CIBLE DE SÉCURITÉ
BRO
CSPN

Référence : SGD005-CDS-1.02

Date : 17 août 2009

SIRET : 493 348 890 000 36 • NAF : 6202 A • RCS Rennes B 493 348 890 • SAS au capital de 38.000 Euros

Maîtrise du document

	Société	Nom	Fonction	Date	Signature
Établi par :	AMOSSYS	J-L DEGUILHAUME	Consultant sécurité	29/07/2009	
Approuvé par :	AMOSSYS	G HIET	Responsable d'évaluation	17/08/2009	

Fiche d'évolutions

Révision	Date	Description	Rédacteur
1.00	29/07/2009	Création du document.	J-L DEGUILHAUME
1.01	03/08/2009	Prise en compte des remarques de l'ANSSI.	O TÉTARD
1.02	17/08/2009	Prise en compte des remarques de l'ANSSI.	O TÉTARD, M OLIVIER

SOMMAIRE

1 INTRODUCTION

1.1 OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation du produit Bro selon le schéma CSPN, relatif au marché 09.02167.00.2.12.075.01 notifié le 20 juillet 2009. Il correspond à la version finale du livrable contractuel émis au titre du poste 1 de la phase 1 : « cible de sécurité ».

Il constitue une cible de sécurité selon le référentiel CSPN pour la sonde de détection d'intrusions Bro.

1.2 PROCÉDURE D'APPROBATION ET DE MISE À JOUR

Ce document est soumis au contrôle technique et au contrôle qualité d'AMOSSYS puis à l'approbation de l'ANSSI.

Les mises à jour de ce document sont effectuées par l'équipe projet d'AMOSSYS.

1.3 DOCUMENTS APPLICABLES

Sigle	Nom du document	Identification	Date
[CCTP]	Cahier des clauses techniques particulières	PA 09-02	8/04/2009
[Marché]	Marché SGDN	09.02167.00.2.12.075.01	10/07/2009 (notifié le 20/07/2009)
[Proposition]	Proposition technique	SGD005-PTC01-1.01	17/06/2009
[Livrable1]	Cible de sécurité	SGD005-CDS	
[Livrable2]	Traduction de la documentation utilisateurs	SGD005-DOC	

1.4 ORGANISATION DU DOCUMENT

Chapitre	Intitulé	Contenu
2	Glossaire	Description des différents acronymes et définitions de certains termes du document
3	Identification du produit	Rappel des éléments permettant d'identifier le produit évalué (version, éditeur, etc.)
4	Description du produit	Description générale du produit
5	Description des biens sensibles	Identification des biens sensibles du produit
6	Description des menaces	Identification des menaces portant sur les biens
7	Description des fonctions de sécurité du produit	Identification des fonctions de sécurité du produit et des fonctions du produit impactant sur la sécurité

2 GLOSSAIRE

Acronyme/mot	Définition
DMZ	*Demilitarized zone* (zone démilitarisée)
DNS	*Domain Name System* (système de noms de domaine)
HIDS	*Host Intrusion Detection System* (IDS système)
HTTP	*Hypertext Transfer Protocol* (protocole de transfert hypertexte)
IDS	*Intrusion Detection System* (Système de détection d'intrusions)
NIDS	*Network Intrusion Detection System* (IDS réseau)
OS	*Operating System* (système d'exploitation)
SMTP	*Simple Mail Transfer Protocol* (protocole de transport de courriel)
TCP	*Transmission Control Protocol* (protocole de contrôle de transmission)
TOE	*Target Of Evaluation* (cible d'évaluation)
UDP	*User Datagram Protocol* (protocole de datagramme utilisateur)
Trace	*Liste des événements émis par l'IDS (alertes, avertissements…)*
Faux positif	*Alerte émise par l'IDS alors qu'aucune attaque n'a eu lieu*
Faux négatif	*Absence d'alerte de la part de l'IDS alors qu'une attaque a eu lieu*

3 IDENTIFICATION DU PRODUIT

Éditeur	Lawrence Berkeley National Laboratory University of California, Berkeley USA
Lien vers l'éditeur	http://www.bro-ids.org/license.html ICSI Center for Internet Research (ICIR) International Computer Science Institute Berkeley, CA USA Contact : vern@icir.org (Vern Paxson)
Nom commercial du produit	BRO
Numéro de version évaluée	1.4 (17 octobre 2008)
Catégorie de produit	Sonde de détection d'intrusions réseau (NIDS)

4 DESCRIPTION DU PRODUIT

4.1 DESCRIPTION GÉNÉRALE

Bro est un système de détection d'intrusions réseau (« *Network Intrusion Detection System* ») *open source*, disponible pour les systèmes d'exploitation de type Unix (dont Linux, FreeBSD et OpenBSD), qui analyse le trafic réseau à la recherche de toute activité suspecte. L'analyse se fait de manière passive et transparente, c'est-à-dire qu'il n'altère pas les paquets réseaux qu'il traite[1].

Bro détecte les intrusions en deux temps :

- le premier consiste à capter le trafic réseau et à décoder les différentes couches protocolaires (de manière à en extraire la sémantique applicative). Cette étape fournit des événements de « haut-niveau » qui pourront par la suite être analysés ;
- le second consiste à analyser les événements générés lors de la première étape par des scripts d'analyse. Ces scripts comparent ces événements par rapport à des motifs caractérisant des comportements réputés anormaux. Cette analyse permet à la fois la détection d'attaques connues au préalable (qui sont décrites en termes de signatures ou d'événements) et d'anomalies (par exemple, la présence de connexions de certains utilisateurs vers certains services ou l'occurrence de tentatives de connexions infructueuses).

Bro utilise un langage spécifique qui permet d'adapter son fonctionnement au contexte du réseau à surveiller. Si Bro détecte un scénario d'attaque, il peut réagir de différentes manières :

- il peut générer une entrée de journal (en utilisant éventuellement le système de gestion de journaux de l'OS) ;
- il peut alerter l'opérateur par courriel (le rapport étant chiffré via GPG) ;
- il peut exécuter une commande définie par l'administrateur (par exemple, de mettre fin à une connexion ou de bloquer un hôte malveillant à la volée). Ce système permet donc à l'administrateur d'adapter le type de réponse.

Bro peut générer des journaux détaillés qui sauvegardent les différents événements observés. Ces journaux peuvent s'avérer utiles lors de la phase de diagnostic réalisée lorsqu'une attaque est détectée (analyse *post mortem*).

Bro permet de surveiller des réseaux à haut débit (Gbps). Tout en fonctionnant sur du matériel de type PC, Bro est en mesure d'atteindre les performances nécessaires à la surveillance de réseau à fort trafic en réalisant une combinaison judicieuse de techniques de filtrage de paquets. Il constitue donc une solution peu coûteuse permettant de surveiller le trafic d'une connexion Internet.

---

[1] Il est toutefois possible d'adopter une attitude plus active et mettre fin à certaines connexions pour lesquelles des actions douteuses ont été détectées. Ce n'est cependant pas le mode de fonctionnement standard de Bro.

4.2 PRINCIPALES CARACTÉRISTIQUES

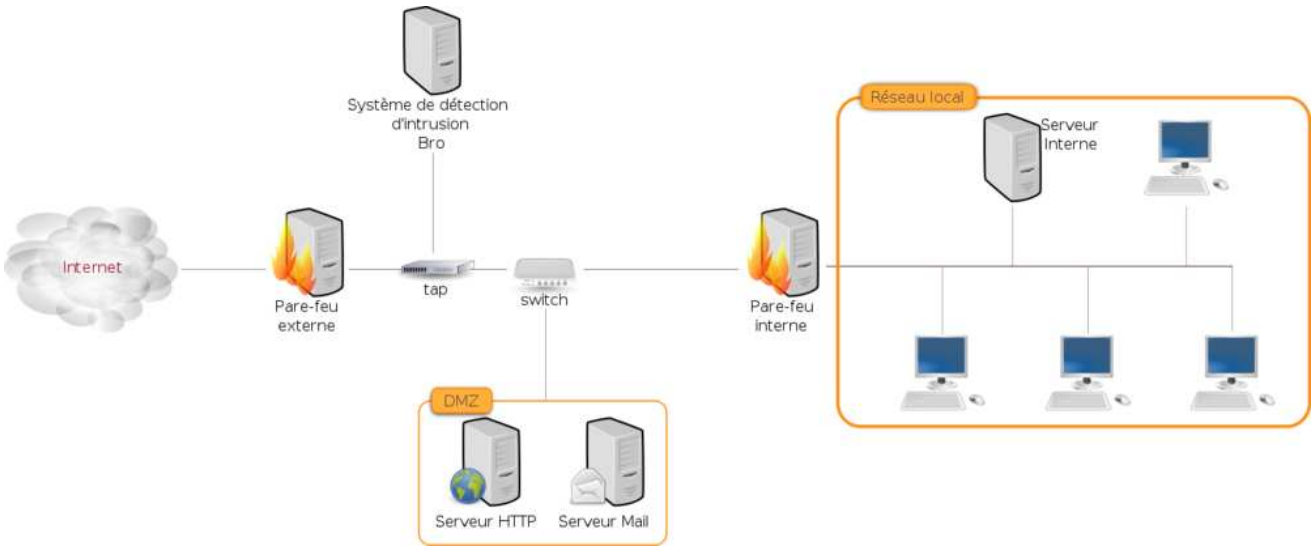


Figure 1 – Exemple d'intégration de Bro dans un réseau

Un IDS réseau

Bro est un IDS réseau. Il recueille, filtre (éventuellement), décode et analyse le trafic qui passe à travers un réseau local. Un seul moniteur Bro, placé à un carrefour stratégique du réseau, peut être utilisé pour surveiller tout le trafic entrant et sortant du réseau. Il est également possible de le placer sur un segment particulier du réseau afin de ne surveiller que le trafic à destination (ou en provenance) d'une zone particulière (par exemple, la « zone démilitarisée » ou DMZ). La figure 1 donne un exemple possible d'intégration d'une sonde Bro dans un réseau. Bro ne nécessite pas l'installation de logiciel client sur chaque ordinateur du réseau. En revanche, il s'agit d'une solution logicielle qui nécessite le support d'une architecture matérielle et d'un OS (de type UNIX).

Analyse détaillée de la couche applicative

Bro a la capacité de comprendre de manière détaillée de nombreux protocoles d'application, et ce, par le biais de codes spécifiques ou « analyseurs ». Ces derniers génèrent un flux d'événements décrivant l'activité observée au niveau sémantique. Ces événements ne constituent pas des alertes[2] de sécurité, mais fournissent plutôt les entrées pour d'autres traitements réalisés par Bro. Ces traitements sont développés dans un langage de script spécifique.

---

[2] Bro différencie les avertissements (« *notice* »), des informations internes qui peuvent être transformés en alertes (« *alarm* »), qui seront remontées à l'exploitant de Bro (par exemple par courriel). Par défaut, Bro transforme tous les avertissements en alertes.

Langage de script spécifique

Les scripts décrivant les politiques d'analyse de Bro sont des programmes écrits dans un langage de script spécifique à Bro. Ils contiennent les « règles » qui décrivent les activités considérées comme problématiques. Ils interprètent les événements issus de l'activité réseau et lancent des traitements complémentaires. L'apprentissage du langage peut nécessiter du temps et des efforts mais une fois maitrisé, l'administrateur Bro dispose d'un outil puissant lui permettant de définir des politiques de détection et d'analyse propres aux besoins du réseau qu'il administre.

Politiques par défaut

Bro est livré avec un ensemble de scripts conçus pour détecter les attaques Internet les plus communes. L'utilisation de ces scripts ne nécessite pas de connaître le langage de script de Bro ni le mécanisme de mise en œuvre des politiques Bro.

Mécanisme de reconnaissance de signatures d'attaques

Bro comprend un mécanisme de reconnaissance de signatures qui permet d'identifier des contenus spécifiques dans le trafic capté. Pour Bro, ces signatures sont exprimées à l'aide d'expressions régulières, plutôt que d'utiliser de simples chaînes de caractères. La richesse du langage Bro complète utilement le mécanisme de reconnaissance de signatures. Il permet en effet de prendre en compte le contexte du réseau à surveiller. Par exemple on pourra définir les types de machines présentes dans le système d'informations ainsi que les services qu'elles offrent. Il sera ainsi possible de réduire potentiellement le nombre de faux positifs.

L'analyse de trafic réseau

Bro recherche des motifs d'attaques par rapport aux signatures dont il dispose, mais il peut aussi analyser les protocoles réseau, les connexions, les transactions, les volumes de données et de nombreuses autres caractéristiques du réseau afin d'y détecter l'occurrence de comportements anormaux. Il dispose de mécanismes permettant de stocker les informations relatives aux événements observés par le passé afin de l'intégrer dans l'analyse de nouvelles activités.

Détection, suivi d'une action

Les scripts Bro peuvent générer des enregistrements de l'activité dans des fichiers de sortie (y compris l'activité normale et non agressive). Ils peuvent également générer des alertes vers le journal d'événements du système d'exploitation, y compris le système de gestion de journaux `syslog`. Les scripts peuvent également exécuter des programmes (script *bash*, etc.) définis par l'administrateur. Ceci peut permettre :

- d'envoyer des courriels à l'utilisateur en charge de la supervision ;
- de mettre fin automatiquement à des connexions existantes ;
- d'insérer des règles de contrôle d'accès à un routeur ;
- etc.

Compatibilité avec le logiciel Snort

Snort est un système de détection d'intrusions réseau (NIDS) par signature. Il est largement répandu et son langage de signature constitue ainsi un standard de fait. Bro inclut un outil de conversion des signatures de l'IDS Snort vers son propre format de signatures : `snort2bro`.

4.3 DESCRIPTION DE L'ENVIRONNEMENT PRÉVU POUR SON UTILISATION

La TOE est évaluée en tant que logiciel implémentant une sonde de détection d'intrusions. Son utilisation nécessite donc le support d'une plate-forme matérielle et d'un OS. La configuration conseillée est la suivante :

- une machine dédiée comprenant au minimum une interface réseau[3], des capacités de stockage et de traitement adaptées (voir la documentation en français de Bro, [Livrable2]) ;
- un OS de type UNIX (FreeBSD est conseillé, Linux et OpenBSD sont également supportés) et les bibliothèques nécessaires à l'installation de Bro[4] ;
- un ensemble de programmes permettant l'administration de l'IDS (et assurant éventuellement les fonctions de manager de l'IDS, celles de Bro étant limitées).

L'IDS doit être relié au réseau observé par un mécanisme (de type *tap* ou un *switch* possédant des capacités de *mirroring*) permettant la capture du trafic de manière transparente et robuste (c'est-à-dire, sans perte de paquets).

La documentation de Bro ne donne pas d'indications précises sur la localisation de l'IDS au sein du réseau. Celle-ci dépend de son utilisation. Dans un cadre général d'utilisation pour de tels systèmes, l'IDS est placé de manière à observer le trafic local (réseau local bureautique ou DMZ)[5].

4.4 DESCRIPTION DES HYPOTHÈSES SUR L'ENVIRONNEMENT

H1 : les exploitants de Bro sont formés à l'élaboration de scripts (et de signatures) additionnels, au paramétrage nécessaire au bon fonctionnement ainsi qu'à l'analyse des alertes et des traces.

H2 : Bro et l'OS sous-jacent sont administrés par la même personne qui dispose des droit d'administration et qui est réputée de confiance.

H3 : la bibliothèque `libpcap` et les outils (éditeur de texte) permettant le paramétrage de Bro sont des modules de confiance dans le sens où ils ne sont pas piégés.

H4 : les ressources de stockage des traces, notamment lorsqu'elles sont distantes, sont uniquement accessibles à des utilisateurs qui disposent du droit d'en connaître et qui mettent en

---

[3] Il est conseillé d'utiliser également une interface supplémentaire dédiée à l'administration de l'IDS.

[4] Dans le cadre de cette CSPN, Bro sera évalué sur le système OpenBSD.

[5] Il n'est souvent par pertinent de le placer sur le point d'accès à Internet, avant les mécanismes de filtrage.

œuvre les bonnes pratiques permettant d'assurer la confidentialité et l'intégrité des informations auxquelles ils accèdent.

H5 : les administrateurs des serveurs sur lequel Bro se repose pour envoyer, par exemple, ses rapports quotidiens (serveur de courriels, serveur de centralisation de journaux système, etc.) sont de confiance.

H6 : l'OS met en œuvre les mécanismes de protection adéquats (confinement, contrôle d'accès, etc.) qui sont paramétrés et configurés selon les bonnes pratiques en vigueur. Ceci permet d'assurer la sécurité des biens hébergés vis-à-vis des applications tierces, qui sont susceptibles d'être malveillantes ou piégées.

H7 : les équipements contenant les services de Bro (différentes sondes, serveurs de courriels permettant l'envoi des rapports quotidien, etc.), ainsi que tous les supports contenant les biens sensibles de Bro (papier, sauvegardes, etc.) se trouvent dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

H8 : le réseau est observé à l'aide d'un mécanisme (de type *tap* ou un *switch* possédant des capacités de *mirroring*) permettant la capture du trafic de manière transparente et suffisamment robuste pour qu'aucune perte de paquets réseau n'intervienne.

4.5 DESCRIPTION DES DÉPENDANCES PAR RAPPORT À DES MATÉRIELS, LOGICIELS ET/ OU DES MICROPROGRAMMES DU SYSTÈME QUI NE SONT PAS FOURNIS AVEC LE PRODUIT

L'interface entre l'OS et le capteur n'est pas intégrée au paquet Bro. Il s'agit de la bibliothèque `libpcap`. Bro est conçu pour être mis en œuvre sur une version Unix, dont OpenBSD.

La configuration et les options sont passées en ligne de commande ou par des fichiers de configurations qui doivent être modifiés par un éditeur externe (généralement fourni par l'OS).

4.6 DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNÉS

Les utilisateurs des services présents dans le périmètre de détection d'intrusion de Bro ne sont pas impactés par les actions de Bro.

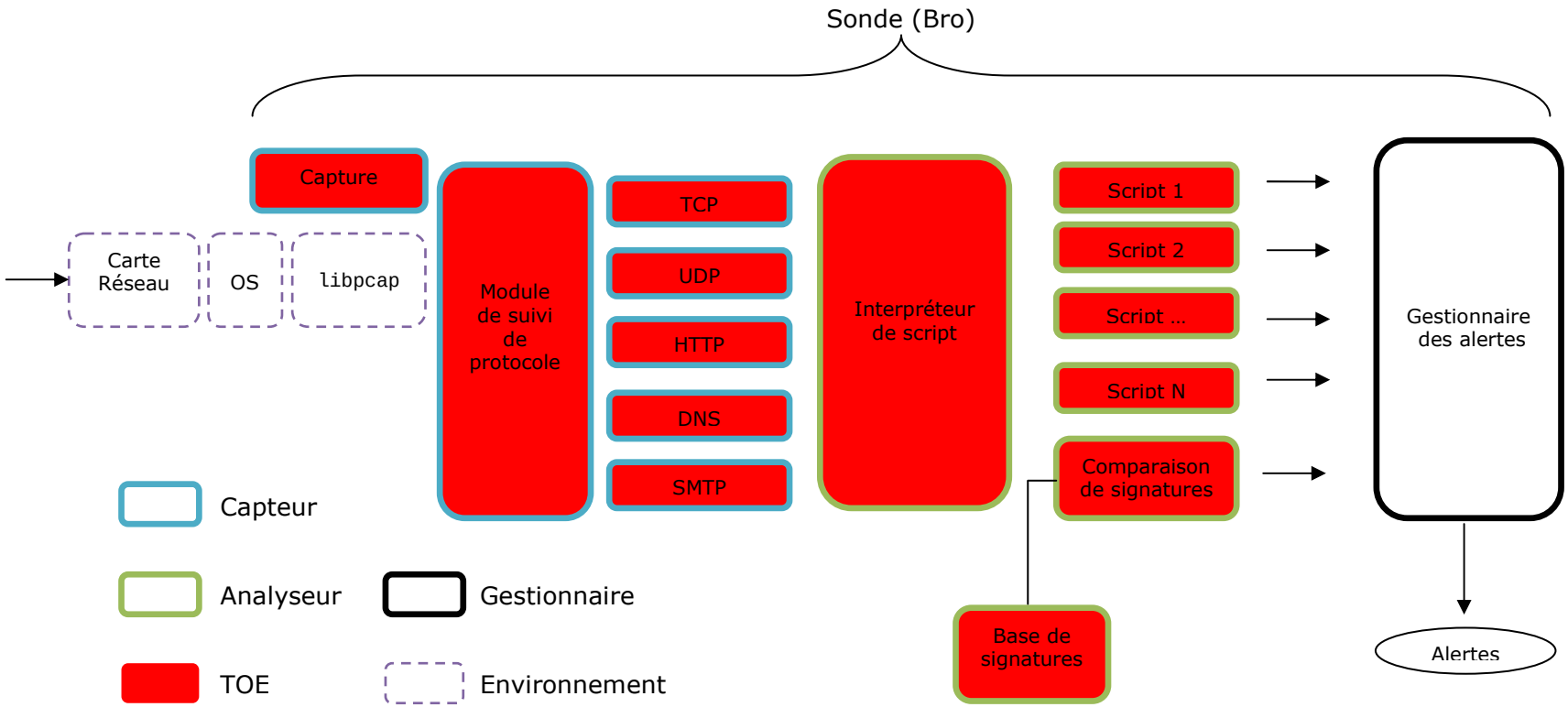
Les seuls utilisateurs qui ont un accès à la TOE sont :

- un **administrateur** de la machine sous-jacente qui a en charge l'installation et la configuration initiale de Bro ;
- un **administrateur de Bro** qui a en charge :
  - les mises à jour de la base de signatures,
  - l'élaboration de scripts répondant à des besoins de détections émergeants ;
- un **exploitant de Bro** qui a en charge :

- la réception des courriels d'alertes (lorsque cette option est mise en œuvre),
- l'analyse des traces générées par Bro.

Ces trois utilisateurs ne disposent d'aucun rôle géré par Bro. Ils peuvent correspondre à un même utilisateur physique.

4.7 DÉFINITION DU PÉRIMÈTRE DE LA TOE



5 DESCRIPTION DES BIENS SENSIBLES

Il existe trois types de biens sensibles :

- les biens fonctionnels liés au processus de détection ;
- les biens propres à la TOE;
- les biens fonctionnels de la sonde qui sont annexes ou accessoires.

Les biens fonctionnels sensibles liés au processus de détection, qui seront examinés lors de l'évaluation, sont :

- **B1** : les fonctions implémentant le module de capture et de suivi des protocoles ;
- **B2** : les fonctions implémentant le module d'interprétation des scripts d'analyse ;
- **B3** : le mécanisme de gestion des règles de signature.

Seuls ces biens (**B1, B2** et **B3)** sont concernés par l'évaluation.

Les biens sensibles propres à la TOE, qui sont gérés par l'environnement, sont :

- **B4** : la base de signatures ;
- **B5** : les politiques d'analyse (scripts) ;
- **B6** : les traces ;
- **B7** : les paramètres de configuration.

Bro ne fournit pas directement de mesure de sécurité pour ces biens. Ils sont typiquement protégés par les mécanismes de protection du système d'exploitation.

Les biens sensibles fonctionnels de la sonde qui sont annexes ou accessoires sont :

- **B8** : le système de diffusion des traces (éventuellement chiffrées via un mécanisme externe) ;
- **B9** : le mécanisme de communication entre plusieurs instances de Bro.

Outre ces biens, la TOE protège implicitement (en détectant les éventuelles attaques) les biens du système qu'elle surveille.

6 DESCRIPTION DES MENACES

Seules les menaces correspondantes aux biens sensibles du processus de détection seront considérées lors de l'évaluation. Ces menaces sont :

- **M1** : un attaquant tente de contourner le système de suivi protocolaire de Bro dans le but de réaliser une attaque indétectable par la TOE ;
- **M2** : un attaquant tente de contourner le système d'interprétation des scripts de Bro dans le but de réaliser une attaque indétectable par la TOE ;
- **M3** : un attaquant tente de contourner le système de reconnaissance de signatures de Bro dans le but de réaliser une attaque indétectable par la TOE ;
- **M4** : un attaquant tente d'inonder le système de détection d'intrusion en émettant de très grandes quantités de données arbitraires, par exemple en initiant un grand nombre de connexions du même type afin de nuire au fonctionnement du système de suivi des connexions ;
- **M5** : un attaquant tente d'inonder le système de détection d'intrusions par du trafic inoffensif (absence d'attaques effectives) mais généré sciemment avec pour objectif de faire réagir l'IDS (émission de faux positifs) ;
- **M6** : un attaquant exploite une vulnérabilité de développement (de type débordement de tampon par exemple) afin de modifier le fonctionnement de l'IDS.

7 DESCRIPTION DES FONCTIONS DE SÉCURITÉ DU PRODUIT

Intrinsèquement, Bro ne dispose d'aucune fonction de sécurité.

La sécurité des biens sensibles identifiés au chapitre 5 repose donc essentiellement sur les meilleures pratiques en termes de sécurisation du système d'exploitation sous-jacent à Bro et sur l'absence de vulnérabilités dans le code source de l'application.

En revanche, de par la nature du produit évalué, il semble pertinent d'évaluer les fonctions principales qui impactent la sécurité des biens du système surveillé. En effet, l'échec du processus de détection d'intrusions peut conduire à l'absence de prise en compte d'éventuels incidents de sécurité, si le système surveillé est effectivement vulnérable et si aucun mécanisme de protection n'a été à même de le protéger. Ces fonctions sont les suivantes :

- la capture et le décodage de protocole, qui sont assurés pour Bro par les modules suivants, définis au chapitre 4.7 :
    - le module de capture (qui constitue l'interface avec la bibliothèque de capture);
    - Le module de suivi des protocoles avec les scripts nécessaires au suivi des protocoles utilisés durant l'évaluation (TCP, UDP, HTTP, DNS et SMTP).
- l'analyse des événements, qui est assurée pour Bro par les modules suivants :
    - Le mécanisme de comparaison et de gestion en mémoire des signatures ;
    - L'interpréteur de script ainsi que les scripts de détection activés par défaut ;
    - Les signatures définies par défaut.