

Network Intrusion Detection Report

Project Title: Network Intrusion Detection using Zeek and Wireshark

Analyst: Brett Banks

Environment: Kali Linux (Attacker) + Windows 10 (Target) | Host-Only VirtualBox Network

Tools: Zeek, Wireshark, tcpdump, FTP, nslookup, nmap

Date: June 01, 2025

🌟 Objective

To simulate and detect malicious network behaviors including insecure credential transmission, DNS tunneling, and port scanning. Analyze traffic using Zeek to extract indicators, evaluate the threat, and summarize actionable findings as would be done in a SOC environment.

🔧 Lab Setup


| Component | Configuration |
|--------------|---------------------------------------|
| Kali Linux | Attacker / Monitor (Wireshark + Zeek) |
| Windows 10 | Victim with FTP service enabled |
| Network Type | Host-Only Adapter (192.168.84.0/24) |
| Capture Tool | tcpdump -i eth1 -w ftp_test.pcap |

📸 Screenshot – Interface Configuration and NAT:

```
--$ sudo dhclient eth0

(kali@kali)~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8e:f4:e6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic eth0
        valid_lft 584sec preferred_lft 584sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:95:88:e8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.84.104/24 brd 192.168.84.255 scope global dynamic noprefixroute eth1
        valid_lft 497sec preferred_lft 497sec
    inet6 fe80::a00:27ff:fe95:88e8/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)~$ ping google.com
PING google.com (142.251.32.46) 56(84) bytes of data:
64 bytes from sfo03s26-in-14.1e100.net (142.251.32.46): icmp_seq=1 ttl=251 time=28.4 ms
64 bytes from sfo03s26-in-14.1e100.net (142.251.32.46): icmp_seq=2 ttl=251 time=29.0 ms
64 bytes from sfo03s26-in-14.1e100.net (142.251.32.46): icmp_seq=3 ttl=251 time=23.0 ms
```

 Screenshot – tcpdump capturing FTP traffic:

```
(kali@kali)~$ sudo tcpdump -i eth0 -w capture.pcap
[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), sn
apshot length 262144 bytes
```



Attack Simulation Actions

FTP Login with Cleartext Credentials

Command: ftp 192.168.84.102

Used fake creds: testuser / weakpass



Zeek Output Analysis

Connection Log (conn.log)

```
kali@kali:~/zeek-run
File Actions Edit View Help
kali@kali:~/zeek-run x kali@kali:~ x
ls -ln *.log
-rw-r--r-- 1 root root 888 Jun 1 12:01 conn.log
-rw-r--r-- 1 root root 559 Jun 1 12:01 dhcp.log
-rw-r--r-- 1 root root 278 Jun 1 12:01 packet_filter.log
$ exit

(kali@kali)~/zeek-run
$ cat conn.log | head -n 20

#separator \n
set_separator (
  empty_field (empty)
  unset_field -
  path conn
  open 2025-06-01-12-01-27
#fields ts uid id.orig_h id.orig_p id.resp_h id.resp_p proto service duration resp_pkt orig_bytes resp_bytes conn
state local_orig local_resp missed_bytes history orig_pkt orig_ip_bytes count string interval count string bool bool count string count coun
t count count set(string) count
1748778498.176839 0x0f333232505056 192.168.84.104 68 192.168.84.2 67 udp dhcp 0.015268 282 548 SF T T
0 0 1 318 1 576 - 17
1748778472.867176 0x0a112233445556 192.168.84.104 57870 192.168.84.102 21 tcp ftp 24.997800 42 236 51 T T
0 0 19 462 36 648 - 8
1748778447.948323 0x2e1huANHcPTLGz 192.168.84.103 50952 239.255.255.254 1988 udp - 3.001069 274 0 50 T T
0 0 2 338 0 0 - 17
fclose 2025-06-01-12-01-27

(kali@kali)~/zeek-run
$
```



Findings Summary

1. FTP Credential Exposure

Protocol: FTP (port 21)

Credential: USER testuser, PASS weakpass

Risk: Exposed credentials could be intercepted on flat networks

Mitre Mapping: T1078 – Valid Accounts



Conclusion

This lab demonstrated how basic attacker techniques can be detected with Zeek when cleartext protocols like FTP are used. Zeek successfully logged the session metadata through conn.log. With additional analyzers or forced module loading, full FTP logging could also be observed.