به نام خدا
تمرین شماره ۲
درس امنیت شبکه پیشرفته
مدرس: محمدرضا رازیان
تدریسیار: مصطفی عبداللهی

سلام.
توجه ۱: ابتدا تمرین هر بخش را به طور کامل بخوانید و بعد به حل آن بپردازید (برخی از نکات در انتهای بخش آمده است).
توجه ۲: در پاسخ‌های تشریحی، برای بنده این مهم است که شما فهم خود را مکتوب کنید نه اینکه ترجمه کنید و یا عیناً متنی را از جایی بنویسید.
توجه ۳: گزارش حل تمرین‌ها را به زبان فارسی بنویسید.
توجه ۴: گزارش حل تمرین‌ها را زیبا، مرتب و خوانا تایپ کنید. علت این امر این است که در محیط کاری خیلی از گزارش‌های خود را به صورت گفته شده باید تحویل دهید. دوستان! واقعاً گزارش نویسی جزئی از کار سپرده شده به ما است که مثل بقیه اجزای کار باید آن را هم به خوبی انجام دهیم. در صورتی که بهترین کار را انجام دهید اما نتوانید به بهترین وجه گزارش انجام آن را ارائه دهید کار انجام شده به بهترین وجه ارزیابی نخواهد شد. نکته آخر اینکه الزاماً ما باید فقط گزارش کاری را که انجام داده‌ایم ارائه دهیم نه فراتر از کار انجام شده.
توجه ۵: گزارش حل تمرین به صورت یک فایل پی.دی.اف در سایت بارگذاری شود.
توجه ۶: کپی دهنده (کپی دهندگان) و کپی گیرنده (کپی گیرندگان) نمره ۱۰۰- خواهند گرفت (حتی در اولین بار!).
توجه ۷: مهلت انجام این تمرین جمعه ۱۶ تیرماه ساعت ۲۳:۵۹:۵۹ می باشد. به ازای هر ساعت تاخیر، از نمره کسر خواهد شد (به استثنای شرایط بسیار بسیار خاص برای دانشجوی با این شرایط).
توجه ۸: گزارش حل تمرین به صورت یک پوشه زیپ شده (Zipped) با شرایط زیر ایمیل شود.

To	en.m.abdollahy@gmail.com
CC	mrazian.email@gmail.com
نام فایل:	LastName-ns-hw-2
عنوان ایمیل:	LastName-ns-hw-2

بخش اول (۵۰ نمره)

در این بخش می‌خواهیم با نرم‌افزارهای فایروال لینوکس، iptables (بخوانید ip tables) و ufw آشنا شویم. مطمئن شوید بر روی سیستم شما نصب می‌باشند.
الف) جدول های NAT،mangle و filter برای چه منظور استفاده می‌شوند؟ (برای هر کدام ۲ الی ۳ خط توضیح کافی است)

به نام خدا
تمرین شماره ۲
درس امنیت شبکه پیشرفته
مدرس: محمدرضا رازیان
تدریسیار: مصطفی عبداللهی

ب) نحوه برخورد با ترافیک ورودی (action) چگونه است؟ در حالت log، اطلاعات بر روی سیستم شما در کجا (کدام مسیر) ثبت می‌شوند؟ چگونه می‌توان Prefix مربوط به log را تغییر داد؟

ج) پارامترهای F- و D- برای چیست؟

د) با چه دستوری در iptables اجازه ping از سیستم شما بسته می‌شود (یعنی سیستم شما نتواند ping کند)؟ (تصویر خروجی iptables -L و ping آورده شود) –برای این بخش یا دو رایانه را شبکه کنید و یا یک VM و سیستم خود را شبکه کنید. قسمت Host ID باید شماره دانشجویی شما و به اضافه یک آن باشد. (مثال: شماره دانشجویی 95112233 آی.پی دو سیستمی که شبکه شده‌اند: 192.168.1.33 و 192.168.1.34)

ه) با چه دستوری در iptables اجازه ping سیستم شما بسته می‌شود (یعنی کسی نتواند سیستم شما را ping کند اما شما بتوانید)؟ (تصویر خروجی iptables -L و ping آورده شود) –برای این بخش یا دو رایانه را شبکه کنید و یا یک VM و سیستم خود را شبکه کنید. قسمت Host ID باید شماره دانشجویی شما و به اضافه یک آن باشد. (مثال: شماره دانشجویی 95112233 آی.پی دو سیستمی که شبکه شده‌اند: 192.168.1.33 و 192.168.1.34)

و) دستور زیر چه کاری را انجام می‌دهد؟

```
iptables -A INPUT -p tcp –dport 80 -s 192.168.1.10 -m time –timestart 07:30 –timestop
14:00 –days Sat,Sun,Mon,Tue,Wed,Thu -j ACCEPT
```

ز) تفاوت ufw و iptables در چیست؟

ح) تصور کنید می‌خواهید با استفاده از ufw، یک دیوار آتش برای یک Mailserver را پیکربندی کنید. چه دستورهایی نیاز است تا تنها بسته‌های SMTP، IMAP وPOP3 از تمام IPها و بسته‌های SSH تنها از IP یک سیستم مشخص (مثلا: 151.241.133.41) به داخل سرور اجازه ورود و خروج را داشته‌باشند؟ چگونه می‌توان این دستورها را غیر فعال کرد؟

ط) خط مشی‌های باز و بسته (Accept base و Deny base) در فایروال (به طور کلی در سیستم‌های کنترل دسترسی) به چه معناست؟

بخش دوم (۵۰ نمره)

به نام خدا
تمرین شماره ۲
درس امنیت شبکه پیشرفته
مدرس: محمدرضا رازیان
تدریسیار: مصطفی عبداللهی

در این بخش با سیستم تشخیص نفوذ snort آشنا خواهید شد.
الف) سیستم تشخیص نفوذ (Intrusion Detection System = IDS) چیست؟ اینکه سیستم تشخیص نفوذ snort مبتنی بر شبکه (NIDS) است به چه معناست؟

ب) آن را در سیستم عامل لینوکس خود نصب کنید (دور راه برای نصب آن وجود دارد: ۱ - از طریق Source آن ۲ - با استفاده از apt-get)

apt-get install snort

و می‌توانید فایل پیکربندی آن را ویرایش کنید (etc/snort/snort.conf). (مواردی مثل HOME NET, Interface و غیره) برای مثال بگویید HOME_NET (آدرس شبکه) شما چیست.

از موارد دیگری که در فایل config می‌توانید تغییر دهید آدرس قوانین (rule) نرم‌افزار snort است (یعنی بگویید قوانین کجا ذخیره شده‌اند). نرم‌افزار snort با توجه به این قوانین تصمیم می‌گیرد که یک ترافیک نرمال است یا حمله.
به مسیر

/etc/snort/rules

بروید. در اینجا قواعد مربوط به حملات مختلف وجود دارند.

```
attack-responses.rules          community-nntp.rules          deleted.rules          netbios.rules          sql.rules
backdoor.rules                  community-oracle.rules        dns.rules              nntp.rules             telnet.rules
bad-traffic.rules               community-policy.rules        dos.rules              oracle.rules           tftp.rules
chat.rules                      community-sip.rules           experimental.rules     other-ids.rules        virus.rules
community-bot.rules             community-smtp.rules          exploit.rules          p2p.rules              web-attacks.rules
community-deleted.rules         community-sql-injection.rules finger.rules           policy.rules           web-cgi.rules
community-dos.rules             community-virus.rules         ftp.rules              pop2.rules             web-client.rules
community-exploit.rules         community-web-attacks.rules   icmp-info.rules        pop3.rules             web-coldfusion.rules
community-ftp.rules             community-web-cgi.rules       icmp.rules             porn.rules             web-frontpage.rules
community-game.rules            community-web-client.rules    imap.rules             rpc.rules              web-iis.rules
community-icmp.rules            community-web-dos.rules       info.rules             rservices.rules        web-misc.rules
community-imap.rules            community-web-iis.rules       local.rules            scan.rules             web-php.rules
community-inappropriate.rules   community-web-misc.rules      misc.rules             shellcode.rules        x11.rules
community-mail-client.rules     community-web-php.rules       multimedia.rules       smtp.rules
community-misc.rules            ddos.rules                    mysql.rules            snmp.rules
```

به عنوان مثال یکی از قواعد موجود در فایل dos.rules را مشاهده می‌کنیم (less /dos.rules).

```
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS Jolt attack"; dsize:408; fragbits:M; reference:cve,1999-0345; classtype:attempted-dos; sid:
268; rev:4;)
```

ج) بخش‌های مختلف قالب قواعد snort را توضیح دهید (بگویید هر یک از بخش‌ها به چه معناست و هر بخش چه حالت‌هایی می‌تواند داشته باشد). توضیحات کامل مدنظر است.

به نام خدا
تمرین شماره ۲
درس امنیت شبکه پیشرفته
مدرس: محمدرضا رازیان
تدریسیار: مصطفی عبداللهی

snort را اجرا کنید

/etc/init.d/snort start

با استفاده از دستور زیر از اجرای snort مطمئن شوید (تصویر خروجی دستور زیر در گزارش آورده شود).

ps auxw | grep snort

snort دو نوع log file تولید می‌کند: Alert log file و Snort log file.

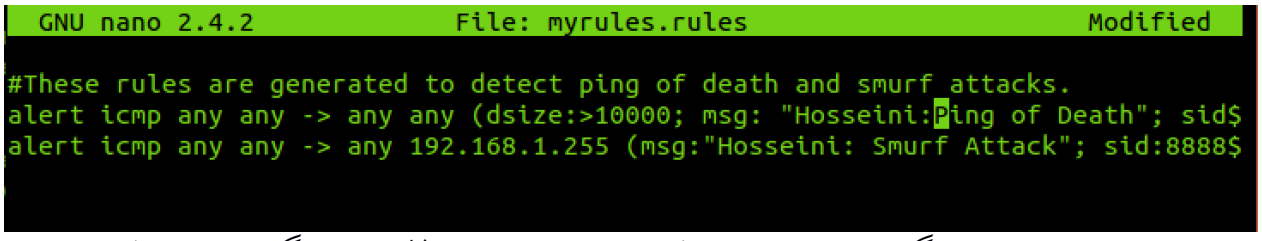
- Alert log file برای ثبت نفوذهایی که توسط موتور تشخیص، شناسایی شده است استفاده می‌شود (موتور تشخیص هم با توجه به قواعدی که در مجموعه قواعد تعریف شده است عمل می‌کند).
- Snort log file جایی است که تمام بسته‌ها (packets activities) در آن ثبت می‌شود.

د) اگر بخواهیم یک مجموعه قوانین را به snort اضافه کنیم و آن‌ها را در فایلی به نام myrules.rules قرار دهیم باید چه تغییری در فایل snort.conf ایجاد کنیم؟ تصویری از نحوه انجام این کار را در گزارش قرار دهید.

ه) دو حمله‌ای که در شبکه‌های رایانه‌ای انجام می‌شوند حمله‌های Smurf Attack و Ping Of Death هستند. این دو حمله را در چند خط توضیح دهید.

می‌خواهیم قوانینی را به snort اضافه کنیم تا در صورت بروز این حملات، هشدار صادر شود. دستورات زیر را در فایل myrules.rules وارد کنید:

```
alert icmp any any -> any any (dsize:>10000; msg: "Hosseini: Ping of Death ";
sid:777777;)
alert icmp any any -> any 192.168.1.255 (msg:"Hosseini: Smurf Attack "; sid:888888;)
```



به جای Hosseini، نام خانوادگی خود را قرار دهید (تصویری مانند تصویر بالا را هم در گزارش بیاورید).

برای وارد کردن دستورات به فایل مورد نظر می‌توانید از دستور زیر در ترمینال استفاده نمایید:

```
# sudo nano /etc/snort/rules/myrules.rules
```

و) حال با استفاده از دستور زیر، snort را اجرا می‌کنیم. این دستور به چه معناست؟

به نام خدا
تمرین شماره ۲
درس امنیت شبکه پیشرفته
مدرس: محمدرضا رازیان
تدریسیار: مصطفی عبداللهی

snort -dev -i wlan0 -c /etc/snort/snort.conf -l /var/log/snort/ -A full
(توجه: بجای wlan0، نام واسط خود را قرار دهید، می توانید از دستور ifconfig کمک بگیرید)

ز) ابتدا از روی سیستمی که IDS بر روی آن قرار دارد به مقصد دلخواه و یا از یک سیستمی که با IDS در یک شبکه قرار گرفته است به مقصد IDS ۵ بسته Ping با اندازه 50000 تولید کنید:
#sudo ping –s 50000 –c 5 DESTINATION_IP_ADDRESS
تصویری از نحوه Ping کردن در گزارش قرار بدهید.
حال به مسیر زیر بروید. از خروجی دستور زیر (که حاوی نام خانوادگی شما است عکس بگیرید و در گزارش بیاورید)

cd /var/log/snort/
cat alert | grep -i Death

ح) از روی سیستمی که IDS بر روی آن قرار دارد و یا از یک سیستمی که با IDS در یک شبکه قرار گرفته است آدرس همه‌پخشی را ۵بار Ping کنید:

#sudo ping –c 5 –b 192.168.1.255
تصویری از نحوه ping کردن خود قرار دهید.
حال به مسیر زیر بروید. از خروجی دستور زیر (که حاوی نام خانوادگی شما است عکس بگیرید و در گزارش بیاورید)

cd /var/log/snort/
cat alert | grep -i Smurf

ط) قانون زیر بیانگر چه چیزی است؟ (به طور دقیق توضیح دهید)
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 (content: "|00 01 86 a5|"; msg: "external mountd access";)

بخش سوم (۳۰ نمره)

انجام این بخش اختیاری است و نمره اضافه دارد

در این بخش با سیستم تشخیص نفوذ ossec آشنا خواهید شد.
الف) اینکه OSSEC یک سیستم تشخیص نفوذ مبتنی بر میزبان (HIDS) است، به چه معنی است؟ این نرم‌افزار چه تفاوتی با Snort دارد؟

به نام خدا
تمرین شماره ۲
درس امنیت شبکه پیشرفته
مدرس: محمدرضا رازیان
تدریسیار: مصطفی عبداللهی

نرم‌افزار OSSEC را بر روی سیستم خود نصب کنید. (می‌توانید از راهنمای نصب آن بر روی اینترنت استفاده کنید)
در حین نصب از شما سوالی مبتنی بر نوع نصب پرسیده می‌شود، از میان گزینه‌های موجود local را انتخاب نمایید.
همچنین در قسمت مربوط به email دستور no را وارد کنید.(در این تمرین نیازی به اخطار توسط ایمیل نیست)
فایل پیکربندی این نرم‌افزار در آدرس زیر قرار گرفته است:

/var/ossec/etc/ossec.conf

این فایل را باز کنید و قسمت زیر را بیابید:

```
<syscheck>
  <!-- Frequency that syscheck is executed - default to every 22 hours -->
 <frequency>79200</frequency>
```

این قسمت مربوط به دوره بررسی سامانه برای تغییرات در درستی فایل‌ها می‌باشد که به صورت پیش‌فرض روی ۲۲ ساعت (بر اساس ثانیه) تنظیم شده است. می‌توانید آن را به مقدار دلخواه تغییر دهید. (مثلا ۶۰ ثانیه)
بلافاصله پس از این بخش قسمت زیر را مشاهده می‌کنید:

```
<!-- Directories to check  (perform all possible verifications) -->
<directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
<directories check_all="yes">/bin,/sbin</directories>
```

این بخش مشخص کننده فولدرهایی است که در هر دوره تحت بررسی قرار می‌گیرند. این بخش را به صورت زیر تغییر دهید تا تغییرات به صورت بلادرنگ هشدار داده شوند:

```
<!-- Directories to check  (perform all possible verifications) -->
<directories report_changes="yes" realtime="yes" check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
<directories report_changes="yes" realtime="yes" check_all="yes">/bin,/sbin</directories>
```

برای اضافه کردن فولدرهای جدید به بررسی می‌توانید دستور زیر را اضافه کنید:

```
<directories report_changes="yes" realtime="yes" restrict=".php|.js|.py|.sh|.html"
check_all="yes">/home/arshiahsn </directories>
```

بجای arshiahsn نام کاربری خود را قرار بدهید.
فولدر مربوط به ruleهای این نرم‌افزار در آدرس زیر قرار گرفته است:

```
apache_rules.xml          ms-exchange_rules.xml   solaris_bsm_rules.xml
arpwatch_rules.xml        ms_ftpd_rules.xml       sonicwall_rules.xml
asterisk_rules.xml        ms-se_rules.xml         spamd_rules.xml
attack_rules.xml          mysql_rules.xml         squid_rules.xml
cimserver_rules.xml       named_rules.xml         sshd_rules.xml
cisco-ios_rules.xml       netscreenfw_rules.xml   symantec-av_rules.xml
clam_av_rules.xml         nginx_rules.xml         symantec-ws_rules.xml
courier_rules.xml         openbsd_rules.xml       syslog_rules.xml
dovecot_rules.xml         ossec_rules.xml         telnetd_rules.xml
dropbear_rules.xml        pam_rules.xml           translated
firewall_rules.xml        php_rules.xml           trend-osce_rules.xml
ftpd_rules.xml            pix_rules.xml           vmpop3d_rules.xml
hordeimp_rules.xml        policy_rules.xml        vmware_rules.xml
ids_rules.xml             postfix_rules.xml       vpn_concentrator_rules.xml
imapd_rules.xml           postgresql_rules.xml    vpopmail_rules.xml
local_rules.xml           proftpd_rules.xml       vsftpd_rules.xml
local_rules.xml.00        pure-ftpd_rules.xml     web_appsec_rules.xml
log-entries               racoon_rules.xml        web_rules.xml
mailscanner_rules.xml     roundcube_rules.xml     wordpress_rules.xml
mcafee_av_rules.xml       rules_config.xml        zeus_rules.xml
msauth_rules.xml          sendmail_rules.xml
ms_dhcp_rules.xml         smbd_rules.xml
```

/var/ossec/rules

به نام خدا
تمرین شماره ۲
درس امنیت شبکه پیشرفته
مدرس: محمدرضا رازیان
تدریسیار: مصطفی عبداللهی

قانون‌هایی که توسط شما نوشته می‌شوند در فایل /var/ossec/rules/local_rules.xml در میان تگ <group></group> قرار می‌گیرند. قانون زیر را به این فایل اضافه کنید تا تغییرات بر روی فولدرها را به صورت هشدار اطلاع دهد، بجای Hosseini نام خانوادگی خود را قرار دهید:

```
<rule id="554" level="7" overwrite="yes">
<category>ossec</category>
<decoded_as>syscheck_new_entry</decoded_as>
<description>Hosseini:File added to the system.</description>
<group>syscheck,</group>
</rule>
```

با استفاده از دستور زیر نرم‌افزار را ریستارت کنید:

```
/var/ossec/bin/ossec-control restart
```

اکنون یک فایل جدید در فولدر کاربری خود ایجاد کنید:

```
touch /home/arshiahsn/arshiahsn.html
```

منتظر بمانید تا اخطاری همانند زیر در آدرس زیر دریافت کنید، تصویری از این هشدار را در گزارش خود بیاورید:
(می‌توانید از دستور tail –f برای بررسی لحظه به لحظه استفاده کنید)
(توجه داشته باشید که OSSEC برای کاهش مصرف منابع سیستم، روند بررسی را به کندی پیش می‌برد، بنابراین فرآیند زیر ممکن است کمی طولانی شود)

آدرس: /var/ossec/logs/alerts/alerts.log

```
OSSEC HIDS Notification.
2016 Nov 10 08:15:20

Received From: ossec2->syscheck
Rule: 554 fired (level 7) -> "Hosseini:File added to the system."
Portion of the log(s):

New file '/home/arshiahsn/arshiahsn.html' added to the file system.
```

ب) حمله Dictionary Attack چه حمله‌ای است؟ چه نرم‌افزارهایی برای انجام این حمله وجود دارد؟
ج) نرم‌افزار Ncrack را بر روی یک سیستم نصب کنید. فایل worst-passwords-۵۰۰.txt را دریافت کنید و با استفاده از محتوی آن یک حمله Dictionary را بر روی سیستمی که OSSEC بر روی آن قرار دارد ترتیب دهید.
د) دستوری که از آن برای انجام حمله استفاده کردید را در گزارش خود بیاورید و در مورد بخش‌های آن توضیح دهید. سامانه OSSEC چگونه در برابر این حمله واکنش نشان می‌دهد؟ تصویری از هشدارهای مربوطه را از فایل‌های زیر در

به نام خدا
تمرین شماره ۲
درس امنیت شبکه پیشرفته
مدرس: محمدرضا رازیان
تدریسیار: مصطفی عبداللهی

گزارش خود بیاورید و توضیح دهید:

/var/ossec/logs/alerts/alerts.log
/var/ossec/logs/active-responses.logs

موفـق بـاشید