Security Gruppo: Auditing

- F. Brasolin R. Cecchini M. Michelotto
- installati 3 PC a BO,FI,PD SL5 + Xen 3.0.3 con 3 macchine virtuali con nessus e nmap

  - audibo 131.154.102.250
  - audifi 192.84.145.82
  - audipd 192.84.143.158

Precauzioni d'uso:

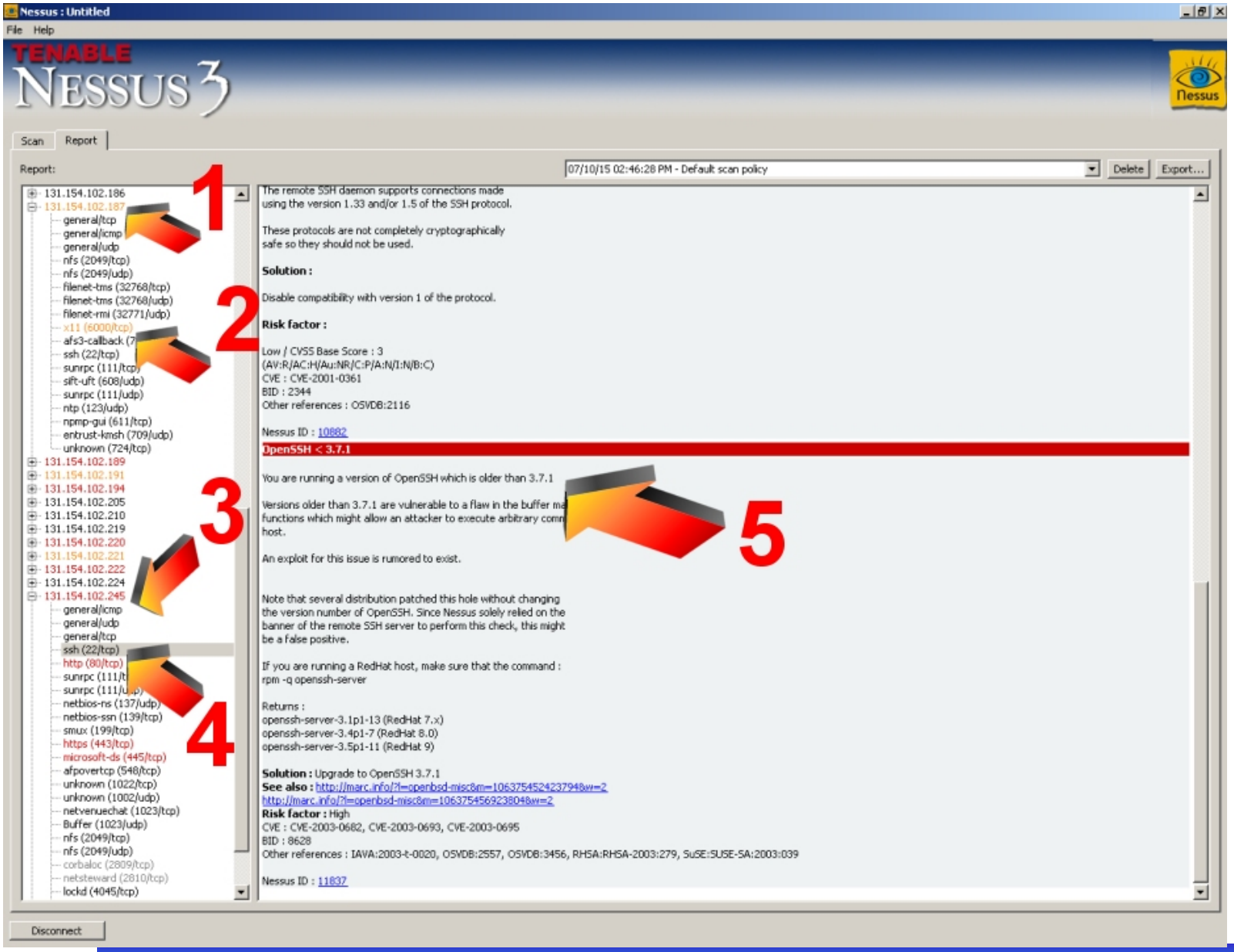
- Le prime volte effettuare lo scan su singoli host, per valutare tempi di esecuzione e impatto.
- avvisare i propri utenti PRIMA di effettuare le scansioni; si potrebbero infatti verificare problemi su:
  - alcuni apparati Switch
  - schede di rete installate non su computer, ie: batterie tampone, sensori temperatura
  - Alpha Digital Unix con funzioni di server NIS-YP
  - Web Server per Controller raid Areca potrebbero segnalare tentativi di intrusione
  - PC Linux potrebbero segnalare tentativi di intrusione con username **n3ssus, bin, root**

Segnalate eventuali altri problemi!!!!

- Richiedete a Brasolin Cecchini Michelotto username/password per potervi connettere con l'apposito client (Win & Linux) ai Nessus Server
- NB: ogni utente può eseguire la scansione *SOLO* delle proprie sottoreti che vanno comunicate quando richiedete l'account
- Si può eseguire la scansione con Nessus o Nmap

documentazione:

http://www.bo.infn.it/calcolo/INFN/audit/index.html



In Arancio (1-2) vulnerabilità medie

In Rosso (3,4,5) vulnerabilità alte (versione SSH)

To Do:

- Acquisto macchine dedicate (1Q08)
- Creazione account per Admin locali
- Preparazione policy per scan mirati
  (ie: ssh version, AP Detection...)
- Preparazione macchine virtuale da esportazione, per chi vuole eseguire Scan all'interno della propria LAN
- Script per estrarre info mirate da output files HTML per distribuire agli utenti solo le vulnerabilità delle loro macchine
- Suggerimenti ? Richieste ? ***Volontari scannatori?!***