SECURITY ONION

PEEL BACK THE LAYERS OF YOUR NETWORK

About Security Onion

- Security Onion is a Linux distro for intrusion for intrusion detcetion, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

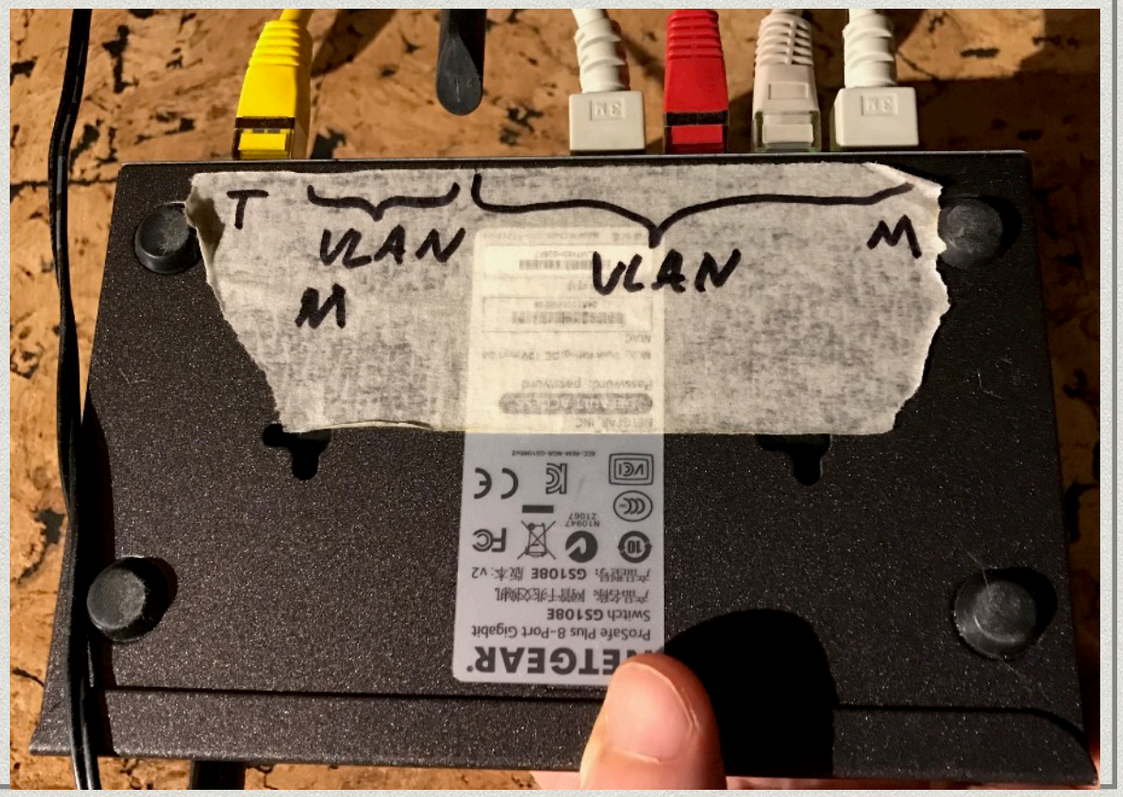
Sniffer-Setup - Switch

- Netgear GS108E
- Vorteile:
  - Billig (5 Port 30€, 8 Port 40€)
  - Funktioniert
  - VLANs
- Nachteile:
  - Scheiss Software (Adobe Air, Broadcast)
- https://www.amazon.de/dp/B00GWKN1Q2/

NETGEAR

Produktmerkmale

- IEEE 802.1Q VLAN Tagging
- Port-based VLAN
- Port-based VLAN
- Port Trunking
- Port Mirroring
- Priority queuing
- Jumbo frame support
- IGMP Snooping (v1, v2 and v3)
- IEEE 802.1p COS
- DHCP Client
- WRED (Weighted Deficit Round Robin)
- Strict Priority queue technology

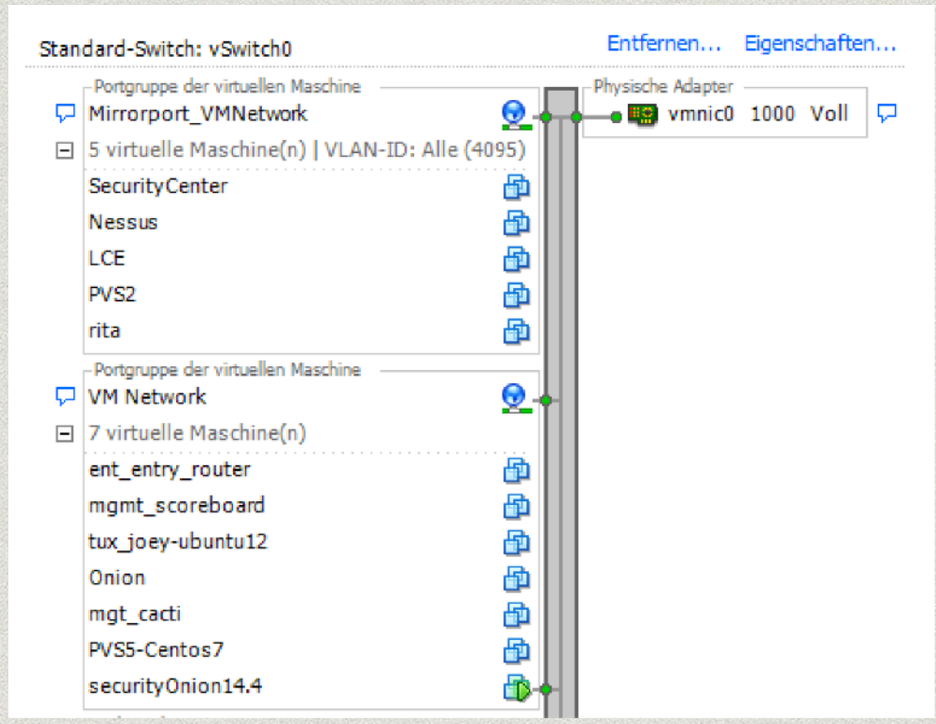


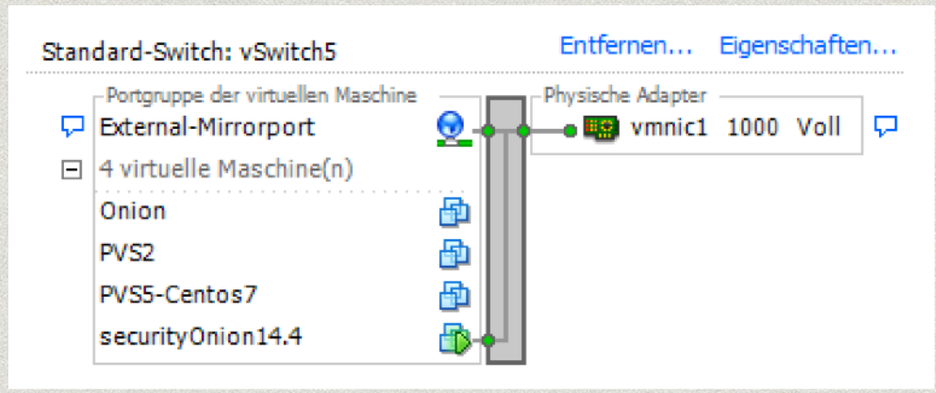
Sniffer-Setup - Server 1/2

- HP Microserver Gen8
- HP RAID 0/1, Dualcore Celeron, 4GB RAM = 170€
- Aufgerüstet: XEON Quadcore CPU + RAID 5 Controller + 16GB RAM
- https://www.amazon.de/dp/B013UBCHVU/
- 2 Netzwerkkarten!

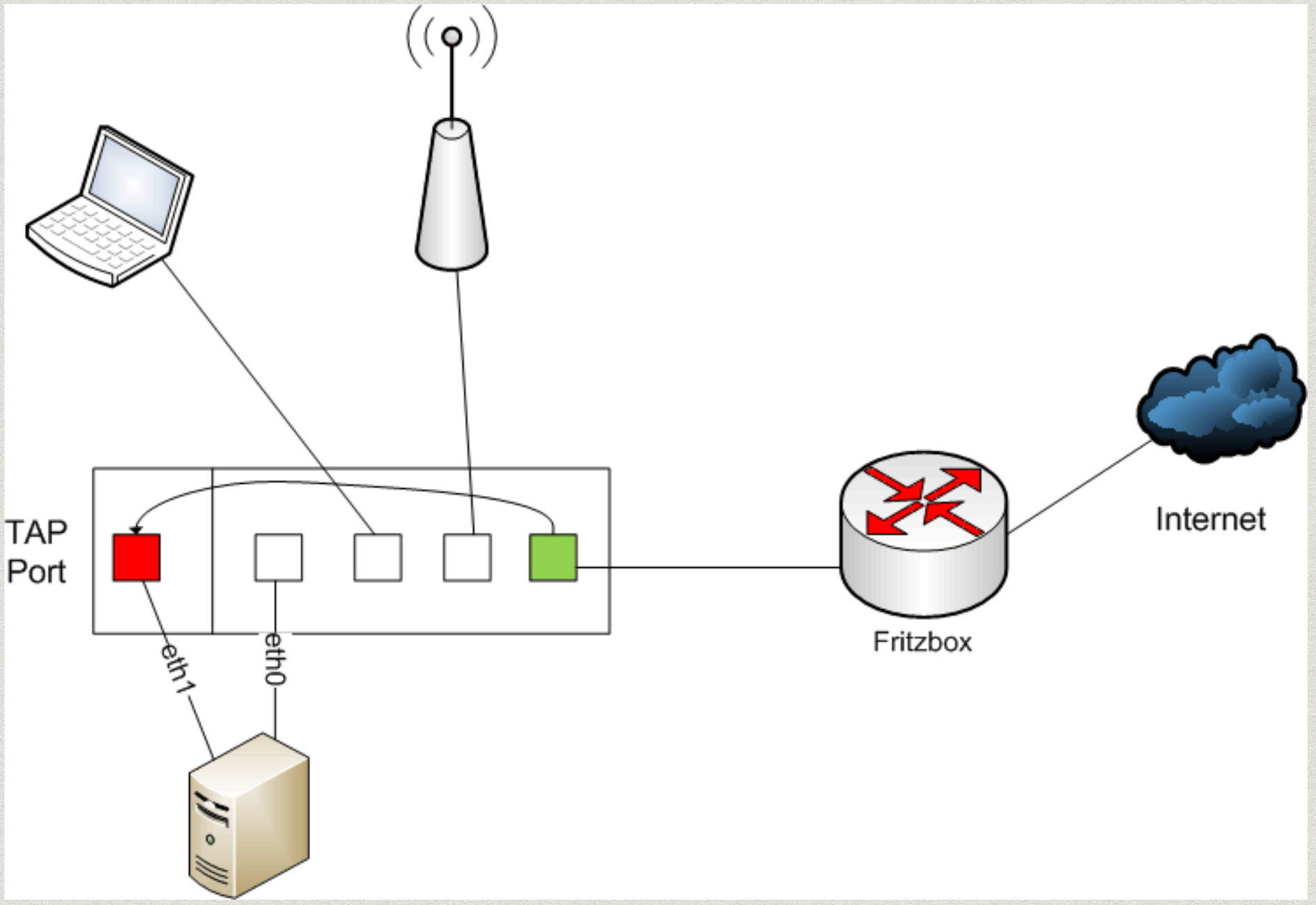
Sniffer-Setup - Server 2/2

- VMWare VSphere Hypervisor (ESXi, kostenlos)
- Port 1 Management SO-VM
- Port 2 Mirror Traffic SO-VM



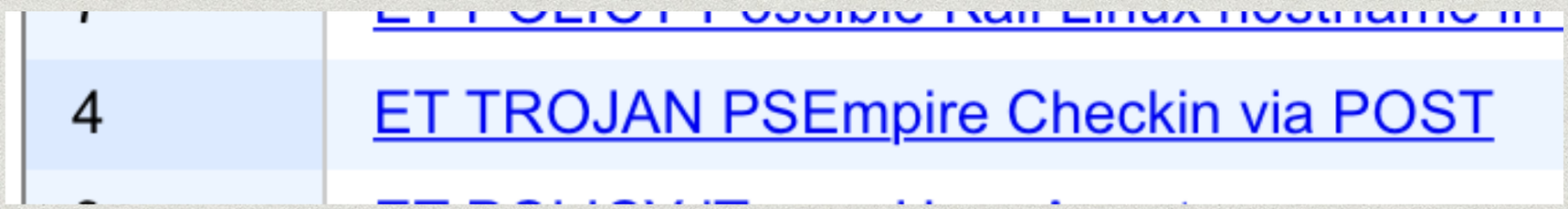


Sniffer-Setup - Netzwerk

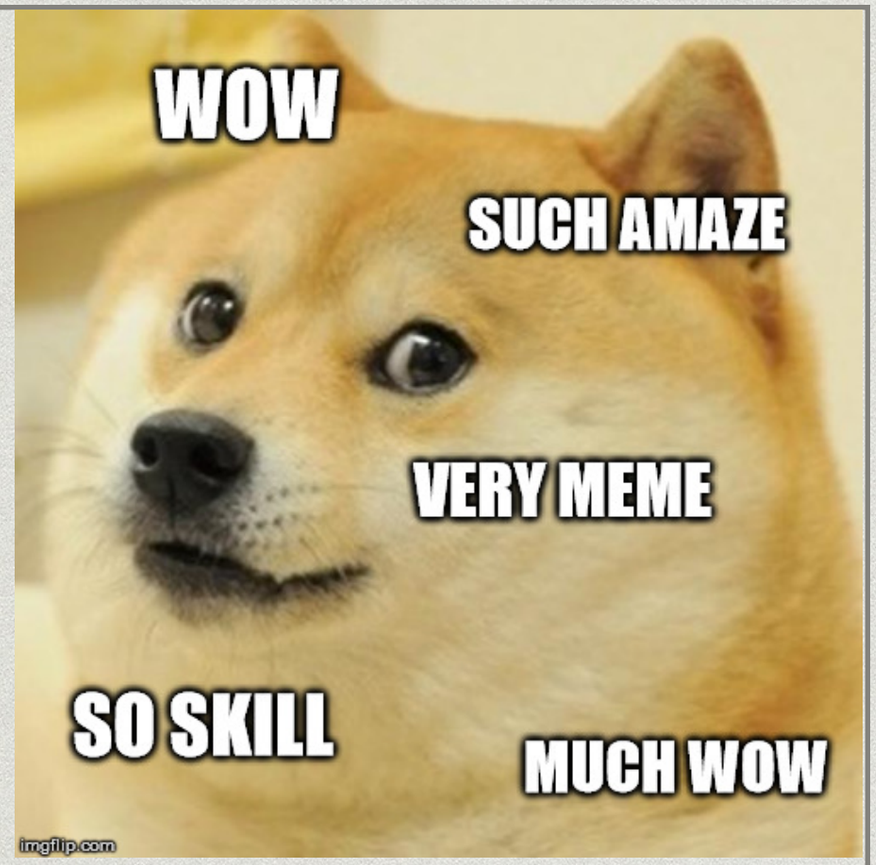


Snort

- Open Sourec IDS
- 1998 von Gründer von Sourcefire entwickelt
- Sourcefire wurde 2013 von Cisco gekauft
- Kostenlose feeds!
- Kann das gut sein?



BRO IDS



- much Packets so WOW
- Eigentlich kein IDS
- Netzwerk Analyse Tool
- Eigene Netzwerk-Analyse Programmiersprache
- Auf die ich hier heute nicht weiter eingehe! :-)

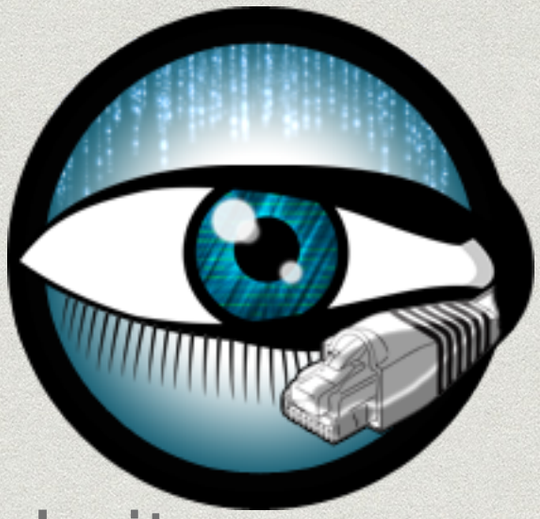
Bro Beispiel

- HTTP Useragents!
- Wie verbindet sich Malware ins Internet zurück
- Über HTTP!
- zcat http* | bro-cut user_agent | sort | uniq -c | sort -n

Bro Beispiel

- Welche DNS TXT Queries wurden abgesetzt?
- zcat dns* | bro-cut qtype_name query | grep TXT| sort | uniq -c | sort -n

Bro Beispiel



- Was für SSL Zertifikate (x509) sind über die Leitung gegangen?
- Waren da noch SHA1 dabei?
- Auslaufdatum?
- Issuer?
- cat x509.log | bro-cut -u certificate.key_alg certificate.not_valid_after certificate.subject | sort | uniq -c | sort -n

Bro Beispiel

- Was für Datein sind über die Leitung gegangen?
  - zcat files*
  - okay unübersichtlich, erstmal nur Dateinamen!
  - zcat files* | bro-cut filename | sort | uniq -c | sort -n

Bro Beispiel

- Notice log!
- Ne menge SSL Zertifikatswarnungen!
- was bleibt über wenn man die rausfiltert?
- Siehe 2016-11-13:
- zcat notice* | bro-cut id.orig_h id.resp_h msg | grep -v "SSL certificate" | sort | uniq -c | sort -n

Bro Beispiel

- Bro extrahiert Datein aus dem Datenstrom (solange sie nicht verschlüsselt übertragen werden)
- Automatisiert Prüfen lassen?
- root@kali:/usr/share/metasploit-framework/tools/exploit/virustotal.rb

Too much cli! ELSA

- https://192.168.0.220