TraceHawk Incident Report: Reconnaissance followed by sensitive HTTP access

Generated	2026-07-12T00:00:00+00:00
Mode	Local-only deterministic report
Incident ID	incident:7b888375da4c
Status	active
Severity	critical
Score	100
First Seen	2026-07-08T11:20:00+00:00
Last Seen	2026-07-08T11:21:23.199999+00:00

Executive Summary

Reconnaissance followed by sensitive HTTP access grouped 12 finding(s) involving dst:10.20.0.53, dst:203.0.113.80, host:10.20.0.53, host:lab-app.internal, ip:10.20.0.25. Scan activity was followed by sensitive HTTP access. A DNS burst was followed by a C2 indicator or high-severity alert. An alert burst included high-severity Suricata evidence. Cross-source corroboration links 20 related evidence pair(s).

Scoring Rationale

Base Severity	95
Finding Volume	20
Sequence Quality	25
Time Window Proximity	10
Cross Source Corroboration	18
Rule Family Diversity	10

- critical severity baseline contributes 95.
- 12 finding(s) contribute 20 volume point(s).
- Sequence quality: pattern scan-to-sensitive-http: Scan activity is followed by sensitive HTTP access.
- Sequence quality: pattern dns-burst-to-c2-alert: DNS burst is followed by a C2 indicator or high-severity alert.
- Sequence quality: pattern alert-burst-to-high-severity: Alert burst includes high-severity Suricata evidence.
- Time-window proximity: related findings occur within five minutes.
- Cross-source corroboration: 20 related link(s) across dns_query_match, http_path_match contribute 18 point(s).
- Rule-family diversity: 6 families (alert, command_and_control, dns, high_severity_alert, network_scan, sensitive_http) contribute 10 point(s).

Entities

- dst:10.20.0.53
- dst:203.0.113.80
- host:10.20.0.53
- host:lab-app.internal
- ip:10.20.0.25
- port:53
- port:80

MITRE ATT&CK

- T1071
- T1071.004
- T1083
- T1190
- T1595.002

Local Assistant Summary

Deterministic correlation joins independent Zeek and Suricata observations. Validate the shared flow, HTTP path, and sequence evidence before escalation.

Findings

Suricata alert burst

Rule	suricata-alert-burst-001
Severity	high
Confidence	medium
Events	11
MITRE	T1595.002 Vulnerability Scanning

Suricata alert burst matched 11 event(s) for 10.20.0.25.

Suricata EVE shows multiple IDS alerts from one source in a short window.

Suricata command and control category alert

Rule	suricata-c2-category-001
Severity	critical
Confidence	medium
Events	1
MITRE	T1071 Application Layer Protocol

Suricata command and control category alert matched 1 event(s) for 10.20.0.25, 203.0.113.80.

Suricata EVE alert category or signature indicates possible command and control activity.

Suricata high severity alert

Rule	suricata-high-severity-alert-001
Severity	high
Confidence	high
Events	1
MITRE	T1190 Exploit Public-Facing Application

Suricata high severity alert matched 1 event(s) for 10.20.0.25, 203.0.113.80, TRACEHAWK LAB HTTP sensitive env path.

Suricata EVE alert has severity 1, indicating a high priority IDS match.

Suricata high severity alert

Rule	suricata-high-severity-alert-001
Severity	high
Confidence	high

Events	1
MITRE	T1190 Exploit Public-Facing Application

Suricata high severity alert matched 1 event(s) for 10.20.0.25, 203.0.113.80, TRACEHAWK LAB HTTP C2 config path.

Suricata EVE alert has severity 1, indicating a high priority IDS match.

Suricata high severity alert

Rule	suricata-high-severity-alert-001
Severity	high
Confidence	high
Events	4
MITRE	T1190 Exploit Public-Facing Application

Suricata high severity alert matched 4 event(s) for 10.20.0.25, 203.0.113.80, TRACEHAWK LAB Nmap HTTP user agent scan.

Suricata EVE alert has severity 1, indicating a high priority IDS match.

Suricata HTTP sensitive path access

Rule	suricata-http-sensitive-path-001
Severity	high
Confidence	medium
Events	4
MITRE	T1083 File and Directory Discovery

Suricata HTTP sensitive path access matched 4 event(s) for 10.20.0.25, lab-app.internal.

Suricata EVE HTTP record shows access to common sensitive files or administrative paths.

Suricata scan signature

Rule	suricata-scan-signature-001
Severity	high
Confidence	medium
Events	4
MITRE	T1595.002 Vulnerability Scanning

Suricata scan signature matched 4 event(s) for 10.20.0.25.

Suricata EVE alert signature indicates scanning or reconnaissance.

Zeek HTTP sensitive path access

Rule	zeek-http-sensitive-path-001
Severity	high
Confidence	medium
Events	4
MITRE	T1083 File and Directory Discovery

Zeek HTTP sensitive path access matched 4 event(s) for 10.20.0.25, lab-app.internal.

Zeek HTTP logs show access to common sensitive files or administrative paths.

Suricata command and control category alert

Rule	suricata-c2-category-001
Severity	critical
Confidence	medium
Events	5
MITRE	T1071 Application Layer Protocol

Suricata command and control category alert matched 5 event(s) for 10.20.0.25, 10.20.0.53.

Suricata EVE alert category or signature indicates possible command and control activity.

Suricata DNS burst

Rule	suricata-dns-burst-001
Severity	medium
Confidence	medium
Events	5
MITRE	T1071.004 DNS

Suricata DNS burst matched 5 event(s) for 10.20.0.25.

Suricata EVE DNS records show repeated queries from one source in a short window.

Suricata high severity alert

Rule	suricata-high-severity-alert-001
Severity	high
Confidence	high
Events	5
MITRE	T1190 Exploit Public-Facing Application

Suricata high severity alert matched 5 event(s) for 10.20.0.25, 10.20.0.53, TRACEHAWK LAB DNS beacon-control query.

Suricata EVE alert has severity 1, indicating a high priority IDS match.

Zeek DNS burst

Rule	zeek-dns-burst-001
Severity	medium
Confidence	medium
Events	5
MITRE	T1071.004 DNS

Zeek DNS burst matched 5 event(s) for 10.20.0.25.

Zeek DNS logs show repeated queries from one source in a short window.

Timeline

- `2026-07-08T11:20:00+00:00 | suricata_alert | 10.20.0.25 | TRACEHAWK LAB HTTP C2 config path`
- `2026-07-08T11:20:00+00:00 | suricata_alert | 10.20.0.25 | TRACEHAWK LAB Nmap HTTP user agent scan`
- `2026-07-08T11:20:00+00:00 | suricata_http | 10.20.0.25 | HTTP GET lab-app.internal/wp-config.php`
- `2026-07-08T11:20:00+00:00 | suricata_alert | 10.20.0.25 | TRACEHAWK LAB Nmap HTTP user agent scan`
- `2026-07-08T11:20:00+00:00 | suricata_http | 10.20.0.25 | HTTP GET lab-app.internal/backup.zip`
- `2026-07-08T11:20:00+00:00 | suricata_alert | 10.20.0.25 | TRACEHAWK LAB Nmap HTTP user agent scan`
- `2026-07-08T11:20:00+00:00 | suricata_http | 10.20.0.25 | HTTP GET lab-app.internal/admin`
- `2026-07-08T11:20:00+00:00 | suricata_alert | 10.20.0.25 | TRACEHAWK LAB HTTP sensitive env path`
- `2026-07-08T11:20:00+00:00 | suricata_alert | 10.20.0.25 | TRACEHAWK LAB Nmap HTTP user agent scan`
- `2026-07-08T11:20:00+00:00 | suricata_http | 10.20.0.25 | HTTP GET lab-app.internal/.env`
- `2026-07-08T11:20:00.029999+00:00 | zeek_http | 10.20.0.25 | Zeek HTTP GET lab-app.internal/.env`
- `2026-07-08T11:20:00.829999+00:00 | zeek_http | 10.20.0.25 | Zeek HTTP GET lab-app.internal/wp-config.php`
- `2026-07-08T11:20:01.629999+00:00 | zeek_http | 10.20.0.25 | Zeek HTTP GET lab-app.internal/admin`
- `2026-07-08T11:20:02.429999+00:00 | zeek_http | 10.20.0.25 | Zeek HTTP GET lab-app.internal/backup.zip`
- `2026-07-08T11:20:03.199999+00:00 | zeek_dns | 10.20.0.25 | Zeek DNS query a1.beacon-control.example`
- `2026-07-08T11:20:03.199999+00:00 | suricata_dns | 10.20.0.25 | DNS query a1.beacon-control.example`
- `2026-07-08T11:20:03.199999+00:00 | suricata_alert | 10.20.0.25 | TRACEHAWK LAB DNS beacon-control query`
- `2026-07-08T11:20:23.199999+00:00 | zeek_dns | 10.20.0.25 | Zeek DNS query a2.beacon-control.example`
- `2026-07-08T11:20:23.199999+00:00 | suricata_alert | 10.20.0.25 | TRACEHAWK LAB DNS beacon-control query`
- `2026-07-08T11:20:23.199999+00:00 | suricata_dns | 10.20.0.25 | DNS query a2.beacon-control.example`
- `2026-07-08T11:20:43.199999+00:00 | zeek_dns | 10.20.0.25 | Zeek DNS query a3.beacon-control.example`
- `2026-07-08T11:20:43.199999+00:00 | suricata_alert | 10.20.0.25 | TRACEHAWK LAB DNS beacon-control query`
- `2026-07-08T11:20:43.199999+00:00 | suricata_dns | 10.20.0.25 | DNS query a3.beacon-control.example`
- `2026-07-08T11:21:03.199999+00:00 | zeek_dns | 10.20.0.25 | Zeek DNS query a4.beacon-control.example`
- `2026-07-08T11:21:03.199999+00:00 | suricata_alert | 10.20.0.25 | TRACEHAWK LAB DNS beacon-control query`
- `2026-07-08T11:21:03.199999+00:00 | suricata_dns | 10.20.0.25 | DNS query a4.beacon-control.example`
- `2026-07-08T11:21:23.199999+00:00 | zeek_dns | 10.20.0.25 | Zeek DNS query a5.beacon-control.example`
- `2026-07-08T11:21:23.199999+00:00 | suricata_alert | 10.20.0.25 | TRACEHAWK LAB DNS beacon-control query`
- `2026-07-08T11:21:23.199999+00:00 | suricata_dns | 10.20.0.25 | DNS query a5.beacon-control.example`

Evidence

Line 10

```
1783509623.199999    C3xeuJ3qgTP9IqGiZa    10.20.0.25    52002    10.20.0.53    53    udp
17410    -    a2.beacon-control.example    1    C_INTERNET    1    A    -    -    F    F    T
    F    0    -    -    F    0    query
```

SHA-256: bb871e8b8bee8c136bbac95f25510e54b17479f13a604eee369d50f0325ce15b

Line 11

```
1783509643.199999    C4bKao4vCEJEypGT83    10.20.0.25    52003    10.20.0.53    53    udp
17411    -    a3.beacon-control.example    1    C_INTERNET    1    A    -    -    F    F    T
    F    0    -    -    F    0    query
```

SHA-256: cc94ddbc81339482ff05e489e0899d36f0079dd0d43c4ca2be9cef2c5cdd1fdf

Line 12

```
1783509663.199999    CRBHJA1DWw7EABKLG2    10.20.0.25    52004    10.20.0.53    53    udp
17412    -    a4.beacon-control.example    1    C_INTERNET    1    A    -    -    F    F    T
    F    0    -    -    F    0    query
```

SHA-256: a397202da05e461a73daad891e0046fd9c788728eb0ff41716bbac43914091d3

Line 13

```
1783509683.199999    CaEQGu4f6N2cbSnoz6    10.20.0.25    52005    10.20.0.53    53    udp
17413    -    a5.beacon-control.example    1    C_INTERNET    1    A    -    -    F    F    T
    F    0    -    -    F    0    query
```

SHA-256: 2bf7fa62d6f019f32fca7c56fe41b16013c89f5a58bf75744deebb19206f7f5e

Line 9

```
1783509603.199999    CyP0Aq30K0aNvpxyy8    10.20.0.25    52001    10.20.0.53    53    udp
17409    -    a1.beacon-control.example    1    C_INTERNET    1    A    -    -    F    F    T
    F    0    -    -    F    0    query
```

SHA-256: 89567328bc4ce64608f7e68842ef7adb99cf643367d9ed19b77ba0a204761796

Line 1


```
{"timestamp":"2026-07-08T11:20:43.199999+0000","flow_id":858989634115848,"pcap_cnt":23,"event_ty
pe":"alert","src_ip":"10.20.0.25","src_port":52003,"dest_ip":"10.20.0.53","dest_port":53,"proto"
:"UDP","ip_v":4,"pkt_src":"wire/pcap","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_i
d":9000004,"rev":1,"signature":"TRACEHAWK LAB DNS beacon-control query","category":"A Network
Trojan was detected","severity":1},"dns":{"version":3,"type":"request","tx_id":0,"id":17411,"fla
gs":"100","rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"a3.beacon-control.example
","rrtype":"A"}]},"app_proto":"dns","direction":"to_server","flow":{"pkts_toserver":1,"pkts_tocl
ient":0,"bytes_toserver":85,"bytes_toclient":0,"start":"2026-07-08T11:20:43.199999+0000","src_ip
":"10.20.0.25","dest_ip":"10.20.0.53","src_port":52003,"dest_port":53}}
```


SHA-256: 73dbc88137b339146507b8e27bb87df88716383be45c3afa2bb838e59889035a

Line 10


```
{"timestamp":"2026-07-08T11:20:03.199999+0000","flow_id":858990587745546,"pcap_cnt":21,"event_ty
pe":"dns","src_ip":"10.20.0.25","src_port":52001,"dest_ip":"10.20.0.53","dest_port":53,"proto":"
UDP","ip_v":4,"pkt_src":"wire/pcap","dns":{"version":3,"type":"request","tx_id":0,"id":17409,"fl
ags":"100","rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"a1.beacon-control.exampl
e","rrtype":"A"}]}}
```


SHA-256: 0b56b689dca88b1288b79804c754ac29d2eb652484675ac03f4b2d704f48f41d

Line 11


```
{"timestamp":"2026-07-08T11:20:00.000000+0000","flow_id":58271976689396,"event_type":"alert","sr
c_ip":"10.20.0.25","src_port":41001,"dest_ip":"203.0.113.80","dest_port":80,"proto":"TCP","ip_v"
:4,"pkt_src":"stream (flow timeout)","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id
":9000002,"rev":1,"signature":"TRACEHAWK LAB HTTP C2 config path","category":"A Network Trojan
was detected","severity":1},"ts_progress":"request_complete","tc_progress":"response_started","h
ttp":{"hostname":"lab-app.internal","url":"/wp-config.php","http_user_agent":"Nmap NSE lab probe
","http_method":"GET","protocol":"HTTP/1.1","length":0},"app_proto":"http","direction":"to_serve
r","flow":{"pkts_toserver":3,"pkts_toclient":2,"bytes_toserver":262,"bytes_toclient":153,"start"
:"2026-07-08T11:20:00.799999+0000","src_ip":"10.20.0.25","dest_ip":"203.0.113.80","src_port":410
01,"dest_port":80}}
```


SHA-256: efdd05839e26f143fdd5ff8372d3e7d3d3cdbe5d54f8aa518d30491238b1d94b

Line 12


```
{"timestamp":"2026-07-08T11:20:00.000000+0000","flow_id":58271976689396,"event_type":"alert","sr
c_ip":"10.20.0.25","src_port":41001,"dest_ip":"203.0.113.80","dest_port":80,"proto":"TCP","ip_v"
:4,"pkt_src":"stream (flow timeout)","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id
":9000003,"rev":1,"signature":"TRACEHAWK LAB Nmap HTTP user agent scan","category":"Attempted
Information Leak","severity":1},"ts_progress":"request_complete","tc_progress":"response_started
","http":{"hostname":"lab-app.internal","url":"/wp-config.php","http_user_agent":"Nmap NSE lab p
robe","http_method":"GET","protocol":"HTTP/1.1","length":0},"app_proto":"http","direction":"to_s
erver","flow":{"pkts_toserver":3,"pkts_toclient":2,"bytes_toserver":262,"bytes_toclient":153,"st
art":"2026-07-08T11:20:00.799999+0000","src_ip":"10.20.0.25","dest_ip":"203.0.113.80","src_port"
:41001,"dest_port":80}}
```


SHA-256: 8099078d5bf2ebd79d2bd72ded13f616a92067c0edfbd33c2555a5deb30b9205

Line 13


```
{"timestamp":"2026-07-08T11:20:00.000000+0000","flow_id":58271976689396,"event_type":"http","src
_ip":"10.20.0.25","src_port":41001,"dest_ip":"203.0.113.80","dest_port":80,"proto":"TCP","ip_v":
4,"pkt_src":"stream (flow timeout)","tx_id":0,"http":{"hostname":"lab-app.internal","url":"/wp-c
onfig.php","http_user_agent":"Nmap NSE lab
probe","http_method":"GET","protocol":"HTTP/1.1","status":404,"length":0}}
```


SHA-256: 15d2ddf368d7ef801c22e5144d7fca9dfa82eb79cd14b815f586bd7703eaed79

Line 15


```
{"timestamp":"2026-07-08T11:20:00.000000+0000","flow_id":592084950371583,"event_type":"alert","s
rc_ip":"10.20.0.25","src_port":41003,"dest_ip":"203.0.113.80","dest_port":80,"proto":"TCP","ip_v
":4,"pkt_src":"stream (flow timeout)","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_i
d":9000003,"rev":1,"signature":"TRACEHAWK LAB Nmap HTTP user agent scan","category":"Attempted
Information Leak","severity":1},"ts_progress":"request_complete","tc_progress":"response_started
","http":{"hostname":"lab-app.internal","url":"/backup.zip","http_user_agent":"Nmap NSE lab prob
e","http_method":"GET","protocol":"HTTP/1.1","length":0},"app_proto":"http","direction":"to_serv
er","flow":{"pkts_toserver":3,"pkts_toclient":2,"bytes_toserver":259,"bytes_toclient":153,"start
":"2026-07-08T11:20:02.399999+0000","src_ip":"10.20.0.25","dest_ip":"203.0.113.80","src_port":41
003,"dest_port":80}}
```


SHA-256: c527e9533a12c4f8807aaf79ac2621da6922f2e59a3aa95d25445c3fd4f4ba83

Line 16


```
{"timestamp":"2026-07-08T11:20:00.000000+0000","flow_id":592084950371583,"event_type":"http","sr
c_ip":"10.20.0.25","src_port":41003,"dest_ip":"203.0.113.80","dest_port":80,"proto":"TCP","ip_v"
:4,"pkt_src":"stream (flow timeout)","tx_id":0,"http":{"hostname":"lab-app.internal","url":"/bac
kup.zip","http_user_agent":"Nmap NSE lab
probe","http_method":"GET","protocol":"HTTP/1.1","status":404,"length":0}}
```


SHA-256: 0b6afcde07acc8586253880b96d946fb3adc01190dd54fd2e7f66c6f0aa31ef9

Line 18


```
{"timestamp":"2026-07-08T11:20:00.000000+0000","flow_id":325177781814277,"event_type":"alert","s
rc_ip":"10.20.0.25","src_port":41002,"dest_ip":"203.0.113.80","dest_port":80,"proto":"TCP","ip_v
":4,"pkt_src":"stream (flow timeout)","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_i
d":9000003,"rev":1,"signature":"TRACEHAWK LAB Nmap HTTP user agent scan","category":"Attempted
Information Leak","severity":1},"ts_progress":"request_complete","tc_progress":"response_started
","http":{"hostname":"lab-app.internal","url":"/admin","http_user_agent":"Nmap NSE lab probe","h
ttp_method":"GET","protocol":"HTTP/1.1","length":0},"app_proto":"http","direction":"to_server","
flow":{"pkts_toserver":3,"pkts_toclient":2,"bytes_toserver":254,"bytes_toclient":153,"start":"20
26-07-08T11:20:01.599999+0000","src_ip":"10.20.0.25","dest_ip":"203.0.113.80","src_port":41002,"
dest_port":80}}
```


SHA-256: 52ad9da4f115837f1a53fa0678ea3f6dc2d4a068840a3fbad506f3ecf891621f

Line 19


```
{"timestamp":"2026-07-08T11:20:00.000000+0000","flow_id":325177781814277,"event_type":"http","sr
c_ip":"10.20.0.25","src_port":41002,"dest_ip":"203.0.113.80","dest_port":80,"proto":"TCP","ip_v"
:4,"pkt_src":"stream (flow
timeout)","tx_id":0,"http":{"hostname":"lab-app.internal","url":"/admin","http_user_agent":"Nmap
 NSE lab probe","http_method":"GET","protocol":"HTTP/1.1","status":404,"length":0}}
```


SHA-256: 97bb01df1cb3a62befcf249039e09a89226ab97f2c605a0930fb55672c683a6e

Line 2


```
{"timestamp":"2026-07-08T11:20:23.199999+0000","flow_id":1984890687060882,"pcap_cnt":22,"event_t
ype":"alert","src_ip":"10.20.0.25","src_port":52002,"dest_ip":"10.20.0.53","dest_port":53,"proto
":"UDP","ip_v":4,"pkt_src":"wire/pcap","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_
id":9000004,"rev":1,"signature":"TRACEHAWK LAB DNS beacon-control query","category":"A Network
Trojan was detected","severity":1},"dns":{"version":3,"type":"request","tx_id":0,"id":17410,"fla
gs":"100","rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"a2.beacon-control.example
","rrtype":"A"}]},"app_proto":"dns","direction":"to_server","flow":{"pkts_toserver":1,"pkts_tocl
ient":0,"bytes_toserver":85,"bytes_toclient":0,"start":"2026-07-08T11:20:23.199999+0000","src_ip
":"10.20.0.25","dest_ip":"10.20.0.53","src_port":52002,"dest_port":53}}
```


SHA-256: f3c7e25f9e49010fbc3036a691c99897e0165263c998dd5272a5ecca10c77fbf

Line 21


```
{"timestamp":"2026-07-08T11:20:00.000000+0000","flow_id":2731975549,"event_type":"alert","src_ip
":"10.20.0.25","src_port":41000,"dest_ip":"203.0.113.80","dest_port":80,"proto":"TCP","ip_v":4,"
pkt_src":"stream (flow timeout)","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":90
00001,"rev":1,"signature":"TRACEHAWK LAB HTTP sensitive env path","category":"Web Application At
tack","severity":1},"ts_progress":"request_complete","tc_progress":"response_started","http":{"h
ostname":"lab-app.internal","url":"/.env","http_user_agent":"Nmap NSE lab probe","http_method":"
GET","protocol":"HTTP/1.1","length":0},"app_proto":"http","direction":"to_server","flow":{"pkts_
toserver":3,"pkts_toclient":2,"bytes_toserver":253,"bytes_toclient":153,"start":"2026-07-08T11:2
0:00.000000+0000","src_ip":"10.20.0.25","dest_ip":"203.0.113.80","src_port":41000,"dest_port":80
}}
```


SHA-256: 407bda53b042b66bf9e36e8f1e0271140c95ca833a0110f2396e68518d7b1139

Line 22


```
{"timestamp":"2026-07-08T11:20:00.000000+0000","flow_id":2731975549,"event_type":"alert","src_ip
":"10.20.0.25","src_port":41000,"dest_ip":"203.0.113.80","dest_port":80,"proto":"TCP","ip_v":4,"
pkt_src":"stream (flow timeout)","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":90
00003,"rev":1,"signature":"TRACEHAWK LAB Nmap HTTP user agent scan","category":"Attempted
Information Leak","severity":1},"ts_progress":"request_complete","tc_progress":"response_started
","http":{"hostname":"lab-app.internal","url":"/.env","http_user_agent":"Nmap NSE lab probe","ht
tp_method":"GET","protocol":"HTTP/1.1","length":0},"app_proto":"http","direction":"to_server","f
low":{"pkts_toserver":3,"pkts_toclient":2,"bytes_toserver":253,"bytes_toclient":153,"start":"202
6-07-08T11:20:00.000000+0000","src_ip":"10.20.0.25","dest_ip":"203.0.113.80","src_port":41000,"d
est_port":80}}
```


SHA-256: ed55759a640c1bd36e10ac4745643ead5a7a6928403c5698ccef4d48bc99f978

Line 23


```
{"timestamp":"2026-07-08T11:20:00.000000+0000","flow_id":2731975549,"event_type":"http","src_ip"
:"10.20.0.25","src_port":41000,"dest_ip":"203.0.113.80","dest_port":80,"proto":"TCP","ip_v":4,"p
kt_src":"stream (flow
timeout)","tx_id":0,"http":{"hostname":"lab-app.internal","url":"/.env","http_user_agent":"Nmap
NSE lab probe","http_method":"GET","protocol":"HTTP/1.1","status":404,"length":0}}
```


SHA-256: dca401de9f6b96a08750344ff5168381bcff2967436a40614b9cf88f229a7b5f

Line 3


```
{"timestamp":"2026-07-08T11:20:43.199999+0000","flow_id":858989634115848,"pcap_cnt":23,"event_ty
pe":"dns","src_ip":"10.20.0.25","src_port":52003,"dest_ip":"10.20.0.53","dest_port":53,"proto":"
UDP","ip_v":4,"pkt_src":"wire/pcap","dns":{"version":3,"type":"request","tx_id":0,"id":17411,"fl
ags":"100","rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"a3.beacon-control.exampl
e","rrtype":"A"}]}}
```


SHA-256: a7150452810a1c048968831aeed5eb3b831c411f0855f6bee31464d9453597c6

Line 4


```
{"timestamp":"2026-07-08T11:21:03.199999+0000","flow_id":1984893022680349,"pcap_cnt":24,"event_t
ype":"alert","src_ip":"10.20.0.25","src_port":52004,"dest_ip":"10.20.0.53","dest_port":53,"proto
":"UDP","ip_v":4,"pkt_src":"wire/pcap","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_
id":9000004,"rev":1,"signature":"TRACEHAWK LAB DNS beacon-control query","category":"A Network
Trojan was detected","severity":1},"dns":{"version":3,"type":"request","tx_id":0,"id":17412,"fla
gs":"100","rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"a4.beacon-control.example
","rrtype":"A"}]},"app_proto":"dns","direction":"to_server","flow":{"pkts_toserver":1,"pkts_tocl
ient":0,"bytes_toserver":85,"bytes_toclient":0,"start":"2026-07-08T11:21:03.199999+0000","src_ip
":"10.20.0.25","dest_ip":"10.20.0.53","src_port":52004,"dest_port":53}}
```


SHA-256: d8684367dc4c72055743a2d6c72807d1174afedf16c5f8d19b0263b38afc028c

Line 5


```
{"timestamp":"2026-07-08T11:20:23.199999+0000","flow_id":1984890687060882,"pcap_cnt":22,"event_t
ype":"dns","src_ip":"10.20.0.25","src_port":52002,"dest_ip":"10.20.0.53","dest_port":53,"proto":
"UDP","ip_v":4,"pkt_src":"wire/pcap","dns":{"version":3,"type":"request","tx_id":0,"id":17410,"f
lags":"100","rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"a2.beacon-control.examp
le","rrtype":"A"}]}}
```


SHA-256: 890ea228ca419932dea7f6d7c4f183280a93fc60b10ed570c914877091c3f242

Line 6


```
{"timestamp":"2026-07-08T11:21:03.199999+0000","flow_id":1984893022680349,"pcap_cnt":24,"event_t
ype":"dns","src_ip":"10.20.0.25","src_port":52004,"dest_ip":"10.20.0.53","dest_port":53,"proto":
"UDP","ip_v":4,"pkt_src":"wire/pcap","dns":{"version":3,"type":"request","tx_id":0,"id":17412,"f
lags":"100","rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"a4.beacon-control.examp
le","rrtype":"A"}]}}
```


SHA-256: d418b371bf4e664c1f270b44db0a64019ea7864f58a8212d878a8ad99cfea51a

Line 7


```
{"timestamp":"2026-07-08T11:21:23.199999+0000","flow_id":858991076225460,"pcap_cnt":25,"event_ty
pe":"alert","src_ip":"10.20.0.25","src_port":52005,"dest_ip":"10.20.0.53","dest_port":53,"proto"
:"UDP","ip_v":4,"pkt_src":"wire/pcap","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_i
d":9000004,"rev":1,"signature":"TRACEHAWK LAB DNS beacon-control query","category":"A Network
Trojan was detected","severity":1},"dns":{"version":3,"type":"request","tx_id":0,"id":17413,"fla
gs":"100","rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"a5.beacon-control.example
","rrtype":"A"}]},"app_proto":"dns","direction":"to_server","flow":{"pkts_toserver":1,"pkts_tocl
ient":0,"bytes_toserver":85,"bytes_toclient":0,"start":"2026-07-08T11:21:23.199999+0000","src_ip
":"10.20.0.25","dest_ip":"10.20.0.53","src_port":52005,"dest_port":53}}
```


SHA-256: 9ce11843b973ea41ece6d4eb1402ea09a471d4ee7694d393a45b64b92224a853

Line 8


```
{"timestamp":"2026-07-08T11:20:03.199999+0000","flow_id":858990587745546,"pcap_cnt":21,"event_ty
pe":"alert","src_ip":"10.20.0.25","src_port":52001,"dest_ip":"10.20.0.53","dest_port":53,"proto"
:"UDP","ip_v":4,"pkt_src":"wire/pcap","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_i
d":9000004,"rev":1,"signature":"TRACEHAWK LAB DNS beacon-control query","category":"A Network
Trojan was detected","severity":1},"dns":{"version":3,"type":"request","tx_id":0,"id":17409,"fla
gs":"100","rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"a1.beacon-control.example
","rrtype":"A"}]},"app_proto":"dns","direction":"to_server","flow":{"pkts_toserver":1,"pkts_tocl
ient":0,"bytes_toserver":85,"bytes_toclient":0,"start":"2026-07-08T11:20:03.199999+0000","src_ip
":"10.20.0.25","dest_ip":"10.20.0.53","src_port":52001,"dest_port":53}}
```


SHA-256: 0b54539398658c179c2e9a7f25d4b41aec1a00ce2f7b23997b9431fc7fb571c2

Line 9


```
{"timestamp":"2026-07-08T11:21:23.199999+0000","flow_id":858991076225460,"pcap_cnt":25,"event_ty
pe":"dns","src_ip":"10.20.0.25","src_port":52005,"dest_ip":"10.20.0.53","dest_port":53,"proto":"
UDP","ip_v":4,"pkt_src":"wire/pcap","dns":{"version":3,"type":"request","tx_id":0,"id":17413,"fl
ags":"100","rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"a5.beacon-control.exampl
e","rrtype":"A"}]}}
```


SHA-256: 53750d5400b9d36cc2b34bf3274f9eb71a217071dd1d355343a476aa10e6de0c

Line 10

```
1783509600.829999    Cxv1l71694nuf2vaY8    10.20.0.25    41001    203.0.113.80    80    1    GET
    lab-app.internal    /wp-config.php    -    1.1    Nmap NSE lab probe    -    0    0    404
    Not Found    -    -    (empty)    -    -    -    -    -    -    -    -    -
```

SHA-256: 78a79e495bff318fcd6400765352bada0385399b3bda2e6b2e25c2a17168c90e

Line 11

```
1783509601.629999    CfmcFT2Sx2NJABguR8    10.20.0.25    41002    203.0.113.80    80    1    GET
    lab-app.internal    /admin    -    1.1    Nmap NSE lab probe    -    0    0    404    Not
Found    -    -    (empty)    -    -    -    -    -    -    -    -    -    -
```

SHA-256: 17f647e18c3eade732b2bb127957cf7e13f593ee45478ea53d444ba189830902

Line 12

```
1783509602.429999    C82q4qJEbKV3XiXIa    10.20.0.25    41003    203.0.113.80    80    1    GET
    lab-app.internal    /backup.zip    -    1.1    Nmap NSE lab probe    -    0    0    404
Not Found    -    -    (empty)    -    -    -    -    -    -    -    -    -    -
```

SHA-256: f4ecb818341f6762447d431a919356a1bdb25ffdee962dcb9266336fa3f89f26

Line 9

```
1783509600.029999    CfJXUp38wOx7cpBtea    10.20.0.25    41000    203.0.113.80    80    1    GET
    lab-app.internal    /.env    -    1.1    Nmap NSE lab probe    -    0    0    404    Not
Found    -    -    (empty)    -    -    -    -    -    -    -    -    -    -
```

SHA-256: 11544cbd40fd9e73087c17765b9703237f558b29b020394c5ce6f959bf33a2cc

Report Integrity Notes

- Findings are deterministic rule outputs.
- Evidence lines are copied from local logs and include content hashes.
- Assistant text, when present, is explanatory and does not alter findings.
- No cloud service is required to generate this report.