**Poison**

==>Nmap<==

Ports: 80,22

Αν τρέξουμε το listfiles.php θα μας δείξει τα αρχεία στον server Yυπάρχει pwdbackup.txt το οποίο ειναι base64 encoded 13 φορές το οποίο αν το κάνεις decode παίρνεις το **Charix!2#4%6&8(0**

**Username: charix**

**Password: Charix!2#4%6&8(0**

Στον σέρβερ τρέχει Xvnc server από χρήστη root. Καθώς το μηχάνημα δεν έχει εγκατεστημένο vcnviewer πρέπει να κάνουμε tunnel την πόρτα 5901 του μηχανήματος στον τοπικό μας υπολογιστή.  
  
**ssh -L 5902:localhost:5901 charix@10.10.10.84**

Μέσα στον φάκελο home υπάρχει ένα secret.zip του οποίου ο κωδικός είναι **Charix!2#4%6&8(0**

Αφού κατεβάσουμε τοπικά και κάνουμε unzip το αρχείο secret.zip τρέχουμε vcnviewer τοπικά με παράμετρο το αρχείο secret που κάναμε unzip προηγουμένως (ως κωδικό):

* vncviewer localhost:5902 -passwd /home/name/secret

All your bases are belong to us!