

Behatolás védelem alapjai

1. Tűzfal áttekintése

- a. ssh firewall
- b. sudo -s
- c. iptables -L
- d. Ezt majd kikapcsoljuk, hogy látványosabb legyen a teszt :-)

2. Suricata

- a. Mi ez?
- b. <http://suricata-ids.org/>
- c. Az Ubuntuban régi van
 - i. apt-cache policy suricata
- d. Van saját PPA, bár nem a legjobb az ott lévő csomag, de legalább már 2.0
 - i. add-apt-repository ppa:oisf/suricata-stable
 - ii. apt-get update
 - iii. apt-cache policy suricata
 - iv. apt-get install suricata
- e. Nincs gyári indító sem :(
 - i. vi /etc/init/suricata.conf
 1. # suricata
 2. description "Intruder Detection System Daemon"
 3. start on runlevel [2345]
 4. stop on runlevel [!2345]
 5. expect fork
 6. exec suricata -D --pidfile /var/run/suricata.pid -c /etc/suricata/suricata.yaml -i eth0
- f. És hiányoznak a könyvtárak is...
 - i. mkdir /var/log/suricata
 - ii. mkdir /etc/suricata/rules
 - iii. ls -lh /etc/suricata

3. Adatbázis letöltés

- a. apt-get install oinkmaster
- b. vi /etc/oinkmaster.conf
 - i. url = <http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz>
- c. oinkmaster -C /etc/oinkmaster.conf -o /etc/suricata/rules
- d. vi /etc/suricata/suricata.yaml
 - i. classification-file: /etc/suricata/rules/classification.config
 - ii. reference-config-file: /etc/suricata/rules/reference.config

4. Finomhangolás

- a. Beállítások
 - i. vi /etc/suricata/suricata.yaml
 1. interface helyek beállítása!
 - a. eth0 a külső
 2. vars: szekció
 - a. hálózatokat ésszerűen beállítani!
 3. host-os-policy: szekció
 - a. operációs rendszerekhez igazítani!
 - b. linux: [192.168.200.0/24,
 4. libhttp: szekció
 - a. personality: IDS
 - b. server-config:
 - i. - apache
 1. address: [192.168.200.30/32]
 2. personality: Apache_2
 3. request-body-limit: 4096
 4. response-body-limit: 4096
 5. double-decode-path: no
 6. double-decode-query: no
- b. Egyes adatbázisok be- és kikapcsolása
 - i. vi /etc/oinkmaster.conf
 1. kikapcs:
 - a. disablesid: SID

2. bekapcs:
 - a. enablesid: SID

5. Adatbázis frissítés

- a. oinkmaster -C /etc/oinkmaster.conf -o /etc/suricata/rules -mq

6. Indítás

- a. Config teszt
 - i. suricata -T -c /etc/suricata/suricata.yaml
- b. suricata --list-app-layer-protos
- c. suricata --list-runmodes
 - i. NFQ / auto
- d. suricata --engine-analysis
- e. suricata -c /etc/suricata/suricata.yaml -i eth0
 - i. service suricata start
- f. másik terminálból ssh firewall
 - i. sudo -s
 - ii. ls -lh /var/log/suricata/

7. Teszt

- a. Tűzfalat kinyitjuk...
 - i. iptables -I INPUT -i eth0 -j ACCEPT
 - ii. iptables -I FORWARD -d 192.168.200.30 -j ACCEPT
 - iii. iptables -t nat -A PREROUTING -i eth0 -p tcp -j DNAT --to-destination 192.168.200.30
- b. tail -f /var/log/suricata/http.log
- c. Attacker\$
 - i. nikto -host firewall.linuxakademia.hu -Cgids /cgi-bin
 1. sok-sok riasztás...

8. Szűrési mód (NFQ)

- a. vi /etc/suricata/suricata.yaml
 - i. host-mode: auto helyett router
 - ii. nfq:
 1. mode: repeat
 2. repeat-mark: 1
 3. repeat-mask: 1
 4. route-queue: 2
 - iii.- drop: szekció (naplózzuk a drop-ot)
 1. enabled: yes
- b. iptables -I FORWARD -m mark ! --mark 1/1 -j NFQUEUE
 - i. ettől kezdve ha nem fut a Suricata NINCS átmenő forgalom!
- c. service suricata stop
- d. vi /etc/init/suricata.conf
 - i. exec suricata -D --pidfile /var/run/suricata.pid -c /etc/suricata/suricata.yaml -q 0
- e. suricata -T
- f. suricata -c /etc/suricata/suricata.yaml -q 0

9. Teszt

- a. tail -f /var/log/suricata/fast.log
- b. Attacker\$
 - i. nikto -host firewall.linuxakademia.hu -Cgids /cgi-bin
 1. megy így is, van sok riasztás

10. Blokkolás

- a. vi /etc/suricata/rules/emerging-scan.rules
 - i. /2002677
- b. vi /etc/oinkmaster.conf
 - i. alert helyett drop:
 1. modifiesid SID "alert" | "drop"
 - ii. pl:
 1. modifiesid 2002677 "alert" | "drop"
 2. modifiesid 2011390 "alert" | "drop"
- c. oinkmaster -C /etc/oinkmaster.conf -o /etc/suricata/rules -mq
- d. suricata -T
- e. suricata -c /etc/suricata/suricata.yaml -q 0

11. Teszt

- a. tail -f /var/log/suricata/fast.log

- b. Attacker\$
 - i. nikto -host firewall.linuxakademia.hu -Cgidirs /cgi-bin
 - 1. elsőre egy riasztás és megáll...
 - 2. még egyszer: már a webszerver sem ismeri fel...
- c. tail /var/log/suricata/drop.log
- d. tail -f /var/log/suricata/fast.log
- e. Attacker\$
 - i. nmap -A -T4 firewall.linuxakademia.hu

12. Frissítés automatizálása

- a. vi /etc/cron.daily/ipsupdate
 - i. #!/bin/bash
 - ii. oinkmaster -C /etc/oinkmaster.conf -o /etc/suricata/rules -mq
 - iii. service suricata restart
- b. chmod +x /etc/cron.daily/ipsupdate
- c. /etc/cron.daily/ipsupdate