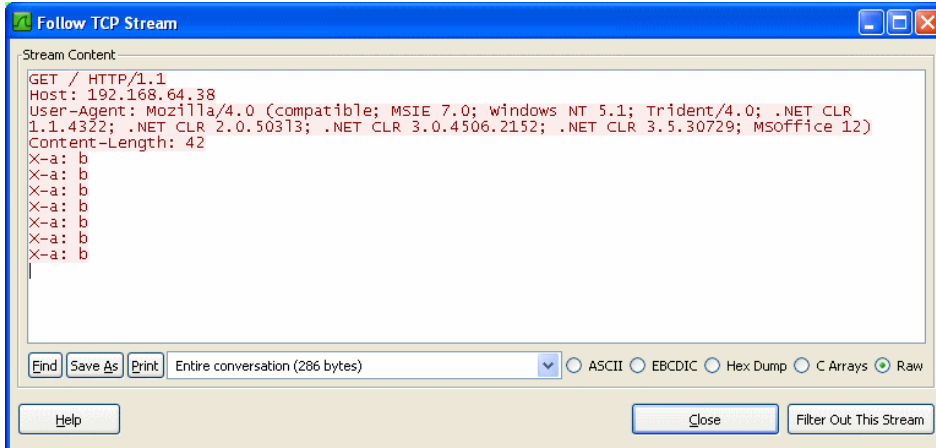
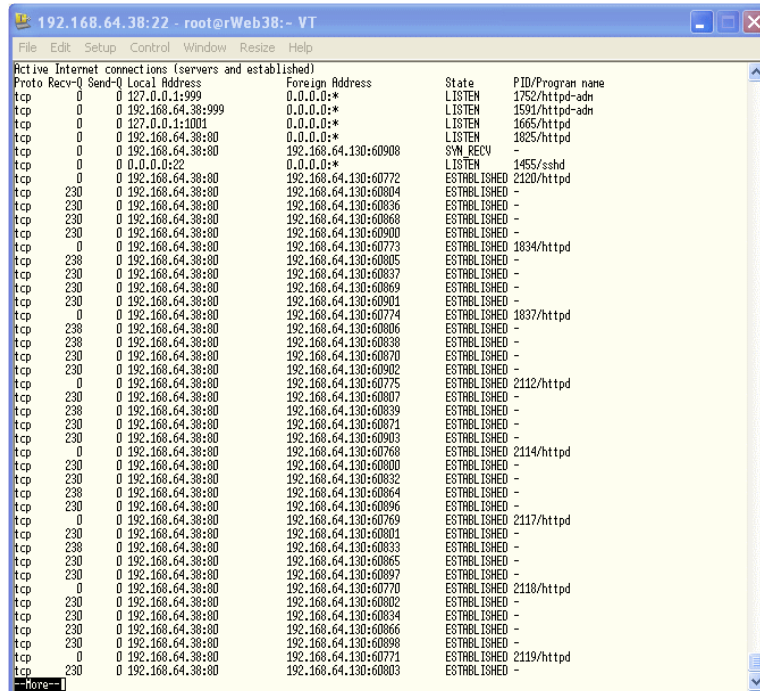


Description de l'attaque

L'attaque consiste à initier des requêtes HTTP sans les terminer, la connexion étant maintenue active par l'envoi répétitif d'en-têtes. La figure ci-dessous montre une trace de ces requêtes, et identifie clairement l'en-tête « X-a : b » utilisé par l'outil.



Le serveur Web Apache ne transmet les requêtes aux modules de traitement qu'une fois ces dernières complétées. Par conséquent le serveur est vulnérable dans la mesure où il ne libère pas les connexions actives établies par l'outil. Pour la même raison les modules de sécurité ne peuvent être appliqués. Une fois l'attaque lancée le serveur cible maintient des connexions ouvertes dans l'état ESTABLISHED, comme le montre la figure ci-dessous.



Après un temps relativement court le serveur n'est plus accessible. Cet état est maintenu pendant toute la durée de l'attaque.

Protection

Aucun patch bloquant de manière effective cette attaque n'a été publié pour Apache jusqu'à présent. Seul DenyAll a publiquement fait état d'un patch pour le cœur du serveur Apache et implémenté dans le reverse proxy rWeb. Une protection peut toutefois être mise en œuvre à l'aide de différents outils externes. Deux mécanismes complémentaires sont appropriés. Le premier consiste à filtrer l'en-tête spécifique utilisé par l'outil slowloris : « X-a : b », et de placer la source de la requête en liste noire. Sur Linux cette opération peut être effectuée via les

iptables de Linux. Les commandes nécessaires sont les suivantes.

```
iptables -A INPUT -m recent --update --seconds 60 -j DROP
iptables -A INPUT -p tcp --dport 80 -m string --algo bm --string "X-a :" -m recent --set -j DROP
```

La première ligne rejette les adresses IP appartenant à la liste noire et initialise un timer de 60 secondes au cours desquelles la source reste dans la liste noire. La seconde ligne identifie la chaîne de caractères « X-a : », bloque la requête et marque la source comme mise en liste noire.

Cette technique permet de bloquer immédiatement les sources utilisées pour lancer l'attaque. Elle s'avère particulièrement efficace dans le cas de botnets, ces derniers utilisant généralement des programmes originaux. Toutefois, en cas de modification du texte de l'en-tête malveillant la protection devient sans effet. Il reste possible cependant de modifier la chaîne de caractères utilisée pour le filtrage et le marquage de la source, ou d'en rajouter de nouvelles en modifiant la seconde ligne et en remplaçant la chaîne "X-a :" par un contenu approprié.

Afin de pallier les limitations du premier mécanisme, il est nécessaire de limiter le nombre de connexions initiées par une même adresse IP. Il peut être mis en œuvre au niveau d'un firewall ou d'un IPS. Avec le firewall iptables la commande à lancer est la suivante :

```
iptables -A INPUT -p tcp --dport 80 -m connlimit --connlimit-above 50 -j REJECT --reject-with tcp-reset
```

Cette solution est plus générique que la précédente. Toutefois elle peut entraîner une baisse de performances du serveur dans le cas d'une attaque largement distribuée.

Conclusion

A ce jour aucune protection native à Apache n'est publiquement disponible. Une telle protection nécessite une modification du mode de fonctionnement interne du serveur.

Cependant les techniques de protection préconisées dans ce document bloquent efficacement l'attaque et présentent une flexibilité suffisante pour adapter la réaction à d'éventuelles modifications de cette dernière. En outre ces mécanismes peuvent être appliqués sur la plupart des équipements de sécurité réseau tels que des IPS et des Firewalls, permettant ainsi une mise en œuvre dans la plupart des environnements.