txt >> ${output_dir}/full_hydra.txt
        sudo rm ${output_dir}/${protocol}_hydra.txt #delete the individual files
    done
}
hydra_login_svcs
```

```
# STAGE 4: MAPPING VULNERABILITIES WITH SEARCHSPLOIT
echo
map_vulns () { #map vulnerabilities using
    if [ $option == "B" ] || [ $option == "b" ]; then #if user chose to do full scan...
        echo -e "${bold}STAGE 4: MAPPING VULNERABILITIES WITH SEARCHSPLOIT...${boldend}"
        echo -e "${bold}POTENTIAL VULNERABILITIES:${boldend}" >> ${output_dir}/potential_vulns.txt #add title to potential vulns file
        searchsploit -u > /dev/null 2>&1 #update searchsploit offline database
        searchsploit --nmap ${output_dir}/full_nmap.xml >> ${output_dir}/potential_vulns.txt 2>&1 #checks all results in Nmap's full scan .xml output file with service version
        echo -e "   ${bold}[@] Vulnerabilities mapped and saved to ${output_dir}/potential_vulns.txt${bold}" #echo to user in terminal where the results are saved
    fi
}
map_vulns
```

```
# END: ALL VulnScanr™ SCANS COMPLETED - LOGGING
workwith_results () {
    echo
    echo
    echo -e "${bold}END: ALL VulnScanr™ SCANS COMPLETED.${boldend}"
    while true; do
        echo "  [?] What would you like to do?:"
        echo "      (A) Display full scan results."
        echo "      (B) Search within scan results."
        echo "      (C) Save results into a ZIP File."
        echo "      (D) Exit VulnScanr™"
        read -r results_option
        case $results_option in
            A|a) #display full scan results
                echo
                echo "  [#] Displaying full scan results:"
                cd $output_dir
                echo -e "${bold}NMAP & MASSCAN RESULTS:${boldend}"
                cat *nmap.txt
                cat masscan.txt
                cat full_hydra.txt
                if [ $option == "B" ] || [ $option == "b" ]; then
                    cat potential_vulns.txt
                fi
                echo -e "   ${bold}[@] Full scan results displayed.${boldend}"
                echo
                ;;
            B|b) #search string in scan results
                echo
                read -p "   [?] Searching within scan results. Please specify your search string: " search_str
                echo "  [#] Search Results:"
                cd $output_dir
                cat * | grep -i "$search_str"
                echo -e "   ${bold}[@] Search for "$search_str" is completed.${boldend}"
                echo
                ;;
            C|c) #save scan results into ZIP file
                echo
                read -p "   [?] Saving scan results into ZIP File. Please specify your desired file name (without file extension): " zip_filename
                sudo cp -r $output_dir /home/kali/${zip_filename}
                sudo zip -j -r /home/kali/${zip_filename}.zip /home/kali/${zip_filename}
                echo -e "   ${bold}[@] Scan results are zipped into new file at: /home/kali/${zip_filename}.zip"
                echo
                ;;
            D|d) #exit script
                echo "  [#] Exiting VulnScanr™..."
                exit
                ;;
            *) #error-handling
                echo "  [!] Invalid input, please choose either 'A', 'B', 'C' or 'D'."
                echo
                continue
                ;;
        esac
    done
}
workwith_results
```

Annex B: Script Results [Basic Scan + Default Password List for Bruteforce]

```
┌──(kali㉿kali)-[~/projectvulner]
└─$ sudo bash /home/kali/Desktop/vulnscanr.sh

Welcome to VulnScanr™ by Keith Tan!

        [?] What is your name? Not Loi Liang Yang
        [#] Welcome Not Loi Liang Yang!

STAGE 1: DEFINING & INVESTIGATING TARGET NETWORK ...

        [?] State the target network you want to scan ...
        [?] Enter an IP Address to scan: 192.168.182.129
        [?] Enter the CIDR Notation: /24
        [@] Your target network is: 192.168.182.129/24; List of hosts within your target network:
                192.168.182.1
                192.168.182.2
                192.168.182.129
                192.168.182.254
                192.168.182.135
```

```
STAGE 2: PERFORMING NMAP & MASSCAN ON TARGET NETWORK ...
        [?] Enter an output directory to save your scan: /home/kali/projectvulner
        [@] Your output directory is: /home/kali/projectvulner
        [?] Choose your preferred Scan Mode:
                (A) Basic Scan: Scan the network for TCP & UDP, including Service Version and Weak Passwords.
                (B) Full Scan: Use NSE, Weak Passwords and Vulnerability Analysis.
A
        [#] Basic Scan mode selected. Basic-scanning the network now ...
        [#] Scanning TCP Ports: sudo nmap -sV  ...
        [@] Scan results saved: /home/kali/projectvulner/basic_nmap.xml & /home/kali/projectvulner/basic_nmap.txt
        [#] Scanning UDP Ports: sudo masscan -pU  ...
        [@] Scan results saved: /home/kali/projectvulner/masscan.txt
        [@] Basic Scan completed.
```

```
STAGE 3: FINDING WEAK PASSWORDS USED IN TARGET NETWORK FOR LOGIN SERVICES ...
        [?] What username do you want to target? polarbear
        [?] What password list do you want to use on the target? (A) Use default list (B) Supply your list
A
        [#] Using default password list. Downloading password.lst file ...
        [@] Default password list saved to your output directory as: /home/kali/projectvulner/password.lst

        [#] Bruteforcing into ssh protocol ...
        [@] Bruteforce completed. No weak passwords were detected.

        [#] Bruteforcing into rdp protocol ...
        [@] Bruteforce completed. No weak passwords were detected.

        [#] Bruteforcing into ftp protocol ...
        [!] Bruteforce successful. Weak password found: 12345678

        [#] Bruteforcing into telnet protocol ...
        [!] Bruteforce successful. Weak password found: 12345678
```

```
END: ALL VulnScanr™ SCANS COMPLETED.
        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
A

        [#] Displaying full scan results:
NMAP & MASSCAN RESULTS:
# Nmap 7.94SVN scan initiated Sun Mar 10 01:09:57 2024 as: nmap -sV -oX /home/kali/projectvulner/basic_nmap.xml -o /home/kali/projec
tvulner/basic_nmap.txt 192.168.182.129/24
Nmap scan report for 192.168.182.1
Host is up (0.00039s latency).
Not shown: 931 filtered tcp ports (no-response), 65 closed tcp ports (reset)
PORT    STATE SERVICE         VERSION
139/tcp open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.182.2
Host is up (0.00013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Cloudflare public DNS
MAC Address: 00:50:56:EE:FE:FE (VMware)

Nmap scan report for 192.168.182.129
Host is up (0.0062s latency).
Not shown: 977 closed tcp ports (reset)
```

```
PORT   STATE SERVICE VERSION
53/tcp open  domain  Cloudflare public DNS
MAC Address: 00:50:56:EE:FE:FE (VMware)

Nmap scan report for 192.168.182.129
Host is up (0.0062s latency).
Not shown: 977 closed tcp ports (reset)
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
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:29:D4:FE (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.182.254
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.182.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E4:6D:67 (VMware)

Nmap scan report for 192.168.182.135
Host is up (0.000030s latency).
All 1000 scanned ports on 192.168.182.135 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Mar 10 01:22:48 2024 -- 256 IP addresses (5 hosts up) scanned in 771.62 seconds
#masscan
open udp 53 192.168.182.2 1710051907
```

```
open udp 53 192.168.182.129 1710051926
open udp 51768 192.168.182.135 1710051927
open udp 137 192.168.182.129 1710051937
open udp 53 192.168.182.0 1710051938
open udp 53 192.168.182.255 1710051965
# end
```

```
FULL HYDRA SCAN RESULTS FOR SSH, RDP, FTP, TELNET:
# Hydra v9.5 run at 2024-03-10 01:30:12 on 192.168.182.1 ssh (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home/k
ali/projectvulner/ssh_hydra.txt 192.168.182.1 ssh)
# Hydra v9.5 run at 2024-03-10 01:30:45 on 192.168.182.2 ssh (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home/k
ali/projectvulner/ssh_hydra.txt 192.168.182.2 ssh)
# Hydra v9.5 run at 2024-03-10 01:30:46 on 192.168.182.129 ssh (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home
/kali/projectvulner/ssh_hydra.txt 192.168.182.129 ssh)
# Hydra v9.5 run at 2024-03-10 01:30:46 on 192.168.182.254 ssh (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home
/kali/projectvulner/ssh_hydra.txt 192.168.182.254 ssh)
# Hydra v9.5 run at 2024-03-10 01:31:19 on 192.168.182.135 ssh (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home
/kali/projectvulner/ssh_hydra.txt 192.168.182.135 ssh)
[@] Bruteforce completed. No weak passwords were detected.
# Hydra v9.5 run at 2024-03-10 01:31:20 on 192.168.182.1 rdp (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home/k
ali/projectvulner/rdp_hydra.txt 192.168.182.1 rdp)
# Hydra v9.5 run at 2024-03-10 01:31:26 on 192.168.182.2 rdp (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home/k
ali/projectvulner/rdp_hydra.txt 192.168.182.2 rdp)
# Hydra v9.5 run at 2024-03-10 01:31:31 on 192.168.182.129 rdp (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home
/kali/projectvulner/rdp_hydra.txt 192.168.182.129 rdp)
# Hydra v9.5 run at 2024-03-10 01:31:36 on 192.168.182.254 rdp (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home
/kali/projectvulner/rdp_hydra.txt 192.168.182.254 rdp)
# Hydra v9.5 run at 2024-03-10 01:32:10 on 192.168.182.135 rdp (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home
/kali/projectvulner/rdp_hydra.txt 192.168.182.135 rdp)
[@] Bruteforce completed. No weak passwords were detected.
# Hydra v9.5 run at 2024-03-10 01:32:15 on 192.168.182.1 ftp (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home/k
ali/projectvulner/ftp_hydra.txt 192.168.182.1 ftp)
# Hydra v9.5 run at 2024-03-10 01:32:48 on 192.168.182.2 ftp (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home/k
ali/projectvulner/ftp_hydra.txt 192.168.182.2 ftp)
# Hydra v9.5 run at 2024-03-10 01:32:52 on 192.168.182.129 ftp (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home
/kali/projectvulner/ftp_hydra.txt 192.168.182.129 ftp)
[21][ftp] host: 192.168.182.129   login: polarbear   password: 12345678
# Hydra v9.5 run at 2024-03-10 01:32:57 on 192.168.182.254 ftp (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home
/kali/projectvulner/ftp_hydra.txt 192.168.182.254 ftp)
# Hydra v9.5 run at 2024-03-10 01:33:30 on 192.168.182.135 ftp (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /home
/kali/projectvulner/ftp_hydra.txt 192.168.182.135 ftp)
[!] Bruteforce successful. Weak password found: 12345678
# Hydra v9.5 run at 2024-03-10 01:33:34 on 192.168.182.1 telnet (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /hom
e/kali/projectvulner/telnet_hydra.txt 192.168.182.1 telnet)
# Hydra v9.5 run at 2024-03-10 01:34:07 on 192.168.182.2 telnet (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /hom
e/kali/projectvulner/telnet_hydra.txt 192.168.182.2 telnet)
# Hydra v9.5 run at 2024-03-10 01:34:11 on 192.168.182.129 telnet (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /h
ome/kali/projectvulner/telnet_hydra.txt 192.168.182.129 telnet)
[23][telnet] host: 192.168.182.129   login: polarbear   password: 12345678
# Hydra v9.5 run at 2024-03-10 01:34:20 on 192.168.182.254 telnet (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /h
ome/kali/projectvulner/telnet_hydra.txt 192.168.182.254 telnet)
# Hydra v9.5 run at 2024-03-10 01:34:53 on 192.168.182.135 telnet (hydra -l polarbear -P /home/kali/projectvulner/password.lst -o /h
ome/kali/projectvulner/telnet_hydra.txt 192.168.182.135 telnet)
[!] Bruteforce successful. Weak password found: 12345678
        [@] Full scan results displayed.
```

```
        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
B

        [?] Searching within scan results. Please specify your search string: password:
        [#] Search Results:
[21][ftp] host: 192.168.182.129   login: polarbear   password: 12345678
[23][telnet] host: 192.168.182.129   login: polarbear   password: 12345678
        [@] Search for password: is completed.

        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
```

```
        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
C

        [?] Saving scan results into ZIP File. Please specify your desired file name (without file extension): basicresultsvuln
  adding: masscan.txt (deflated 63%)
  adding: password.lst (deflated 34%)
  adding: basic_nmap.xml (deflated 87%)
  adding: basic_nmap.txt (deflated 58%)
  adding: full_hydra.txt (deflated 87%)
        [@] Scan results are zipped into new file at: /home/kali/basicresultsvuln.zip

        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
D
        [#] Exiting VulnScanr™...
```

```
┌──(kali㉿kali)-[~/projectvulner]
└─$ cd && ls
basicresultsvuln      Desktop    go         impacket                    Pictures       Responder    TheFatRat    zphisher-master
basicresultsvuln.zip  Documents  gobuster   mongodb-linux-x86_64-3.4.7  projectvulner  resultsvuln  Videos
beef                  Downloads  home       Music                       Public         Templates    webseclab9

┌──(kali㉿kali)-[~]
└─$ unzip basicresultsvuln.zip
Archive:  basicresultsvuln.zip
  inflating: masscan.txt
  inflating: password.lst
  inflating: basic_nmap.xml
  inflating: basic_nmap.txt
  inflating: full_hydra.txt

┌──(kali㉿kali)-[~]
└─$ ls
basic_nmap.txt        beef       full_hydra.txt  impacket                    password.lst   Responder    Videos
basic_nmap.xml        Desktop    go              masscan.txt                 Pictures       resultsvuln  webseclab9
basicresultsvuln      Documents  gobuster        mongodb-linux-x86_64-3.4.7  projectvulner  Templates    zphisher-master
basicresultsvuln.zip  Downloads  home            Music                       Public         TheFatRat

┌──(kali㉿kali)-[~]
└─$
```

Annex C: Script Results [Full Scan + Own Password List for Bruteforce]

```
┌──(kali㉿kali)-[~/projectvulner]
└─$ sudo bash /home/kali/Desktop/vulnscanr.sh

Welcome to VulnScanr™ by Keith Tan!

        [?] What is your name? Not Loi Liang Yang
        [#] Welcome Not Loi Liang Yang!

STAGE 1: DEFINING & INVESTIGATING TARGET NETWORK ...

        [?] State the target network you want to scan ...
        [?] Enter an IP Address to scan: 192.168.182.129
        [?] Enter the CIDR Notation: /24
        [@] Your target network is: 192.168.182.129/24; List of hosts within your target network:
            192.168.182.1
            192.168.182.2
            192.168.182.129
            192.168.182.254
            192.168.182.135
```

```
STAGE 2: PERFORMING NMAP & MASSCAN ON TARGET NETWORK ...
        [?] Enter an output directory to save your scan: /home/kali/projectvulner
        [@] Your output directory is: /home/kali/projectvulner
        [?] Choose your preferred Scan Mode:
            (A) Basic Scan: Scan the network for TCP & UDP, including Service Version and Weak Passwords.
            (B) Full Scan: Use NSE, Weak Passwords and Vulnerability Analysis.
B
        [#] Full Scan mode selected. Full-scanning the network now ...
        [#] Scanning TCP Ports: sudo nmap -p- -sV -sC  ...
        [@] Scan results saved: /home/kali/projectvulner/full_nmap.xml & /home/kali/projectvulner/full_nmap.txt
        [#] Scanning UDP Ports: sudo masscan -pU  ...
        [@] Scan results saved: /home/kali/projectvulner/masscan.txt
        [@] Full Scan completed.
```

```
STAGE 3: FINDING WEAK PASSWORDS USED IN TARGET NETWORK FOR LOGIN SERVICES ...
        [?] What username do you want to target? polarbear
        [?] What password list do you want to use on the target? (A) Use default list (B) Supply your list
B
        [?] Using your password list. Please state its file path: /home/kali/Desktop/myprivatedir/myownpwlist.txt
        [#] Using custom password list: /home/kali/Desktop/myprivatedir/myownpwlist.txt

        [#] Bruteforcing into ssh protocol ...
        [@] Bruteforce completed. No weak passwords were detected.

        [#] Bruteforcing into rdp protocol ...
        [@] Bruteforce completed. No weak passwords were detected.

        [#] Bruteforcing into ftp protocol ...
        [!] Bruteforce successful. Weak password found: 12345678

        [#] Bruteforcing into telnet protocol ...
        [@] Bruteforce completed. No weak passwords were detected.
```

```
STAGE 4: MAPPING VULNERABILITIES WITH SEARCHSPLOIT ...
        [@] Vulnerabilities mapped and saved to /home/kali/projectvulner/potential_vulns.txt
```

```
END: ALL VulnScanr™ SCANS COMPLETED.
        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
A

        [#] Displaying full scan results:
NMAP & MASSCAN RESULTS:
# Nmap 7.94SVN scan initiated Sat Mar  9 23:18:40 2024 as: nmap -sV -sC -oX /home/kali/projectvulner/full_nmap.xml -o /home/kali/proj
ectvulner/full_nmap.txt 192.168.182.129/24
Nmap scan report for 192.168.182.1
Host is up (0.0011s latency).
Not shown: 932 filtered tcp ports (no-response), 64 closed tcp ports (reset)
PORT    STATE SERVICE         VERSION
139/tcp open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-03-10T04:29:37
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: MSI, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:c0:00:08 (VMware)

Nmap scan report for 192.168.182.2
Host is up (0.00018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Cloudflare public DNS
MAC Address: 00:50:56:EE:FE:FE (VMware)

Nmap scan report for 192.168.182.129
Host is up (0.00098s latency).
Not shown: 977 closed tcp ports (reset)
```


```
PORT    STATE SERVICE         VERSION
139/tcp open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-03-10T04:29:37
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: MSI, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:c0:00:08 (VMware)

Nmap scan report for 192.168.182.2
Host is up (0.00018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Cloudflare public DNS
MAC Address: 00:50:56:EE:FE:FE (VMware)

Nmap scan report for 192.168.182.129
Host is up (0.00098s latency).
Not shown: 977 closed tcp ports (reset)
```


```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.182.135
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
```

```
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside
US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-03-09T21:18:18+00:00; -7h11m38s from scanner time.
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      34190/tcp   mountd
|   100005  1,2,3      52132/udp   mountd
|   100021  1,3,4      50185/udp   nlockmgr
|   100021  1,3,4      57877/tcp   nlockmgr
|   100024  1          51589/udp   status
|_  100024  1          55863/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 86
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, SupportsTransactions, SupportsCompression, Speaks41ProtocolNew, ConnectWithDatabase
, Support41Auth, LongColumnFlag
```

```
|   Status: Autocommit
|_  Salt: 8LVIL"aG|[2)t/,/HZk,
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside
US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-03-09T21:18:17+00:00; -7h11m38s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 12:45:07
|   source ident: nmap
|   source host: A710FF72.72AD8716.FFFA6D49.IP
|_  error: Closing Link: hdqxyhlgp[192.168.182.135] (Quit: hdqxyhlgp)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 00:0C:29:29:D4:FE (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-03-09T16:17:57-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

```
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -5h56m37s, deviation: 2h30m01s, median: -7h11m38s

Nmap scan report for 192.168.182.254
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.182.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E4:6D:67 (VMware)

Nmap scan report for 192.168.182.135
Host is up (0.000029s latency).
All 1000 scanned ports on 192.168.182.135 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Mar  9 23:30:03 2024 -- 256 IP addresses (5 hosts up) scanned in 683.41 seconds
#masscan
open udp 53 192.168.182.0 1710045016
open udp 137 192.168.182.129 1710045259
open udp 53 192.168.182.129 1710045294
open udp 53 192.168.182.2 1710045297
# end
```

```
FULL HYDRA SCAN RESULTS FOR SSH, RDP, FTP, TELNET:
# Hydra v9.5 run at 2024-03-09 23:37:33 on 192.168.182.1 ssh (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt -
o /home/kali/projectvulner/ssh_hydra.txt 192.168.182.1 ssh)
# Hydra v9.5 run at 2024-03-09 23:38:06 on 192.168.182.2 ssh (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt -
o /home/kali/projectvulner/ssh_hydra.txt 192.168.182.2 ssh)
# Hydra v9.5 run at 2024-03-09 23:38:07 on 192.168.182.129 ssh (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt
 -o /home/kali/projectvulner/ssh_hydra.txt 192.168.182.129 ssh)
# Hydra v9.5 run at 2024-03-09 23:38:08 on 192.168.182.254 ssh (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt
 -o /home/kali/projectvulner/ssh_hydra.txt 192.168.182.254 ssh)
# Hydra v9.5 run at 2024-03-09 23:38:41 on 192.168.182.135 ssh (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt
 -o /home/kali/projectvulner/ssh_hydra.txt 192.168.182.135 ssh)
[@] Bruteforce completed. No weak passwords were detected.
# Hydra v9.5 run at 2024-03-09 23:38:41 on 192.168.182.1 rdp (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt -
o /home/kali/projectvulner/rdp_hydra.txt 192.168.182.1 rdp)
# Hydra v9.5 run at 2024-03-09 23:38:46 on 192.168.182.2 rdp (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt -
o /home/kali/projectvulner/rdp_hydra.txt 192.168.182.2 rdp)
# Hydra v9.5 run at 2024-03-09 23:38:50 on 192.168.182.129 rdp (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt
 -o /home/kali/projectvulner/rdp_hydra.txt 192.168.182.129 rdp)
# Hydra v9.5 run at 2024-03-09 23:38:55 on 192.168.182.254 rdp (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt
 -o /home/kali/projectvulner/rdp_hydra.txt 192.168.182.254 rdp)
# Hydra v9.5 run at 2024-03-09 23:39:28 on 192.168.182.135 rdp (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt
 -o /home/kali/projectvulner/rdp_hydra.txt 192.168.182.135 rdp)
[@] Bruteforce completed. No weak passwords were detected.
# Hydra v9.5 run at 2024-03-09 23:39:32 on 192.168.182.1 ftp (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt -
o /home/kali/projectvulner/ftp_hydra.txt 192.168.182.1 ftp)
# Hydra v9.5 run at 2024-03-09 23:40:05 on 192.168.182.2 ftp (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt -
o /home/kali/projectvulner/ftp_hydra.txt 192.168.182.2 ftp)
# Hydra v9.5 run at 2024-03-09 23:40:09 on 192.168.182.129 ftp (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt
 -o /home/kali/projectvulner/ftp_hydra.txt 192.168.182.129 ftp)
[21][ftp] host: 192.168.182.129   login: polarbear   password: 12345678
# Hydra v9.5 run at 2024-03-09 23:40:14 on 192.168.182.254 ftp (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt
 -o /home/kali/projectvulner/ftp_hydra.txt 192.168.182.254 ftp)
# Hydra v9.5 run at 2024-03-09 23:40:47 on 192.168.182.135 ftp (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.txt
 -o /home/kali/projectvulner/ftp_hydra.txt 192.168.182.135 ftp)
[!] Bruteforce successful. Weak password found: 12345678
# Hydra v9.5 run at 2024-03-09 23:40:51 on 192.168.182.1 telnet (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.tx
t -o /home/kali/projectvulner/telnet_hydra.txt 192.168.182.1 telnet)
# Hydra v9.5 run at 2024-03-09 23:41:24 on 192.168.182.2 telnet (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.tx
t -o /home/kali/projectvulner/telnet_hydra.txt 192.168.182.2 telnet)
# Hydra v9.5 run at 2024-03-09 23:41:28 on 192.168.182.129 telnet (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.
txt -o /home/kali/projectvulner/telnet_hydra.txt 192.168.182.129 telnet)
# Hydra v9.5 run at 2024-03-09 23:41:32 on 192.168.182.254 telnet (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.
txt -o /home/kali/projectvulner/telnet_hydra.txt 192.168.182.254 telnet)
# Hydra v9.5 run at 2024-03-09 23:42:05 on 192.168.182.135 telnet (hydra -l polarbear -P /home/kali/Desktop/myprivatedir/myownpwlist.
txt -o /home/kali/projectvulner/telnet_hydra.txt 192.168.182.135 telnet)
[@] Bruteforce completed. No weak passwords were detected.
```

```
POTENTIAL VULNERABILITIES:
[i] SearchSploit's XML mode (without verbose enabled).   To enable: searchsploit -v --xml ...
[i] Reading: '/home/kali/projectvulner/full_nmap.xml'

[i] /usr/bin/searchsploit -t netbios ssn
[i] /usr/bin/searchsploit -t microsoft windows netbios ssn
[i] /usr/bin/searchsploit -t microsoft ds
[-] Skipping output: microsoft ds   (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t microsoft ds)

[i] /usr/bin/searchsploit -t vmware auth
---------------------------------------------------------------------------------------------
 Exploit Title                                                    |  Path
---------------------------------------------------------------------------------------------
VMware 2.5.1 - 'VMware-authd' Remote Denial o                     | multiple/dos/7647.txt
VMware GSX Server 2.0 - Authentication Server                     | windows/remote/21639.c
VMware Player / VMware Workstation 6.5.3 - 'V                     | windows/dos/33271.py
VMware vCenter Server 6.7 - Authentication By                     | multiple/webapps/48535.txt
VMware vCenter Server 7.0 - Remote Code Execu                     | multiple/webapps/50056.py
VMware vCenter Server 7.0 - Unauthenticated F                     | multiple/webapps/49602.py
---------------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results


[i] /usr/bin/searchsploit -t vmware authentication daemon
[i] /usr/bin/searchsploit -t vmware authentication daemon 1.10
[i] /usr/bin/searchsploit -t vmware authentication daemon 1.0
[i] /usr/bin/searchsploit -t domain
[-] Skipping output: domain   (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t domain)

[i] /usr/bin/searchsploit -t cloudflare public dns
[-] Skipping term: ftp   (Term is too general. Please re-search manually: /usr/bin/searchsploit -t ftp)

[i] /usr/bin/searchsploit -t vsftpd
---------------------------------------------------------------------------------------------
 Exploit Title                                                    |  Path
---------------------------------------------------------------------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote M                     | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Deni                     | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Deni                     | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                  | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                         | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Me                     | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                           | multiple/remote/49719.py
---------------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
```

```
[i] /usr/bin/searchsploit -t vsftpd 2.3.4
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution     | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Me | unix/remote/17491.rb
---------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results


[-] Skipping term: ssh   (Term is too general. Please re-search manually: /usr/bin/searchsploit -t ssh)

[i] /usr/bin/searchsploit -t openssh
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
Debian OpenSSH - (Authenticated) Remote SELin | linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIEN | multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execut | freebsd/remote/17462.txt
glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9x -  | linux/local/258.sh
Novell Netware 6.5 - OpenSSH Remote Stack Ove | novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite    | linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration      | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC | linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by | unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Bu | linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overf | unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Overf | unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote Deni | multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Esc | linux/local/41173.c
OpenSSH 7.2 - Denial of Service               | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration          | linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Execution  | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution        | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disab | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Libr | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)          | linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files    | multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Users | linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discovery  | linux/remote/25.c
OpenSSHd 7.2p2 - Username Enumeration         | linux/remote/40113.txt
Portable OpenSSH 3.6.1p-PAM/4.1-SuSE - Timing | multiple/remote/3303.sh
---------------------------------------------- ---------------------------------
Shellcodes: No Results
---------------------------------------------- ---------------------------------
 Paper Title                                  |  Path
---------------------------------------------- ---------------------------------
Roaming Through the OpenSSH Client: CVE-2016- | english/39247-roaming-through-th
```

```
[i] /usr/bin/searchsploit -t openssh 4.7p1 debian 8ubuntu1
[i] /usr/bin/searchsploit -t telnet
---------------------------------------------------------- ---------------------------------
 Exploit Title                                            |  Path
---------------------------------------------------------- ---------------------------------
3Com SuperStack II PS Hub 40 - TelnetD Weak P | hardware/remote/21011.pl
602Pro LAN SUITE 2002 - Telnet Proxy localhos | windows/dos/21694.pl
AbsoluteTelnet 10.16 - 'License name' Denial  | windows/dos/46874.py
AbsoluteTelnet 11.12 - 'license name' Denial  | windows/dos/48006.py
AbsoluteTelnet 11.12 - 'SSH1/username' Denial | windows/dos/48305.py
AbsoluteTelnet 11.12 - 'SSH2/username' Denial | windows/dos/48010.py
AbsoluteTelnet 11.12 - _license name_ Denial  | windows/dos/48005.py
AbsoluteTelnet 11.21 - 'Username' Denial of S | windows/dos/48493.py
AbsoluteTelnet 11.24 - 'Phone' Denial of Serv | windows/dos/50511.py
AbsoluteTelnet 11.24 - 'Username' Denial of S | windows/dos/50510.py
Accu-Time Systems MAXIMUS 1.0 - Telnet Remote | hardware/remote/50620.py
APC WEB/SNMP Management Card (9606) Firmware  | hardware/dos/20654.pl
Apple Mac OSX 10.2 - Terminal.APP Telnet Link | osx/local/21815.txt
Arescom NetDSL-1000 - 'TelnetD' Remote Denial | hardware/dos/1464.c
Beck IPC GmbH IPC@CHIP - TelnetD Login Accoun | multiple/remote/20881.txt
BSD - 'TelnetD' Remote Command Execution (1)  | bsd/remote/409.c
BSD - 'TelnetD' Remote Command Execution (2)  | bsd/remote/19520.txt
Byte Fusion BFTelnet 1.1 - Long Username Deni | windows/dos/19596.txt
CCProxy 6.2 - Telnet Proxy Ping Overflow (Met | windows/remote/4360.rb
Celestial Software AbsoluteTelnet 2.0/2.11 -  | windows/remote/22229.pl
CHIYU IoT Devices - 'Telnet' Authentication B | hardware/remote/49936.py
Cypress Solutions CTM-200/CTM-ONE - Hard-code | hardware/remote/50407.py
D-Link Devices - UPnP SOAP TelnetD Command Ex | unix/remote/28333.rb
Denver Smart Wifi Camera SHC-150 - 'Telnet' R | hardware/remote/50160.txt
FreeBSD - Telnet Service Encryption Key ID Bu | bsd/remote/18369.rb
FreeBSD 7.0-RELEASE - Telnet Daemon Privilege | freebsd/local/8055.txt
GNU inetutils < 1.9.4 - 'telnet.c' Multiple O | linux/dos/45982.txt
GoodTech Telnet Server 4.0 - Remote Denial of | windows/dos/23506.txt
GoodTech Telnet Server 5.0.6 - Remote Buffer  | windows/remote/16817.rb
GoodTech Telnet Server < 5.0.7 - Buffer Overf | windows/dos/882.cpp
GoodTech Telnet Server < 5.0.7 - Remote Buffe | windows/remote/883.c
GoodTech Telnet Server NT 2.2.1 - Denial of S | windows/dos/19666.txt
Herospeed - 'TelnetSwitch' Remote Stack Overf | hardware/remote/43997.py
Hilgraeve HyperTerminal 6.0 - Telnet Buffer O | windows/dos/20307.txt
IRIX 5.2/5.3/6.x - TelnetD Environment Variab | irix/remote/20149.c
Jordan Windows Telnet Server 1.0/1.2 - 'Usern | windows/remote/23491.pl
Jordan Windows Telnet Server 1.0/1.2 - 'Usern | windows/remote/23492.c
Jordan Windows Telnet Server 1.0/1.2 - 'Usern | windows/remote/23493.txt
Kroum Grigorov KpyM Telnet Server 1.0 - Remot | windows/dos/23530.c
Linux BSD-derived Telnet Service Encryption K | linux/remote/18368.rb
Microsoft Internet Explorer 5.0.1/5.5/6.0 - T | windows/remote/20680.html
Microsoft Windows 95/98 Internet Explorer 5/T | windows/local/19462.c
Microsoft Windows NT 3.5.1 SP2/3.5.1 SP3/3.5. | windows/remote/19113.txt
Microsoft Windows Server 2000 - 'telnet.exe'  | windows/remote/20222.cpp
Microsoft Windows Server 2000 - Telnet 'Usern | windows/dos/20907.sh
Microsoft Windows Server 2000 - Telnet Server | windows/dos/20047.txt
```

```
Mocha Telnet Lite for iOS 4.2 - 'User' Denial | windows/dos/48728.py
Multiple Vendor Telnet Client - Env_opt_add H | linux/dos/25303.txt
Netgear - 'TelnetEnable' Magic Packet (Metasp | hardware/remote/44245.rb
netkit-telnet-0.17 telnetd (Fedora 31) - 'Bra | linux/remote/48170.py
NUUO NVRMini2 3.8 - 'cgi_system' Buffer Overf | hardware/remote/45427.py
Polycom HDX - Telnet Authentication Bypass (M | hardware/remote/24494.rb
Pragma Systems InterAccess TelnetD Server 4.0 | windows/dos/19755.txt
Pragma Systems InterAccess TelnetD Server 4.0 | windows/dos/19760.txt
Pragma Systems InterAccess TelnetD Server 4.0 | windows/dos/20904.pl
Pragma TelnetServer 7.0.4.589 - NULL-Pointer  | multiple/dos/30991.txt
PragmaSys TelnetServer 2000 - rexec Buffer Ov | windows/dos/20175.pl
ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet | linux/remote/16878.rb
ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet I | linux/remote/16851.rb
Sagem F@st 3304-V2 - Telnet Crash (PoC)       | hardware/dos/36309.py
Sagem Router Fast 3304/3464/3504 - Telnet Aut | hardware/remote/17670.py
Solaris 10/11 Telnet - Remote Authentication  | solaris/remote/9918.rb
Solaris 2.6/7/8 - 'TTYPROMPT in.telnet' Remot | solaris/remote/57.txt
Solaris 2.x/7.0/8 / IRIX 6.5.x / OpenBSD 2.x  | unix/remote/21018.c
Solaris TelnetD - 'TTYPROMPT' Remote Buffer O | solaris/remote/16327.rb
Solaris TelnetD - 'TTYPROMPT' Remote Buffer O | solaris/remote/9917.rb
Sun Solaris Telnet - Remote Authentication By | solaris/remote/16328.rb
SunOS 5.10/5.11 in.TelnetD - Remote Authentic | solaris/remote/3293.sh
Telnet-Ftp Service Server 1.x - (Authenticate | windows/remote/8273.c
TelnetD encrypt_keyid - Function Pointer Over | linux/remote/18280.c
Verso NetPerformer Frame Relay Access Device  | multiple/dos/28542.pl
---------------------------------------------- ----------------------------------
---------------------------------------------- ----------------------------------
 Shellcode Title                              |  Path
---------------------------------------------- ----------------------------------
Google Android - Bind (1035/TCP) Telnetd Shel | android/38194.c
Linux/MIPS (Little Endian) - system(telnetd - | linux_mips/27132.txt
Linux/x86 - Reverse (200.182.207.235/TCP) Tel | linux_x86/13435.c
Windows/x86 - Add Administrator User (GAZZA/1 | windows_x86/13508.asm
---------------------------------------------- ----------------------------------
Papers: No Results


[i] /usr/bin/searchsploit -t linux telnetd
Exploits: No Results
---------------------------------------------- ----------------------------------
 Shellcode Title                              |  Path
---------------------------------------------- ----------------------------------
Linux/MIPS (Little Endian) - system(telnetd - | linux_mips/27132.txt
---------------------------------------------- ----------------------------------
Papers: No Results
```

```
[i] /usr/bin/searchsploit -t smtp
---------------------------------------------- ----------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ----------------------------------
AA SMTP Server 1.1 - Crash (PoC)              | windows/dos/14990.txt
Alt-N MDaemon 6.5.1 - IMAP/SMTP Remote Buffer | windows/remote/473.c
Alt-N MDaemon 6.5.1 SMTP Server - Multiple Co | windows/remote/24624.c
Alt-N MDaemon Server 2.71 SP1 - SMTP HELO Arg | windows/dos/23146.c
Apache James Server 2.2 - SMTP Denial of Serv | multiple/dos/27915.pl
BaSoMail 1.24 - SMTP Server Command Buffer Ov | windows/dos/22668.txt
BaSoMail Server 1.24 - POP3/SMTP Remote Denia | windows/dos/594.pl
BL4 SMTP Server < 0.1.5 - Remote Buffer Overf | windows/dos/1721.pl
Blat 2.7.6 SMTP / NNTP Mailer - Local Buffer  | windows/local/38472.py
BulletProof FTP Server 2019.0.0.50 - 'SMTP Se | windows/dos/46422.py
Cisco PIX Firewall 4.x/5.x - SMTP Content Fil | hardware/remote/20231.txt
Citadel SMTP 7.10 - Remote Overflow           | windows/remote/4949.txt
Cobalt Raq3 PopRelayD - Arbitrary SMTP Relay  | linux/remote/20994.txt
CodeBlue 5.1 - SMTP Response Buffer Overflow  | windows/remote/21643.c
CommuniCrypt Mail 1.16 - 'ANSMTP.dll/AOSMTP.d | windows/remote/12663.html
CommuniCrypt Mail 1.16 - SMTP ActiveX Stack B | windows/remote/16566.rb
Computalynx CMail 2.3 SP2/2.4 - SMTP Buffer O | windows/remote/19495.c
DeepOfix SMTP Server 3.3 - Authentication Byp | linux/remote/29706.txt
dSMTP Mail Server 3.1b (Linux) - Format Strin | linux/remote/981.c
EasyMail Objects 'EMSMTP.DLL 6.0.1' - ActiveX | windows/remote/10007.html
EType EServ 2.9x - SMTP Remote Denial of Serv | windows/dos/22123.pl
Eudora 7.1 - SMTP ResponseRemote Remote Buffe | windows/remote/3934.py
Exim ESMTP 4.80 - glibc gethostbyname Denial  | linux/dos/35951.py
FloosieTek FTGate PRO 1.22 - SMTP MAIL FROM B | windows/dos/22568.pl
FloosieTek FTGate PRO 1.22 - SMTP RCPT TO Buf | windows/dos/22569.pl
Free SMTP Server 2.2 - Spam Filter            | windows/remote/1193.pl
Free SMTP Server 2.5 - Denial of Service (PoC | windows/dos/46937.py
GetSimple CMS My SMTP Contact Plugin 1.1.1 -  | php/webapps/49774.py
GetSimple CMS My SMTP Contact Plugin 1.1.2 -  | php/webapps/49798.py
GoodTech SMTP Server 5.14 - Denial of Service | windows/dos/1162.pl
Hastymail 1.x - IMAP SMTP Command Injection   | php/webapps/28777.txt
i.Scribe SMTP Client 2.00b - 'wscanf' Remote  | windows/dos/7249.php
Inetserv 3.23 - SMTP Denial of Service        | windows/dos/16035.py
Inframail Advantage Server Edition 6.0 < 6.37 | windows/dos/1165.pl
Ipswitch Imail Server 5.0 - SMTP HELO Argumen | windows/dos/23145.c
iScripts AutoHoster - 'main_smtp.php' Travers | php/webapps/38889.txt
Jack De Winter WinSMTP 1.6 f/2.0 - Buffer Ove | windows/dos/20221.pl
LeadTools Imaging LEADSmtp - ActiveX Control  | windows/remote/35880.html
Lotus Domino 4.6.1/4.6.4 Notes - SMTPA MTA Ma | multiple/dos/19368.sh
Lotus Domino SMTP Router & Email Server and C | multiple/dos/17549.txt
MailEnable 1.x - SMTP 'HELO' Remote Denial of | windows/dos/28103.pl
MailEnable 2.x - SMTP NTLM Multiple Authentic | windows/dos/28735.pl
MailEnable 3.13 SMTP Service - 'VRFY/EXPN' De | windows/dos/5235.py
MailEnable Enterprise 1.x - SMTP Remote Denia | windows/dos/916.pl
MAILsweeper SMTP 4.2.1 + F-Secure Anti-Virus  | windows/dos/21006.txt
Mailtraq 2.1.0.1302 - Remote Format String SM | windows/dos/22780.txt
```

```
Majordomo2 - 'SMTP/HTTP' Directory Traversal  | multiple/remote/16103.txt
MDaemon SMTP Server 5.0.5 - Null Password Aut | windows/remote/23002.txt
Mercury/32 Mail Server 3.32 < 4.51 - SMTP EIP | windows/remote/4316.cpp
Mercury/32 Mail SMTPD - AUTH CRAM-MD5 Buffer  | windows/remote/16821.rb
Mercury/32 Mail SMTPD - Remote Stack Overrun  | windows/dos/4294.pl
Mercury/32 Mail SMTPD 4.51 - SMTPD CRAM-MD5 R | windows/remote/4301.cpp
Microsoft Exchange Server 4.0/5.0 - SMTP HELO | windows/remote/23113.c
Microsoft IIS 4.0/5.0 - SMTP Service Encapsul | windows/remote/21613.txt
Microsoft Windows - ANI LoadAniIcon() Chunk S | windows/remote/16698.rb
MIMEsweeper For SMTP - Multiple Cross-Site Sc | asp/webapps/38318.txt
Mock SMTP Server 1.0 - Remote Crash (PoC)     | windows/dos/37954.py
nbSMTP 0.99 - 'util.c' Client-Side Command Ex | linux/remote/1138.c
NetcPlus SmartServer 3.5.1 - SMTP Buffer Over | windows/remote/19494.c
Network Associates Webshield SMTP 4.5 - Inval | windows/dos/20432.txt
NJStar Communicator 3.00 - MiniSMTP Server Re | windows/remote/18057.rb
NJStar Communicator MiniSmtp - Buffer Overflo | windows/dos/18196.py
OpenSMTPD - MAIL FROM Remote Code Execution ( | linux/remote/48038.rb
OpenSMTPD - OOB Read Local Privilege Escalati | linux/local/48185.rb
OpenSMTPD 6.4.0 < 6.6.1 - Local Privilege Esc | openbsd/remote/48051.pl
OpenSMTPD 6.6.1 - Remote Code Execution       | linux/remote/47984.py
OpenSMTPD 6.6.3 - Arbitrary File Read         | linux/remote/48139.c
OpenSMTPD < 6.6.3p1 - Local Privilege Escalat | openbsd/remote/48140.c
Postcast Server Pro 3.0.61 / Quiksoft EasyMai | windows/remote/4328.html
Postfix SMTP 4.2.x < 4.2.48 - 'Shellshock' Re | linux/remote/34896.py
Python smtplib 2.7.11 / 3.4.4 / 3.5.1 - Man I | multiple/local/43500.txt
QK SMTP 3.01 - 'RCPT TO' Remote Buffer Overfl | windows/remote/2649.c
QK SMTP 3.01 - 'RCPT TO' Remote Buffer Overfl | windows/remote/3067.py
QK SMTP 3.01 - 'RCPT TO' Remote Denial of Ser | windows/dos/2625.c
QK SMTP Server - Malformed Commands Multiple  | multiple/dos/30885.txt
Qmail SMTP - Bash Environment Variable Inject | linux/remote/42938.rb
Qmail SMTP 1.03 - Bash Environment Variable I | multiple/remote/48651.txt
Qwik SMTP 0.3 - Format String                 | linux/remote/620.c
Sitemagic CMS - 'SMTpl' Directory Traversal   | php/webapps/35877.txt
SmartMax MailMax 1.0 - SMTP Buffer Overflow   | windows/remote/20600.c
Softek MailMarshal 4 / Trend Micro ScanMail 1 | multiple/remote/21029.pl
SoftiaCom wMailServer 1.0 - SMTP Remote Buffe | windows/remote/1463.pm
SPECTral Personal SMTP Server 0.4.2 - Denial  | windows/dos/899.pl
SquirrelMail PGP Plugin - Command Execution ( | linux/remote/16888.rb
sSMTP 2.62 - 'standardize()' Buffer Overflow  | linux/dos/34375.txt
SynaMan 4.0 build 1488 - SMTP Credential Disc | windows/webapps/45387.txt
SysGauge 1.5.18 - SMTP Validation Buffer Over | windows/remote/41672.rb
TABS MailCarrier 2.51 - SMTP 'EHLO' / 'HELO'  | windows/remote/598.py
TABS MailCarrier 2.51 - SMTP EHLO Overflow (M | windows/remote/16822.rb
YahooPOPs 1.6 - SMTP Port Buffer Overflow     | windows/remote/577.c
YahooPOPs 1.6 - SMTP Remote Buffer Overflow   | windows/remote/582.c
---------------------------------------------- ----------------------------------
Shellcodes: No Results
Papers: No Results
```

```
[i] /usr/bin/searchsploit -t postfix smtpd
[i] /usr/bin/searchsploit -t isc bind
---------------------------------------------- ----------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ----------------------------------
ISC BIND (Linux/BSD) - Remote Buffer Overflow | linux/remote/19111.c
ISC BIND (Multiple OSes) - Remote Buffer Over | linux/remote/19112.c
ISC BIND 4.9.7 -T1B - named SIGINT / SIGIOT S | linux/local/19072.txt
ISC BIND 4.9.7/8.x - Traffic Amplification an | multiple/remote/19749.txt
ISC BIND 8 - Remote Cache Poisoning (1)       | linux/remote/30535.pl
ISC BIND 8 - Remote Cache Poisoning (2)       | linux/remote/30536.pl
ISC BIND 8.1 - Host Remote Buffer Overflow    | unix/remote/20374.c
ISC BIND 8.2.2 / IRIX 6.5.17 / Solaris 7.0 -  | unix/dos/19615.c
ISC BIND 8.2.2-P5 - Denial of Service         | linux/dos/20388.txt
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow | linux/remote/277.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow | linux/remote/279.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow | linux/remote/282.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow | solaris/remote/280.c
ISC BIND 8.3.x - OPT Record Large UDP Denial  | linux/dos/22011.c
ISC BIND 9 - Denial of Service                | multiple/dos/40453.py
ISC BIND 9 - Remote Dynamic Update Message De | multiple/dos/9300.c
ISC BIND 9 - TKEY (PoC)                       | multiple/dos/37721.c
ISC BIND 9 - TKEY Remote Denial of Service (P | multiple/dos/37723.py
Microsoft Windows Kernel - 'win32k!NtQueryCom | windows/dos/42750.cpp
Zabbix 2.0.5 - Cleartext ldap_bind_Password P | php/webapps/36157.rb
---------------------------------------------- ----------------------------------
Shellcodes: No Results
Papers: No Results


[i] /usr/bin/searchsploit -t isc bind 9.4.2
[-] Skipping term: http   (Term is too general. Please re-search manually: /usr/bin/searchsploit -t http)

[i] /usr/bin/searchsploit -t apache httpd
---------------------------------------------- ----------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ----------------------------------
Apache 0.8.x/1.0.x / NCSA HTTPd 1.x - 'test-c | cgi/remote/20435.txt
Apache 1.1 / NCSA HTTPd 1.5.2 / Netscape Serv | multiple/dos/19536.txt
Apache Httpd mod_proxy - Error Page Cross-Sit | multiple/webapps/47688.md
Apache Httpd mod_rewrite - Open Redirects     | multiple/webapps/47689.md
NCSA 1.3/1.4.x/1.5 / Apache HTTPd 0.8.11/0.8. | multiple/remote/20595.txt
---------------------------------------------- ----------------------------------
Shellcodes: No Results
Papers: No Results
```

```
[i] /usr/bin/searchsploit -t apache httpd 2.2.8
[i] /usr/bin/searchsploit -t rpcbind 2
---------------------------------------------------------------------------------------------
 Exploit Title                                                |  Path
---------------------------------------------------------------------------------------------
Wietse Venema Rpcbind Replacement 2.1 - Denia                 | unix/dos/20376.txt
---------------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results


[i] /usr/bin/searchsploit -t samba smbd
[i] /usr/bin/searchsploit -t samba smbd 3.x   4.x
[i] /usr/bin/searchsploit -t samba smbd 3.0.20 debian
[i] /usr/bin/searchsploit -t exec
[-] Skipping output: exec   (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t exec)

[i] /usr/bin/searchsploit -t netkit rsh rexecd
[i] /usr/bin/searchsploit -t login
[-] Skipping output: login   (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t login)

[i] /usr/bin/searchsploit -t tcpwrapped
[i] /usr/bin/searchsploit -t java rmi
---------------------------------------------------------------------------------------------
 Exploit Title                                                |  Path
---------------------------------------------------------------------------------------------
HPE iMC 7.3 - RMI Java Deserialization                        | windows/remote/43927.txt
Java - RMIConnectionImpl Deserialization Priv                 | multiple/remote/16305.rb
Java RMI - Server Insecure Default Configurat                 | multiple/remote/17535.rb
Jenkins CLI - RMI Java Deserialization (Metas                 | java/remote/38983.rb
Oracle WebLogic 12.1.2.0 - RMI Registry Unica                 | multiple/webapps/44998.py
---------------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results


[i] /usr/bin/searchsploit -t gnu classpath grmiregistry
[i] /usr/bin/searchsploit -t bindshell
[i] /usr/bin/searchsploit -t metasploitable root shell
[i] /usr/bin/searchsploit -t nfs 2 4
---------------------------------------------------------------------------------------------
 Exploit Title                                                |  Path
---------------------------------------------------------------------------------------------
Apple Mac OSX (Lion) Kernel xnu-1699.32.7 exc                 | osx/local/32813.c
Linux Kernel < 2.6.31-rc4 - 'nfs4_proc_lock()                 | linux/dos/10202.c
NfSen < 1.3.7 / AlienVault OSSIM < 5.3.6 - Lo                 | linux/local/42305.txt
---------------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
```

```
[i] /usr/bin/searchsploit -t proftpd
---------------------------------------------------------------------------------------
 Exploit Title                                                         |  Path
---------------------------------------------------------------------------------------
FreeBSD - 'ftpd / ProFTPd' Remote Command Exe                          | freebsd/remote/18181.txt
ProFTPd - 'ftpdctl' 'pr_ctrls_connect' Local                           | linux/local/394.c
ProFTPd - 'mod_mysql' Authentication Bypass                            | multiple/remote/8037.txt
ProFTPd - 'mod_sftp' Integer Overflow Denial                           | linux/dos/16129.txt
ProFTPd 1.2 - 'SIZE' Remote Denial of Service                          | linux/dos/20536.java
ProFTPd 1.2 < 1.3.0 (Linux) - 'sreplace' Remo                          | linux/remote/16852.rb
ProFTPd 1.2 pre1/pre2/pre3/pre4/pre5 - Remote                          | linux/remote/19475.c
ProFTPd 1.2 pre1/pre2/pre3/pre4/pre5 - Remote                          | linux/remote/19476.c
ProFTPd 1.2 pre6 - 'snprintf' Remote Root                              | linux/remote/19503.txt
ProFTPd 1.2.0 pre10 - Remote Denial of Servic                          | linux/dos/244.java
ProFTPd 1.2.0 rc2 - Memory Leakage                                     | linux/dos/241.c
ProFTPd 1.2.10 - Remote Users Enumeration                              | linux/remote/581.c
ProFTPd 1.2.7 < 1.2.9rc2 - Remote Code Execut                          | linux/remote/110.c
ProFTPd 1.2.7/1.2.8 - '.ASCII' File Transfer                           | linux/dos/23170.c
ProFTPd 1.2.9 RC1 - 'mod_sql' SQL Injection                            | linux/remote/43.pl
ProFTPd 1.2.9 rc2 - '.ASCII' File Remote Code                          | linux/remote/107.c
ProFTPd 1.2.9 rc2 - '.ASCII' File Remote Code                          | linux/remote/3021.txt
ProFTPd 1.2.x - 'STAT' Denial of Service                               | linux/dos/22079.sh
ProFTPd 1.3 - 'mod_sql' 'Username' SQL Inject                          | multiple/remote/32798.pl
ProFTPd 1.3.0 (OpenSUSE) - 'mod_ctrls' Local                           | unix/local/10044.pl
ProFTPd 1.3.0 - 'sreplace' Remote Stack Overf                          | linux/remote/2856.pm
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' 'support'                           | linux/local/3330.pl
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' 'support'                           | linux/local/3333.pl
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' exec-shiel                          | linux/local/3730.txt
ProFTPd 1.3.0a - 'mod_ctrls' 'support' Local                           | linux/dos/2928.py
ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet                          | linux/remote/16878.rb
ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet I                          | linux/remote/16851.rb
ProFTPd 1.3.3c - Compromised Source Backdoor                           | linux/remote/15662.txt
ProFTPd 1.3.5 - 'mod_copy' Command Execution                           | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Exe                          | linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Exe                          | linux/remote/49908.py
ProFTPd 1.3.5 - File Copy                                              | linux/remote/36742.txt
ProFTPD 1.3.7a - Remote Denial of Service                              | multiple/dos/49697.py
ProFTPd 1.x - 'mod_tls' Remote Buffer Overflo                          | linux/remote/4312.c
ProFTPd IAC 1.3.x - Remote Command Execution                           | linux/remote/15449.pl
ProFTPd-1.3.3c - Backdoor Command Execution (                          | linux/remote/16921.rb
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFT                          | linux/remote/19086.c
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFT                          | linux/remote/19087.c
WU-FTPD 2.4/2.5/2.6 / Trolltech ftpd 1.2 / Pr                          | linux/remote/20690.sh
---------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results


[i] /usr/bin/searchsploit -t proftpd 1.3.1
[i] /usr/bin/searchsploit -t mysql
```

```
[-] Skipping output: mysql   (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t mysql)

[i] /usr/bin/searchsploit -t mysql 5.0.51a 3ubuntu5
---------------------------------------------------------------------------------------
 Exploit Title                                                         |  Path
---------------------------------------------------------------------------------------
MySQL < 5.6.35 / < 5.7.17 - Integer Overflow                           | multiple/dos/41954.py
MySQL < 5.6.35 / < 5.7.17 - Integer Overflow                           | multiple/dos/41954.py
Oracle MySQL < 5.1.49 - 'DDL' Statements Deni                          | linux/dos/34522.txt
Oracle MySQL < 5.1.49 - 'WITH ROLLUP' Denial                           | multiple/dos/15467.txt
Oracle MySQL < 5.1.49 - Malformed 'BINLOG' Ar                          | linux/dos/34521.txt
Oracle MySQL < 5.1.50 - Privilege Escalation                           | multiple/remote/34796.txt
---------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results


[i] /usr/bin/searchsploit -t postgresql
---------------------------------------------------------------------------------------
 Exploit Title                                                         |  Path
---------------------------------------------------------------------------------------
PnPSCADA v2.x - Unauthenticated PostgreSQL In                          | hardware/webapps/51448.txt
PostgreSQL - 'bitsubstr' Buffer Overflow                               | linux/dos/33571.txt
PostgreSQL 6.3.2/6.5.3 - Cleartext Passwords                           | immunix/local/19875.txt
PostgreSQL 7.x - Multiple Vulnerabilities                              | linux/dos/25076.c
PostgreSQL 8.01 - Remote Reboot (Denial of Se                          | multiple/dos/946.c
PostgreSQL 8.2/8.3/8.4 - UDF for Command Exec                          | linux/local/7855.txt
PostgreSQL 8.3.6 - Conversion Encoding Remote                          | linux/dos/32849.txt
PostgreSQL 8.3.6 - Low Cost Function Informat                          | multiple/local/32847.txt
PostgreSQL 8.4.1 - JOIN Hashtable Size Intege                          | multiple/dos/33729.txt
PostgreSQL 9.3 - COPY FROM PROGRAM Command Ex                          | multiple/remote/46813.rb
PostgreSQL 9.3-11.7 - Remote Code Execution (                          | multiple/remote/50847.py
PostgreSQL 9.4-0.5.3 - Privilege Escalation                            | linux/local/45184.sh
PostgreSQL 9.6.1 - Remote Code Execution (RCE                          | multiple/remote/51247.py
---------------------------------------------------------------------------------------
Shellcodes: No Results
---------------------------------------------------------------------------------------
 Paper Title                                                           |  Path
---------------------------------------------------------------------------------------
Advanced PostgreSQL SQL Injection and Filter                           | docs/english/12909-advanced-post
Having Fun With PostgreSQL                                             | english/13084-having-fun-with-po
---------------------------------------------------------------------------------------
```

```
[i] /usr/bin/searchsploit -t postgresql db
[i] /usr/bin/searchsploit -t postgresql db 8.3.0   8.3.7
[i] /usr/bin/searchsploit -t vnc
---------------------------------------------------------------------------------------------
 Exploit Title                                                    |  Path
---------------------------------------------------------------------------------------------
AMX Corp. VNC ActiveX Control - 'AmxVnc.dll 1                     | windows/remote/4123.html
Chicken of the VNC 2.0 - 'NULL-pointer' Remot                     | osx/dos/3257.php
EchoVNC Viewer - Remote Denial of Service                         | windows/dos/27292.py
QEMU 0.9 / KVM 36/79 - VNC Server Remote Deni                     | linux/dos/32675.py
RealVNC - Authentication Bypass (Metasploit)                      | windows/remote/17719.rb
RealVNC 3.3.7 - Client Buffer Overflow (Metas                     | windows/remote/16489.rb
RealVNC 4.1.0 < 4.1.1 - VNC Null Authenticati                     | multiple/remote/1791.patch
RealVNC 4.1.0 < 4.1.1 - VNC Null Authenticati                     | multiple/remote/1794.pm
RealVNC 4.1.0 < 4.1.1 - VNC Null Authenticati                     | multiple/remote/1799.txt
RealVNC 4.1.0/4.1.1 - Authentication Bypass                       | windows/remote/36932.py
RealVNC 4.1.2 - 'vncviewer.exe' RFB Protocol                      | windows/dos/7943.py
RealVNC 4.1.3 - 'ClientCutText' Message Remot                     | windows/dos/33924.py
RealVNC Server 4.0 - Remote Denial of Service                     | windows/dos/24412.c
RealVNC Windows Client 4.1.2 - Remote Denial                      | windows/dos/6181.php
SmartCode ServerX VNC Server ActiveX 1.1.5.0                      | windows/dos/14634.txt
SmartCode VNC Manager 3.6 - 'scvncctrl.dll' D                     | windows/dos/3873.html
Sun SunPCi II VNC Software 2.3 - Password Dis                     | unix/local/21592.c
ThinVNC 1.0b1 - Authentication Bypass                             | windows/remote/47519.py
TightVNC - Authentication Failure Integer Ove                     | windows/dos/8024.py
Ultr@VNC 1.0.1 - 'client Log::ReallyPrint' Bu                     | windows/dos/1643.c
Ultr@VNC 1.0.1 - 'client Log::ReallyPrint' Re                     | windows/remote/1664.py
Ultr@VNC 1.0.1 - VNCLog::ReallyPrint Remote B                     | windows/dos/1642.c
UltraVNC 1.0.1 - Client Buffer Overflow (Meta                     | windows/remote/16490.rb
UltraVNC 1.0.1 - Multiple Remote Error Loggin                     | windows/remote/27568.py
UltraVNC 1.0.1 - Multiple Remote Error Loggin                     | windows/remote/27569.txt
UltraVNC 1.0.2 Client - 'vncviewer.exe' Remot                     | windows/remote/18666.rb
UltraVNC 1.0.8.2 - DLL Loading Arbitrary Code                     | windows/remote/34542.c
UltraVNC Launcher 1.2.2.4 - 'Path' Denial of                      | windows/dos/46703.py
UltraVNC Launcher 1.2.4.0 - 'Password' Denial                     | windows/dos/48290.py
UltraVNC Launcher 1.2.4.0 - 'RepeaterHost' De                     | windows/dos/48288.py
UltraVNC Viewer 1.2.2.4 - 'VNC Server' Denial                     | windows/dos/46702.py
UltraVNC Viewer 1.2.4.0 - 'VNCServer' Denial                      | windows/dos/48291.py
UltraVNC/TightVNC (Multiple VNC Clients) - Mu                     | windows/dos/7990.py
Vino VNC Server 3.7.3 - Persistent Denial of                      | linux/dos/28338.txt
VNC Keyboard - Remote Code Execution (Metaspl                     | multiple/remote/37598.rb
WinVNC Web Server 3.3.3r7 - GET Overflow (Met                     | windows/remote/16491.rb
---------------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
```

```
[i] /usr/bin/searchsploit -t x11
---------------------------------------------------------------------------------------------
 Exploit Title                                                    |  Path
---------------------------------------------------------------------------------------------
ASUS DSL-X11 ADSL Router - DNS Change                             | cgi/webapps/40373.sh
BSD/OS 2.1 / DG/UX 7.0 / Debian 1.3 / HP-UX 1                     | unix/local/19173.c
Eterm 0.8.10 / rxvt 2.6.1 / PuTTY 0.48 / X11R                     | multiple/dos/19984.c
Gnome 1.0/1.1 / Group X 11.0 / XFree86 X11R6                      | linux/dos/20023.c
SCO Open Server 5.0.5 / IRIX 6.2 ibX11/X11 To                     | multiple/local/19684.c
Slackware Linux 3.1 - '/usr/X11/bin/SuperProb                     | linux/local/19283.c
Solaris 5.5.1 X11R6.3 - xterm '-xrm' Local Pr                     | solaris/local/338.c
Tor (Linux) - X11 Linux Sandbox Breakout                          | linux/local/42626.c
X 11.0/3.3.3/3.3.4/3.3.5/3.3.6/4.0 - libX11 '                     | linux/local/20045.c
X.Org X11 (X11R6.9.0/X11R7.0) - Local Privile                     | linux/local/1596.txt
X.Org xorg-x11-xfs 1.0.2-3.1 - Local Race Con                     | linux/local/5167.sh
X11R6 3.3.3 - Symlink                                             | linux/local/19257.c
X11R6 < 6.4 XKEYBOARD (sco x86) - Local Buffe                     | sco/local/2332.c
X11R6 < 6.4 XKEYBOARD (solaris x86) - Local B                     | solaris/local/2331.c
X11R6 < 6.4 XKEYBOARD (Solaris/SPARC) - Local                     | solaris/local/2330.c
X11R6 < 6.4 XKEYBOARD (Solaris/SPARC) - Local                     | solaris/local/2360.c
XFree86 X11R6 3.3 XDM - Session Cookie Guessi                     | unix/remote/20993.c
XFree86 X11R6 3.3.2 XMan - ManPath Environmen                     | linux/local/21010.sh
XFree86 X11R6 3.3.5/3.3.6/4.0 Xserver - Denia                     | linux/dos/19950.c
XFree86 X11R6 3.3.x - Font Server Remote Buff                     | unix/remote/22036.pl
Xorg X11 Server (AIX) - Local Privilege Escal                     | aix/local/45938.pl
Xorg X11 Server - Local Privilege Escalation                      | unix/local/47701.rb
Xorg X11 Server - SUID privilege escalation (                     | multiple/local/45908.rb
xorg-x11-server 1.20.3 - Privilege Escalation                     | openbsd/local/45742.sh
xorg-x11-server < 1.20.1 - Local Privilege Es                     | linux/local/45832.py
xorg-x11-server < 1.20.3 (Solaris 11) - 'init                     | solaris/local/46142.sh
xorg-x11-server < 1.20.3 - 'modulepath' Local                     | multiple/local/45922.sh
xorg-x11-server < 1.20.3 - Local Privilege Es                     | multiple/local/45697.txt
---------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------
 Shellcode Title                                                  |  Path
---------------------------------------------------------------------------------------------
OSX/PPC - execve(/usr/X11R6/bin/xterm) Shellc                     | osx_ppc/13487.c
---------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------
 Paper Title                                                      |  Path
---------------------------------------------------------------------------------------------
PoC || GTFO 0x11                                                  | docs/english/40623-poc--gtfo-0x1
---------------------------------------------------------------------------------------------

[i] /usr/bin/searchsploit -t irc
[-] Skipping output: irc   (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t irc)
```

```
[i] /usr/bin/searchsploit -t unrealircd
 ---------------------------------------------- ---------------------------------
  Exploit Title                                |  Path
 ---------------------------------------------- ---------------------------------
UnrealIRCd 3.2.8.1 - Backdoor Command Executi | linux/remote/16922.rb
UnrealIRCd 3.2.8.1 - Local Configuration Stac | windows/dos/18011.txt
UnrealIRCd 3.2.8.1 - Remote Downloader/Execut | linux/remote/13853.pl
UnrealIRCd 3.x - Remote Denial of Service     | windows/dos/27407.pl
 ---------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results


[i] /usr/bin/searchsploit -t ajp13
[i] /usr/bin/searchsploit -t apache jserv
[i] /usr/bin/searchsploit -t apache tomcat coyote jsp engine
[i] /usr/bin/searchsploit -t apache tomcat coyote jsp engine 1.1
        [@] Full scan results displayed.

        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
```

```
        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
B

        [?] Searching within scan results. Please specify your search string: password:
        [#] Search Results:
[21][ftp] host: 192.168.182.129   login: polarbear   password: 12345678
        [@] Search for password: is completed.

        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
```

```
        [?] What would you like to do?:
                (A) Display full scan results.
                (B) Search within scan results.
                (C) Save results into a ZIP File.
                (D) Exit VulnScanr™
C

        [?] Saving scan results into ZIP File. Please specify your desired file name (without file extension): resultsvuln
  adding: masscan.txt (deflated 54%)
  adding: potential_vulns.txt (deflated 77%)
  adding: full_nmap.xml (deflated 82%)
  adding: full_nmap.txt (deflated 58%)
  adding: full_hydra.txt (deflated 87%)
        [@] Scan results are zipped into new file at: /home/kali/resultsvuln.zip
```

```
        [?] What would you like to do?:
            (A) Display full scan results.
            (B) Search within scan results.
            (C) Save results into a ZIP File.
            (D) Exit VulnScanr™
D
        [#] Exiting VulnScanr™ ...

┌──(kali㉿kali)-[~/projectvulner]
└─$ cd

┌──(kali㉿kali)-[~]
└─$ ls
beef       Downloads  home                       Music          Public       resultsvuln.zip  Videos
Desktop    go         impacket                   Pictures       Responder    Templates        webseclab9
Documents  gobuster   mongodb-linux-x86_64-3.4.7 projectvulner  resultsvuln  TheFatRat        zphisher-master

┌──(kali㉿kali)-[~]
└─$ sudo bash /home/kali/Desktop/vulnscanr.sh
[sudo] password for kali:
sudo: a password is required

┌──(kali㉿kali)-[~]
└─$ unzip resultsvuln.zip
Archive:  resultsvuln.zip
  inflating: masscan.txt
  inflating: potential_vulns.txt
  inflating: full_nmap.xml
  inflating: full_nmap.txt
  inflating: full_hydra.txt

┌──(kali㉿kali)-[~]
└─$ ls
beef       full_hydra.txt  gobuster     mongodb-linux-x86_64-3.4.7  projectvulner  resultsvuln.zip  webseclab9
Desktop    full_nmap.txt   home         Music                       Public         Templates        zphisher-master
Documents  full_nmap.xml   impacket     Pictures                    Responder      TheFatRat
Downloads  go              masscan.txt  potential_vulns.txt         resultsvuln    Videos

┌──(kali㉿kali)-[~]
└─$
```

END.