target metasploitable

- ricerca host su rete
  - nmap 192.168.1.*
    - trovato host 192.168.1.115
- ricerca OS
  - nmap -O 192.168.1.115
    - Linux 2.6.X per utilizzo generico
- servizi in ascolto, versione e porte aperte
  - nmap -sV 192.168.1.115
    - 21/tcp
      - vsftpd 2.3.4
        - server FTP
    - 22/tcp
      - OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
    - 23/tcp
      - Linux telnetd
        - protocollo che permette di effettuare un collegamento con un altro elaboratore ed operare su quello
    - 25/tcp
      - Postfix smtpd
        - demone per gestione email in arrivo
    - 53/tcp
      - ISC BIND 9.4.2
    - 80/tcp
      - Apache httpd 2.2.8
        - server http
    - 111/tcp
      - Samba smbd 3.X -4.X
        - server samba per condivisione file e stampanti
    - 139/tcp
      - Samba smbd 3.X -4.X
        - server samba per condivisione file e stampanti
    - 512/tcp
      - netkit-rsh rexecd
        - fa parte del pacchetto netkit, che consente di creare e simulare reti virtuali
    - 513/tcp
    - 514/tcp
      - Netkit rshd
        - fa parte del pacchetto netkit, che consente di creare e simulare reti virtuali
    - 1099/tcp
      - GNU Classpath grmiregistry
        - servizio registrazione servizi RMI (Remote Method Invocation)
    - 1524/tcp
      - Metasploitable root shell
        - servizio specifico dell'OS metasploitable
    - 2049/tcp
      - 2-a (RPC #100003)
        - protocollo di comunicazione NFS
    - 2121/tcp
      - ProFTPD 1.3.1
        - servizio per trasferimento file
    - 3306/tcp
      - MySQL 5.0.51a-3ubuntu5
        - database SQL
    - 5432/tcp
      - PostregreSQL DB 8.3.0 - 8.3.7
        - consente agli utenti di creare gestire e manipolare database
    - 5900/tcp
      - VNC (protocol 3.3)
        - consente di controllare e visualizzare in remoto il desktop di un computer da un altro dispositivo
    - 6000/tcp
      - X11 (access denied)
        - servizio per gestione interfaccia grafica di sistemi unix-like
    - 6667/tcp
      - UnrealIRCd
        - servizio per chat in tempo reale per IRC
    - 8009/tcp
      - Apache Jserv (Protocol v1.3)
        - teconologia osbsoleta che faceva parte di Apache Tomcat
    - 8180/tcp
      - Apache Tomcat/Coyote JSP engine 1.1
        - versione specifica del motore JSP nel framework di Apache Tomcat

Si allegano screenshot comandi eseguiti su repo github github: https://github.com/heskarioth94/NewProject/tree/master/M.3%20Penetration%20Testing/W.10/05.02/NMAP%20SCAN