

2015-02-24 - TRAFFIC ANALYSIS EXERCISE

SCENARIO

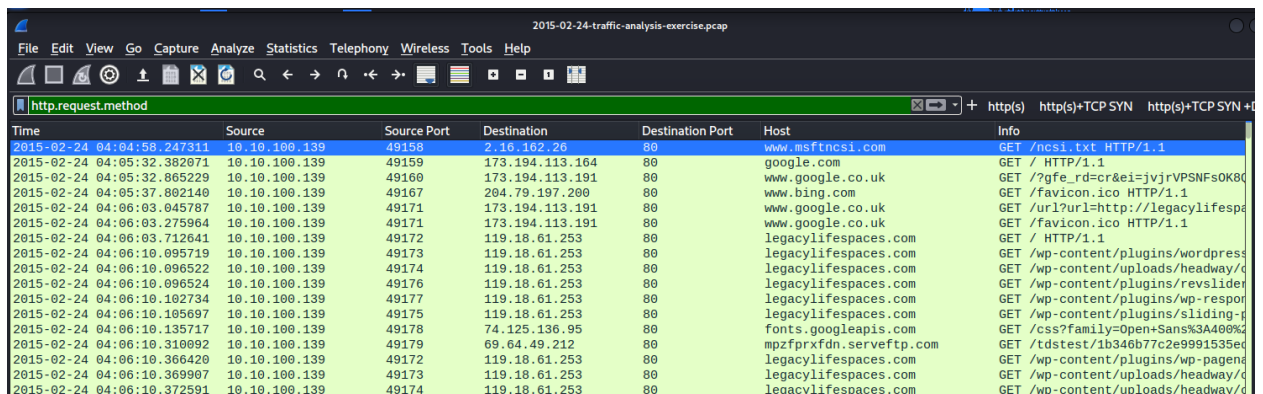
It's another evening shift at your organization's Security Operations Center (SOC). One of the analysts is looking through some traffic that occurred while your snort-based Intrusion Detection System (IDS) was off-line. The traffic had triggered a non-specific alert of possible malicious activity from another IDS.

The analyst is relatively new and is not experienced with malicious traffic. That analyst asks you for help.

- 1) Date and time of the activity

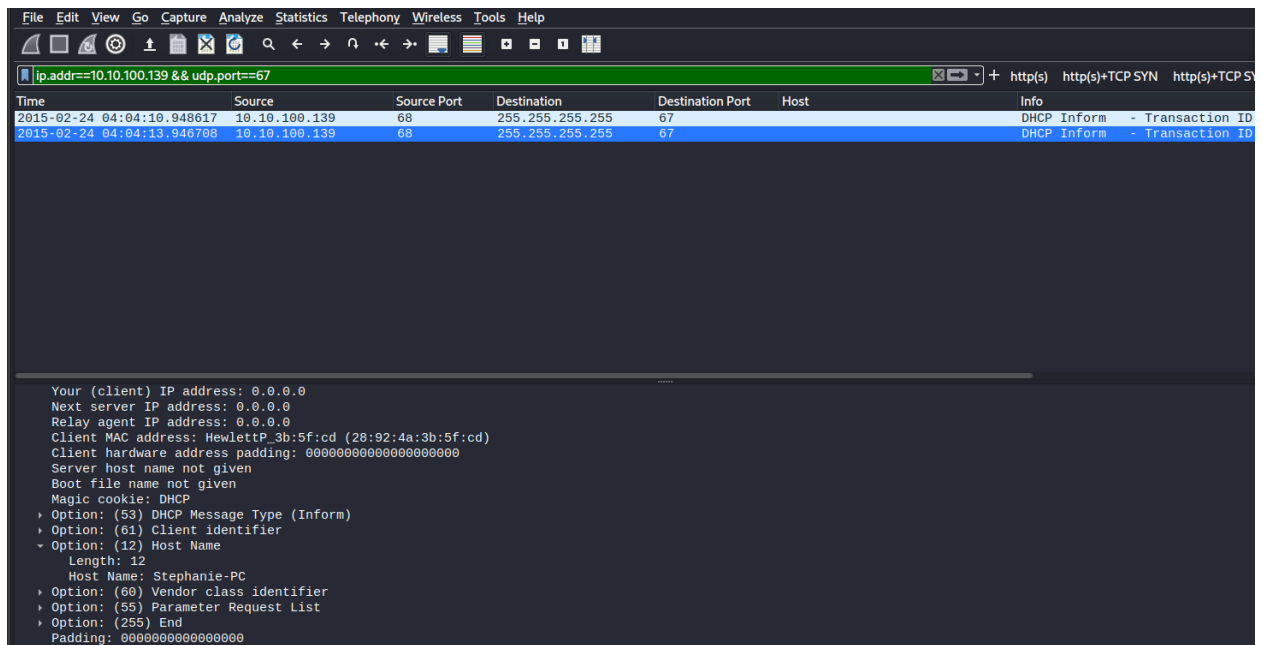
2015-02-24 4:04 to 4:07 UTC

- 2) IP address of the associated desktop (or laptop) computer
10.10.100.139

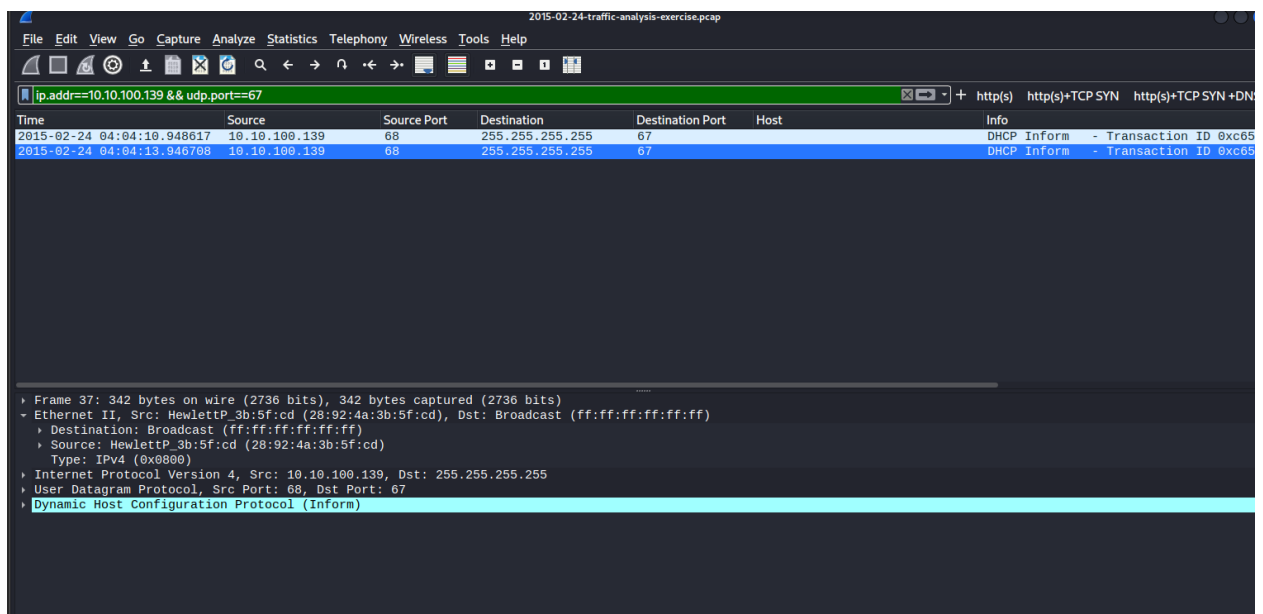


Time	Source	Source Port	Destination	Destination Port	Host	Info
2015-02-24 04:04:58.247311	10.10.100.139	49158	2.16.162.26	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
2015-02-24 04:05:32.382071	10.10.100.139	49159	173.194.113.164	80	google.com	GET / HTTP/1.1
2015-02-24 04:05:32.865229	10.10.100.139	49160	173.194.113.191	80	www.google.co.uk	GET /?gfe_rd=cr&ei=jvjrVPSNFsOK8Q
2015-02-24 04:05:37.802140	10.10.100.139	49167	204.79.197.200	80	www.bing.com	GET /favicon.ico HTTP/1.1
2015-02-24 04:06:03.045787	10.10.100.139	49171	173.194.113.191	80	www.google.co.uk	GET /url?url=http://legacylifesp
2015-02-24 04:06:03.275964	10.10.100.139	49171	173.194.113.191	80	www.google.co.uk	GET /favicon.ico HTTP/1.1
2015-02-24 04:06:03.712641	10.10.100.139	49172	119.18.61.253	80	legacylifespaces.com	GET / HTTP/1.1
2015-02-24 04:06:10.095719	10.10.100.139	49173	119.18.61.253	80	legacylifespaces.com	GET /wp-content/plugins/wordpress
2015-02-24 04:06:10.096522	10.10.100.139	49174	119.18.61.253	80	legacylifespaces.com	GET /wp-content/uploads/headway/d
2015-02-24 04:06:10.096524	10.10.100.139	49176	119.18.61.253	80	legacylifespaces.com	GET /wp-content/plugins/revslider
2015-02-24 04:06:10.102734	10.10.100.139	49177	119.18.61.253	80	legacylifespaces.com	GET /wp-content/plugins/wp-respor
2015-02-24 04:06:10.185697	10.10.100.139	49175	119.18.61.253	80	legacylifespaces.com	GET /wp-content/plugins/sliding-f
2015-02-24 04:06:10.135717	10.10.100.139	49178	74.125.136.95	80	fonts.googleapis.com	GET /css?family=Open+Sans%3A400%3
2015-02-24 04:06:10.310892	10.10.100.139	49179	69.64.49.212	80	mpzfprfxdn.serveftp.com	GET /tdstest/1b346b77c2e9991535ec
2015-02-24 04:06:10.366420	10.10.100.139	49172	119.18.61.253	80	legacylifespaces.com	GET /wp-content/plugins/wp-pagena
2015-02-24 04:06:10.369907	10.10.100.139	49173	119.18.61.253	80	legacylifespaces.com	GET /wp-content/uploads/headway/d
2015-02-24 04:06:10.372591	10.10.100.139	49174	119.18.61.253	80	legacylifespaces.com	GET /wp-content/uploads/headway/d

- 3) Host name of the associated desktop (or laptop) computer
Stephanie PC



- 4) MAC Address of the associated desktop or computer
28:92:4a:3b:5f:cd



- 5) Brief summary of the activity
User viewed a vulnerable website which has Fiesta exploit kit in it and was hit.

Visiting Compromised Site



Gate Redirection



Fiesta EK Landing Page



Exploitation



Installation