INTRANODE
YOUR E-SECURITY PARTNER

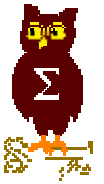
Observatoire de la Sécurité des Systèmes d'Information & des Réseaux

Présentation OSSIR Juin 01

# CanSecWest CORE 01

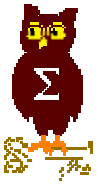
## 28-29-30 mars 01, Vancouver

Franck.veysset@intranode.com

# Contexte

- Deuxième conférence de ce type
- Présentations réparties sur 3 journées
  - Du 28 au 30 mars 2001, à Vancouver, BC, Canada
- Orientation relativement technique, *Black and White*
- Présence de grands noms de la sécurité « Internet »
- *Autant d'information hors que dans les conférences*
- *http://www.cansecwest.com/*
- Subventionnée en partie par l'OSSIR

# Public

- Environ 150 personnes
- 4 Français
  - Alcatel * 2, Mr Deraison, et Mr Veysset
- 2 Suisses (COLT & Securite.org)
- 50% d'Américains
- 25% proche région Vancouver
- Pays-bas, Allemagne…

# Détail des présentations

- Pas moins de 18 présentations dont :

| | |
|---|---|
| Renaud Deraison | **The Nessus Project** |
| Securite.org | **Kerberos in an ISP env.** |
| Martin Roesch | **Road to Snort V2.0** |
| Dave Dittrich | **Digging Through Compromised Systems and Tracking Intruders** |
| K2 | **Polymorphic Shellcode** |
| Lance Spitzner | **The Honeynet Project** |
| Robert Graham | **IDS Evasion vs. Protocol Analysis** |

Et Fyodor, Jay Beale, Theo de Raadt, RFP, Dug Song…


# IDS : Le sujet à la mode

Les « pro-IDS »

Marty Roesch, Snort (Ou SourceFire ?)

Robert Graham, Network Ice

Les autres

K2, polymorphic shellcode

Fyodor, stealth scanning & IDS evasion

Et les sujets annexes

Gary Golomb (Dragon), analyse of rootkit

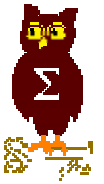
# SNORT… road to V2.0


- Première étape, Snort 1.8
  - Encore en β début juin
  - Nouveaux formats de règles
  - Nouveaux plugins, notion d'URI, décodeur Unicode
- Et la V2.0
  - Travail sur la *libpcap* (remplacement) car trop restrictive
  - Nouvelles sondes, architecture plus modulaire, nouveaux algorithmes plus performants…
  - Et Sourcefire…

# Sourcefire

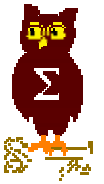

- Fondée par Martin Roesch, Stephen Northcutt, et Dragos Ruiu (*www.sourcefire.com*) (et *SiliconDefense?*)
- Propose(ra ?) deux produits :
  - OpenSnort Sensor (système 1U)
  - OpenSnort Management Console (2U)
- Promet de supporter SNORT en OpenSource…

  *Snort.org has received over 8.5 million hits in its first year of operation. Snort is downloaded approximately 2000 times per week from snort.org. Because of its popularity and widespread success, Sourcefire is committed to maintaining Snort as an Open Source solution.*



# IDS evasion vs. protocol analysis

- Présentation de techniques d'analyse protocolaire
  - Analyse intelligente des données (pas de *pattern matching*)
- Les plus :
  - Meilleure détection, contournement difficile
  - *0 day detection (sur protocoles connus)*
  - Bonne performance
- Les moins :
  - Complexe (donc dangereux…)
  - Notion d'états
  - Mise à jour du moteur parfois nécessaire



# Exemple, avec SideStep

- Contournement des IDS utilisant le *pattern matching*
  - Recompilation des outils, avec modification des signatures
  - Utilisation de proxy (fragrouter, RFPProxy…)
- Démo de *SideStep*
  - Support de HTTP, DNS, SMTP, BO et RPC/Portmapper
- Et quelques mots sur Network Ice…

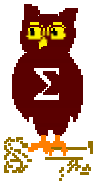
# Polymorphic shellcode

- Présentation de méthodes de contournement d'IDS
- Polymorphisme : possibilité d'exister sous plusieurs formes… → Application aux exploits de type buffer overflow
  - Modification de signature NOPS
  - Encodage des *Shellcode*, avec décodage sur le système cible (XOR)
- ADMutate, API multi plate-forme… (Intel, Sparc, HPPA et prochainement PPC, MIPS et Alpha..)


# Stealth scanning & IDS evasion

- Présentation d'attaques et réactions IDS
  - Exemple de scan TCP Connect, SYN…
  - Utilisation d'option DECOY, d'adresse usurpée
  - Scan très lent
  - Contournement d'IDS par modification de NMAP
- Plaisanterie et humour sur BlackIce
  - Windentd, spoofing de réponse Windows NMB
  - Icepick, un scanner d'IDS BlackIce…





# Un-TCP and Driver-Programs

- Présentation de « Rootkit 2000 », *built on NT technology*
- Interception des appels système :
  - *Camouflage dans la base de registre*
  - *Invisible dans la table process*
- Utilisation de TCP en protocole *« stateless »*
  - Sur une adresse réseau libre
  - Non respect de TCP (RST, FIN…)
  - Contournement des IDS
  - Et inefficacité des réponses automatiques… (RST !)

INTRANODE
YOUR E-SECURITY PARTNER

# Le projet Honeynet

Cf. http://project.honeynet.org

Présentation de Lance Spitzner sur l'architecture et le but de ce projet

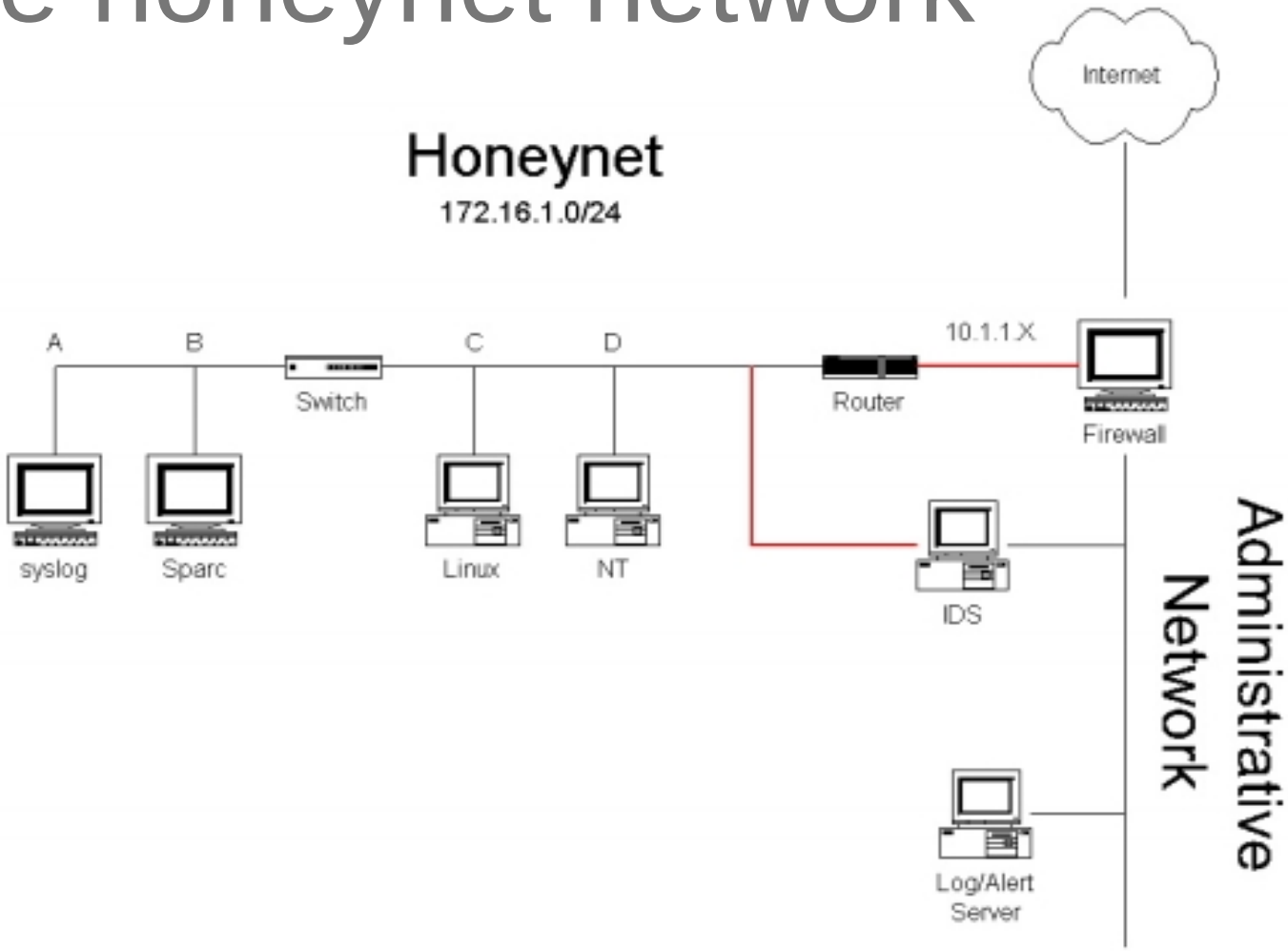
Présentation de Dave Dittrich, « The Forensic Challenge »

# The honeynet project


- *To learn the tools, tactics, and motives of the blackhat community and share the lessons learned*
- *We take the initiative by gathering intelligence on the enemy*

- Démarche active d'apprentissage des techniques undergrounds

# The honeynet network



# The forensic Challenge

- Cas concret issu du Honeynet project
- Il s'agit d'un concours d'analyse d'une attaque
- Les données :
  - Infos sur le système compromis : RedHat 6.2
  - Trace d'un IDS (SNORT) durant l'attaque
  - Copie binaire de partition disque
- Challenge : Qui, Quoi, Quand, Ou, Comment…

# Challenge : Résultats (1/2)

- Compromission via démon *rpc.statd*
- Installation de backdoors
  - *Sniffer (capture de mot de passe)*
  - *IRC bot (eggdrop)*
  - *Scanning, Intrusion et DDOS tools*
  - *Rootkit classique (*ls, ps, top, tcpd…)
  - *Destruction des secteurs de boot*
- Installation pratiquement totalement scriptée / automatique

# Challenge : Résultats (2/2)

Pour l'analyse du système : 13 réponses

- Temps d'investigation :
  - Moyen : 48.0 heures
  - Jusqu'à 104 heures pour un des participants
- Coût de l'analyse :
  - Autour de US$ 2,067.46 +/- US$310.12
  - Par un cabinet spécialisé : @ US$300.00/hr, $ 22 620

INTRANODE
YOUR E-SECURITY PARTNER

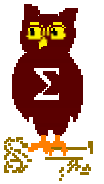
# Sécurisation des systèmes

Jay Beale, Bastille Linux

Présentation des fonctions de sécurisation

Theo De Raadt

Le projet OpenBSD, « Secure by default »



# Bastille Linux

- Projet de sécurisation, via scripts, de systèmes Linux
  - Pour RedHat 6, 7, et  Mandrake (7, 8)
- Nouvelle version en cours de développement :
  - Bastille 1.2.0, avec GUI sous X-Window
- Fonctionnement
  - Mise en place d'un firewall
  - Désactivation des démon inutiles
  - Modification de droit d'accès, chrootage…

# OpenBSD


- Un OS sécurisé par défaut
- Travail de « guide » dans la communauté : *suivre et s'inspirer de ce que fait OpenBSD…*

- Quelques citations de Theo sur l'OpenSource
  - Le code source est plus sûr car il est relu : FAUX
  - Les personnes utilisant du code source le corrigent et l'améliorent : FAUX

INTRANODE
YOUR E-SECURITY PARTNER

# Les techniques d'intrusion

RFP, RFProxy

Outil d'audit de site Web

A. Reiter & C. Abad, WIN32 format string exploit

Présentation des attaques de type Buffer Overflow

HD Moore, Making Windows NT bleed

Attaques sur des serveurs NT

# RFP & Scan Web

- Rappel sur Whisker, un scanner furtif de CGI
  - Et sur ces limites…
    - Processus automatisé
    - Problème de la diversité des web, et le non respect des standards

- Présentation de RFProxy
  - Proxy de modification de donnée à la volée
  - Réécriture HTML (header, form…)
  - Manipulation de cookies
  - Log / journalisation des données


HP