```
#!/bin/sh

#This script was inspired by Shields UP! to be a within-network network scanner, but with
#options not found with GRC's free version. Thus far, the script only scans and reports online
#devices and their first 1024 ports and is organized by menus from case conditionals within
#functions. The ability to close ports of own system from this shell script via user input
#will, hopefully, be added before 2015. The ability to close ports of other devices on own
#network using Ruby with Metasploit will, hopefully, be added before graduation for potential
#Student Innovation Project admission.

#Another way to think of this is as Nmap with readable, well-organized options


clear
echo " "
echo "Welcome to Cloaks&&Daggers - Shields UP! made multi-functional & interactive with
Nmap"
echo "Which option would you prefer? (Each option is exported to its own scan.txt file)"
echo " "
echo "1 - Network scan" #Scans all hosts on network without port scans
echo "2 - Network & port scan - submenu" #Scans all hosts on network with chosen port scans
echo "3 - Port scan of own system - submenu" #Scans own system with chosen port scans
echo "4 - Quit" #Exits out of the script
echo " "
echo -n "Option: "
read OPTION

case $OPTION in
        1)      echo "Scanning all IP addresses on network..."
                echo `nmap -sP 192.168.1.0/24` >netscan1.txt ;;

        2)      echo " "
                echo "Accessing network and port scan submenu..."
                echo " "
                echo "1 - Basic port scan" #Basic port scan of first 1024 ports
                echo "2 - TCP connect() scan" #3-way handshake to target OS for TCP
connection
                echo "3 - TCP SYN scan" #Sends raw packets to target and awaits response.
Open - SYN/ACK, Closed - RST, Filtered - no response
                echo "4 - TCP FIN scan" #Like SYN, but sends FIN packets can slip some non-
stateful firewalls. Closed - RST, Open/Filtered - no response
                echo "5 - TCP XMAS scan" #Like FIN, but uses FIN, URG, and PSH vs just FIN
                echo "6 - TCP NULL scan" #Like FIN and XMAS, but without activating flags
```

```
		echo "7 - TCP ACK scan" #SYN scan for (non)stateful firewalls. Non & no response - ACK, Non & Open/Closed - RST, Stateful - no response
		echo "8 - TCP Window scan" #Like ACK, but filters Open and Closed. Open - window size > 0, Closed - window size = 0
		echo "9 - UDP scan" #Used for DNS/DHCP. Closed - ICMP Port Unreachable, Filtered - other ICMP Unreachable, Open - UDP
		echo "10 - IP Protocol scan" #Not a true port scan. UDP scan with raw IP packets. Closed - ICMP Port Unreachable, Filtered - other ICMP Unreachable, Open - UDP
		echo "0 - return to previous menu"

		echo " "
		echo -n "Option: "
		read OPTION2

		case $OPTION2 in
			1)	echo "Running basic port scan of all live hosts..."
				echo `nmap 192.168.1.0/24 -p0-1023` >netportscan1.txt ;;

			2)	echo "Running TCP connect() scan of all live hosts..."
				echo `nmap -sT 192.168.1.0/24 -p0-1023` >netportscan2.txt ;;

			3)	echo "Running TCP SYN scan of all live hosts..."
				echo `nmap -sS 192.168.1.0/24 -p0-1023` >netportscan3.txt ;;

			4)	echo "Running TCP FIN scan of all live hosts..."
				echo `nmap -sF 192.168.1.0/24 -p0-1023` >netportscan4.txt ;;

			5)	echo "Running TCP XMAS scan of all live hosts..."
				echo `nmap -sX 192.168.1.0/24 -p0-1023` >netportscan5.txt ;;

			6)	echo "Running TCP NULL scan of all live hosts..."
				echo `nmap -sN 192.168.1.0/24 -p0-1023` >netportscan6.txt ;;

			7)	echo "Running TCP ACK scan of all live hosts..."
				echo `nmap -sA 192.168.1.0/24 -p0-1023` >netportscan7.txt ;;

			8)	echo "Running TCP Window scan of all live hosts..."
				echo `nmap -sW 192.168.1.0/24 -p0-1023` >netportscan8.txt ;;

			9)	echo "Running UDP scan of all live hosts..."
				echo `nmap -sU 192.168.1.0/24 -p0-1023` >netportscan9.txt ;;

			10)	echo "Running IP Protocol scan of all live hosts..."
				echo `nmap -sO 192.168.1.0/24` >netportscan10.txt ;;
```

```
                0)      echo "Returning to previous menu..."
                        ./script2.sh ;; #Breaking and exiting a single loop is impossible in basic shell apparently

                *)      echo "That's not at option. Please try again."
        esac ;;

3)      echo " "
        echo "Accessing system-only port scan submenu..."
        echo " "
        echo "1 - Basic port scan" #Basic port scan of first 1024 ports (like Shields UP!)
        echo "2 - TCP connect() scan" #3-way handshake to target OS for TCP connection
        echo "3 - TCP SYN scan" #Sends raw packets to target and awaits response. Open - SYN/ACK, Closed - RST, Filtered - no response
        echo "4 - TCP FIN scan" #Like SYN, but sends FIN packets can slip some non-stateful firewalls. Closed - RST, Open/Filtered - no response
        echo "5 - TCP XMAS scan" #Like FIN, but uses FIN, URG, and PSH vs just FIN
        echo "6 - TCP NULL scan" #Like FIN and XMAS, but without activating flags
        echo "7 - TCP ACK scan" #SYN scan for (non)stateful firewalls. Non & no response - ACK, Non & Open/Closed - RST, Stateful - no response
        echo "8 - TCP Window scan" #Like ACK, but filters Open and Closed. Open - window size > 0, Closed - window size = 0
        echo "9 - UDP scan" #Used for DNS/DHCP. Closed - ICMP Port Unreachable, Filtered - other ICMP Unreachable, Open - UDP
        echo "10 - IP Protocal scan" #Not a true port scan. UDP scan with raw IP packets. Closed - ICMP Port Unreachable, Filtered - other ICMP Unreachable, Open - UDP
        echo "0 - return to previous menu"

        echo " "
        echo -n "Option: "
        read OPTION3

        case $OPTION3 in
                1)      echo "Running basic port scan of host..."
                        echo `nmap -O localhost -p0-1023` >portscan1.txt ;;

                2)      echo "Running TCP connect() scan of host..."
                        echo `nmap -sT localhost -p0-1023` >portscan2.txt ;;

                3)      echo "Running TCP SYN scan of host..."
                        echo `nmap -sS localhost -p0-1023` >portscan3.txt ;;
```

```
                4)      echo "Running TCP FIN scan of host..."
                        echo `nmap -sF localhost -p0-1023` >portscan4.txt ;;

                5)      echo "Running TCP XMAS scan of host..."
                        echo `nmap -sX localhost -p0-1023` >portscan5.txt ;;

                6)      echo "Running TCP NULL scan of host..."
                        echo `nmap -sN localhost -p0-1023` >portscan6.txt ;;

                7)      echo "Running TCP ACK scan of host..."
                        echo `nmap -sA localhost -p0-1023` >portscan7.txt ;;

                8)      echo "Running TCP Window scan of host..."
                        echo `nmap -sW localhost -p0-1023` >portscan8.txt ;;

                9)      echo "Running UDP scan of host..."
                        echo `nmap -sU localhost -p0-1023` >portscan9.txt ;;

                10)     echo "Running IP Protocol scan of host..."
                        echo `nmap -sO localhost` >portscan10.txt ;;

                0)      echo "Returning to previous menu..."
                        ./script2.sh ;; #Breaking and exiting a single loop is impossible in
basic shell apparently

                *)      echo "That's not at option. Please try again."
        esac ;;

4)      echo "Exiting... Thank you for using Cloaks&&Daggers! Goodbye!"
        exit ;;

*)      echo "That's not at option. Please try again."
esac
```