Rapport de Compromission

- **Date de l'Incident :** 29/11/2023
- **Heure de l'Incident :** 15h41
- **Événement/Projet :** Shellshock Attack detected
- **Auteur du Rapport :** Alexandre Calvez
- **Équipe Blue Team :** Damien remusat, Sebastien Venturinni, Mathilde Sallac, Mélanie Budnyk, Seb P

Résumé de l'Incident :
L'incident a été initié par l'exploitation de la vulnérabilité Shellshock CVE-2014-6278, octroyant à un attaquant la capacité d'exécuter des commandes arbitraires sur le serveur Apache du système hébergé sur la machine à l'adresse IP 10.0.1.53.

Détails de l'Incident :

1. **Détection :**
   - **Méthode de détection :** Surveillance des journaux d’event Wazuh
   - **Outils utilisés pour la détection :** Wazuh
2. **Analyse de l'Attaque :**
   - **Type d'attaque :** shellshock attack (CVE-2014-6271)
   - **Vecteur d'attaque :** L'attaque exploite la vulnérabilité Shellshock (CVE-2014-6271 et CVE-2014-6278), qui est une faille de sécurité dans le shell Bash. Cette vulnérabilité permet à un attaquant d'exécuter du code arbitraire sur un serveur qui utilise Bash pour interpréter des commandes. Dans le contexte HTTP, cette injection de code se produit en manipulant les en-têtes de la requête.
   - **Points d'entrée identifiés :** Le point d'entrée clé de cette attaque réside dans le champ User-Agent ou tout autre champ de la requête HTTP qui est interprété par le serveur. Ces champs constituent les vecteurs à travers lesquels l'attaquant a introduit le payload malveillant, exploitant ainsi une vulnérabilité potentielle dans le processus d'interprétation des données par le serveur.

- **Mouvements latéraux :** L'intégralité du payload a été soigneusement conçu pour exploiter une vulnérabilité dans le shell Bash de la machine cible. L'objectif sous-jacent était vraisemblablement d'exécuter des commandes arbitraires sur le système compromis. La détection de la vulnérabilité a été accompagnée d'une réponse du serveur indiquant une redirection, suggérant ainsi une tentative de manipulation du comportement du serveur par l'attaquant. Ce mouvement latéral visait à étendre l'emprise de l'attaque et à potentiellement compromettre davantage de ressources au sein de l'environnement cible.

3. **Impact Initial :**
    - **Services ou données compromis(e)s :** serveur Apache
    - **Durée de la compromission initiale :** 1h
4. **Réponse Initiale :**
    - **Actions immédiates prises :** Application immédiate de correctifs pour la vulnérabilité CVE-2014-6278 impliquant la mise à jour du Bash vers une version corrigée, ainsi qu'une mise à jour du serveur apache **p**ar mesure de précaution, une procédure de changement immédiat des identifiants a été mise en place.
    - **Isolation des systèmes affectés :** 10.0.1.53

Analyse Post-Compromission :

1. **Identification de la Vulnérabilité :**
    - **Vulnérabilité exploitée :** vulnérabilité shellshock CVE-2014-6278
    - **Recommandations pour la mitigation :** Une vigilance accrue a été instaurée en renforçant la surveillance des logs et du trafic réseau. Ainsi qu'une analyse forensique des logs du serveur Apache a été déployée pour scruter les traces de l'attaque.
2. **Activités de l'Attaquant :**
    - **Comportements observés :** Au cours de l'analyse des logs du serveur Apache effectuée, des tentatives manifestes d'injection XSS (Cross-Site Scripting) ont été identifiées. Ces incidents ont été relevés au cours de la même journée que celle de l'attaque principale, signalant une série coordonnée de tentatives d'exploiter des vulnérabilités de type XSS.
3. **Réponse et Contre-Mesures :**

- **Mesures immédiates prises :** Pour renforcer immédiatement la sécurité de notre site web, nous avons pris des mesures importantes. Tout d'abord, nous avons installé un pare-feu d'application web (WAF) appelé ModSecurity. ModSecurity est une solution open source qui agit comme une défense contre les attaques ciblant les applications web, aidant ainsi à détecter et à prévenir les menaces potentielles, par l'instauration de règles. En parallèle, nous avons optimisé les fichiers de configuration d'Apache pour améliorer la sécurité globale du site. Nous avons spécifiquement configuré Apache pour éviter la surcharge de fichiers de configuration via les fichiers ".htaccess", assurant ainsi une gestion plus centralisée des paramètres de sécurité. De plus, nous avons mis en place des restrictions d'accès à certains répertoires du serveur web, renforçant ainsi la sécurité en limitant l'accès à ces zones sensibles.
- **Contre-mesures à long terme :** En vue de renforcer la sécurité de manière durable, nous avons instauré une politique de gestion des correctifs rigoureuse. Cela garantit que notre système bénéficie constamment des dernières mises à jour de sécurité, avec une surveillance régulière des annonces de vulnérabilités. La sensibilisation à la sécurité des applications est une priorité constante. Nous avons intégré la formation continue des développeurs à nos pratiques de développement pour prévenir les erreurs de codage pouvant conduire à des vulnérabilités XSS. Cette approche proactive garantit que notre équipe demeure informée et apte à prévenir les risques de sécurité à mesure qu'ils évoluent dans le paysage numérique.

4. **Leçons Apprises :**

- **Points forts de la défense :** Réactivité de notre équipe dans l'observation des événements sur Wazuh, combinée à une réponse immédiate pour remédier aux vulnérabilités.
- **Possibles améliorations :** Une proposition majeure consisterait à renforcer notre infrastructure de sécurité en intégrant les logs du système Apache via notre système d'information et de gestion des événements de sécurité (SIEM). Cette intégration permettrait une surveillance centralisée et en temps réel des activités des différents systèmes, améliorant ainsi notre capacité à détecter rapidement les incidents de sécurité et à prendre des mesures préventives.

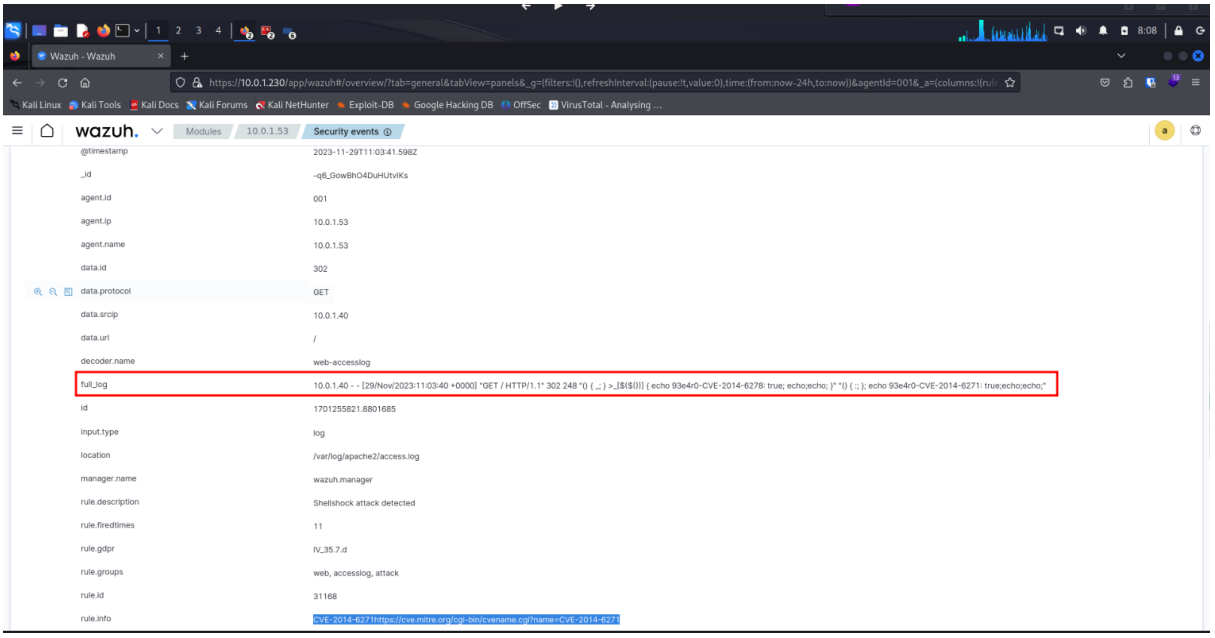
Conclusion :

Cet incident met en évidence l'impératif de maintenir une posture proactive en matière de sécurité face aux menaces émergentes. L'exploitation de la vulnérabilité Shellshock CVE-2014-6278 souligne la nécessité d'une réactivité accrue dans l'application rapide de correctifs et dans la mise à jour continue des systèmes.

L'analyse forensique des logs du serveur Apache a révélé l'impact de l'attaque initiale, ainsi que des tentatives simultanées d'injection XSS au cours de la même journée. Ces observations soulignent l'importance d'une surveillance constante des activités malveillantes et de l'amélioration continue des mécanismes de détection.

Dans cette perspective, envisager l'intégration des logs du système Apache via un SIEM représente une avancée significative. Cette initiative renforce notre capacité à anticiper, détecter et répondre de manière proactive aux incidents de sécurité. Notamment, les points positifs de l'équipe de défense dans la mise en place rapide de correctifs sont à souligner. Associée à des pratiques de mise à jour rigoureuses et à la formation continue de notre équipe, cette approche constitue un élément crucial pour assurer une protection solide contre les menaces futures.

Annexes :



CVE 2014-6271

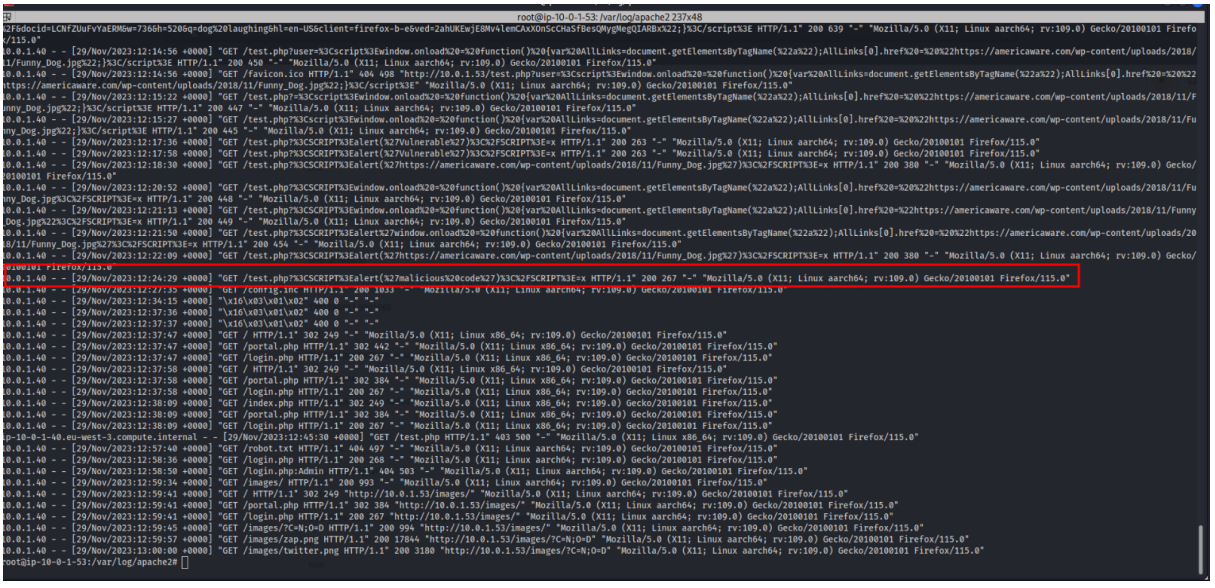
Tags	Vide
Endpoints	10.0.1.53
Owners	Alexandre Calvez
Parent item	Vide
Priority	Vide
Remediations	Vide
Security Events	Vide
Status	Patched
Sub-item	Vide
Vulnerability type	shellshock

Ajouter une propriété

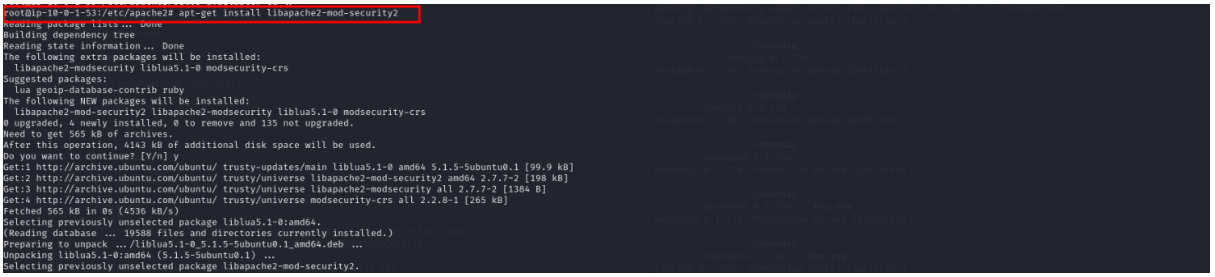
Ajouter un commentaire...

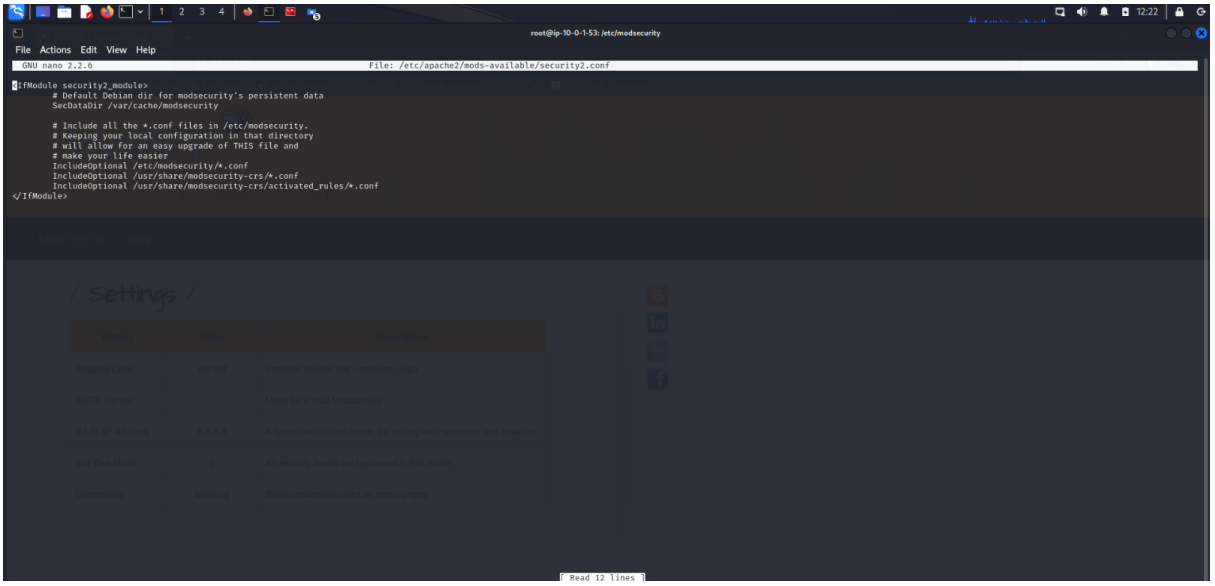
suite à un event wazuh, J'ai effectué une mise à jours sur bash

```
apt upgrade bash
```




File Actions Edit View Help
GNU nano 2.2.6
File: 000-default.conf
<VirtualHost *:80>
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>
<Directory /var/www/html>
Options Indexes FollowSymLinks MultiViews
To make wordpress .htaccess work
AllowOverride None
Order allow,deny
allow from all
</Directory>
ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
<Directory "/usr/lib/cgi-bin">
AllowOverride None
Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
Order allow,deny
Allow from all
</Directory>
<Directory /admin/>
Require all denied
Autres directives ...
</Directory>
<Location "/admin/">
Require host 10.0.1.53
</Location>
ErrorLog ${APACHE_LOG_DIR}/error.log
Possible values include: debug, info, notice, warn, error, crit,
alert, emerg.
LogLevel warn
CustomLog ${APACHE_LOG_DIR}/access.log combined
#
Set HTTPS environment variable if we came in over secure
channel.
SetEnvIf x-forwarded-proto https HTTPS=on
</VirtualHost>


root@ip-10-0-1-53:/etc/apache2# apt-get install libapache2-mod-security2
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following extra packages will be installed:
libapache2-modsecurity liblua5.1-0 modsecurity-crs
Suggested packages:
lua geoip-database-contrib ruby
The following NEW packages will be installed:
libapache2-mod-security2 libapache2-modsecurity liblua5.1-0 modsecurity-crs
0 upgraded, 4 newly installed, 0 to remove and 135 not upgraded.
Need to get 565 kB of archives.
After this operation, 4143 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu/ trusty-updates/main liblua5.1-0 amd64 5.1.5-5ubuntu0.1 [99.9 kB]
Get:2 http://archive.ubuntu.com/ubuntu/ trusty/universe libapache2-mod-security2 amd64 2.7.7-2 [198 kB]
Get:3 http://archive.ubuntu.com/ubuntu/ trusty/universe libapache2-modsecurity all 2.7.7-2 [1384 B]
Get:4 http://archive.ubuntu.com/ubuntu/ trusty/universe modsecurity-crs all 2.2.8-1 [265 kB]
Fetched 565 kB in 0s (4536 kB/s)
Selecting previously unselected package liblua5.1-0:amd64.
(Reading database ... 19588 files and directories currently installed.)
Preparing to unpack .../liblua5.1-0_5.1.5-5ubuntu0.1_amd64.deb ...
Unpacking liblua5.1-0:amd64 (5.1.5-5ubuntu0.1) ...
Selecting previously unselected package libapache2-mod-security2.


root@ip-10-0-1-53: /etc/modsecurity
File Actions Edit View Help
GNU nano 2.2.6
File: /etc/apache2/mods-available/security2.conf
<IfModule security2_module>
Default Debian dir for modsecurity's persistent data
SecDataDir /var/cache/modsecurity
Include all the *.conf files in /etc/modsecurity.
Keeping your local configuration in that directory
will allow for an easy upgrade of THIS file and
make your life easier
IncludeOptional /etc/modsecurity/*.conf
IncludeOptional /usr/share/modsecurity-crs/*.conf
IncludeOptional /usr/share/modsecurity-crs/activated_rules/*.conf
</IfModule>
[Read 12 lines]