Защита веб-приложений от современных хакерских атак

Романов Роман, Pentestit
rr@pentestit.ru

Pentestit

информационная безопасность

Услуги и решения

- Аудит безопасности и расследование кибер-преступлений;
- Web Application Firewall, Security Operation Center;
- Программы профессиональной подготовки.

Некоммерческая деятельность

- Лаборатории тестирования на проникновении «Test lab»;
- Тематический ИБ-блог - Defcon.ru.

Триада ИБ

Доступность

Конфиденциальность

Целостность

Компоненты

Linux

iptables

Nginx + WAF

OSSEC + Fail2ban +SIEM

Доступность (Dos\DDoS)

Атаки на ОС

Атаки на канал

Атаки на веб-приложение

Intel(R) Xeon(R) … / ~ 16 GB

```
## Kernel panic reboot
kernel.panic = 10

## Memory optimization
kernel.shmmax = 8380211200
kernel.shmall = 2045950

## MSG limits
kernel.msgmnb = 65536
kernel.msgmax = 65536

## Swap
vm.swappiness=10
vm.dirty_ratio = 40
vm.dirty_background_ratio = 5

## Too many open files fix
fs.file-max = 2097152

## Net optimization
net.core.somaxconn = 65535

net.netfilter.nf_conntrack_max = 10000000
net.netfilter.nf_conntrack_tcp_loose = 0
net.netfilter.nf_conntrack_tcp_timeout_established = 1800
net.netfilter.nf_conntrack_tcp_timeout_close = 10
net.netfilter.nf_conntrack_tcp_timeout_close_wait = 10
net.netfilter.nf_conntrack_tcp_timeout_fin_wait = 20
net.netfilter.nf_conntrack_tcp_timeout_last_ack = 20
net.netfilter.nf_conntrack_tcp_timeout_syn_recv = 20
net.netfilter.nf_conntrack_tcp_timeout_syn_sent = 20
net.netfilter.nf_conntrack_tcp_timeout_time_wait = 10

net.ipv4.tcp_congestion_control = hybla

net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.ip_local_port_range = 1024 65000
net.ipv4.ip_no_pmtu_disc = 1
net.ipv4.route.flush = 1
net.ipv4.route.max_size = 8048576
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.tcp_mem = 65536 131072 262144
net.ipv4.udp_mem = 65536 131072 262144

net.ipv4.tcp_rmem = 4096 87380 33554432
net.ipv4.udp_rmem_min = 16384

net.ipv4.tcp_wmem = 4096 87380 33554432
net.ipv4.udp_wmem_min = 16384
net.ipv4.tcp_max_tw_buckets = 1440000
net.ipv4.tcp_tw_recycle = 0
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_max_orphans = 400000
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_rfc1337 = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_synack_retries = 1
net.ipv4.tcp_syn_retries = 2
net.ipv4.tcp_max_syn_backlog = 16384
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
net.ipv4.tcp_fack = 1
net.ipv4.tcp_ecn = 2
net.ipv4.tcp_fin_timeout = 10
net.ipv4.tcp_keepalive_time = 600
net.ipv4.tcp_keepalive_intvl = 60
net.ipv4.tcp_keepalive_probes = 10
net.ipv4.tcp_no_metrics_save = 1

net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.rp_filter = 1
```

iptables

-A INPUT -i eth0 -p tcp –syn -m multiport --dports 80,443 -m connlimit --connlimit-above 25 --connlimit-mask 32 -j DROP

-A INPUT -i eth0 -p tcp -m multiport –dports 80,443 -j ACCEPT

Целостность\Конфиденциальность

Атаки на ОС

Атаки на канал

Атаки на веб-приложение

https://defcon.ru/?s='+or+1%3D1+--

403

ПОДОЗРИТЕЛЬНАЯ АКТИВНОСТЬ
ДОСТУП ЗАПРЕЩЕН

Мы обнаружили подозрительную активность и заблокировали доступ к сайту. Попробуйте воспользоваться другим бразуером. Если вы считаете, что блокировка ошибочная, сообщите, пожалуйста, на почту info@pentestit.ru, указав ваш IP-адрес.

Inspector | Console | Debugger | Style Editor | Perform... | Network

✓	Method	File	Domain	Type	Transferred	Size	0 ms
	POST	29846554?rn=982349265&page-url=https://defcon.ru/&w...	mc.yandex.ru	plain	—	0 KB	→ 0 ms
	POST	29846554?rn=261863254&page-url=https://defcon.ru/&w...	mc.yandex.ru	plain	—	0 KB	→ 0 ms
403	GET	/?s='+or+1=1+--	defcon.ru	html	1,04 KB	0 KB	→ 170 ms
	GET	/?s='+or+1=1+--	defcon.ru				
200	GET	29846554?rn=982349265&page-url=https://defcon.ru/...	mc.yandex.ru	gif	0,04 KB	0 KB	→ 721 ms
200	GET	29846554?rn=261863254&page-url=https://defcon.ru/...	mc.yandex.ru	gif	0,04 KB	0 KB	→ 495 ms
200	GET	css?family=Lato:100	fonts.googleapis.com	css	0,31 KB	0 KB	→ 134 ms
200	GET	shark403.png	defcon.ru	png	108,77 KB	0 KB	→ 878 ms
200	GET	GtRkRNTnri0g82CjKnEB0Q.woff2	fonts.gstatic.com	woff2	cached	0 KB	

New Request Send Cancel

GET https://defcon.ru/?s=%27+or+1%3D1+--

Query String:

s='+or+1=1+--

Request Headers:

Host: defcon.ru
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:45.0) Gecko/201001(
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://defcon.ru/
Cookie: PHPSESSID=5jv88296kgp6kl2dh8rie2nvg0; _ym_uid=146047266388
Connection: keep-alive

Request Body:

All | HTML | CSS | JS | XHR | Fonts | Images | Media | Flash | Other

8 requests, 0 KB, 0,42 s Clear

Атаки со смежных\доверенных узлов

DMZ (pivoting)

Shared hosting

Эмуляция атак и сбор данных

Создавайте копии для тестов

Собирайте информацию об атаках

Анализируйте данные

$logs =~ /собрать (,нельзя|нельзя,) распарсить/

Не хватает правил «из коробки»?*

Как минимизировать количество событий, при этом не пропустив важные?

Как быть?

Контроль

Утро начинается с SIEM

Оперативное информирование о подозрительной активности (SMS, Telegram, E-mail)

Prewikka company ltd. **Prelude console**

Alerts | CorrelationAlerts | ToolAlerts — admin on monday 13 june 2016 — logout

- Events
- Agents
- Statistics
- Settings
- About

3 x Login session opened. (succeeded)		
6 x Nginx: limiting requests. (succeeded)	31.171.	13:54:59
10 x Nginx: limiting requests. (succeeded)	176.19	13:54:59
2 x Nginx: limiting requests. (succeeded)	46.242.	13:54:55
5 x Nginx: limiting requests. (succeeded)	91.78.2	13:54:55
[redacted] Request blocked. (succeeded) 1 x Nginx error message. (succeeded)	66.249.	13:49:12
[redacted] Request blocked. (succeeded) 6 x Nginx error message. (succeeded)	66.249.	13:36:35 - 2016-06-12 05:49:24
[redacted]	109.188	13:19:52 - 13:19:32
7 x Web server 500 error code (Internal Error). (succeeded)	46.188.	13:07:08 - 2016-06-12 13:05:36
[redacted] Request blocked. (succeeded) 1 x Nginx error message. (succeeded)	157.55.	12:37:11
Attempt to use mail server as relay (client host rejected). (succeeded) (vendor-specific:Rule:3301, vendor-specific:Group:syslog, vendor-specific:Group:postfix, vendor-specific:Group:spam)	93.35.6	12:31:38
[redacted] (succeeded) 3 x Nginx error message. (succeeded)	95.24.1	12:30:15
[redacted] (succeeded) 3 x Nginx error message. (succeeded)	37.110.	12:30:08
[redacted] (succeeded) 3 x Nginx error message. (succeeded)	109.173	12:29:57
[redacted] (succeeded) 3 x Nginx error message. (succeeded)	176.77.	12:29:55
2 x SQL injection attempt. (succeeded)	195.154	12:20:29 - 12:20:27
[redacted] Request blocked. (succeeded) 1 x Nginx error message. (succeeded)	195.154	12:20:29
Nginx error message. (succeeded) (vendor-specific:Rule:31301, vendor-specific:Group:apache)	185.93.	12:13:28
6 x Receipent address must contain FQDN (504: Command parameter not implemented). (succeeded)	195.209	11:59:36 - 2016-06-12 11:56:12
[redacted] Request blocked. (succeeded) 4 x Nginx error message. (succeeded)	157.55.	11:21:32 - 01:33:34
Web server 400 error code. (succeeded) (vendor-specific:Rule:31101, vendor-specific:Group:web, vendor-specific:Group:accesslog)	91.109.	10:48:24
3 x Receipent address must contain FQDN (504: Command parameter not implemented). (succeeded)	111.249	10:30:09
1 x Fail2ban Unban (succeeded) 1 x Fail2ban Ban (succeeded) 1 x Fail2ban: host already banned (succeeded) 13 x Web server 400 error code. (succeeded)	67.81.2	10:23:32 - 2016-06-12 07:59:27
Receipent address must contain FQDN (504: Command parameter not implemented). (succeeded) (vendor-specific:Rule:3305, vendor-specific:Group:syslog, vendor-specific:Group:postfix, vendor-specific:Group:spam)	114.37.	09:56:25
Receipent address must contain FQDN (504: Command parameter not implemented). (succeeded) (vendor-specific:Rule:3305, vendor-specific:Group:syslog, vendor-specific:Group:postfix, vendor-specific:Group:spam)	118.160	09:18:39
[redacted]	91.200.	08:58:18 - 2016-06-11 17:20:38

Filter
Period 48 Hours
Timezone Frontend localtime
Limit 1000 By time (desc
Refresh 0:00 1:00

Apply Save

2016-06-11 14:10:53
2016-06-13 14:10:53
+03:00

prev current next

<< < > >>

1 ... 141 (total:141)

DATA SAFETY
HYBRID SIEM SYSTEM

CYBERATTACK WORLD MAP

location	port
Kiev , UA	443
Frankfurt, DE	1935
Moscow, RU	1935
Moscow, RU	1935
Odesa, UA	443
Moscow, RU	1935
Moscow, RU	1935
Odesa, UA	443
Moscow, RU	1935
Frankfurt, DE	1935

CYBERATTACK ACTIVITY

PENTESTIT
PENETRATION TESTING LABORATORIES

9378 REGISTERED

56 ONLINE

HOW TO CONNECT

SIGN IN

CYBERATTACK WORLD MAP

location	port
Sodra Forstaden, SE	16810
Krasnodar, RU	80
Moscow, RU	17650
Los Angeles, US	9159
Saint Petersburg, RU	80
Moscow, RU	3330
Krasnodar, RU	80
Ashburn, US	4207
San Francisco, US	17075

CYBERATTACK ACTIVITY

Стандарты безопасности (PCI DSS etc)

Что не разрешено – то запрещено

Установка обновлений

Периодический аудит безопасности

Анализ исходного кода

Web Application Firewall

Технические подробности

Обеспечение безопасности сайта
https://defcon.ru/web-security/22/

Обеспечение безопасности сетевого периметра с использованием Snort, OSSEC и Prelude SIEM
https://defcon.ru/network-security/484/

Защита сайта от DDoS-атак средствами iptables и nginx

https://defcon.ru/web-security/2860/

Лаборатории тестирования на проникновение «Test lab»

https://lab.pentestit.ru

PENTESTIT

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

info@pentestit.ru