Radware Intelligent Application

delivers total application performance

enabling the absolute security,

optimization and full availability of all

critical applications

radware

availability | performance | security

APSolute Application Delivery

IPS – Mythes & Réalité

Renaud Bidou
Security Consultant, EMEA

radware
availability | performance | security

APSolute Application Delivery

Agenda

- Mythes
- Stopper les inondations
- Investiguer les tunnels
- Gérez ces patches!
- Je ne veux pas être injecté
- Réalité

Mythes

Renaud Bidou
Security Consultant, EMEA

APSolute Application Delivery

“Les menaces sont nouvelles”

- Vers : 1988 (*Morris Worm*)
- DoS : 1995 (*ping of death*)
- Buffer Overflows : avant 1996 (*Phrack 49)*
- Distributed Denial of Service : 1998 (*smurf*)
- Data flooding : 1998 (*Nasa & universities*)
- Format Strings : avant 2000 (Rapports de *Theso Team*)
- SYNFloods : Depuis que TCP existe …
- Injection : Depuis que les ordinateurs existent…
- Contournement de la politique de sécurité : depuis que les BOFH existent…

“Je fais confiance à mes produits de sécurité”

1. “Security is a process, not a product” from Bruce Schneier

2. Comment expliquer …
   - L’accroissement des tentatives d’extorsion basées sur les dénis de service;
   - L’histoire sans fin de la propagation des vers;
   - Les nouvelles techniques de backdoors;
   - L’impunité des canaux cachés;
   - Tous ces patches que vous n’avez même pas le temps d’installer!

“IPS = IDS + Firewall + Marketing”

- Le syndrome snort-inline
  1. Snort + Netfilter
  2. Conçu pour les Homeypots
- Le jeux des éditeurs
  1. Les fournisseurs de firewalls disent intégrer des fonctions de type IDS
  2. Les fournisseurs d’IDS mettent leur produit en coupure
- Revers
  1. Le besoin de performance
  2. Les faux-positifs et les fonctions “d’auto-DoS”

Stopper les inondations

Renaud Bidou
Security Consultant, EMEA

radware
availability | performance | security

APSolute Application Delivery

Techniques de Flooding - I

1. *"3-way handshakes"* incomplets : Aucune réponse au SYN-ACK du serveur, laissant des milliers de connexions dans l'état TIME_WAIT.

   # hping3 --syn --rand-source --p 80 <target> --flood

2. "Pending sessions" : Session TCP établie mais la session est laissée ouverte.

   # webdevil <target> 80 10000

3. Attaques par réflexion : à la « smurf ». SYNs envoyés à des destinations aléatoires. La source est spoofée et devient la cible. La cible est saturée de SYN-ACK et doit envoyer un RST.

   # hping3 --syn –a <target> --rand-dest --p 80 --flood

Techniques de Flooding - II

4. Anomalies protocolaires : cas limites ou indéfinis (ex. aucun/tous les flags TCP). Génère un accroissement de l'utilisation CPU sur la cible.

```
# hping3 -SAFRUP --rand-source -p 80 <target> --flood
```

5. Valeurs incorrectes : Même effet mais obtenu en utilisant des valeurs incorrectes (checksums, versions/numéros de protocoles etc.)

```
# hping3 -A -b -p 80 <target> --flood
```

6. Fragmentation : Consommation excessive de CPU par utilisation de paramètres de fragmentation incorrects.

```
# boink <source> <target> 12345 135 100000
```

Le besoin de performance

- Les techniques sont triviales

MAIS

- Elles nécessitent beaucoup de ressources :

1. Les serveurs ont de meilleures performances que les PCs;
2. Les techniques de load-balancing diluent les effets;
3. La bande passante peut devenir un problème.

Effets de leviers

1. Hacking de masse … et faire travailler les victimes
   - Zombies : TFN(2k), Trinoo, Stacheldraht, DDNSF
   - Vers : Code Red contre la maison blanche
2. Rebondir sur de réseaux de grande taille mal protégés
   - Smurf
   - Attaques par réflexion
3. Economiser les ressources du système attaquant
   - Utilisation d'un système tiers pour "reseter" les sessions établies ⇨ Naphta

Lutter contre les SYNFloods

- Les SYNCookies évitent l'utilisation de la TCB
  - SYN_ACK_SEQ = f(net_params.time)
  - L'absence de ACK final n'est pas important
  - Un ACK final hors délais est rejeté
- Le choix de f()
  - Sécurité : SYN_ACK_SEQ ne doit pas être prédictible
    1. Fonction de hashage
    2. Ajout d'un paramètre "secret"

       SYN_ACK_SEQ = f(seed.net_params.time)
  - Performance : f doit supporter la précalculation

Contenir l'impact

- Problème
  1. Une attaque par saturation est dirigée vers un serveur spécifique
  2. Cette cible est interconnectée à une infrastructure mutualisée
  3. La saturation a un impact sur d'autres plates-formes dépendant de la même infrastructure…
- Solution
  - Isoler le trafic
  - Gérer la bande passante

OK, où ?

- Sur chaque serveur
  - Tous les OS ne supportent pas les SYNCookies
  - Echantillonage de trafic + IDS
    - Utilisation intensive de CPU
    - Impossible pour des milliers de systèmes
- Inline ?
  - Les performances sont encore plus critiques !
    - ⇨ La latence n'est pas une option
  - Suggestion : un IPS

Investiguer les tunnels

Renaud Bidou
Security Consultant, EMEA

APSolute Application Delivery

Contourner la politique de sécurité

- Les tunnels utilisent des ports légitimes
  1. Connection à des redirecteurs de ports
     - ⇨ stunnel, httptunel
  2. Masquer des applications, P2P?
     - ⇨ exosee, port hopping
- Les systèmes internes attendent les ordres
  - Backdoor / trojan asynchrones
    - ⇨ Casper (http://valgasu.rstack.org/casper/)
    - ⇨ CCTT (http://www.entreelibre.com/cctt/)
  - Et ne faites pas confiance aux firewalls personnels
    - ⇨ http://www.security.nnov.ru/advisories/bypassing.asp

Canaux cachés

- Exemples (une liste exhaustive serait trop longue)
  1. icmpchat
     - Discussion chiffrée à travers ICMP
     - ⇨ Utilisent n'importe quel type ICMP
  2. stegtunnel
     - Cache les données dans les champs IPID et les numéros de séquence
  3. MailTunnel
     - Lance des commandes via mail
  4. Tunnelshell
     - Utilise des fragments sans en-tête

  + Stegano + Chiffrement + Encapsulation IPv4/IPv6 + …

Détection d'anomalies

- Respect des RFC couches 3 à 7
  - Structure des paquets (taile, fragmentation,en-têtes etc.)
  - Valeurs des adresses (URL)
  - Validité des variables (types, flags, commandes, etc…)
- Gestion des sessions
  - Protège des communications hors-session
  - Relativement trivial pour TCP
    - ⇨ Attention aux techniques de base d'injection
  - ICMP et UDP sont plus complexes
    - ⇨ Définition d'un timeout
    - ⇨ Couples (requète, réponse) autorisés

Investigation en profondeur

- Signatures des tunnels
  - Analyse des communications conformes aux RFC
  - Signatures types dans les URI ou le contenu
  - ⇨ Fasttrack (URL =~/\/\.hash=/)
  - ⇨ Kazaa (content =~ /X-Kazaa-(Username|Network|IP|supernodeIP):/)
- Analyse comportementale
  - Basée sur les modèles typiques des protocoles
  - Durée des session
  - Taille des fenêtre TCP et des paquets
  - Taille totale des données transmises
  - Types de données

Gérer ces patches

Renaud Bidou
Security Consultant, EMEA

radware
availability | performance | security

APSolute Application Delivery

Une histoire sans fin

- La gestion des patches est une problématique majeure.
- Les vulnérabilités sont trouvées dans tous les logiciels
  - Les SI hétérogènes sont difficiles à maintenir
  - Les fonctions de téléchargement et d'installation varient d'un éditeur à l'autre
- Les patches peuvent avoir un impact sur la stabilité du système.
  - Patcher immédiatement est dangereux
  - Les procédures de tests et de validation sont trop longues

⇨ SECURITE ou STABILITE

Mise à jour des logiciels de sécurité

- Les logiciels de sécurité doivent aussi être mis à jours
  - Bases de virus
  - Moteurs d'analyse
- Pièges communs
  - Tout serveur ou station de travail est concerné
  - Les weekend et les vacances exposent les PCs
  - Une opération humaine est parfois nécessaire
    - ⇨ Problématiques de sensibilisation et de bonne volonté des utilisateurs habituelles

Howto

- Protéger toutes les cibles potentielles à partir d'un point unique
  - Une procédure de mise à jour unique est nécessaire
    - ⇨ Rapide simple, automatisée et fiable
    - ⇨ Ne pas être dépendant de multiples éditeurs et des utilisateurs
  - Plus de temps disponible pour l'application des patches
    - ⇨ les systèmes sont protégés
- Puis application des patches en accord avec :
  - Les procédure de gestion des changements
  - La politique de sécurité

Pièges

- Performances
  - Protection sur des LAN à haut débit
    - ⇨ Réseaux multi-gigabit
    - ⇨ Aucune latence n'est acceptable
  - Sur plusieurs segments
    - ⇨ Protection de l'ensemble des liens du SI
- Mise à jour des signatures
  - Travail 24x7x365
  - Besoin d'experts dans plusieurs domaines
  - PAS de faux-positifs … ou vous tuez le réseau
- Ne pas patcher les systèmes

Solution

1. Plateforme fournissant de hautes performances
   - Capacité de gérer :
     - ⇨ Une charge de trafic importante
     - ⇨ Des signatures de niveau 3 à 7
2. Définition de signatures intelligentes
   - Intégration de l'environnement
     - ⇨ Limiter les signatures aux OS/applications concernés
   - Définir un groupe spécifique de signatures
     - ⇨ Attaques, virus et vers les plus récents
     - ⇨ Attaques les plus critiques
     - ⇨ Attaques, même obsolètes, toujours présentent sur le réseau

radware

Je ne veux pas être injecté

Renaud Bidou
Security Consultant, EMEA

radware
availability | performance | security

APSolute Application Delivery

HTML

- HTML injection
  - Accures par les langages de script php, perl, asp etc.
    - ⇨ `<? phpinfo()?>`
  - XS* injection
    - Cross Site Scripting
      - `document.(cookie|location)` et les autres
      - Rebond via des utilisateurs innocents
      - ⇨ `<frame src="ftp://server/AAAAAAAAAAoverflowAAA">`
      - Exploitation des droits des utilisateurs
      - ⇨ `<img src="passchange.php?new=a&again=a">`
    - Cross Site Tracing

SQL injection

- Immédiat
  - ⇨ La fameuse injection - user' OR '1 -
- Injection avancée (?)
  - Inspecter la structure SQL
  - ⇨ `http://server/index.asp?id=1 UNION SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES`
  - Insertion de données
  - ⇨ `http://server/index.asp?id=10; UPDATE 'admin_login' SET 'password' = 'newpas5' WHERE login_name='neo'-`
- Rebind sur les procédures stockées
  - Habituellement avec les opérations UNION et OR

Commandes externes

- Utilisation de scripts cgi et de requêtes SQL
  - L'utilitaire web "ping"
    - ⇨ `194.98.65.65;cat /etc/passwd`
  - Shell intégré à la base SQL
    - ⇨ `'; exec master..xp_cmdshell 'ping 10.10.1.2'--`
- Exploiter les spécificités des langages
  - Le *pipe* en PERL
    - ⇨ `open(FILE,"<filename>") = open <filename>`
    - ⇨ `open(FILE,"<filename>|") = execute <fimename>`
  - L'exception du caractère NULL (\0)
    - ⇨ Interpreté comme un caractère par PERL
    - ⇨ Fin de chaîne en C

Protection ?

- Signatures
  - Codées en dur ⇨ stupide et inutile
  - RegExp ⇨ L'efficacité dépend du moteur (NFA vs. DFA)
  - Réseaux de neurones ⇨ Encore en R&D
  - Sandbox… ⇨ Science-Fiction
- Et encore les performances
  - Signatures de niveau 7
    ⇨ URL, contenu et *parsing*
  - Plus sophistiqué = plus de CPU

Réalité

Renaud Bidou
Security Consultant, EMEA

APSolute Application Delivery

Tout ensemble

- Besoins techniques
  - SYNCookies, Echantillonage de traffic, gestion de la bande passante
  - Conformité aux RFC, analyse *stateful*, signature et anomalies
  - Base de signatures d'attaques, de vers et de virus à jour et fiable
  - Moteur d'analyse des signatures "intelligent"
- ET PERFORMANCE

Des mythes

- Rien de difficile

MAIS

- Etes vous sûr que votre solution IDS/IPS/snort-inline
  1. Mettra en oeuvre ces fonctionnalités
  2. Sans introduire de latence
  3. Dans votre architecture

Les IPS existent

- Ils ne sont pas (ou ne devraient pas être…)
  - Des solutions hybrides Firewalls/IDS
  - La résultante d'un nuage marketing
- Il sont (ou devraient être…)
  - Un hardware dédié
    - Une architecure distribuée reposant sur des ASIC's
      - ⇨ Opération de traitement des couches 3/4
      - ⇨ Analyse avancée de niveau 7
  - Des équipements de sécurité supplémentaires
    - Ne jetez pas vos firewalls !

Questions?

Renaud Bidou
Security Consultant, EMEA