LYCÉE 9ZENNE

UT1 Sciences Sociales TOULOUSE

LES HONEYPOTS

RéSIST DU 24/05/04

Matthieu.carayon@9online.fr

PLAN

- Rappels
- Présentation des outils existants
- Conception d'un honeynet avec Honeyd
- L'exploitation des résultats
- Questions

Matthieu.carayon@9online.fr

Rappels

- Les honeypots
  - Machine réelle ou simulée
  - Attaquée, scannée, compromise

Matthieu.carayon@9online.fr

Rappels

- Les honeynets
  - Réseau
  - Réel ou simulé
  - Forte interaction

Matthieu.carayon@9online.fr

Rappels

- Les honeytokens
  - Document Word
  - Tableau Excel
  - Une ligne dans une BD
  - …

Matthieu.carayon@9online.fr

Rappels

- Les différentes utilisations des Honeypots
  - Les honeypots dans la détection d'intrusion
  - Les honeypots de recherche

Matthieu.carayon@9online.fr

Rappels

- Utilité d'un honeypot dans l'entreprise
  - Le pour : le contrôle interne
  - Les limites : l'ouverture vers l'extérieur

Matthieu.carayon@9online.fr

Les outils existants

- DTK (Deception ToolKit)
  - http://all.net/dtk
- UML (User Mode Linux)
  - http://user-mode-linux.sourceforge.net/honeypots.html
  - http://project.honeynet.org/papers/uml
- VMWare
  - http://vmware.com
- Specter
  - http://www.specter.com

Matthieu.carayon@9online.fr

HONEYD

- http://honeyd.org/
- http://project.honeynet.org/

Matthieu.carayon@9online.fr

Honeyd

- L'installation
  - Extraction du tar.gz
  - ./configure (--without –py)
  - Make
  - Make install

Matthieu.carayon@9online.fr

Honeyd

- La configuration
  - L'option –p *chemin*
  - L'option –x *chemin*
  - L'option –a *chemin*
  - L'option –f *chemin*
  - L'option – l *chemin*
  - L'option –d
  - L'option –i
  - Les adresses simulées

Matthieu.carayon@9online.fr

Honeyd

- Exemple d'utilisation

[root@xxx honeyd] # honeyd –d –p nmap.prints –f config.file 10.0.0.1-10.0.0.100 10.0.0.254 192.168.49.0/24

Matthieu.carayon@9online.fr

Honeyd

- Les Hôtes virtuels (templates)
  - Nom
  - Ports / Protocoles / Actions correspondantes
  - Droprate
  - Uptime
  - Uid / Gid
  - Adresses IPs

Matthieu.carayon@9online.fr

Honeyd

- Exemple de template

```
Create mon-windows
Set mon-windows personality “Microsoft Windows 2000 Advanced Server SP3”
Add mon-windows tcp port 25 “ /chemin/smtp.sh $ipsrc $ipdst $sport $dport”
Add mon-windows tcp port 80 “ /chemin/ web.py $ipsrc $ipdst”
Add mon-windows tcp port 110 “ /chemin/ pop3.pl $dport”
Set  mon-windows tcp action reset
Set mon-windows udp action block
Add mon-windows  tcp port 113 open
Set mon-windows droprate in 15
Set mon-windows uptime 5000
Set mon-windows uid 35700 gid 35700
Bind 172.16.2.1 mon-windows
Bind 172.16.2.2 mon-windows
```

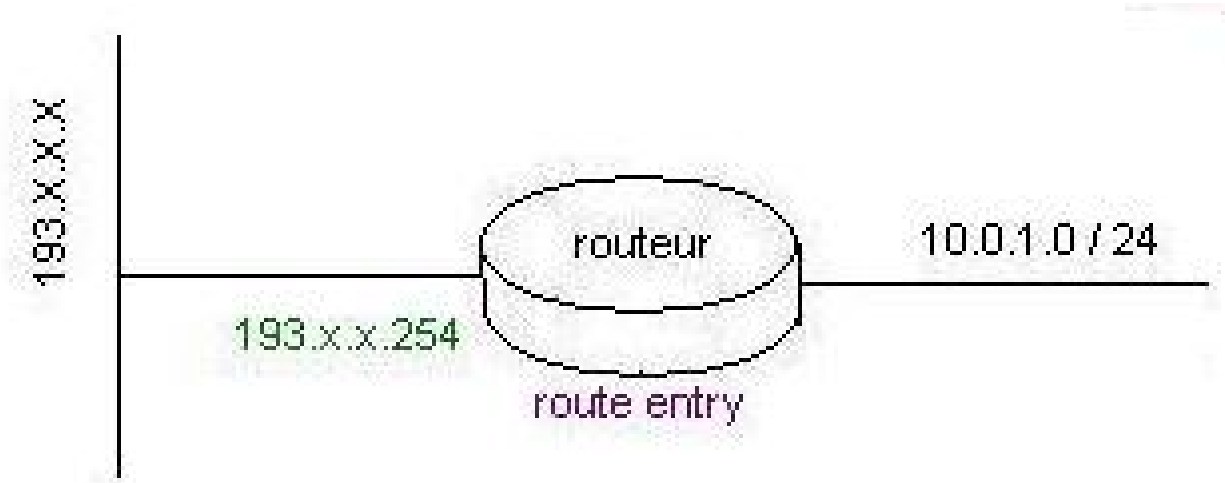

Matthieu.carayon@9online.fr

Honeyd

- Le routage
  - Route entry @routeur
  - Route @routeur link @réseau
  - Route @routeur add net @réseau @routeur2
  - Bandwidth 100Mbps

Matthieu.carayon@9online.fr

Honeyd

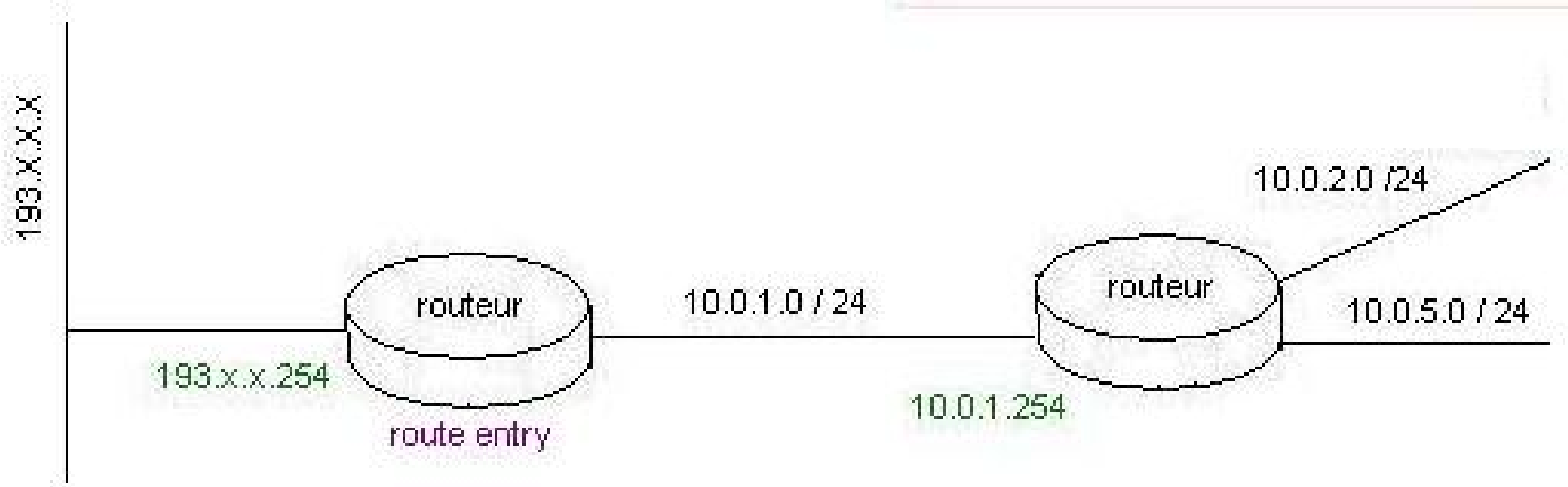


route entry 193.X.X.254

route 193.X.X.254 link 10.0.1.0 / 24

Matthieu.carayon@9online.fr

Honeyd



route 193.X.X.254 add net 10.0.2.0/24 10.0.1.254

route 193.X.X.254 add net 10.0.5.0/24 10.0.1.254

route 10.0.1.254 link 10.0.2.0 /24

route 10.0.1.254 link 10.0.2.0 /24

Matthieu.carayon@9online.fr

Honeyd

- Les services

Par défaut : proxy, telnet, smtp, snmp, test, web

Installés dans : /usr/local/share/honeyd

Sinon : MSftp, IIS, Apache, POP3,VNC, imap, ssh, Bo …

  - http://www.honeyd.org/contrib.php
  - http://www.honeynet.org.br/tools
  - http://www.think-future.de/CS/honeyd/contrib

Matthieu.carayon@9online.fr

Honeyd

- La gestion des logs
  - 1 seul fichier
  - Plusieurs fichiers
  - IDS sur le réseau simulé

Matthieu.carayon@9online.fr

Honeyd

- Les difficultés rencontrées (1/4) :
  - La philosophie
    - Principe de « Blackholing »
    - Pas de Blackholing car solution marginale

Matthieu.carayon@9online.fr

Honeyd

- Les difficultés rencontrées (2/4) :
  - Le routage
    - No reverse routing map for 192.168.0.254 (= route entry)
    - Route 192.168.0.254 link 192.168.0.254/32

Matthieu.carayon@9online.fr

Honeyd

- Les difficultés rencontrées (3/4) :
  - Les empreintes Nmap
    - Hôte réel = 96%
    - Version 0.8 = 10%
    - Version 0.8a = 90%
    - Changer d'adresse ip pour l'hôte qui pose problèmes.

Matthieu.carayon@9online.fr

Honeyd

- Les difficultés rencontrées (4/4) :
  - Les scripts
    - Crédibilité générale des services simulés
    - Cas du serveur ftp
    - Nom de domaine identique
    - Correspondance entre les consoles de management
    - …

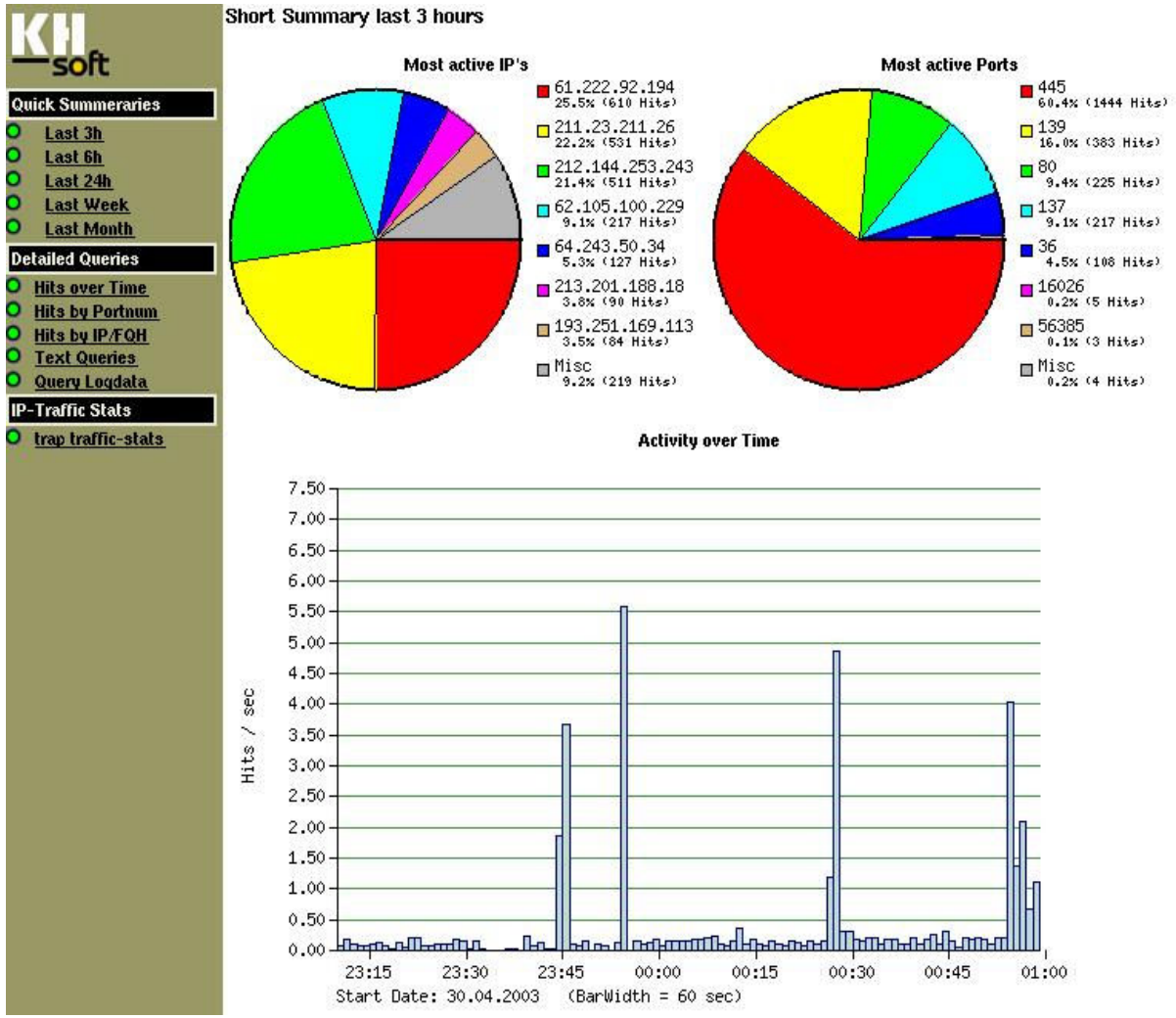
Matthieu.carayon@9online.fr

Honeyd

- Exploitation des résultats
  - Analyse des logs capturés par les scripts
  - Analyse des logs capturés par Honeyd Honeyview

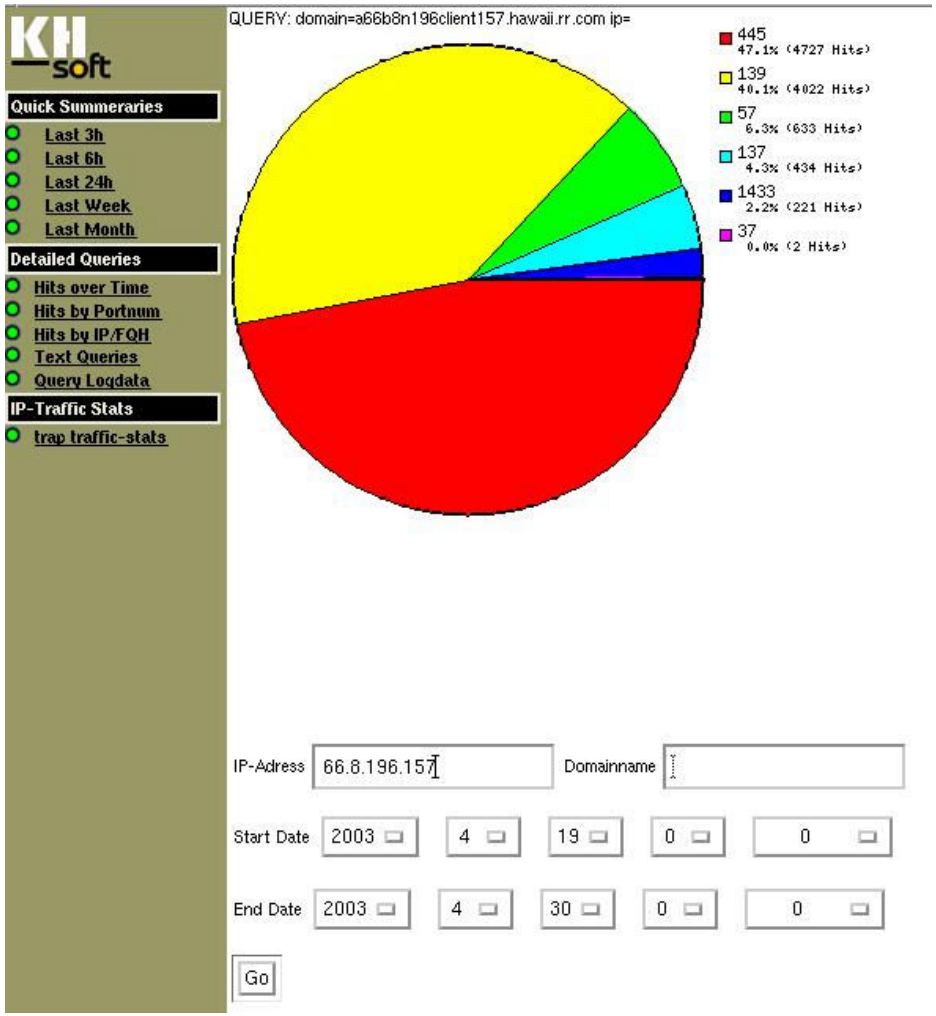
Matthieu.carayon@9online.fr

Honeyview

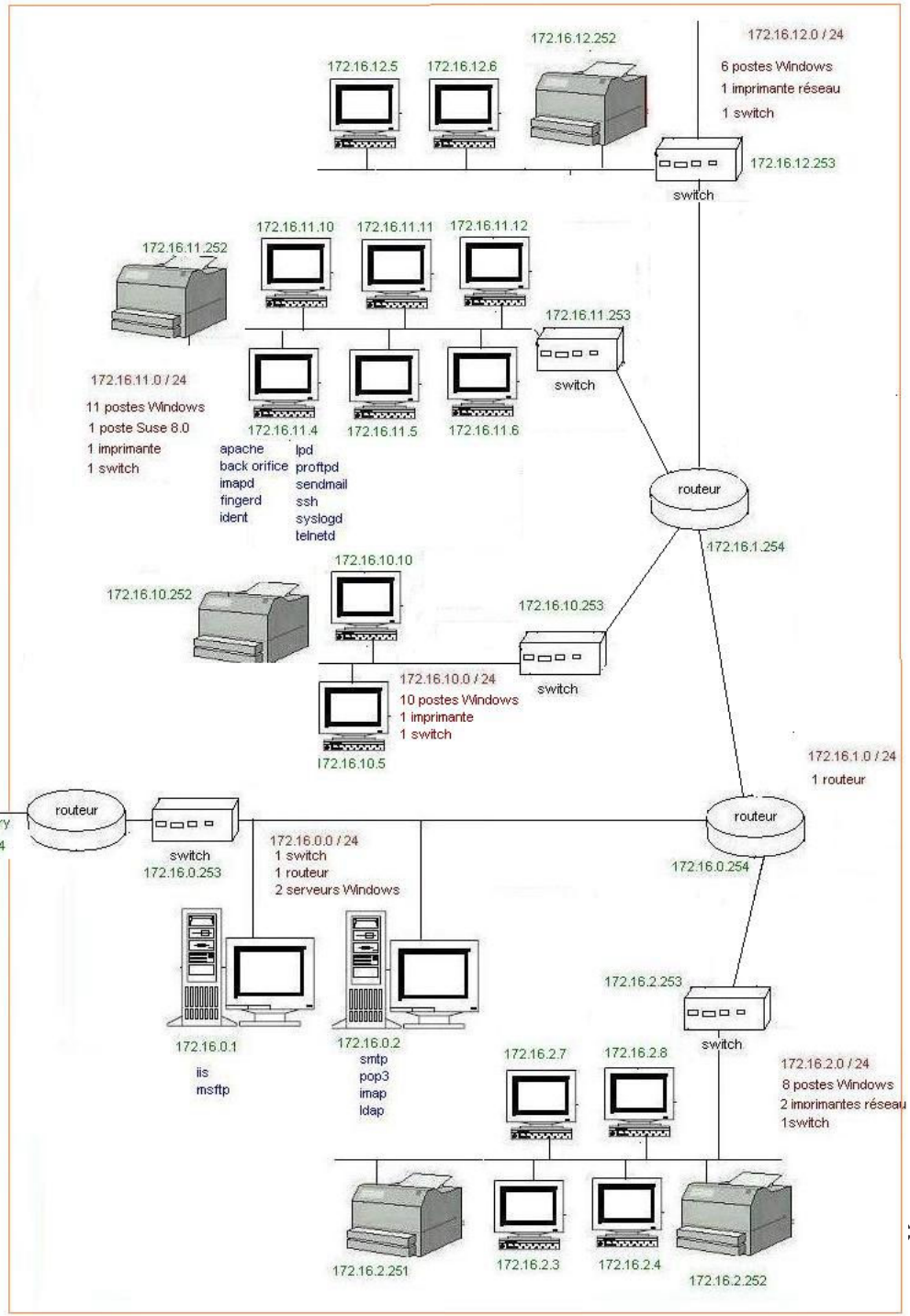


Matthieu.carayon@9online.fr

Honeyview



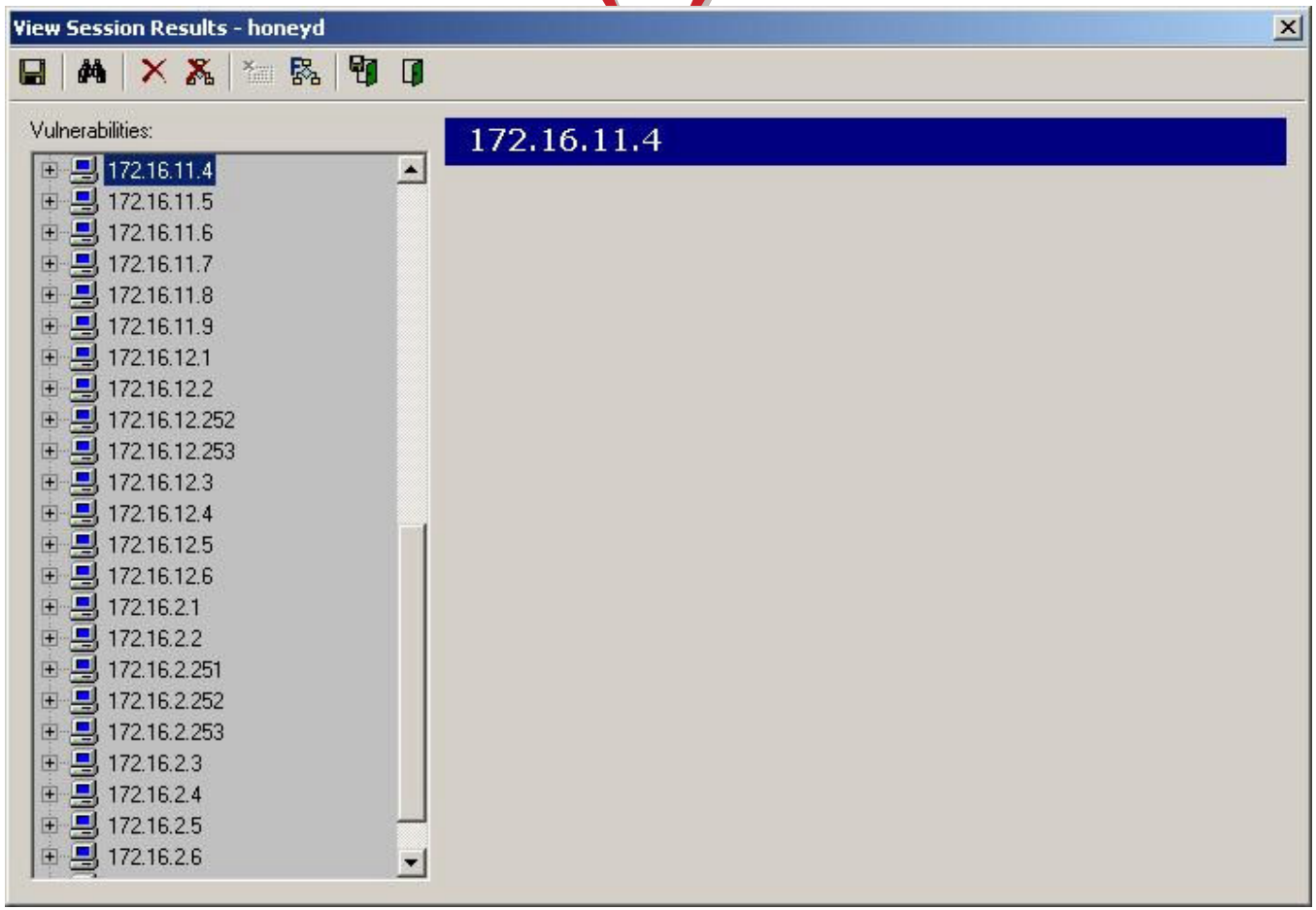
Matthieu.carayon@9online.fr



RéSIST DU

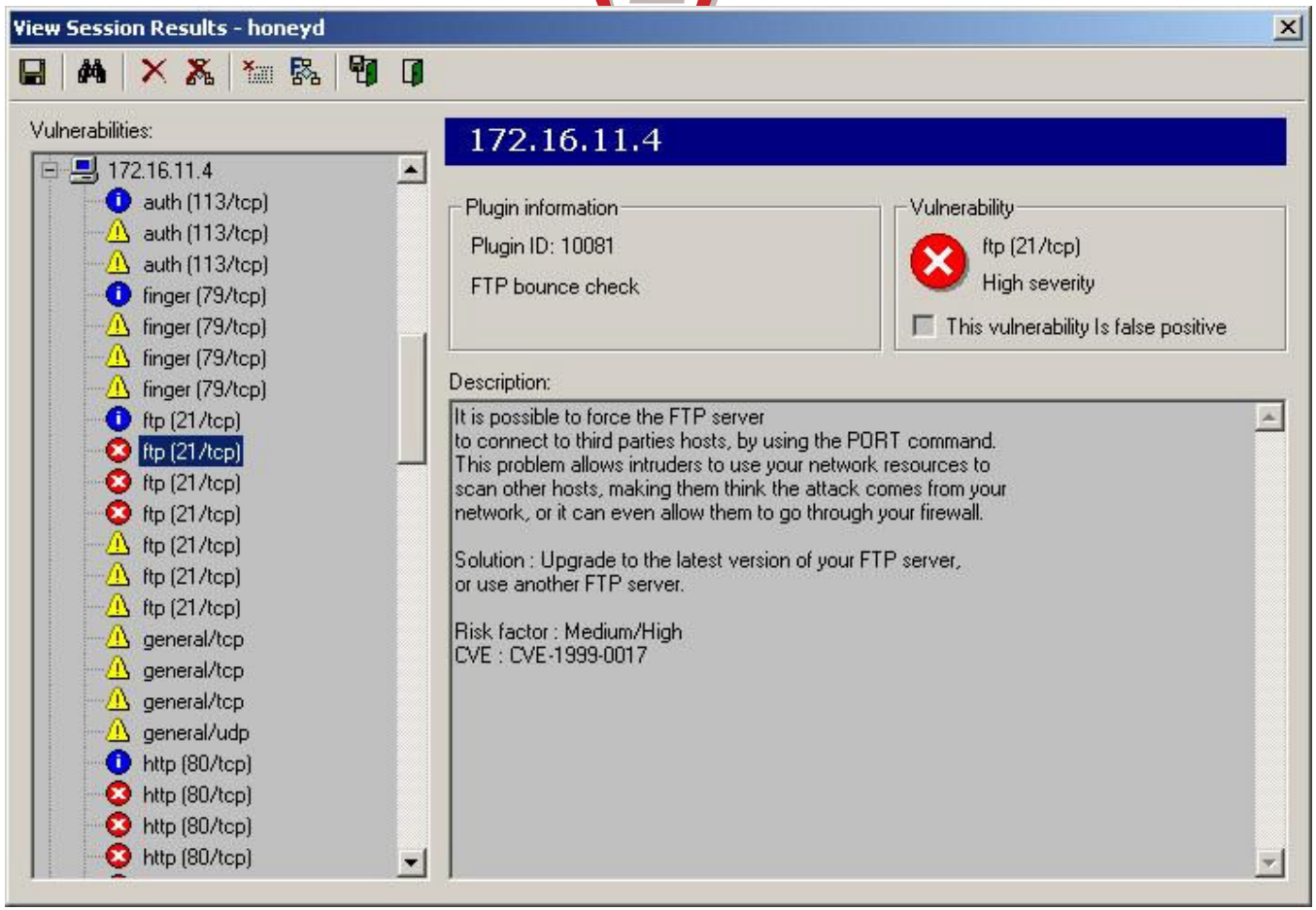
arayon@9online.fr

Le honeynet vu par Nessus (1)



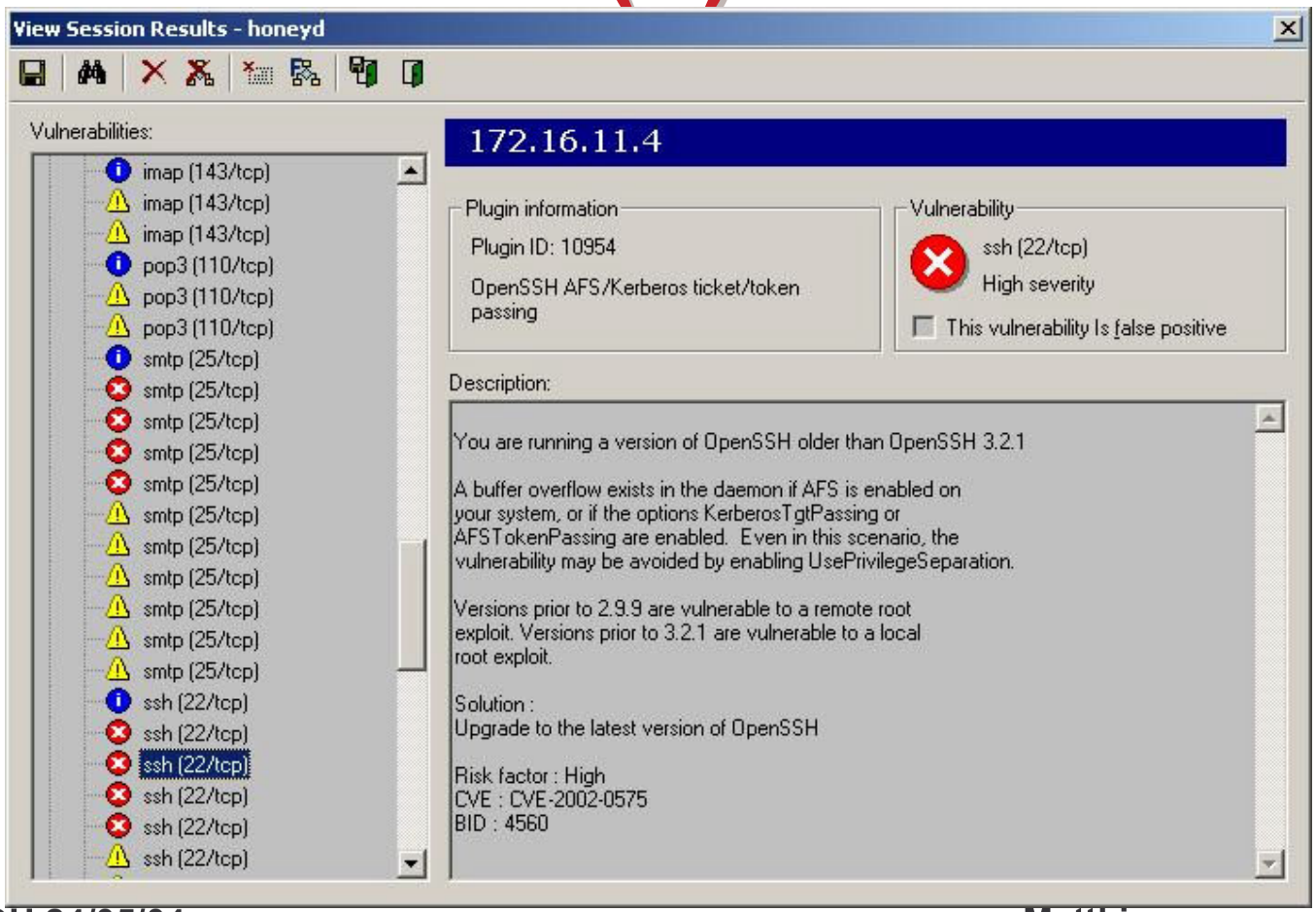
Matthieu.carayon@9online.fr

Le honeynet vu par Nessus (2)



Matthieu.carayon@9online.fr

Le honeynet vu par Nessus (3)



Matthieu.carayon@9online.fr

Rébus

/

Matthieu.carayon@9online.fr