A09:2021 - Журнал безопасности и сбои мониторинга

Недостаточное ведение журнала и мониторинг это уязвимость, возникающая, когда приложение или система неадекватно записывает и отслеживает события, что

- затрудняет обнаружение инцидентов безопасности
- реагирование на них

Это может позволить злоумышленникам проводить атаки, оставаясь незамеченными, а также может помешать усилиям по реагированию на инциденты.

Описание

Без регистрации и мониторинга невозможно обнаружить нарушения. Недостаточное ведение журнала, обнаружение, мониторинг и активное реагирование возникают в любое время:

- Проверяемые события, такие как входы в систему, неудачные входы в систему и транзакции с высокой стоимостью, не регистрируются.
- Предупреждения и ошибки приводят к отсутствию, неадекватности или неясности сообщений журнала.
- Журналы приложений и API не отслеживаются на предмет подозрительной активности.
- Журналы хранятся только в определенном месте.

Недостаточное ведение журнала и мониторинг уязвимостей подвиды уязвимостей

- Утечки данных
- Несанкционированный доступ
- Вредоносные действия
- Нарушения соответствия требованиям

Недостаточное ведение журнала и мониторинг Примеры эксплуатации

Кража данных: Злоумышленники могут использовать недостаточное ведение журнала и мониторинг для кражи конфиденциальной информации, такой как учетные данные для входа, личные данные и финансовая информация, из систем, не будучи обнаруженными.

Недостаточное ведение журнала и мониторинг Примеры эксплуатации

Вредоносные атаки: Злоумышленники могут использовать вредоносное ПО для использования уязвимостей, связанных с недостаточным ведением журнала и мониторингом, для получения доступа к системам и осуществления вредоносных действий, таких как кража данных, проведение DDoS-атак и распространение спама.

Недостаточное ведение журнала и мониторинг Примеры эксплуатации

Отказ в обслуживании: Злоумышленники могут использовать недостаточное ведение журнала и мониторинг для проведения атак типа "отказ в обслуживании", которые перегружают систему и приводят к ее сбою или отказу отвечать на запросы.

Методы повышения привилегий при недостаточном ведении журнала и мониторинге уязвимые места

- Использование "слепых зон" (CWE-778)
- Внесение ложной информации в журналы (CWE-527)
- Использование административных привилегий и раскрытие данных журналов (CWE-532)

Dashboard
Search
Ongoing Labs 0
Latest Additions
Community Labs

EARN CREDENTIALS
Verifiable Badges

WINDOWS SECURITY
Reconnaissance
Basic Exploitation
Post Exploitation
Service Exploitation
Privilege Escalation
Maintaining Access

CLOUD SECURITY
AWS Cloud Security
Bootcamp

LINUX SECURITY
Linux Basics
Reconnaissance
Exploitation
Post Exploitation
Privilege Escalation
Pivoting
Maintaining Access

Log Anomaly Detection Basics

log-analysis-webserver-logs | Level: Easy | Total Lab Runs: 0 | Premium Lab |

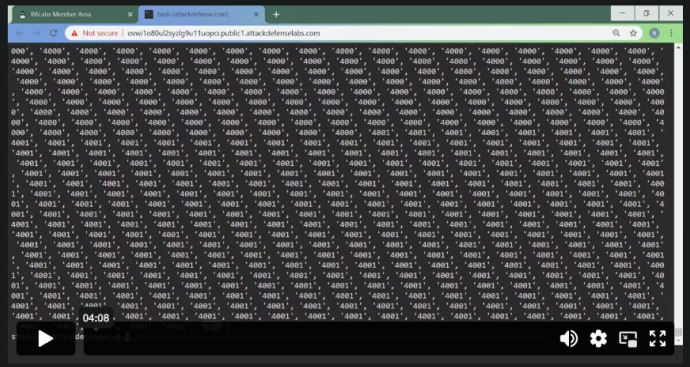
Subscribe to Run Lab | Subscriber? Login Here

Lab Scoreboard

# Played on AD	# Played by you	Mark Complete

Mission | Prohibited Activities | Technical Support

Lab Walkthrough Video:



Download Lab Manual

An already parsed web access log file **logs.txt** is provided. The log file contains more than 1 million logs that follow a pattern/ruleset. However, in addition to real logs, there are 5 anomalous log entries in the file.

You have to identify the ruleset/pattern and then use it to find the 5 anomalous log entries.

The motive of the exercise is to help you learn to spot anomalies in logs.

Also, Python2 and Python3 are present in the lab system.

```
GET http://example.net/access_object.php?param1=2262&param2=brachy&param3=13MAR2012
CONNECT http://example.net/access_object.php?param1=2543&param2=brachi&param3=01JUN2010
CONNECT http://example.net/access_object.php?param1=3252&param2=brachi&param3=25AUG2018
HEAD http://example.net/access_object.php?param1=3607&param2=brachi&param3=18MAR2011
POST http://example.net/access_object.php?param1=2952&param2=brachi&param3=21NOV2015
TRACE http://example.net/access_object.php?param1=1804&param2=brachy&param3=15JUL2016
DELETE http://example.net/access_object.php?param1=1377&param2=brachy&param3=06APR2010
HEAD http://example.net/access_object.php?param1=1094&param2=brachi&param3=15SEP2011
OPTIONS http://example.net/access_object.php?param1=2330&param2=brachy&param3=27APR2018
CONNECT http://example.net/access_object.php?param1=3791&param2=bracht&param3=26FEB2011
DELETE http://example.net/access_object.php?param1=2719&param2=brachy&param3=06JUN2017
PUT http://example.net/access_object.php?param1=2023&param2=brachy&param3=20OCT2018
TRACE http://example.net/access_object.php?param1=3275&param2=brachi&param3=14OCT2016
OPTIONS http://example.net/access_object.php?param1=3594&param2=brachy&param3=22JUN2013
TRACE http://example.net/access_object.php?param1=3287&param2=brachy&param3=19FEB2012
POST http://example.net/access_object.php?param1=1167&param2=brachy&param3=22JUL2013
POST http://example.net/access_object.php?param1=2830&param2=brachy&param3=27OCT2015
OPTIONS http://example.net/access_object.php?param1=2645&param2=brachi&param3=02JUL2011
HEAD http://example.net/access_object.php?param1=3382&param2=brachs&param3=19JUN2019
PUT http://example.net/access_object.php?param1=3095&param2=brachy&param3=17NOV2015
POST http://example.net/access_object.php?param1=1503&param2=brachy&param3=15APR2013
CONNECT http://example.net/access_object.php?param1=1859&param2=brachy&param3=05JAN2012
OPTIONS http://example.net/access_object.php?param1=1530&param2=brachy&param3=12MAY2015
POST http://example.net/access_object.php?param1=1008&param2=brachy&param3=21NOV2012
PUT http://example.net/access_object.php?param1=2643&param2=brachy&param3=26NOV2010
POST http://example.net/access_object.php?param1=3633&param2=brachy&param3=02JUN2018
POST http://example.net/access_object.php?param1=2086&param2=brachi&param3=15JAN2011
POST http://example.net/access_object.php?param1=1974&param2=brachi&param3=15MAY2010
"logs.txt" [readonly] 1000005L, 85875399C
```

```
Anomalous entry:  crachy
set(['HEAD', 'TRACE', 'GET', 'HEADER', 'CONNECT', 'PUT', 'POST', 'OPTIONS', 'DELETE'])
set(['07', '02', '25', '26', '01', '20', '21', '22', '05', '08', '09', '28', '24', '03', '27', '06', '14', '11', '10', '13', '12', '15', '04',
'17', '16', '19', '18', '23', '33'])
set(['MAR', 'FEB', 'AUG', 'SEP', 'APR', 'XYZ', 'JUN', 'JUL', 'JAN', 'MAY', 'NOV', 'DEC', 'OCT'])
set(['2020', '2019', '2018', '2015', '2014', '2017', '2016', '2011', '2010', '2013', '2012'])
```

```
root@ubuntu-zukov-host:~/page_test# cat app_failtures_no_logging.py
import logging
from flask import Flask, render_template, request

app = Flask(__name__,template_folder='templates')
logging.basicConfig(filename='auth.log', level=logging.INFO)

@app.route('/')
def index():
    return render_template('login.html')

@app.route('/login', methods=['POST'])
def login():
    username = request.form['username']
    password = request.form['password']
    if password == 'mypassword':
        logging.info(f'{username} logged in successfully')
        return f'Welcome, {username}!'
    else:
        return 'Invalid password'

if __name__ == '__main__':
    app.run(host="167.99.243.187", port=8090, debug=True)
```

```
root@ubuntu-zukov-host:~/page_test# tail -f auth.log
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:38] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:38] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:39] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:39] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:39] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:39] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:39] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:39] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:40] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:40] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:56] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:57] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:57] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:57] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:57] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:57] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:58] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:58] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:58] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:58] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:58] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:59] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:59] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:59] "POST /login HTTP/1.1" 200 -
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:14:59] "POST /login HTTP/1.1" 200 -
```

POST http://167.99.243.187:8090/login

200 OK 134 ms 16 B

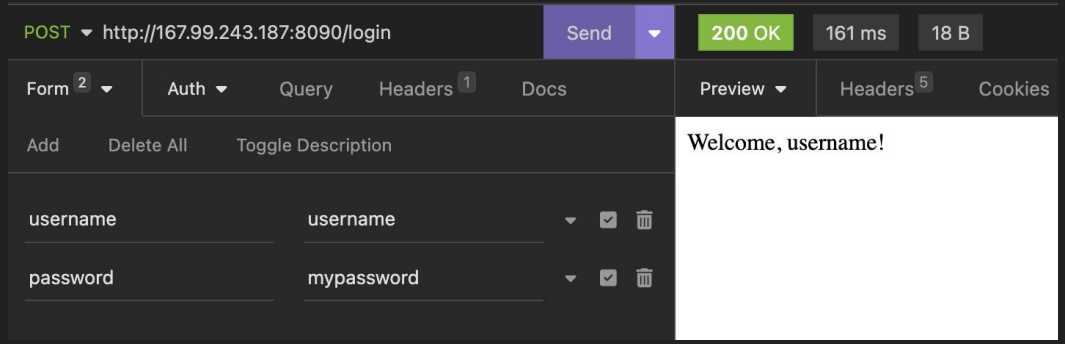
username: username

password: mypassword1

Invalid password

```
root@ubuntu-zukov-host:~/page_test# cat app_pass_in_logs.py
import logging
from flask import Flask, render_template, request

app = Flask(__name__,template_folder='templates')
logging.basicConfig(filename='auth.log', level=logging.INFO)

@app.route('/')
def index():
    return render_template('login.html')

@app.route('/login', methods=['POST'])
def login():
    username = request.form['username']
    password = request.form['password']
    if password == 'mypassword':
        logging.info(f'{username} logged in successfully with password {password}')
        return f'Welcome, {username}!'
    else:
        logging.warning(f'{username} entered an incorrect password {password}')
        return 'Invalid password'

if __name__ == '__main__':
    app.run(host="167.99.243.187", port=8090, debug=True)
```

```
WARNING:root:username entered an incorrect password mypassword1
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:18:08] "POST /login HTTP/1.1" 200
WARNING:root:username entered an incorrect password mypassword12
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:18:10] "POST /login HTTP/1.1" 200
WARNING:root:username entered an incorrect password mypassword123
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:18:12] "POST /login HTTP/1.1" 200
WARNING:root:username entered an incorrect password mypassword1234
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:18:13] "POST /login HTTP/1.1" 200
WARNING:root:username entered an incorrect password mypassword12345
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:18:15] "POST /login HTTP/1.1" 200
WARNING:root:username entered an incorrect password mypassword12345!
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:18:17] "POST /login HTTP/1.1" 200
WARNING:root:username entered an incorrect password mypassword12345!@
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:18:19] "POST /login HTTP/1.1" 200
WARNING:root:username entered an incorrect password mypassword12345!@#
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:18:21] "POST /login HTTP/1.1" 200
WARNING:root:username entered an incorrect password mypassword1!@#
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:18:25] "POST /login HTTP/1.1" 200
WARNING:root:username entered an incorrect password mypasswor1!@#
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:18:28] "POST /login HTTP/1.1" 200
INFO:root:username logged in successfully with password mypassword
INFO:werkzeug:45.137.112.194 - - [08/Apr/2023 08:18:33] "POST /login HTTP/1.1" 200
```



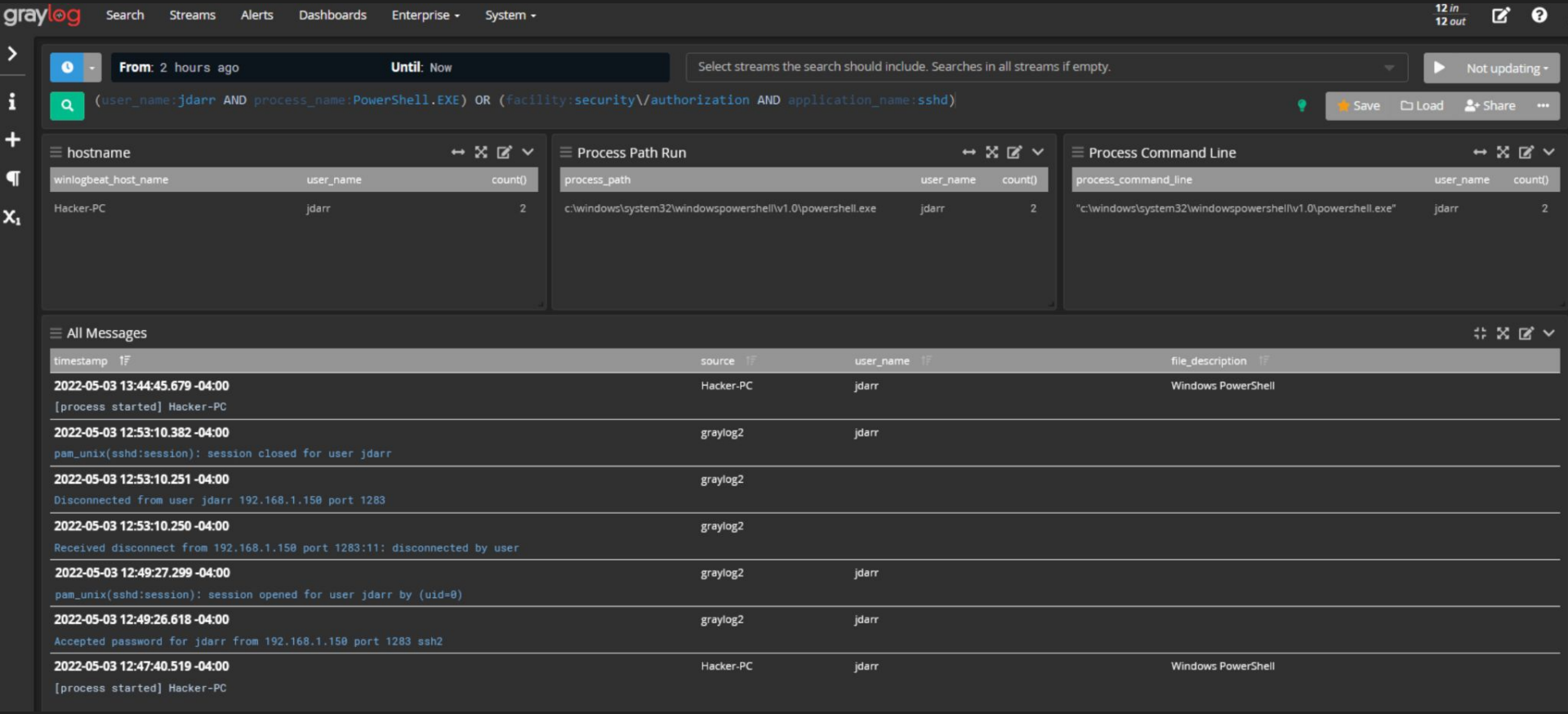
Инструменты для ручного анализа логов

- OWASP ZAP
- Burp Suite
- Nmap
- Nikto
- Metasploit Framework
- Nessus
- OpenVAS
- Acunetix
- Qualys
- Lynis

Инструменты для автоматического анализа логов

- Loggly
- Splunk
- XpoLog
- Graylog
- ELK Stack
- McAfee Enterprise Security Manager

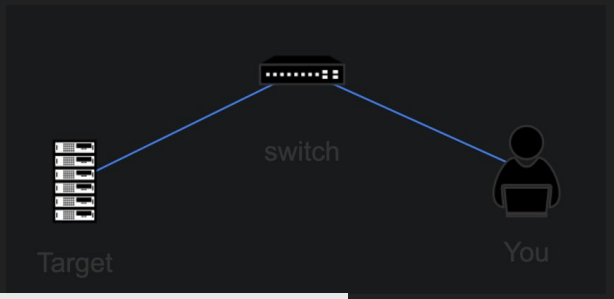
Graylog


graylog
Search
Streams
Alerts
Dashboards
Enterprise
System
12 in
12 out
From: 2 hours ago
Until: Now
Select streams the search should include. Searches in all streams if empty.
Not updating
(user_name:jdarr AND process_name:PowerShell.EXE) OR (facility:security\/authorization AND application_name:sshd)
Save
Load
Share
hostname
winlogbeat_host_name
user_name
count()
Hacker-PC
jdarr
2
Process Path Run
process_path
user_name
count()
c:\windows\system32\windowspowershell\v1.0\powershell.exe
jdarr
2
Process Command Line
process_command_line
user_name
count()
"c:\windows\system32\windowspowershell\v1.0\powershell.exe"
jdarr
2
All Messages
timestamp
source
user_name
file_description
2022-05-03 13:44:45.679 -04:00
[process started] Hacker-PC
Hacker-PC
jdarr
Windows PowerShell
2022-05-03 12:53:10.382 -04:00
pam_unix(sshd:session): session closed for user jdarr
graylog2
jdarr
2022-05-03 12:53:10.251 -04:00
Disconnected from user jdarr 192.168.1.150 port 1283
graylog2
2022-05-03 12:53:10.250 -04:00
Received disconnect from 192.168.1.150 port 1283:11: disconnected by user
graylog2
2022-05-03 12:49:27.299 -04:00
pam_unix(sshd:session): session opened for user jdarr by (uid=0)
graylog2
jdarr
2022-05-03 12:49:26.618 -04:00
Accepted password for jdarr from 192.168.1.150 port 1283 ssh2
graylog2
jdarr
2022-05-03 12:47:40.519 -04:00
[process started] Hacker-PC
Hacker-PC
jdarr
Windows PowerShell

Grafana


Stats Overview
Last 1 hour
Memory / CPU
memory
cpu
logins
timeshift -1h
logins
logins (-1 hour)
Memory
80 B
Sign ups
275
Logouts
161
Sign outs
279
server requests
web_server_01
web_server_02
web_server_03
web_server_04
client side full page load
70 GB
60 GB
60 GB
30 GB
40 GB
83 GB
44 GB
47 GB
94 GB
4 GB
73 GB
44 GB
19 GB
22 GB
20 GB
81 GB
sda1
sda2
sda3
sda4
sda5
sda6
sda7
sda8
sda9
sda10
sda11
sda12
sda13
sda14
sda15
sda16

Kibana: FTP Log analysis



attackdefense.com/listing?lab | Console - Kibana

o8uy757e804oq4auv0j2pzwps.mumbaix.attackdefenselabs.com/app/kibana#/dev_tools/console?_g=(filters:!(),refreshInterval:(pause:!t,

Dev Tools

History Settings Help

Console

```
GET ftp-logs/_search
{
  "size" : 0,
  "aggs": {
    "most_active_client": {
      "terms": {

        "field" : "sender_ip.keyword",
        "size" : 1

      }
    }
  }
}
```

```
{
  "took" : 15,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 5796,
      "relation" : "eq"
    },
    "max_score" : null,
    "hits" : [ ]
  },
  "aggregations" : {
    "most_active_client" : {
      "doc_count_error_upper_bound" : 0,
      "sum_other_doc_count" : 318,
      "buckets" : [
        {
          "key" : "192.168.202.102",
          "doc_count" : 5478
        }
      ]
    }
  }
}
```

attackdefense.com/listing?labt

Console - Kibana

o8uy757e804oq4auv0j2pzwps.mumbaix

There were 9 connection requests where the credentials are incorrec

Dev Tools

History Settings Help

Console

```
GET ftp-logs/_search
{
  "size": 0,
  "query": {
    "match": {
      "reply_msg": "incorrect"
    }
  },
  "aggs": {
    "clients": {
      "terms": {
        "field" : "sender_ip.keyword"
      }
    },
    "reply_msg" : {
      "terms" : {
        "field" : "reply_msg.keyword"
      }
    }
  }
}
```

```
{
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 9,
      "relation" : "eq"
    },
    "max_score" : null,
    "hits" : [ ]
  },
  "aggregations" : {
    "clients" : {
      "doc_count_error_upper_bound" : 0,
      "sum_other_doc_count" : 0,
      "buckets" : [
        {
          "key" : "192.168.202.102",
          "doc_count" : 9
        }
      ]
    },
    "reply_msg" : {
      "doc_count_error_upper_bound" : 0,
      "sum_other_doc_count" : 0,
      "buckets" : [
        {
          "key" : "Login or password incorrect!",
          "doc_count" : 9
        }
      ]
    }
  }
}
```

Как предотвратить

Необходимо реализовать следующие элементы управления:

- Все ошибки входа в систему, контроля доступа и проверки ввода на стороне сервера необходимо зарегистрировать для выявления подозрительных или вредоносных учетных записей и хранить в течение достаточного времени для проведения анализа.
- Эффективный мониторинг и оповещение для быстрого обнаружения подозрительных действий и реагирования на них.
- План реагирования на инциденты и восстановления после них.

Литература

- “Ведение журнала и управление журналами: Авторитетное руководство по пониманию концепций, связанных с ведением журнала и управлением журналами” Антон Чувакин и Кевин Шмидт
- “Hacking Exposed 7: секреты и решения сетевой безопасности” Стюарт Макклюр, Джоэл Скамбрей и Джордж Курц
- “Практика мониторинга сетевой безопасности: понимание обнаружения инцидентов и реагирования на них” Ричард Бейтлих