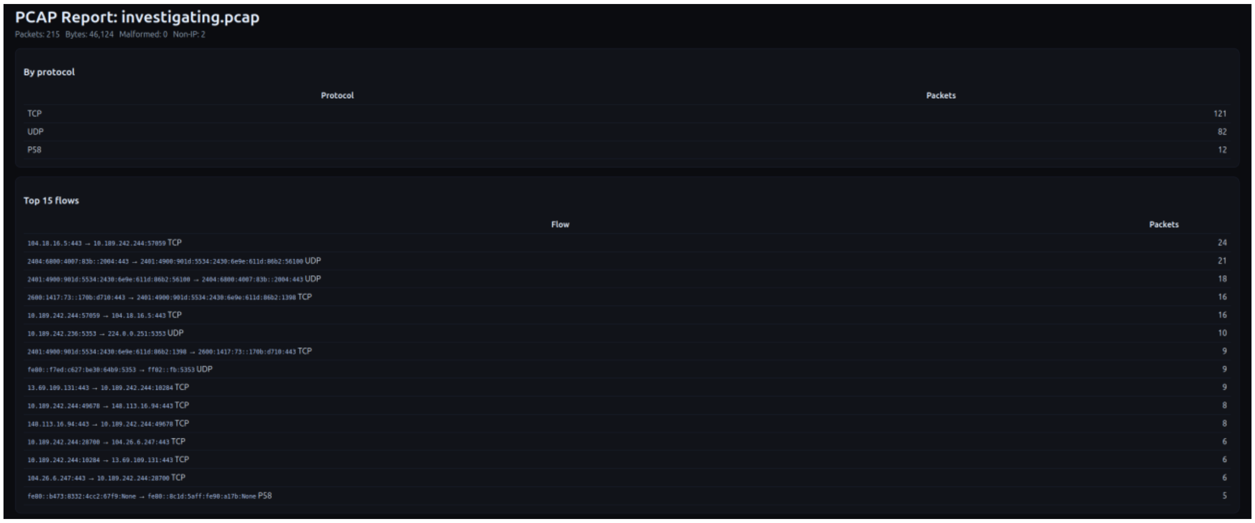


PCAP Report: investigating.pcap

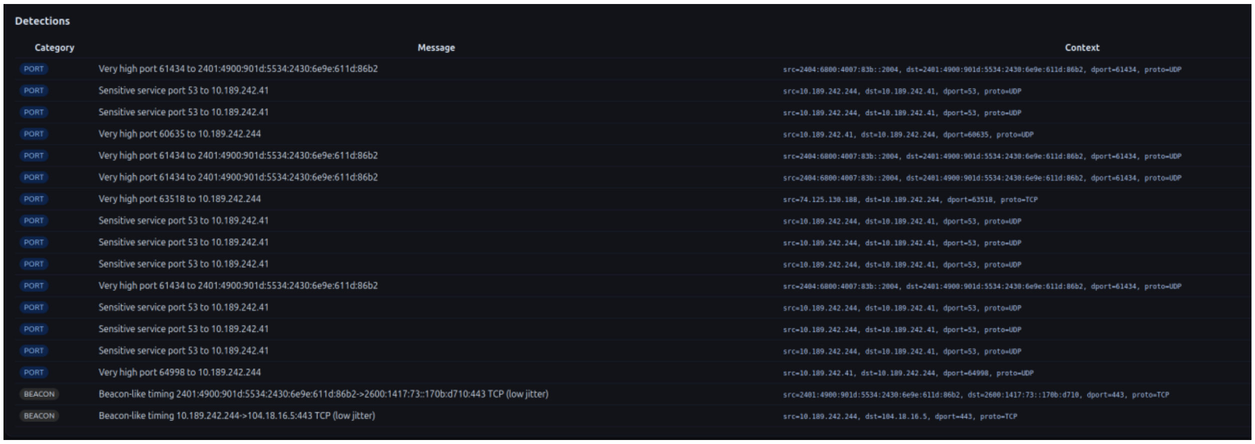
Packets: 215 Bytes: 46,124 Malformed: 0 Non-IP: 2

By protocol

Protocol	Packets
TCP	121
UDP	82
P58	12

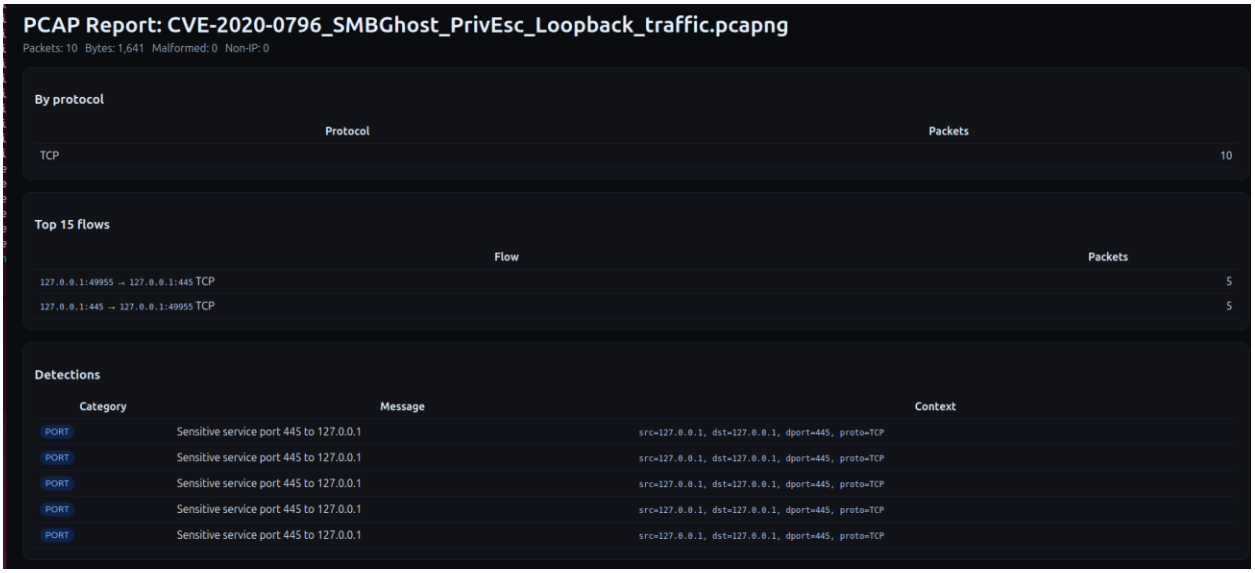
Top 15 flows

Flow	Packets
104.18.16.5:443 → 10.189.242.244:57059 TCP	24
2404:6800:4007:83b::2004:443 → 2401:4900:901d:5534:2430:6e9e:611d:86b2:56100 UDP	21
2401:4900:901d:5534:2430:6e9e:611d:86b2:56100 → 2404:6800:4007:83b::2004:443 UDP	18
2600:1417:73::170b:d710:443 → 2401:4900:901d:5534:2430:6e9e:611d:86b2:1398 TCP	16
10.189.242.244:57059 → 104.18.16.5:443 TCP	16
10.189.242.236:5353 → 224.0.0.251:5353 UDP	10
2401:4900:901d:5534:2430:6e9e:611d:86b2:1398 → 2600:1417:73::170b:d710:443 TCP	9
fe80::f7ed:c627:be30:64b9:5353 → ff02::fb:5353 UDP	9
13.69.109.131:443 → 10.189.242.244:10284 TCP	9
10.189.242.244:49678 → 148.113.16.94:443 TCP	8
148.113.16.94:443 → 10.189.242.244:49678 TCP	8
10.189.242.244:28700 → 104.26.6.247:443 TCP	6
10.189.242.244:10284 → 13.69.109.131:443 TCP	6
104.26.6.247:443 → 10.189.242.244:28700 TCP	6
fe80::b473:8332:4cc2:67f9:None → fe80::8c1d:5aff:fe90:a17b:None P58	5



Detections

Category	Message	Context
PORT	Very high port 61434 to 2401:4900:901d:5534:2430:6e9e:611d:86b2	`src=2404:6800:4007:83b::2004, dst=2401:4900:901d:5534:2430:6e9e:611d:86b2, dport=61434, proto=UDP`
PORT	Sensitive service port 53 to 10.189.242.41	`src=10.189.242.244, dst=10.189.242.41, dport=53, proto=UDP`
PORT	Sensitive service port 53 to 10.189.242.41	`src=10.189.242.244, dst=10.189.242.41, dport=53, proto=UDP`
PORT	Very high port 60635 to 10.189.242.244	`src=10.189.242.41, dst=10.189.242.244, dport=60635, proto=UDP`
PORT	Very high port 61434 to 2401:4900:901d:5534:2430:6e9e:611d:86b2	`src=2404:6800:4007:83b::2004, dst=2401:4900:901d:5534:2430:6e9e:611d:86b2, dport=61434, proto=UDP`
PORT	Very high port 61434 to 2401:4900:901d:5534:2430:6e9e:611d:86b2	`src=2404:6800:4007:83b::2004, dst=2401:4900:901d:5534:2430:6e9e:611d:86b2, dport=61434, proto=UDP`
PORT	Very high port 63518 to 10.189.242.244	`src=74.125.130.188, dst=10.189.242.244, dport=63518, proto=TCP`
PORT	Sensitive service port 53 to 10.189.242.41	`src=10.189.242.244, dst=10.189.242.41, dport=53, proto=UDP`
PORT	Sensitive service port 53 to 10.189.242.41	`src=10.189.242.244, dst=10.189.242.41, dport=53, proto=UDP`
PORT	Sensitive service port 53 to 10.189.242.41	`src=10.189.242.244, dst=10.189.242.41, dport=53, proto=UDP`
PORT	Very high port 61434 to 2401:4900:901d:5534:2430:6e9e:611d:86b2	`src=2404:6800:4007:83b::2004, dst=2401:4900:901d:5534:2430:6e9e:611d:86b2, dport=61434, proto=UDP`
PORT	Sensitive service port 53 to 10.189.242.41	`src=10.189.242.244, dst=10.189.242.41, dport=53, proto=UDP`
PORT	Sensitive service port 53 to 10.189.242.41	`src=10.189.242.244, dst=10.189.242.41, dport=53, proto=UDP`
PORT	Sensitive service port 53 to 10.189.242.41	`src=10.189.242.244, dst=10.189.242.41, dport=53, proto=UDP`
PORT	Very high port 64998 to 10.189.242.244	`src=10.189.242.41, dst=10.189.242.244, dport=64998, proto=UDP`
BEACON	Beacon-like timing 2401:4900:901d:5534:2430:6e9e:611d:86b2->2600:1417:73::170b:d710:443 TCP (low jitter)	`src=2401:4900:901d:5534:2430:6e9e:611d:86b2, dst=2600:1417:73::170b:d710, dport=443, proto=TCP`
BEACON	Beacon-like timing 10.189.242.244->104.18.16.5:443 TCP (low jitter)	`src=10.189.242.244, dst=104.18.16.5, dport=443, proto=TCP`



PCAP Report: CVE-2020-0796_SMBGhost_PrivEsc_Loopback_traffic.pcapng

Packets: 10 Bytes: 1,641 Malformed: 0 Non-IP: 0

By protocol

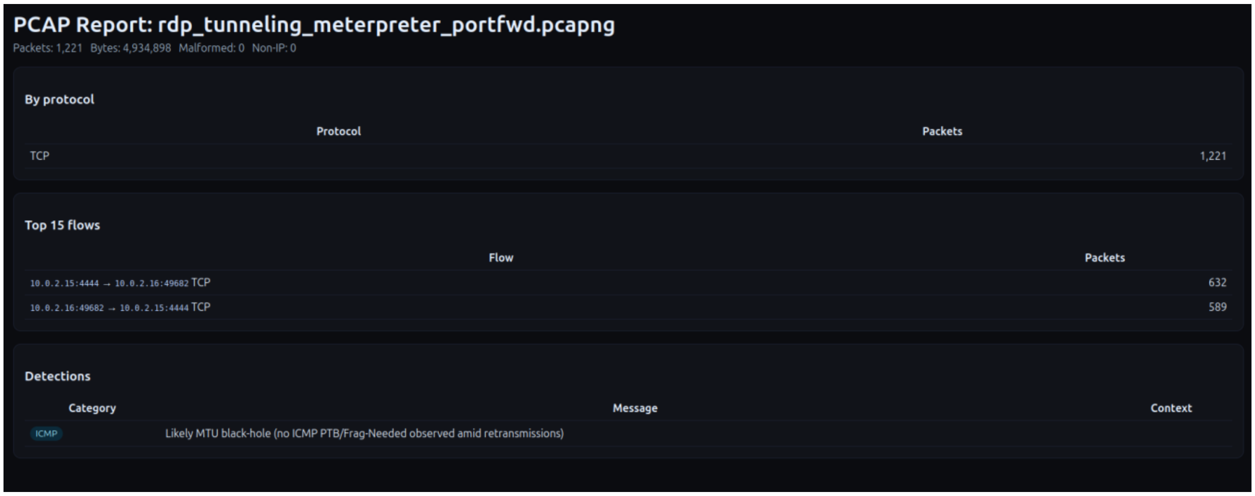
Protocol	Packets
TCP	10

Top 15 flows

Flow	Packets
`127.0.0.1:49955 → 127.0.0.1:445` TCP	5
`127.0.0.1:445 → 127.0.0.1:49955` TCP	5

Detections

Category	Message	Context
PORT	Sensitive service port 445 to 127.0.0.1	`src=127.0.0.1, dst=127.0.0.1, dport=445, proto=TCP`
PORT	Sensitive service port 445 to 127.0.0.1	`src=127.0.0.1, dst=127.0.0.1, dport=445, proto=TCP`
PORT	Sensitive service port 445 to 127.0.0.1	`src=127.0.0.1, dst=127.0.0.1, dport=445, proto=TCP`
PORT	Sensitive service port 445 to 127.0.0.1	`src=127.0.0.1, dst=127.0.0.1, dport=445, proto=TCP`
PORT	Sensitive service port 445 to 127.0.0.1	`src=127.0.0.1, dst=127.0.0.1, dport=445, proto=TCP`



PCAP Report: rdp_tunneling_meterpreter_portfwd.pcapng

Packets: 1,221 Bytes: 4,934,898 Malformed: 0 Non-IP: 0

By protocol

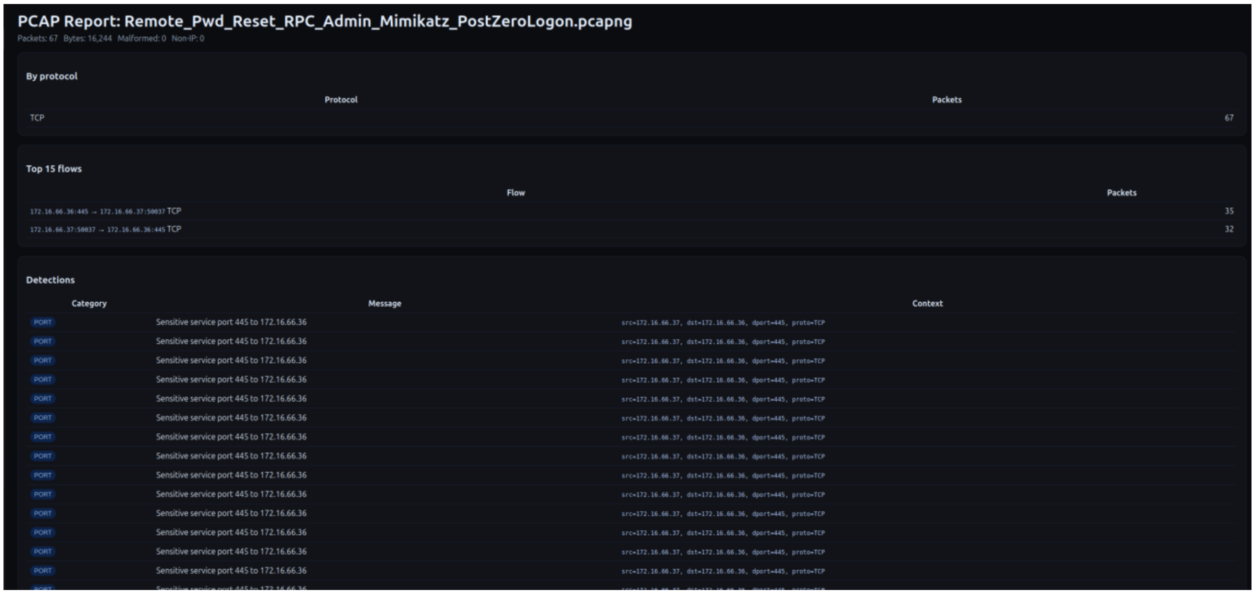
Protocol	Packets
TCP	1,221

Top 15 flows

Flow	Packets
10.0.2.15:4444 → 10.0.2.16:49682 TCP	632
10.0.2.16:49682 → 10.0.2.15:4444 TCP	589

Detections

Category	Message	Context
ICMP	Likely MTU black-hole (no ICMP PTB/Frag-Needed observed amid retransmissions)	



PCAP Report: Remote_Pwd_Reset_RPC_Admin_Mimikatz_PostZeroLogon.pcapng

Packets: 67 Bytes: 16,244 Malformed: 0 Non-IP: 0

By protocol

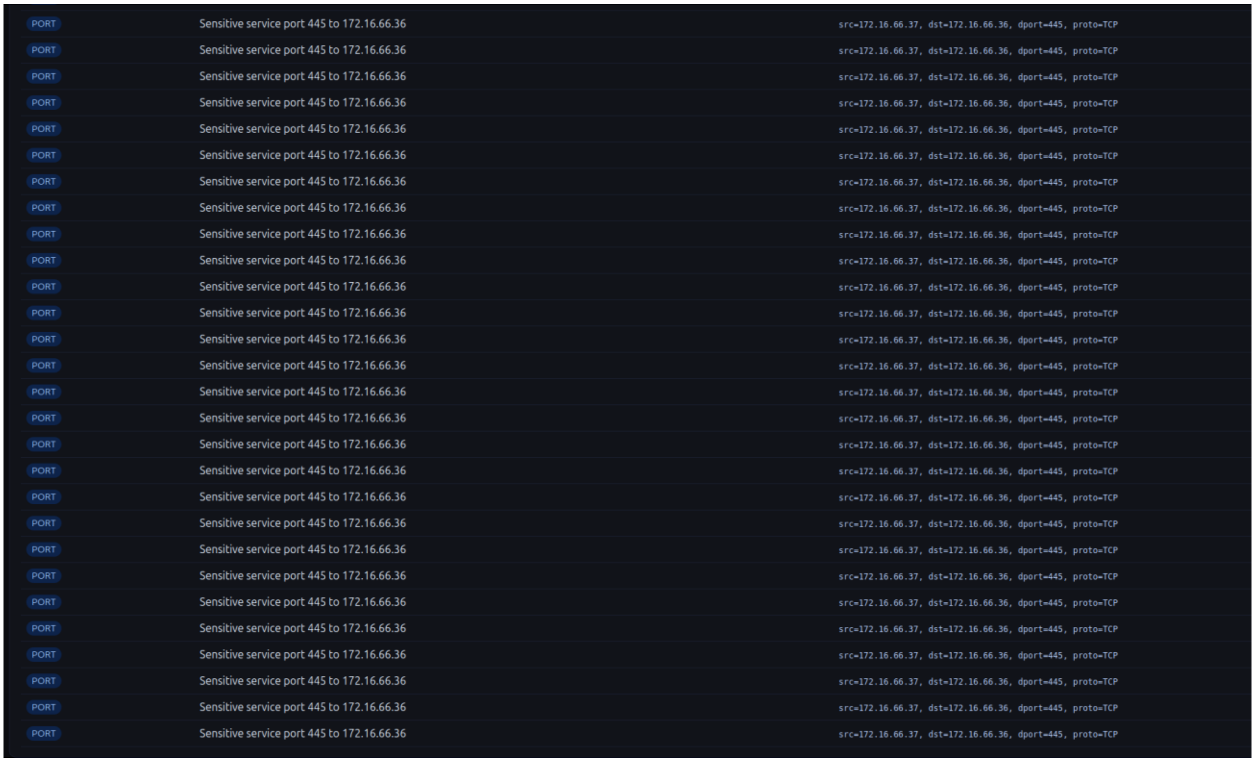
Protocol	Packets
TCP	67

Top 15 flows

Flow	Packets
172.16.66.36:445 → 172.16.66.37:50037 TCP	35
172.16.66.37:50037 → 172.16.66.36:445 TCP	32

Detections

Category	Message	Context
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP



PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP
PORT	Sensitive service port 445 to 172.16.66.36	src=172.16.66.37, dst=172.16.66.36, dport=445, proto=TCP