Network Log Analysis BY P3NGU1N

Generic Log Analysis (Netflow)

🎯 Can “Layer 7 - Application Layer” information be obtained with Netflow analysis?

ANSWER: N

🎯 Which of the followings are not produced through Netflow logs?

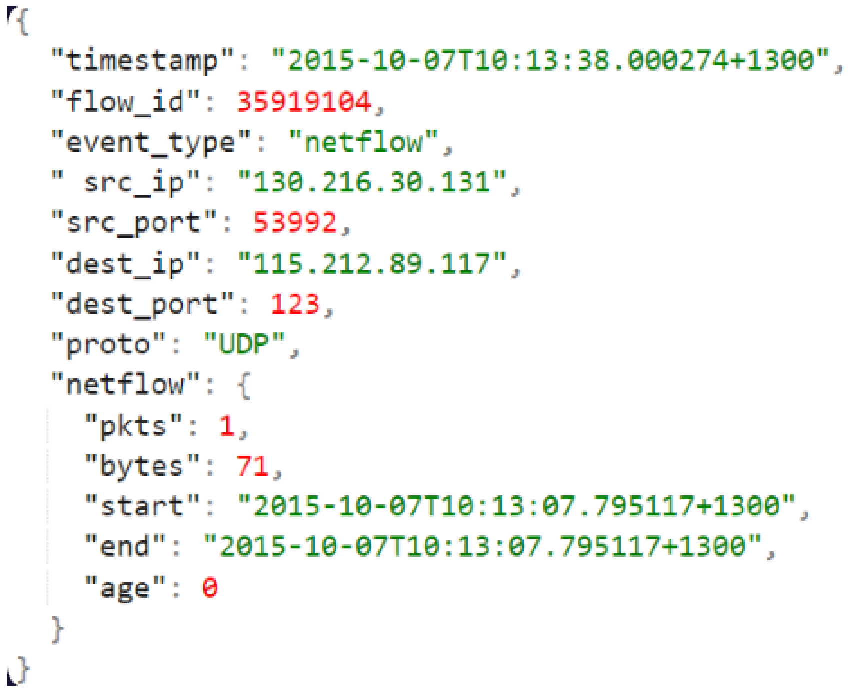
- IP Information
- XFF IP Information
- Port Information
- Interface Information

ANSWER: xff ip Information

🎯 What types of attacks can be detected with Netflow data?

- Network Anomaly Detection
- Detection of an Infected System
- Detection of malicious applications running on the Endpoint
- Suspicious Domain Requests

ANSWER: network anomaly detection

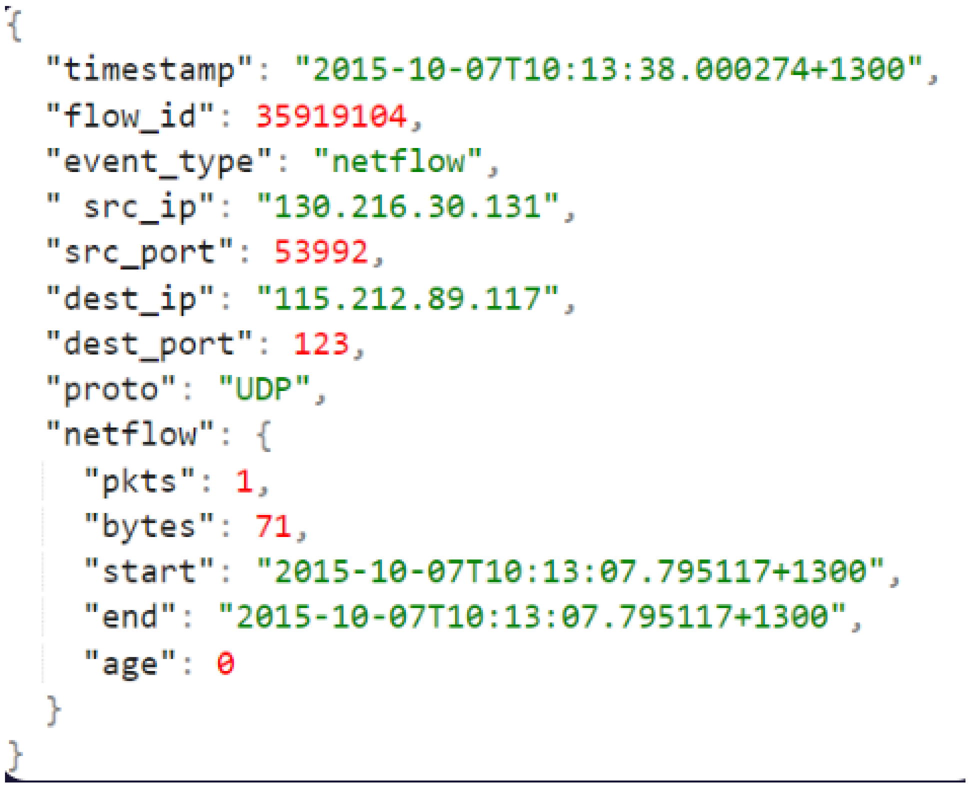


```
{
  "timestamp": "2015-10-07T10:13:38.000274+1300",
  "flow_id": 35919104,
  "event_type": "netflow",
  " src_ip": "130.216.30.131",
  "src_port": 53992,
  "dest_ip": "115.212.89.117",
  "dest_port": 123,
  "proto": "UDP",
  "netflow": {
    "pkts": 1,
    "bytes": 71,
    "start": "2015-10-07T10:13:07.795117+1300",
    "end": "2015-10-07T10:13:07.795117+1300",
    "age": 0
  }
}
```

🎯 According to the NetFlow data above, what could it be to see 10k requests from different source IPs to the same destination within 2 minutes?

- SYN Flood
- UDP Flood
- ICMP Flood
- DNS Flood

ANSWER: udp flood



```
{
  "timestamp": "2015-10-07T10:13:38.000274+1300",
  "flow_id": 35919104,
  "event_type": "netflow",
  " src_ip": "130.216.30.131",
  "src_port": 53992,
  "dest_ip": "115.212.89.117",
  "dest_port": 123,
  "proto": "UDP",
  "netflow": {
    "pkts": 1,
    "bytes": 71,
    "start": "2015-10-07T10:13:07.795117+1300",
    "end": "2015-10-07T10:13:07.795117+1300",
    "age": 0
  }
}
```

Which of the following is not true according to the NetFlow data above?

A) Total number of package is 1.

B) The amount of data transmitted is 71 bytes.

C) NTP service is definitely running on the target port 123.

ANSWER: c

Firewall Log Analysis

🎯 **Note:**

Use the "/root/Desktop/QuestionFiles/firewall.log" file for solving the questions below.

Question:

How many different ports did the attacker attempt to access?

ANSWER: 12

🎯

What kind of attack/activity could have been made according to the logs above?

A) Brute-Force Attack

B) Port-scan activity

C) TCP-SYN-Flood Attack

D) No suspicious activities detected

ANSWER: b

🎯 How does Firewall determine whether to forward an incoming packet to the destination or not?

A) By analyzing behaviorally

B) According to the rule policy

C) According to the size of the traffic

D) According to the location information

ANSWER: b

🎯 How many open ports did the attacker detect?

ANSWER: 3

🎯 Will the attacker get a response from the Firewall stating that its access request was blocked?

ANSWER: y

VPN Log Analysis

🎯 Which of the followings are true for the user3 VPN User?

A) Brute-Force Attack

B) user3 made a successful VPN connection

C) There were failed login attempts from different locations within short period of time

D) user3 made a successful VPN connection from the US location

ANSWER: c

Note:

Use the "/root/Desktop/QuestionFiles/vpn.log" file for solving the questions below.

Question:

Which of the following is not a type of VPN?

A) SSL-VPN

B) Site-to-Site VPN

C) IPSec VPN

D) DNS over VPN

ANSWER: d

VPN only works on firewall devices. (True/False)

ANSWER: false

Which one is true for the "letsdefend" user logs?

A) Brute-Force Attack

B) 4 Successful VPN connections were established with Letsdefend user

C) Letsdefend user has successfully logged in from DE location

ANSWER: a

Proxy Log Analysis

🎯 Proxy is only used for accessing the internet via the web. (True/False)

ANSWER: false

🎯

```
Mar 30 19:07:16 10.60.28.21
CEF:0|Forcepoint|Security|8.5.4|1900|Transaction permitted|164|
act=permitted app=https dst=18.11.96.7 dhost=letsdefend.io dpt=443
src=172.20.40.42 spt=59228 suser=user1 requestMethod=CONNECT
cs1Label=Policy cs1=default-user-policy
request=https://letsdefend.io/
```

According to the Proxy log above, which of the following is not true?

A) SSL/TLS used.

B) User1 made the query.

C) The proxy device has blocked this request.

D) The domain accessed works on the server with the address "18.11.96.7".

ANSWER: c

🎯 Through which logs do we verify the response from the requested target in the proxy log above? (assuming that there are Firewall, AV, DLP, IPS/IDS, EDR, WAF devices in the environment.)

A) From the antivirus logs

B) From Email Gateway logs

C) From Firewall logs

D) From DLP logs

ANSWER: c

🎯

```
Mar 30 19:07:16 10.60.28.21
CEF:0|Forcepoint|Security|8.5.4|1900|Transaction permitted|164|
act=permitted app=https dst=18.11.96.7 dhost=letsdefend.io dpt=443
src=172.20.40.42 spt=59228 suser=user1 requestMethod=CONNECT
cs1Label=Policy cs1=default-user-policy
request=https://letsdefend.io/
```

When the above proxy log record turns into an alert, which action below is not required?

A) Checking domain reputation

B) Dynamic analysis of the accessed address

C) Controlling which different systems accessed the requested domain

D) Obtaining information by contacting the user who made the request

E) Blocking access to the domain

F) Check of Windows Application Events of the requesting system

ANSWER: f

IDS/IPS Log Analysis

🎯 IDS is a system that .... the attacks. IPS is a system that .... the attacks.

Fill in the blanks.

A) prevent - detect

B) detect - prevent

C) detect - detect

D) prevent - prevent

ANSWER: b

🎯

```
{"timestamp":"2022-06-13T08:25:36", "in_iface":"ens1f1",
"event_type":"alert","vlan":1,"src_ip":"192.168.1.11",
"src_port":53,"dest_ip":"172.16.2.25", "dest_port":1029,"proto":"UDP",
"alert":{"action":"allowed", "gid":1, "signature_id":2811577, "rev":3,
"signature":"ETPRO TROJAN Possible Virut DGA NXDOMAIN
Responses", "category":"A Network Trojan was detected",
"severity":1, "metadata":{"updated_at":["2021_09_22"],"created_at":
["2015_06_18"]}}, "app_proto":"failed"},
"payload":"dnV5ZWltLmNvbQo=", "payload_printable":"vuyeim.com",
"stream":0}
```

Answer the following questions according to the above referenced IDS log:

Which of the following is not correct?

A) The system making malicious domain request may be infected.

B) The relevant domain has not been accessed.

C) The DNS server has responded to the domain request.

D) The domain categorized as DGA is vuyeim.com.

ANSWER: b

🎯

```
{"timestamp":"2022-06-13T08:25:36", "in_iface":"ens1f1",
"event_type":"alert","vlan":1,"src_ip":"192.168.1.11",
"src_port":53,"dest_ip":"172.16.2.25", "dest_port":1029,"proto":"UDP",
"alert":{"action":"allowed", "gid":1, "signature_id":2811577, "rev":3,
"signature":"ETPRO TROJAN Possible Virut DGA NXDOMAIN
Responses", "category":"A Network Trojan was detected",
"severity":1, "metadata":{"updated_at":["2021_09_22"],"created_at":
["2015_06_18"]}}, "app_proto":"failed"},
"payload":"dnV5ZWltLmNvbQo=", "payload_printable":"vuyeim.com",
"stream":0}
```

What is the IP address related to the malicious domain?

ANSWER: 172.16.2.25

🎯

```
{"timestamp":"2022-06-13T08:25:36", "in_iface":"ens1f1",
"event_type":"alert","vlan":1,"src_ip":"192.168.1.11",
"src_port":53,"dest_ip":"172.16.2.25", "dest_port":1029,"proto":"UDP",
"alert":{"action":"allowed", "gid":1, "signature_id":2811577, "rev":3,
"signature":"ETPRO TROJAN Possible Virut DGA NXDOMAIN
Responses", "category":"A Network Trojan was detected",
"severity":1, "metadata":{"updated_at":["2021_09_22"],"created_at":
["2015_06_18"]}}, "app_proto":"failed"},
"payload":"dnV5ZWltLmNvbQo=", "payload_printable":"vuyeim.com",
"stream":0}
```

Which of the following is a true statement?

A) The request is blocked by the firewall.

B) The related IDS has caught the DNS request in the return traffic.

C) The category of the IDS rule is in the "DNS attack" category.

ANSWER: b

🎯 Which of the following information is normally not included in the IDS/IPS alarm outputs?

A) Payload information

B) IP and Port information

C) Parent process information

D) Action information

E) Signature information

ANSWER: c

WAF Log Analysis

🎯

```
date=2022-01-26 time=19:47:26 type=attack main_type="Signature
Detection" sub_type="SQL Injection" severity_level=High proto=tcp
service=https/tls1.2 action=Alert policy="Alert_Policy"
src=199.26.150.138 src_port=56334 dst=172.16.10.10 dst_port=443
http_method=get http_url="?v=" OR 1 = 1 -- -"
http_host="app.letsdefend.io" http_agent="Mozilla/5.0 (Nikto/2.1.6)"
srccountry="Italy" attack_type="SQL Injection"
```

Which of the following is not true according to the WAF log above?

A) The request has reached the server

B) The server responded to the request successfully

C) According to the log record, the request came through the automated web browsing tool

D) The request method is GET

ANSWER: b

🎯 Which of the following actions should be taken when the above WAF log is examined?

A) Whether the attack was successful or not should be simulated.

B) Requests with high source port numbers should be blocked on the firewall.

C) SSL certificate should be reviewed.

ANSWER: a

Web Log Analysis

🎯 Which of the following is not an HTTP request method?

A) GET

B) OPTIONS

C) TRACE

D) HEAD

E) BLOCK

ANSWER: e

🎯 **Note:**

Use the "/root/Desktop/QuestionFiles/http.log" file for solving the questions below.

Question:

Are there any SQL injection attacks with a status code of 200? (True or False)

ANSWER: true

🎯 Identify the highest requesting IP address.

ANSWER: 192.168.203.63

🎯 How many web requests are made with "DELETE" method in total?

ANSWER: 223

🎯 Are there web logs with “Nmap Scripting Engine” in the user-agent information among the web requests made? (True or False)

ANSWER: true

DNS Log Analysis

🎯 Which of the following is not a DNS record type?

A) MX

B) NS

C) A

D) IP

ANSWER: d

🎯 DNS log;

```
Feb 5 09:12:11 ns1 named[80090]: client 192.168.10.3#3261: query: dns.google IN A
```

Firewall log;

```
date=2022-05-21 time=09:12:13 type="traffic" subtype="forward" srcip=192.168.10.3 srcport=50495 srcintfrole="lan" dstip=8.8.4.4 dstport=853 dstintfrole="wan" proto=6 action="accept"
```

What could the suspicious activity be at the DNS and firewall logs above?

A) DNS Flood

B) DNS Tunnel

C) DNS over HTTPS

D) DNS Hijacking

ANSWER: c

```
Mar 5 19:12:11 ns1 named[80090]: client 172.16.11.34#3261: query: am4wuz3zifexz5u.onion IN A
```

What could the suspicious activity be at the DNS log above?

A) DNS Proxy

B) DNS Tunnel

C) DNS over HTTPS

D) Access to the TOR network

ANSWER: d

QUIZ:

Which of the following technologies provides the opportunity to work in a remote environment as if it were connected locally?

ANSWER: VPN

WAF examines the contents of which of the following?

ANSWER: WEB

Which of the following is not true for IDS?

ANSWER: **It blocks**

🎯 **What is the meaning of 403 HTTP status code in web logs?**

ANSWER: **Access denied**

🎯 **Which of the following cannot be obtained by NetFlow analysis?**

ANSWER: **Most used application**

🎯 **Which of the following is that the Firewalls can’t do?**

ANSWER: **Creating web logs**

🎯 **Which of the following is not true for IPS?**

ANSWER: **Makes code analysis**

🎯 **Which of the following is not the purpose to use a proxy?**

ANSWER: **Bypassing the Firewall**

🎯 **Which of the following is an attack type to be detected by examining DNS audit activities?**

ANSWER: **DNS Hijacking**

🎯 **Would a request blocked by WAF be visible in the web server logs?**

ANSWER: NO