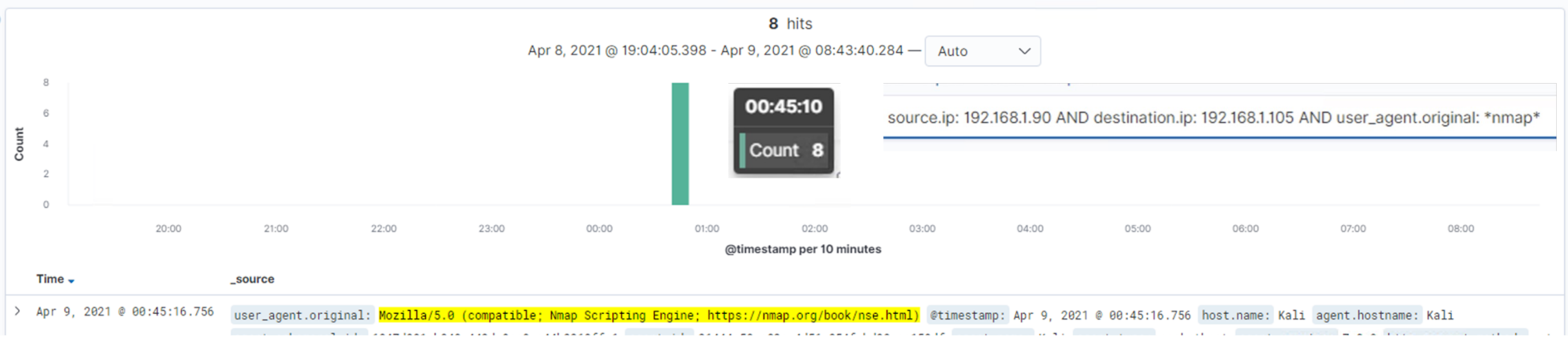
# Blue Team

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

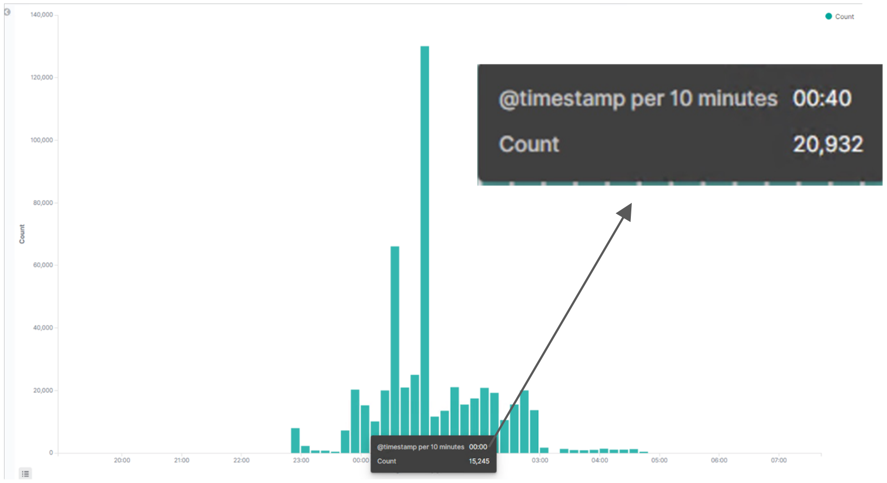


Apr 8, 2021 @ 19:04:05.398 - Apr 9, 2021 @ 08:43:40.284 —

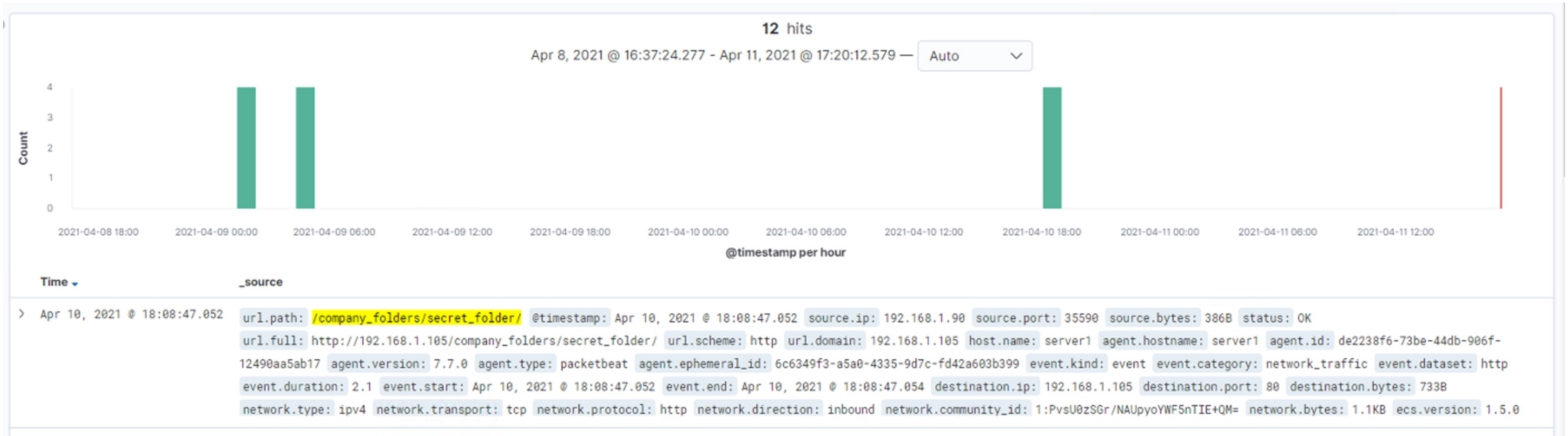
source.ip: 192.168.1.90 AND destination.ip: 192.168.1.105 AND user_agent.original: *nmap*

| Time | _source |
|---|---|
| Apr 9, 2021 @ 00:45:16.756 | user_agent.original: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html) @timestamp: Apr 9, 2021 @ 00:45:16.756 host.name: Kali agent.hostname: Kali |

- We know the port scan occurred at 0:45 on 04-09-2021 from 192.168.1.90
- After analyzing the network flow, we can approximate that 20,932 packets were sent during the scan.
- The user_agent was used to indicate that a port scan occurred by utilizing nmap (top).
- The network_flow indicated the amount of packets sent (right).

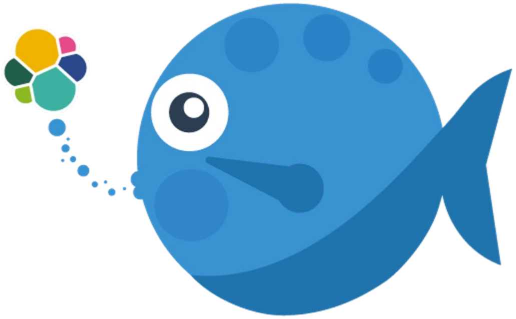


# Analysis: Finding the Request for the Hidden Directory

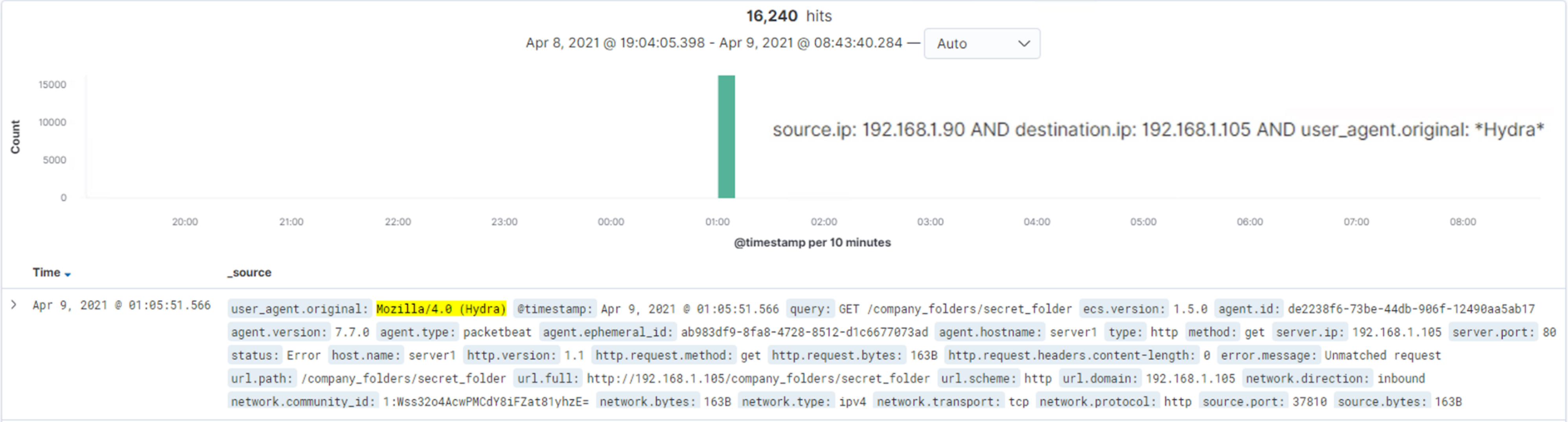


```
Time        _source
> Apr 10, 2021 @ 18:08:47.052   url.path: /company_folders/secret_folder/ @timestamp: Apr 10, 2021 @ 18:08:47.052 source.ip: 192.168.1.90 source.port: 35590 source.bytes: 386B status: OK
url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: http url.domain: 192.168.1.105 host.name: server1 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-
12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 6c6349f3-a5a0-4335-9d7c-fd42a603b399 event.kind: event event.category: network_traffic event.dataset: http
event.duration: 2.1 event.start: Apr 10, 2021 @ 18:08:47.052 event.end: Apr 10, 2021 @ 18:08:47.054 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 733B
network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:PvsU0zSGr/NAUpyoYWF5nTIE+QM= network.bytes: 1.1KB ecs.version: 1.5.0
```

- Requests for the hidden /secret_folder/ directory started at 1:00pm
- 12 Requests total were made from IP address 192.168.1.90
- The Connect_to_corp_server text file was the file that the attackers accessed.



# Analysis: Uncovering the Brute Force Attack



**16,240** hits

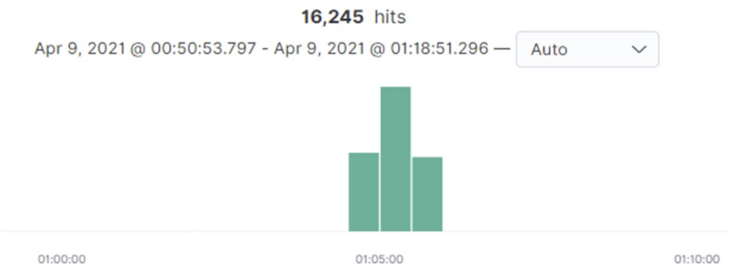
Apr 8, 2021 @ 19:04:05.398 - Apr 9, 2021 @ 08:43:40.284 —

source.ip: 192.168.1.90 AND destination.ip: 192.168.1.105 AND user_agent.original: *Hydra*

```
Time                      _source
> Apr 9, 2021 @ 01:05:51.566   user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Apr 9, 2021 @ 01:05:51.566 query: GET /company_folders/secret_folder ecs.version: 1.5.0 agent.id: de2238f6-73be-44db-906f-12490aa5ab17
                             agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: ab983df9-8fa8-4728-8512-d1c6677073ad agent.hostname: server1 type: http method: get server.ip: 192.168.1.105 server.port: 80
                             status: Error host.name: server1 http.version: 1.1 http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 error.message: Unmatched request
                             url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 network.direction: inbound
                             network.community_id: 1:Wss32o4AcwPMCdY8iFZat81yhzE= network.bytes: 163B network.type: ipv4 network.transport: tcp network.protocol: http source.port: 37810 source.bytes: 163B
```

16,245 requests were made during the attack.
16,240 requests were made by the attacker before the correct password was discovered.
A user_agent search was used to determine the attacking software used is Hydra (top)
An http.status_code: 401 search was used to determine the total attempts made (right).

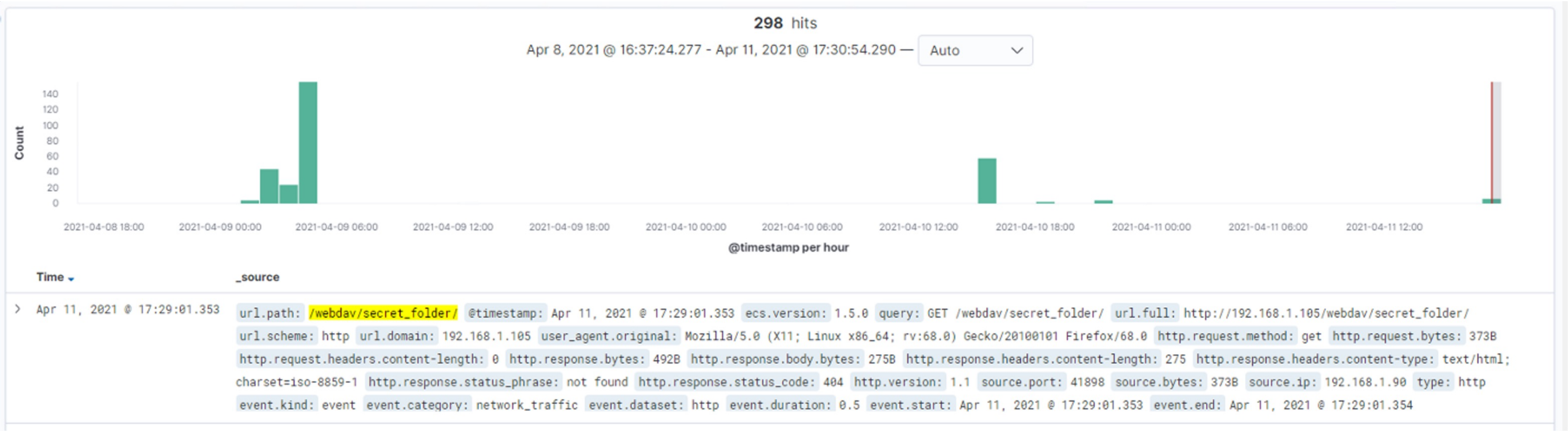
### HTTP 401 Unauthorized



**16,245** hits

Apr 9, 2021 @ 00:50:53.797 - Apr 9, 2021 @ 01:18:51.296 —

# Analysis: Finding the WebDAV Connection



**298** hits

Apr 8, 2021 @ 16:37:24.277 - Apr 11, 2021 @ 17:30:54.290 — Auto

| Time | _source |
|---|---|
| Apr 11, 2021 @ 17:29:01.353 | url.path: /webdav/secret_folder/ @timestamp: Apr 11, 2021 @ 17:29:01.353 ecs.version: 1.5.0 query: GET /webdav/secret_folder/ url.full: http://192.168.1.105/webdav/secret_folder/ url.scheme: http url.domain: 192.168.1.105 user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 http.request.method: get http.request.bytes: 373B http.request.headers.content-length: 0 http.response.bytes: 492B http.response.body.bytes: 275B http.response.headers.content-length: 275 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: not found http.response.status_code: 404 http.version: 1.1 source.port: 41898 source.bytes: 373B source.ip: 192.168.1.90 type: http event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.5 event.start: Apr 11, 2021 @ 17:29:01.353 event.end: Apr 11, 2021 @ 17:29:01.354 |

- 298 requests were made to the /WebDav folder during the attack
- The files requested were the passwd.dav file and the webdav.php file
- The webdav.php was the malicious payload that granted remote access to the attacker.

# Blue Team

## Proposed Alarms and Mitigation Strategies