|  |  |  |
| --- | --- | --- |
| portsentry  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  portsentry (suite)    http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  portsentry (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  portsentry (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  portsentry (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  portsentry (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png |  | Blocage des balayages de ports  **Présentation**  Les serveurs accessibles depuis internet sont de plus en plus vulnérables aux attaques.  portsentry est un outil qui permet de détecter et de bloquer tout individu balayant les ports d’un hôte.  portsentry est une application qui permet à un serveur de détecter un balayage (*scan*) de ports mais aussi d’agir car …   * les attaques seront inscrites dans les journaux (*logs*) ; * le balayeur de ports est automatiquement bloqué puisque son adresse IP sera ajouté dans le fichier /etc/hosts.deny ; * toutes les communications venant de l’hôte attaquant seront bloquées à l’aide du pare-feu ; * l’interface de communication peut être éventuellement coupée en cas d’attaque.   Il est donc très utile d’installer et configurer portsentry sur un serveur.  Afin d’obtenir de meilleurs résultats, il est possible de le combiner à fail2ban et à un script iptables.  **Installation**  L’installation se fait simplement via *apt* …  **>> sudo apt update && sudo apt --yes upgrade >> sudo apt install --yes portsentry**  Lors de l’installation, un message indique que portsentry ne bloque rien par défaut et les points importants pour la modification de comportement de portsentry.    **Configuration**  Avant de commencer il est préférable de copier le fichier de configuration initial (par précaution) …  **>> sudo cp --verbose /etc/portsentry/portsentry.conf /etc/portsentry/portsentry.conf.otiginal '/etc/portsentry/portsentry.conf' -> '/etc/portsentry/portsentry.conf.otiginal'**  Par défaut, portsentry ne bloque rien et il faut le configurer afin de détecter et de bloquer le balayage de ports.  Pour commencer, il faut modifier le fichier où sont colligé les adresses IP à ne pas bloquer afin de ne pas se bloquer soi‑même.  Pour cela il existe 2 fichiers …   * **/etc/portsentry/portsentry.ignore**  et * **/etc/portsentry/portsentry.ignore.static**.   Toutes les adresses IP qui seront ajoutée dans le fichier/etc/portsentry/portsentry.ignore.static seront ajoutées dans le fichier /etc/portsentry/portsentry.ignore après un redémarrage du service portsentry.  On peut consulter le fichier /etc/portsentry/portsentry.ignore afin de vérifier que l’adresse 127.0.0.1 y est définie …  **>> sudo cat /etc/portsentry/portsentry.ignore # /etc/portsentry/portsentry.ignore: Contains all IPs portsentry(8)**  **# will never block.**  **#**  **# This file was generated by /usr/lib/portsentry/portsentry-build-ignore-file.**  **# DO NOT EDIT - edit /etc/portsentry/portsentry.ignore.static instead and use**  **# "/etc/init.d/portsentry restart" to reload the configuration.**  **# IPs from /etc/portsentry/portsentry.ignore.static:**  **127.0.0.1/32**  **0.0.0.0**  **# dynamically fetched IPs(via ifconfig -a):**  En choisissant les modes **atcp** et **audp** (a signifiant avancé) dans le fichier **/etc/defaults/portsentry**, inutile de préciser les ports, portsentry va vérifier les ports utilisés et automatiquement lier les ports disponibles.  C’est l’option la plus efficace.  Donc, avec cette option, portsentry établit une liste des ports d’écoute, TCP et UDP, et bloque l’hôte se connectant sur ces ports sauf s’il est présent dans le fichier /etc/portsentry/portsentry.ignore configuré auparavant.  **Modification du fichier** */etc/default/portsentry* …  On remplace …  **TCP\_MODE="tcp"**  **UDP\_MODE="udp"**  par  **TCP\_MODE="atcp"**  **UDP\_MODE="audp"**  À présent il faut s’attaquer au fichier de configuration principale …  /etc/portsentry/portsentry.conf  **>> sudo nano /etc/portsentry/portsentry.conf**  Mettre en place le blocage en modifiant la section **Ignore options** de la façon suivante …  **##################**  **# Ignore Options #**  **##################**  **...**  **# 0 = Do not block UDP/TCP scans.**  **# 1 = Block UDP/TCP scans.**  **# 2 = Run external command only (KILL\_RUN\_CMD)**  **BLOCK\_UDP="1"**  **BLOCK\_TCP="1"**  **Liens avec iptables**  Si iptablesest utilisé comme pare-feu, il faut commenter toutes les lignes commençant par KILL\_ROUTE sauf cette dernière qui permet de bloquer les adresses IP des hôtes pirates …  **KILL\_ROUTE="/sbin/iptables --insert INPUT --source $TARGET$ --jump DROP"**  La section **Dropping Routes** indique qu'il faut décommenter la ligne correspondant au système d’exploitation choisi et qu'une seule ligne doit être décommentée, par défaut …  **# Newer versions of Linux support the reject flag now. This**  **# is cleaner than the above option.**  **KILL\_ROUTE="/sbin/route add -host $TARGET$ reject"**  Cette commande crée une route rejetée pour l'adresse de l'attaquant.  Elle sera annulée avec …  **>> sudo route del -host 10.9.8.7 reject**  Dans la section TCP Wrappers il est préférable de conserver …  **KILL\_HOSTS\_DENY="ALL: $TARGET$ : DENY"**  qui ajoute l'adresse de l'attaquant au fichier /etc/hosts.deny.  Il est possible de l'enlever en éditant ce dernier fichier.  Dans la section **External Command**, il est suggéré d’ajouter l'une des commandes non retenues de la section Dropping Routes en la corrigeant (DEBUG → debug) …  **KILL\_RUN\_CMD="/sbin/iptables -I INPUT -s $TARGET$ -j DROP && /sbin/iptables -I INPUT -s $TARGET$ -m limit   --limit 3/minute --limit-burst 5 -j LOG --log-level debug --log-prefix 'Portsentry: dropping: '"**  Cette commande est double   * Elle ajoute une entrée dans iptables qui bannit l'attaquant.  Elle pourra être annulée par … **>> sudo iptables --delete INPUT --source 10.9.8.7 --jump DROP** * Elle ajoute aussi une entrée dans le fichier /var/log/syslog.  Le module **limit** restreint les enregistrements à 3 entrées par minutes, dans la cible **LOG**. **Limit** est un module additionnel de correspondance de paquets.  **LOG** fait partie des extensions de cibles incluses en standard. * La ligne créatrice de *iptables* sera supprimée grâce à … **>> sudo iptables --delete INPUT --source 10.9.8.7 --match limit --limit 3/minute --limit-burst 5 -j LOG   --log-level debug --log-prefix 'Portsentry: dropping:'**   On redémarre le service portsentry …  **>> sudo systemctl reload-or-restart portsentry.service**  On vérifier que portsentry a bien démarré …  **>> sudo** **tail -n 5 /var/log/syslog**  Cette dernière devrait retourner ce message les événements souvent … **Jun 3 11:33:41 debian11 portsentry[50208]: adminalert: Going into listen mode on UDP port: 32773**  **Jun 3 11:33:41 debian11 portsentry[50208]: adminalert: Going into listen mode on UDP port: 32774**  **Jun 3 11:33:41 debian11 portsentry[50208]: adminalert: Going into listen mode on UDP port: 31337**  **Jun 3 11:33:41 debian11 portsentry[50208]: adminalert: Going into listen mode on UDP port: 54321**  **Jun 3 11:33:41 debian11 portsentry[50208]: adminalert: PortSentry is now active and listening.**    **Tests**  Sur un autre hôte, la prochaine étape consiste à effectuer un balayage des ports de l’hôte précédemment configurée avec l’utilitaire nmap …  **>> sudo nmap -v <Adresse IP de la cible> >> sudo nmap -v 192.168.1.100**  Le résultat de nmap devrait ressembler à ce qui suit …  **Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-03 11:37 EDT**  **Initiating Parallel DNS resolution of 1 host. at 11:37**  **Completed Parallel DNS resolution of 1 host. at 11:37, 0.00s elapsed**  **Initiating SYN Stealth Scan at 11:37**  **Scanning debian11 (192.168.1.124) [1000 ports]**  **Discovered open port 80/tcp on 192.168.1.124**  **Discovered open port 111/tcp on 192.168.1.124**  **Discovered open port 22/tcp on 192.168.1.124**  **<…>**  **Discovered open port 1080/tcp on 192.168.1.124**  **Completed SYN Stealth Scan at 11:37, 0.01s elapsed (1000 total ports)**  **Nmap scan report for debian11 (192.168.1.124)**  **Host is up (0.0000040s latency).**  **Not shown: 983 closed ports**  **PORT STATE SERVICE**  **1/tcp open tcpmux**  **22/tcp open ssh**  **79/tcp open finger**  **80/tcp open http**  **111/tcp open rpcbind**  **<…>**  **32773/tcp open sometimes-rpc9**  **32774/tcp open sometimes-rpc11**  **Read data files from: /usr/bin/../share/nmap**  **Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds**  **Raw packets sent: 1000 (44.000KB) | Rcvd: 2017 (84.748KB)**  Il suffit d’observer à présent différents fichiers sur l’hôte hébergeant portsentry …  **>> sudo grep attackalert /var/log/syslog**  **portsentry[30084]: attackalert: TCP SYN/Normal scan from host: 192.168.x.x/192.168.x.x to TCP port: 22 portsentry[30084]: attackalert: Host: 192.168.x.x/192.168.x.x is already blocked Ignoring portsentry[18127]: attackalert: TCP SYN/Normal scan from host: 192.168.x.x/192.168.x.x to TCP port: 79**  **portsentry[18127]: attackalert: Host 192.168.x.x has been blocked via wrappers with string: "ALL: 192.168.x.x : DENY" portsentry[18127]: attackalert: Host 192.168.x.x has been blocked via dropped route using command: "/sbin/iptables -I  NPUT -s 192.168.x.x -j DROP" portsentry[18127]: attackalert: External command run for host: 192.168.x.x using command: "/sbin/iptables -I INPUT -s 192.168.x.x -j DROP &amp;&amp; /sbin/iptables -I INPUT -s 1**  **>> sudo** **cat /etc/hosts.deny**  **ALL: 192.168.1.14 : DENY**  **>> sudo** **iptables --list-rules**  --**Append INPUT --source 192.168.1.14/32 --jump DROP**  **>> sudo route**  **192.168.1.14 - 255.255.255.255 !H 0 - 0 -**  À présent l’adresse IP de l’attaquant a été détectée par portsentry et bloquée par iptables.  **Références**   * <http://www.it-connect.fr/bloquer-les-individus-qui-scannent-votre-machine-avec-portsentry/> * <https://www.isalo.org/wiki.debian-fr/Portsentry> * <https://www.deblan.io/post/455/detection-de-scan-serveur> * <http://cyrille.balland.free.fr/site-esmith/securite/portsenty.htm> * <https://www.nicolashug.com/articles/pentest-et-securite/bloquer-les-scans-de-port-avec-portsentry> * <http://www.how-to.ovh/viewtopic.php?f=25&p=439> |
|  |  |  |