



HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Solutions Linux 2005

Thème sécurité

2 février 2005

Ethereal : un analyseur réseau libre et un outil de sécurité indispensable

Jean-Baptiste Marchand
<Jean-Baptiste.Marchand@hsc.fr>

- x Introduction à Ethereal
- x Architecture
- x Aperçu des fonctionnalités
- x Mécanismes de fonctionnement
 - x Décodage des protocoles
 - x Réassemblage
- x Exemples d'utilisation en sécurité
- x Sécurité
- x Développement
- x Conclusion
- x Références

- x Ethereal
 - x Analyseur réseau libre sous licence GPL, fonctionnant sous Unix et Windows
 - x Projet démarré en 1997 par Gerald Combs, rapidement rejoint par d'autres contributeurs
 - x Version 0.2.0 en Juillet 1998
 - x Version courante : 0.10.9, sortie le 20 Janvier 2005
- x Fonctionnalités d'Ethereal
 - x Capture sur le réseau, via la bibliothèque pcap sous Unix ou Winpcap sous Windows
 - x <http://www.ethereal.com/media.html>
 - x Lecture de nombreux formats de traces, générés par d'autres analyseurs réseau
 - x Décodage de nombreux protocoles, via des dissecteurs dédiés

- x Ensemble d'outils du projet Ethereal
 - x ethereal : analyseur réseau graphique (GTK+ et GTK+2)
 - x tethereal : version en ligne de commande d'ethereal
 - x editcap, mergecap : outils d'édition de traces réseau
 - x capinfos : aperçu du contenu d'un fichier de trace réseau
 - x text2pcap : conversion d'un fichier texte en trace réseau au format pcap

- x Wiretap
 - x Assure la récupération des données, venant du réseau ou d'un fichier de trace réseau
- x Dissecteurs
 - x Modules assurant le décodage d'un protocole réseau spécifique
 - x Protocoles supportés se situent à tous les niveaux du modèle réseau
- x Interface utilisateur
 - x En mode graphique (GTK+) : ethereal
 - x Présentation sous la forme de 3 panneaux
 - x Résumé des trames, détail d'une trame décodée, données brutes décodées
 - x En mode ligne de commande : tethereal
 - x Mode résumé ou mode détaillé (option `-v`)

HSC ethereal

No.	Time	Source	Destination	Protocol	Info
18	2005-02-01 11:52:40.333469	199.128.212.234	199.128.212.145	TCP	65000 > 8082 [ACK] Seq=175642167 Ack=3318023095 Win=6
19	2005-02-01 11:52:40.353281	199.128.212.145	199.128.212.234	TCP	[TCP segment of a reassembled PDU]
20	2005-02-01 11:52:40.450817	199.128.212.234	199.128.212.145	TCP	65000 > 8082 [ACK] Seq=175642167 Ack=3318024507 Win=6
21	2005-02-01 11:52:40.475335	199.128.212.145	199.128.212.234	TCP	[TCP segment of a reassembled PDU]
22	2005-02-01 11:52:40.498322	199.128.212.145	199.128.212.234	TCP	[TCP segment of a reassembled PDU]
23	2005-02-01 11:52:40.498373	199.128.212.234	199.128.212.145	TCP	65000 > 8082 [ACK] Seq=175642167 Ack=3318027331 Win=6
24	2005-02-01 11:52:40.521430	199.128.212.145	199.128.212.234	TCP	[TCP segment of a reassembled PDU]
25	2005-02-01 11:52:40.592512	199.128.212.145	199.128.212.234	TCP	[TCP segment of a reassembled PDU]
26	2005-02-01 11:52:40.592556	199.128.212.234	199.128.212.145	TCP	65000 > 8082 [ACK] Seq=175642167 Ack=3318030155 Win=6
27	2005-02-01 11:52:40.601629	199.128.212.145	199.128.212.234	HTTP	HTTP/1.0 200 OK (GIF89a)
28	2005-02-01 11:52:40.601636	199.128.212.145	199.128.212.234	TCP	8082 > 65000 [FIN, ACK] Seq=3318030779 Ack=175642167
29	2005-02-01 11:52:40.601670	199.128.212.234	199.128.212.145	TCP	65000 > 8082 [ACK] Seq=175642167 Ack=3318030780 Win=6
30	2005-02-01 11:52:40.601809	199.128.212.234	199.128.212.145	TCP	65000 > 8082 [FIN, ACK] Seq=175642167 Ack=3318030780
31	2005-02-01 11:52:40.602499	199.128.212.145	199.128.212.234	TCP	8082 > 65000 [ACK] Seq=3318030780 Ack=175642168 Win=5

- [-] Frame 27 (678 bytes on wire, 678 bytes captured)
- [-] Ethernet II, Src: 00:01:02:a4:98:10, Dst: 00:0d:60:60:42:a1
- [-] Internet Protocol, Src Addr: 199.128.212.145 (199.128.212.145), Dst Addr: 199.128.212.234 (199.128.212.234)
- [-] Transmission Control Protocol, Src Port: 8082 (8082), Dst Port: 65000 (65000), Seq: 3318030155, Ack: 175642167, Len: 624
- [-] Hypertext Transfer Protocol
- [-] CompuServe GIF, Version: GIF89a

```

0120 3a 20 63 6c 6f 73 65 0d 0a 0d 0a 47 49 46 38 39 : close. ...GIF89
0130 51 14 01 6e 00 e7 00 00 ff ff ff f7 fb ff e7 eb a..n.c.. 000+00cè
0140 ff c6 d7 ff bd cf ef ad c7 f7 a5 be ef f7 f7 ff 0E×ÿÿii- C+*ÿi+ÿ
0150 84 aa f7 59 81 d6 31 65 d6 21 59 d6 18 4d c6 18 .@+Y_01e 01Y0_M0C.
0160 49 b5 10 45 b5 4a 7d e7 63 96 ef ce d3 e7 ef ef [p.Eu]c c.iif0cii
0170 ef 18 51 ce 08 3c a5 a5 b6 d6 d6 db e7 f7 f7 f7 i.Qf.<#¥ 0000c+++
0180 ff fb ff 73 a2 ef 18 45 ad 10 3c 94 29 49 94 3b 00ÿs0i.E -.<.)I.:
0190 59 93 4a 61 94 52 6d ad 39 71 de 94 ae de e7 e7 Y.Ja.Rm- 9qP.0Pcc
01a0 ef 29 51 b5 63 79 a4 94 9e b5 c6 c7 ce d6 d3 d6 i)Qucyx. µE0i000
01b0 de db d6 d6 d7 d6 d9 d7 cb ce cf ce c6 c7 c6 b5 P000×00× éiif0C0µ
01c0 b6 bd 73 8e ce da e5 ff b5 ba c6 de db de de df 0s.i0âÿ µ0E0P0P0
01d0 de c6 c3 c6 c6 be bd bd be bd a5 a6 ad 5a 8a ef P0E0E0ÿÿÿ 0ÿÿi-Z.i
01e0 10 34 84 bd ba bd b5 b2 b5 b5 b6 b5 84 92 b5 bd .4.ÿ0ÿµ² µµ0µ..µÿ
01f0 b6 bd 9c 9a 9c 39 61 b5 08 24 63 73 79 8c ce cb 0ÿ...9ap .0csÿ.iE
0200 ce ad aa a5 e7 e3 e7 84 86 94 ad ae ad ef eb ef i-@#çç. ..0-ièi
0210 f7 f3 ef e7 e7 e7 8c 92 94 49 55 73 de df e7 ad +0iccc.. .IUsP0c-
0220 a6 ad f7 f3 f7 b5 b2 ad a5 a6 a5 9c 9e 9c a5 a2 |-+0+µ² - #!ÿ...#0
0230 a5 ad aa ad 5a 69 7c 29 41 6b b5 c3 de 7b 86 ad 0-@-Zil) Akµ0P(-
  
```

Frame (678 bytes) Reassembled TCP (9165 bytes)

Filter: Add Expression... Clear Apply CompuServe GIF (image-gif), 8866 bytes



- x Aperçu des fonctionnalités
 - x Réassemblage
 - x Datagrammes IP, segments TCP, ...
 - x Fonctionnalité *Follow TCP stream* : affichage du contenu d'un flux TCP
 - x Aperçu rapide du trafic
 - x Fonction *Protocol Hierarchy*
 - x Fonctions *Conversations* et *Endpoints*
 - x Filtrage des trames affichés via les *display filters*
 - x La plupart des dissecteurs rendent disponibles les champs décodés sous forme de champs
 - x Fonctions *Prepare a Filter*, *Apply a Filter*, *Add Expression*
 - x Fonction *Export selected packet bytes*
 - x Permet de sauvegarder une partie des données
 - x Fonctionne également sur des données après réassemblage de segments TCP
 - x Ex : sauvegarder une image dans un flux HTTP

- x Les dissecteurs peuvent être appelés de plusieurs façons différentes
 - x Dissecteurs appelés lorsque certaines valeurs sont décodées dans une couche de niveau inférieure
 - x Adaptés pour les dissecteurs des protocoles des couches basses, où un champ de l'en-tête spécifie le protocole de niveau supérieur
 - x Ex : dissecteur HTTP s'enregistre pour 80/tcp, 8080/tcp, 3128/tcp, 3132/tcp, 3689/tcp, 11371/tcp, 1900/tcp et 1900/udp
 - x Peut conduire à des identifications incorrectes si du trafic sur ce port est observé et que le dissecteur ou le protocole lui-même est peu discriminant
 - x D'autres dissecteurs sont dits heuristiques et sont appelés pour voir s'ils reconnaissent des données semblables à celles du protocole qu'ils décodent
 - x Ex : protocoles travaillant sur des ports dynamiques tels que des RPC sur TCP/IP
 - x Lorsque le trafic n'est pas sur un port pour lequel un dissecteur est enregistré, ces dissecteurs sont appelés et peuvent conduire à des identifications incorrectes
 - x D'autres dissecteurs sont appelés explicitement par d'autres dissecteurs

- x Lorsque le décodage proposé par Ethereal est incorrect
 - x Utiliser la fonctionnalité *Decode As* avec un dissecteur non-heuristique
 - x Permet de spécifier un dissecteur à appeler pour décoder les données
 - x Typiquement utilisés pour des protocoles au dessus de TCP ou UDP
 - x Exemple : décoder du trafic HTTP sur le port 81/tcp
 - x Désactiver temporairement un dissecteur heuristique qui pose problème
 - x Via l'entrée *Enabled Protocols* du menu *Analyze*
 - x Peut permettre qu'un autre dissecteur heuristique soit appelé
- x Egalement, possibilité d'inverser l'ordre dans lequel les dissecteurs sont appelés par les dissecteurs TCP et UDP
 - x Option *Try heuristic sub-dissectors first* des dissecteurs TCP et UDP
 - x Si ces options sont activées, *Decode As* peut **ne rien changer** au résultat car les dissecteurs heuristiques sont appelés avant
 - x Dans ce cas, il est possible de **désactiver** le protocole qui pose problème

- x Dissecteur IP sait réassembler les datagrammes d'un paquet IP
 - x Option (dissecteur IP) *Reassemble fragmented IP datagrams*
 - x Typiquement à activer
- x Dissecteur TCP peut réassembler des segments
 - x Permet aux dissecteurs de protocoles sur TCP d'accéder aux données réassemblées à partir de plusieurs segments
 - x Option (dissecteur TCP) *Allow subdissector to reassemble TCP streams*
- x Les dissecteurs pouvant utiliser le réassemblage TCP ont souvent une option pour l'activer
 - x Activée pour la plupart des dissecteurs au dessus de TCP, à l'exception de quelques-uns (ex : HTTP)
 - x Options du type *Reassemble xxx spanning multiple TCP segments*

- x Décodage des protocoles Windows en audits intrusifs
 - x Dissecteurs SMB et interfaces MSRPC
- x Relecture de trafic réseau 802.11 après des audits de réseau Wifi
 - x Avec déchiffrement du WEP, lorsque les clés sont fournies
- x Décodage des protocoles utilisés par la VoIP
 - x Protocoles de la famille H323 : H225, H235, H245, H248, H450
 - x Dissecteurs générés de façon automatique à partir de la grammaire ASN.1
 - x Statistiques pour H225 et conversations H323
 - x Protocole de l'IETF : SIP
 - x Protocoles média : RTP (sauvegarde des flux, y compris audio), RTCP, RTSP
 - x <http://wiki.ethereal.com/VOIPProtocolFamily>

- x Décodage des certificats X509 par le dissecteur SSL
 - x Dissecteur généré à partir de la grammaire ASN.1
 - x Pas de déchiffrement des données, voir ssldump
- x Déboggage de tunnels IPsec (IKE)
- x Déchiffrement des tickets Kerberos (avec Heimdal sous Unix)
 - x Fournir un fichier keytab avec les clés des principaux du royaume

- x Ethereal == multitude de dissecteurs pour le support des protocoles
 - x Régulièrement, des vulnérabilités dans les dissecteurs
 - x <http://www.ethereal.com/appnotes/>
- x Recommandation : éviter d'utiliser Ethereal sous une identité privilégiée
 - x Vient du fait que pour capturer les données sur le réseau, il faut une identité privilégiée
 - x Pas nécessaire sur les systèmes Unix qui gèrent des permissions sur les périphériques bpf (systèmes BSD notamment)
 - x Pas nécessaire sous Windows avec la Winpcap, une fois que le driver a été chargé une fois...
- x Ce qui reste à faire : séparation des privilèges
 - x http://wiki.ethereal.com/Development_2fPrivilegeSeparation
 - x 3 rôles : capture, décodage, interaction avec le système de fichiers

- x Le modèle de développement ouvert est particulièrement adapté à un logiciel tel qu'Ethereal
 - x Nombreux dissecteurs contribués par des professionnels du monde des réseaux et des télécom
- x Ethereal devient l'outil standard pour l'analyse réseau
 - x Les constructeurs de matériels spécifiques fournissent un dissecteur pour leurs protocoles propriétaires, sous la forme de plugin

- x La maîtrise d'un outil d'analyse réseau est incontournable dans beaucoup de tâches liées à la sécurité informatique
- x Ethereal est un outil parfaitement adapté à cette tâche
 - x Support inégalé de nombreux protocoles de toute nature
 - x De nouvelles fonctionnalités sont régulièrement ajoutées, grâce au modèle de développement
- x Les nombreuses fonctionnalités d'Ethereal gagnent à être connues, pour être exploitées au mieux

- x Adresse de cette présentation
 - x <http://www.hsc.fr/ressources/presentations/sl2005-ethereal/>
- x Ethereal
 - x <http://www.ethereal.com/>
 - x <http://wiki.ethereal.com/>
- x Ethereal user's guide
 - x <http://www.ethereal.com/docs/user-guide/>
- x Ethereal sample captures
 - x <http://wiki.ethereal.com/SampleCaptures>
- x Ethereal's useful links
 - x <http://www.ethereal.com/links.html>