

Security and privacy in networks - TP

Damien Saucez
Inria Sophia Antipolis

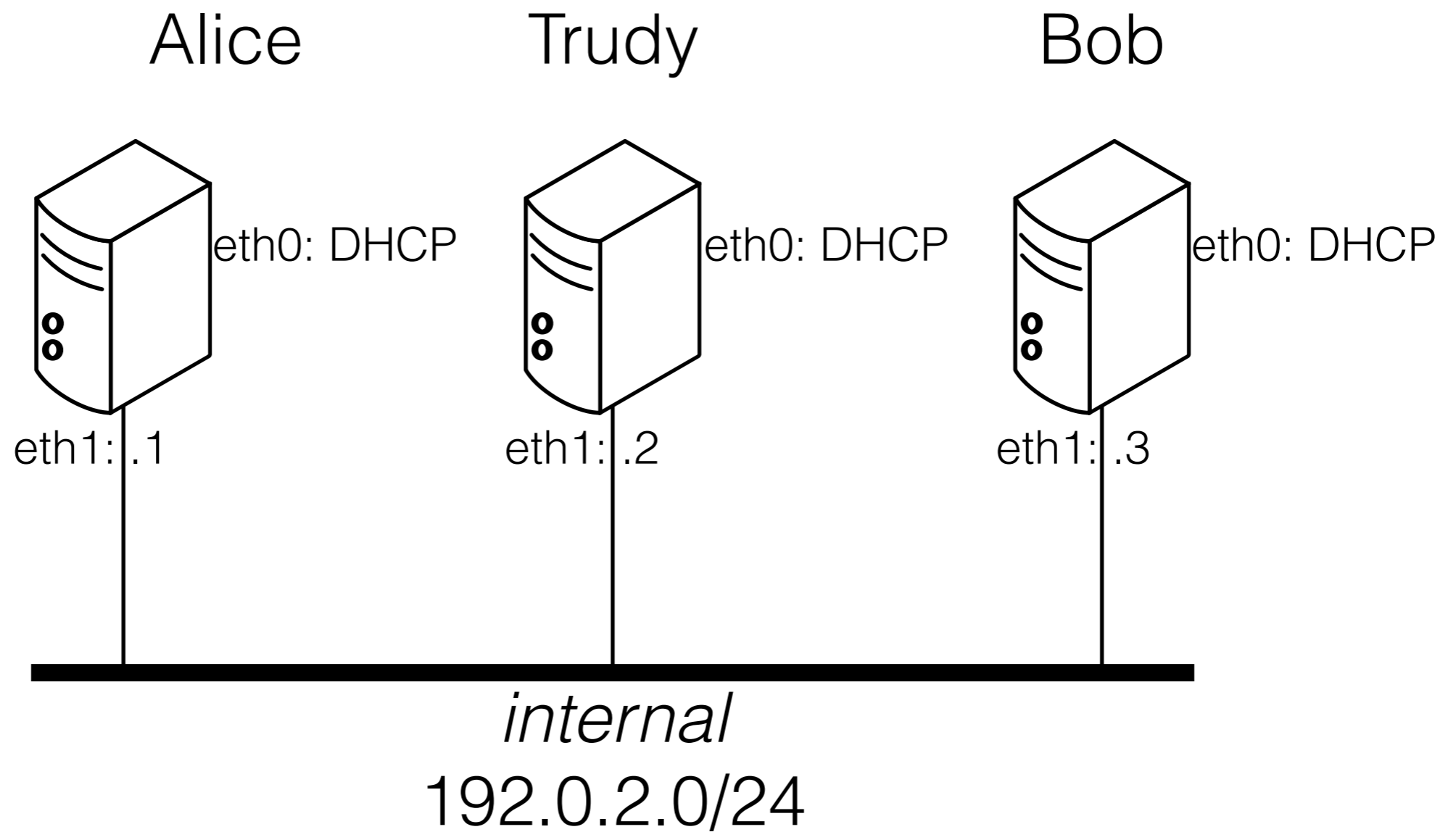
Modalités

- Le TP est évalué sur base du rapport que vous remettrez le vendredi 2 décembre à 13:00 en format papier (pas de mail).
- Le rapport sera composé d'une page par question, toute page supplémentaire sera ignorée.
- Le TP se fait en binôme.
 - En cas de nombre impair d'étudiant, un trinôme sera composé.
- Bon travail!
- Image VM: <https://drive.google.com/file/d/0B95IZs9CRF1FRnBZUmJwbkFGdIE/view?usp=sharing>

Question 1 - préparation du labo

- Créez trois machines virtuelles VirtualBox (Alice, Bob et Trudy) depuis l'appliance qui vous sera fournie (login: *stud*, password: *stud*)
- Vérifiez que chaque machine dispose de deux interfaces réseaux
 - eth0 est attachée au NAT VirtualBox
 - eth1 est attachée au réseau interne dénommé "internal"
- Assignez les adresses comme indiqué en page 4 et assurez-vous que toutes les machines peuvent communiquer entre elles via le réseau interne de VirtualBox
- Configurez le serveur SSH de Bob de sorte à n'autoriser que l'accès par clé (pensez à regarder */etc/ssh/sshd_config*)
 - Générez une paire clé privée/clé publique (avec *ssh-keygen*) sur Alice, autorisez l'accès via cette clé sur Bob

Plan d'adressage



Question 2 - analyse de trafic

- Lancez *Wireshark* sur Alice
- Accédez au server web installé sur Bob avec Firefox
 - Expliquez le role des 3 volets de visualisation de Wireshark, quels concepts généraux peut-on observer?
- Connectez-vous au serveur FTP de Bob depuis Alice en utilisant le compte *stud*
 - Qu'observez-vous avec Wireshark?
- Connectez-vous à Bob avec SSH
 - Que constatez-vous?
- Sur base de vos observations, que pouvez-vous conclure sur les protocoles HTTP, FTP et SSH d'un point de vue de la sécurité? Quels conclusions générales pouvez-vous en tirer?

Question 3 - scan TCP avec Scapy

- Parcourez la page <http://www.secdev.org/projects/scapy/doc/usage.html> et expliquez le but de Scapy
- Depuis Alice, à l'aide de Scapy, envoyez un segment TCP à Bob, le packet vise le port 80 et contient un segment avec le flag SYN uniquement, qu'observez-vous avec Wireshark?
 - envoyez le même paquet, mais sur le port 45005, que constatez-vous?
- Ecrivez un script Scapy pour envoyer à Bob un paquet de type SYN sur tous les ports compris entre 0 et 65535
 - Quels services tournent sur la machine?
- Ce que vous avez fait au point précédent est un scan.
 - A quoi servent-ils et comment peut-on les utiliser en pratique?
 - Depuis Bob, essayez la commande `telnet localhost ssh`, qu'observez-vous?
 - Sont-ils dangereux pour l'intégrité du réseau? Peut-on s'en protéger? Comment?

Question 4 - ARP cache poisoning

- Configurez Alice pour utiliser Bob comme passerelle par défaut
- Affichez la table ARP d'Alice et de Bob (*arp -n*)
- Affichez la table de routage d'Alice (*netstat -rn*)
- Sur Trudy, utilisez Scapy pour polluer la cache d'Alice et dévier tout son trafic Internet vers Trudy au lieu de Bob
 - Affichez la table ARP d'Alice et de Bob
- Félicitation vous avez fait votre première véritable attaque! Affichez une page web dans Firefox depuis Alice
 - Que se passe-t'il? Comment s'appelle cette attaque?
- Est-il possible de rendre votre attaque plus sournoise (et surtout invisible)
 - Pensez à utiliser *net.ipv4.ip_forward...*
 - Affichez une page web sur Alice que constatez-vous?
 - Que se passe-t'il? Comment s'appelle cette attaque?

Question 5 - BGP prefix hijacking

- Construisez la topologies présentée en page 9 avec GNS3 (commande *gns3*) (utilisez des Cisco 7200 comme router)
- Configurez chaque router (tutoriel sur <http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13751-23.html>)
 - Vérifiez le routage et que pour pouvez joindre les adresses 10.100.0.1 et 10.200.0.1 depuis chacun des routeurs
- Construisez et déployez une attaque BGP prefix highjacking de sorte que l'AS 300 attire le trafic de l'AS 100
- Déployez une contre-mesure pour mitiger l'attaque

Topologie BGP

