

1. Gunakan salah satu tools forensic dan beri penjelasan.

Pada tugas kali ini, penulis akan menggunakan salah satu tools forensic free for windows yang bernama "Network Miner". Apa itu Network Miner? Network Miner adalah alat analisis forensik jaringan (NFAT) untuk Windows. NetworkMiner dapat digunakan sebagai alat pengintai paket jaringan pasif yang dapat digunakan untuk mendeteksi sistem operasi, sesi, nama host, open port dll tanpa perlu menempatkan lalu lintas di jaringan secara langsung. NetworkMiner juga dapat menguraikan file PCAP untuk analisis off-line dan meregenerasi / menyusun kembali file yang dikirim dan sertifikat dari file PCAP.

Tujuan NetworkMiner adalah untuk mengumpulkan data (seperti bukti forensik) tentang host di jaringan, daripada mengumpulkan data mengenai lalu lintas jaringan. Tampilan utama adalah host centric (informasi dikelompokkan per host) daripada packet centric (informasi ditampilkan sebagai daftar paket / frame).

NetworkMiner melakukan OS fingerprinting berdasarkan TCP SYN dan SYN + ACK paket dengan menggunakan database OS fingerprinting dari p0f dan Ettercap. NetworkMiner juga dapat melakukan fingerprinting OS berdasarkan paket DHCP dengan memanfaatkan Satori OS fingerprinting database dari FingerBank. NetworkMiner juga menggunakan daftar vendor-MAC dari Nmap.

NetworkMiner dapat mengekstrak file dan sertifikat yang ditransfer melalui jaringan dengan memarsing file PCAP atau dengan menyadap lalu lintas langsung dari jaringan. Ini adalah salah satu fungsi yang apik yang dapat digunakan untuk mengekstrak dan menyimpan file media (seperti file audio atau video) yang dialirkan melalui jaringan. Protokol yang didukung untuk ekstraksi file adalah FTP, HTTP dan SMB.

Kredensial pengguna (nama pengguna dan kata sandi) untuk protokol yang didukung diekstrak oleh NetworkMiner dan ditampilkan di bawah tab "Kredensial". Maka dari pada itu, harap memperhatikan saat menampilkan konten dari tab ini ke publik.

Fitur lain yang sangat berguna adalah bahwa pengguna dapat mencari data yang disadap atau disimpan untuk kata kunci. NetworkMiner memungkinkan pengguna untuk memasukkan string arbitrary atau pola byte yang harus dicari dengan fungsi pencarian kata kunci.

Versi 0.84 (dan yang lebih baru) NetworkMiner telah support atau dapat digunakan untuk menyadap dan mengurai lalu lintas WLAN (IEEE 802.11). NetworkMiner saat ini hanya mendukung WiFi sniffing dengan adaptor AirPcap. Ada juga versi komersial yang tersedia dari NetworkMiner dari Netresec. Versi komersial disebut NetworkMiner Professional dan memiliki fitur tambahan seperti :

- Port Independent Protocol Identification (PIPI)
- Mengekspor hasil ke CSV / Excel
- Direktori keluaran file yang dapat dikonfigurasi
- Pelokalan Geo IP
- Dukungan pewarnaan tuan rumah
- Dukungan skrip baris perintah

Beberapa capture dari penggunaan Network Miner pada windows 10 :

NetworkMiner 2.3  
Socket: Realtek PCIe GBE Family Controller (10.100.203.18)

Hosts (279) | Files | Images | Messages | Credentials | Sessions (116) | DNS (624) | Parameters | Keywords | Anomalies

Sort Hosts On: IP Address (ascending) | Sort and Refresh

Hosts	IP Address
5.153.8.144	[vap.lit.com] [ap.lit.com] [sbaeacon.lit.com] [ce.lit.com]
5.153.15.173	[vap.lit.com] [ap.lit.com] [sbaeacon.lit.com] [ce.lit.com]
8.41.222.241	[sync.rhythmchange.com] [sync.lnx.io]
10.100.130.5	
10.100.130.10	
10.100.203.10	
10.100.203.18	[DESKTOP-N9V0GN0] (Windows)
10.100.203.255	
13.55.182.40	[n314.com]
13.57.1.30	[adserver-clarium-1718981494.us-west-1.elb.amazonaws.com] [protected-by-clarium.io]
13.107.21.200	[a-0001.msedge.net] [e-bing.com a-0001.msedge.net]
13.211.250.21	[n314.com]
13.228.101.4	[hgrn-bcp-stack-A-21488747.ap-southeast-1.elb.amazonaws.com] [jd.crowdfunder.net]
13.228.147.53	[as-eb-2.3ft.com] [eb-2.3ft.com]
13.228.187.7	[hgrn-bcp-stack-A-21488747.ap-southeast-1.elb.amazonaws.com] [jd.crowdfunder.net]
13.250.76.141	[as-eb-2.3ft.com] [eb-2.3ft.com]
18.195.251.238	[adserver-clarium-1405844056.eu-central-1.elb.amazonaws.com] [protected-by-clarium.io]
18.196.169.146	[hirdparty-logserver-b.global.prod1.sharethis.net] [pd.sharethis.com]
18.197.28.220	[hirdparty-logserver-b.global.prod1.sharethis.net] [pd.sharethis.com]
23.20.105.102	[match-us-east-1.sharethrough.com] [match.sharethrough.com]
23.67.4.112	[p13541.x.akamaiedge.net] [ags.bluekai.com edgekey.net]
34.202.122.19	[ix.powerlinks.com]
34.206.80.26	[match-us-east-1.sharethrough.com] [match.sharethrough.com]
34.224.45.160	[daas-production-us-east-1.elasticbeanstalk.com] [kadm.com]
34.233.49.149	
34.239.239.138	[match-us-east-1.sharethrough.com] [match.sharethrough.com]
34.241.170.25	[sync.adotmob.com]
34.248.51.249	[sync.adotmob.com]
34.248.254.195	[ec2eu-de-delivery-m3hpri9vc-1867114727.eu-west-1.elb.amazonaws.com] [ec2eu-de-1-vc-20170223.deliveryengine.adswitx.com]
34.252.51.85	[ec2eu-de-delivery-m3hpri9vc-1867114727.eu-west-1.elb.amazonaws.com] [ec2eu-de-1-vc-20170223.deliveryengine.adswitx.com]
35.156.203.184	[adserver-clarium-1405844056.eu-central-1.elb.amazonaws.com] [protected-by-clarium.io]
35.170.118.45	[sync.predicative.com]
35.187.194.39	[pcep.bidswitch.net]
35.187.209.206	[x.bidswitch.net] [baw.digtru.at]
35.187.209.245	[x.bidswitch.net] [baw.digtru.at]
35.187.219.92	[pcep.bidswitch.net]
35.187.221.61	[x.bidswitch.net] [baw.digtru.at]
35.189.131.178	[x.bidswitch.net] [baw.digtru.at]
35.189.137.99	[x.bidswitch.net] [baw.digtru.at]
35.189.138.118	[x.bidswitch.net] [baw.digtru.at]
35.189.141.94	[x.bidswitch.net] [baw.digtru.at]
35.200.52.77	[x.bidswitch.net] [baw.digtru.at]

Case Panel  
Filename: MD5  
NM\_201...

Reload Case Files

Buffered Frames to Parse:

NetworkMiner 2.3  
Socket: Realtek PCIe GBE Family Controller (10.100.203.18)

Hosts (289) | Files | Images | Messages | Credentials | Sessions (136) | DNS (688) | Parameters | Keywords | Anomalies

Sort Hosts On: IP Address (ascending) | Sort and Refresh

Hosts	IP Address
5.153.8.144	[vap.lit.com] [ap.lit.com] [sbaeacon.lit.com] [ce.lit.com]
5.153.15.173	[vap.lit.com] [ap.lit.com] [sbaeacon.lit.com] [ce.lit.com]
8.41.222.241	[sync.rhythmchange.com] [sync.lnx.io]
10.100.130.5	
10.100.130.10	
10.100.203.10	
10.100.203.18	[DESKTOP-N9V0GN0] (Windows)
10.100.203.255	
13.55.182.40	[n314.com]
13.57.1.30	[adserver-clarium-1718981494.us-west-1.elb.amazonaws.com] [protected-by-clarium.io]
13.107.21.200	[a-0001.msedge.net] [e-bing.com a-0001.msedge.net]
13.211.250.21	[n314.com]
13.228.101.4	[hgrn-bcp-stack-A-21488747.ap-southeast-1.elb.amazonaws.com] [jd.crowdfunder.net]
13.228.147.53	[as-eb-2.3ft.com] [eb-2.3ft.com]
13.228.187.7	[hgrn-bcp-stack-A-21488747.ap-southeast-1.elb.amazonaws.com] [jd.crowdfunder.net]
13.250.76.141	[as-eb-2.3ft.com] [eb-2.3ft.com]
18.195.251.238	[adserver-clarium-1405844056.eu-central-1.elb.amazonaws.com] [protected-by-clarium.io]
18.196.169.146	[hirdparty-logserver-b.global.prod1.sharethis.net] [pd.sharethis.com]
18.197.28.220	[hirdparty-logserver-b.global.prod1.sharethis.net] [pd.sharethis.com]
23.20.105.102	[match-us-east-1.sharethrough.com] [match.sharethrough.com]
23.67.4.112	[p13541.x.akamaiedge.net] [ags.bluekai.com edgekey.net]
34.202.122.19	[ix.powerlinks.com]
34.206.80.26	[match-us-east-1.sharethrough.com] [match.sharethrough.com]
34.224.45.160	[daas-production-us-east-1.elasticbeanstalk.com] [kadm.com]
34.233.49.149	
34.239.239.138	[match-us-east-1.sharethrough.com] [match.sharethrough.com]
34.241.170.25	[sync.adotmob.com]
34.248.51.249	[sync.adotmob.com]
34.248.254.195	[ec2eu-de-delivery-m3hpri9vc-1867114727.eu-west-1.elb.amazonaws.com] [ec2eu-de-1-vc-20170223.deliveryengine.adswitx.com]
34.252.51.85	[ec2eu-de-delivery-m3hpri9vc-1867114727.eu-west-1.elb.amazonaws.com] [ec2eu-de-1-vc-20170223.deliveryengine.adswitx.com]

Case Panel  
Filename: MD5  
NM\_201...

Reload Case Files

Buffered Frames to Parse:

IP: 10.100.203.18  
MAC: Unknown  
NIC Vendor: Unknown  
Hostname: DESKTOP-N9V0GN0  
OS: Windows  
TTL: 128 (distance: 0)  
Open TCP Ports:  
Sent: 6241 packets (1,012,946 Bytes), 0.00% cleartext (0 of 0 Bytes)  
Received: 176 packets (60,565 Bytes), 0.00% cleartext (0 of 0 Bytes)  
Incoming sessions: 0  
Outgoing sessions: 13  
Host Details

NetworkMiner 2.3

Socket: Realtek PCIe GBE Family Controller (10.100.203.18)

Hosts (290) Files Images Messages Credentials Sessions (160) DNS (697) Parameters Keywords Anomalies

Case Panel  
Filename MD5  
NM\_201...

Filter keyword:  Case sensitive ExactPhrase Any column Clear Apply

Frame nr.	Client h...	C. port	Server...	S. port	Protocol...	Start time
167	10.100...	61658	74.125...	443	Ssl	2018-04...
271	10.100...	61657	74.125...	443		2018-04...
273	10.100...	61660	74.125...	443		2018-04...
275	10.100...	61659	74.125...	443		2018-04...
413	10.100...	61675	74.125...	443	Ssl	2018-04...
1703	10.100...	61674	74.125...	443	Ssl	2018-04...
1687	10.100...	61673	74.125...	443	Ssl	2018-04...
44	10.100...	61678	74.125...	443		2018-04...
178	10.100...	61551	52.175...	443		2018-04...
271	10.100...	61657	74.125...	443		2018-04...
273	10.100...	61660	74.125...	443		2018-04...
275	10.100...	61659	74.125...	443		2018-04...
337	10.100...	61682	74.125...	443		2018-04...
277	10.100...	61680	74.125...	443		2018-04...
278	10.100...	61681	74.125...	443		2018-04...
941	10.100...	61721	52.196...	443		2018-04...
942	10.100...	61722	52.196...	443		2018-04...
429	10.100...	61686	74.125...	443		2018-04...
431	10.100...	61687	74.125...	443		2018-04...
1132	10.100...	61733	151.101...	443		2018-04...
823	10.100...	61705	72.34.2...	443		2018-04...
1443	10.100...	61770	64.124...	443		2018-04...
1527	10.100...	61777	208.100...	443		2018-04...
1351	10.100...	61753	104.193...	443		2018-04...
1349	10.100...	61751	104.193...	443		2018-04...
1491	10.100...	61775	64.124...	443		2018-04...
1350	10.100...	61752	104.193...	443		2018-04...
1592	10.100...	61780	208.100...	443		2018-04...
760	10.100...	61698	52.15.2...	443		2018-04...
1617	10.100...	61782	208.100...	443		2018-04...
1296	10.100...	61748	8.41.22...	443		2018-04...
952	10.100...	61723	35.203...	443		2018-04...
847	10.100...	61709	52.15.2...	443		2018-04...
976	10.100...	61724	67.231...	443		2018-04...
977	10.100...	61725	54.173...	443		2018-04...
1563	10.100...	61779	103.15...	443		2018-04...
1112	10.100...	61732	35.200...	443		2018-04...
928	10.100...	61718	13.107...	443		2018-04...
550	10.100...	61692	104.16...	443		2018-04...
552	10.100...	61694	104.16...	443		2018-04...

Buffered Frames to Parse:

Reload Case Files