Unified Threat Management

Introduction

Message Capture

Log Analysis

SNMP

Netflow

SNMP Traps

Proxy Services

Unified Threat Management

Authentication

Network Discovery

Monitoring and Log Management

Unified Threat Management Systems

- In typical networks, individual hosts and servers are responsible for securing the services they provide (e.g. routers should selectively route, web servers should sanitize requests and results, mail servers should run antivirus and antispam tools, etc.)
- A significant percentage of problematic access and data does not necessarily originate on the hosts or servers, but instead may arrive from other machines over the network
- Implementing security defense only at the service host can significantly decrease the complexity and difficulty of successfully breaching it, layering is the preferred approach

UTM Concept

- Unified threat management takes advantage of the proxy concept to simplify threat management by consolidating a set of threat management activities on a single host or group of hosts and adding that as a defense layer external to the hosts being protected
- This requires inserting a threat management device into the network physically between your service provision machines and the service consumption entities, i.e. creating a choke point for traffic
- Since traffic is funnelled through one or more choke points, we can not only measure and manipulate that traffic, we can inspect it for unwanted characteristics such as content, ip address, or protocol
- Traffic content blocking or substitution can be done on the choke point machine(s) based on the result of the inspection, to a much greater level than a firewall without impacting the content server

UTM Advantages

- UTMS can provide benefits in the right situations
- Consolidating functions into a single piece of hardware, or group of machines can reduce the overall cost of those functions
- Using UTMs can reduce the complexity of server monitoring and maintenance
- Single sourcing UTMs can greatly simplify vendor contracts for equipment, software, and support as well as streamlining your change management
- UTMs can be implemented in virtual machines to improve scalability and reduce downtime in the event of a change activity or security incident

UTM Disadvantages

- UTMs without redundancy introduce a single point of failure which may not have existed without the UTM
- UTMs can significantly impact your network performance if they are not actively managed and sized appropriately
- UTMs can create a false sense of security if they do not cover all normal traffic patterns for your network (e.g. might secure POP3, but not IMAP4)
- UTMS only handle traffic which passes through them, so you still require some ability to handle threats on internal hosts and servers, layers still matter

Deployment Choices

- Build a definition of functionality required and then research both hardware and software products which provide that functionality
- pfsense can perform many functions as a UTM mainly through addon packages, you can also handcraft a UTM on any Linux system using quagga, iptables, clamav, squid, spamassassin, etc. as required
- Watchguard, Sophos, Fortinet, and Cisco sell small business products
- CheckPoint, Dell, Fortinet, and Juniper sell enterprise grade products
- There are many other vendors and products, most are designed to perform threat management on a routing device
- Some consumer grade routers include limited UTM functionality

Inline UTM

- A UTM can be installed as a router or a bridge, both configurations can be set up for transparent traffic inspection, both configurations need to use at least 2 physically separate interfaces to reduce the potential for traffic to bypass your UTM
- If you build your UTM as a router, turn on ip_forward and set up routes as required on the UTM
- To configure it as an inline or bridged server, we need to set up the interfaces to do bridging and turn on ip_forward, no routing needs to be configured on the UTM or anywhere else in the network
- There are no decisive advantages or disadvantages specific to threat management with either approach
- UTMs can significantly impact throughput and require the ability to install and configure software, so routers and servers are the hardware environment required - something like a switch is not usable for this

DIY UTM - Firewall

- Firewalls using iptables or nftables provide a solid base for threat management
- iptables allows us to trivially prevent delivery of unwanted traffic based on source or destination, as well as arrival rates and other connection characteristics
- We can also redirect traffic to other destinations than the source intended which lets us set up transparent traffic inspection services

DIY UTM - Web Proxy

- Squid provides a scalable, high performance, highly configurable platform for proxying requests
- The basic configuration will cache web results, but not do threat management of web requests or replies
- E2Guardian is a replacement for the popular but no longer maintained Dansguardian web filtering solution
- ClamAV is a popular open source antivirus solution for Linux servers, freshclam keeps signature databases up to date

DIY UTM - Web Filtering

- E2Guardian is a web content filter (e2guardian.org)
- It filters on several aspects of requests and responses
- Typically you will filter on the server IP, server name, resource name, request or response headers, request type, request body content, time of day
- There are allow and block lists available for preloading your filters
- E2Bn (e2bn.org) is an example of an organization that builds devices based on this technology and sells managed solutions to specific markets

DIY UTM - E2Guardian

- The package for E2Guardian is in the repositories, but may need to be downloaded from github (https://github.com/e2guardian/e2guardian/releases) because the repo versions may not be current (Ubuntu 20.04 repo was current with version 5.3.4 when this slide was last updated)
- Installing the package will start the e2guardian service running on port 8080 with some blocking enabled
- E2Guardian uses configuration lists in /etc/e2guardian/lists to define what is blocked, and what is allowed
- Lists you could use used to be easy to find online, but some of the most popular have been shut down (shallalist.de, urlblacklist.com) - AV vendors and search engine companies still have them but do not provide them for free, generally, and do not have the same motivations as the original lists which were not driven by profit/loss or political positions
- These used to be referred to as blacklists and whitelists, but are now called blocklists and allowlists and unless you want someone else choosing what to allow or block without your knowledge or consent, you will most likely have to build your own
- The lists at https://zeltser.com/malicious-ip-blocklists/ are a good starting point as they try to provide lists of malicious websites

DIY UTM - HTTP Antivirus

- HTTP is used to transport a great variety of traffic, not just html
- Antivirus-scanning all web traffic can be a significant load on the UTM, and can be ineffective for non-webpage oriented traffic
- By default, content retrieved that matches the E2Guardian exception allowlist is not scanned even if the clamdscan is enabled
- Internal servers which are actively monitored and managed can usually be allowlisted
- HTTPS filtering is limited to MITM configs or URL-based filtering only

DIY UTM - ClamAV

- The Clam AV scanner can be installed using apt install clamav-daemon, or you can get it along with documentation from clamav.net
- Enabling the Clam AV scanner is done by:
  - uncommenting the contentscanner = '/etc/e2guardian/contentscanners/clamdscan.conf' line in /etc/e2guardian/e2guardian.conf
  - making sure your clamav socket file name (clamdudsfile) in clamdscan.conf matches the socket name in /etc/clamav/clamd.conf (run dpkg-reconfigure clamav-base to rebuild that file if needed)
  - setting the e2guardian daemongroup to clamav in /etc/e2guardian/e2guardian.conf
  - restart both clamav-daemon and e2guardian services
- Scanning allowlisted sites' content can be changed with the contentscanexceptions line

DIY UTM - Email Filtering

- Email is a difficult thing to filter well
- Attachments may be encrypted
- Emails may be very large
- Spammers and spam definition providers are locked in a game of leap-frog played to the death
- Email transports may be encrypted with TLS/SSL

DIY UTM - Email Filtering

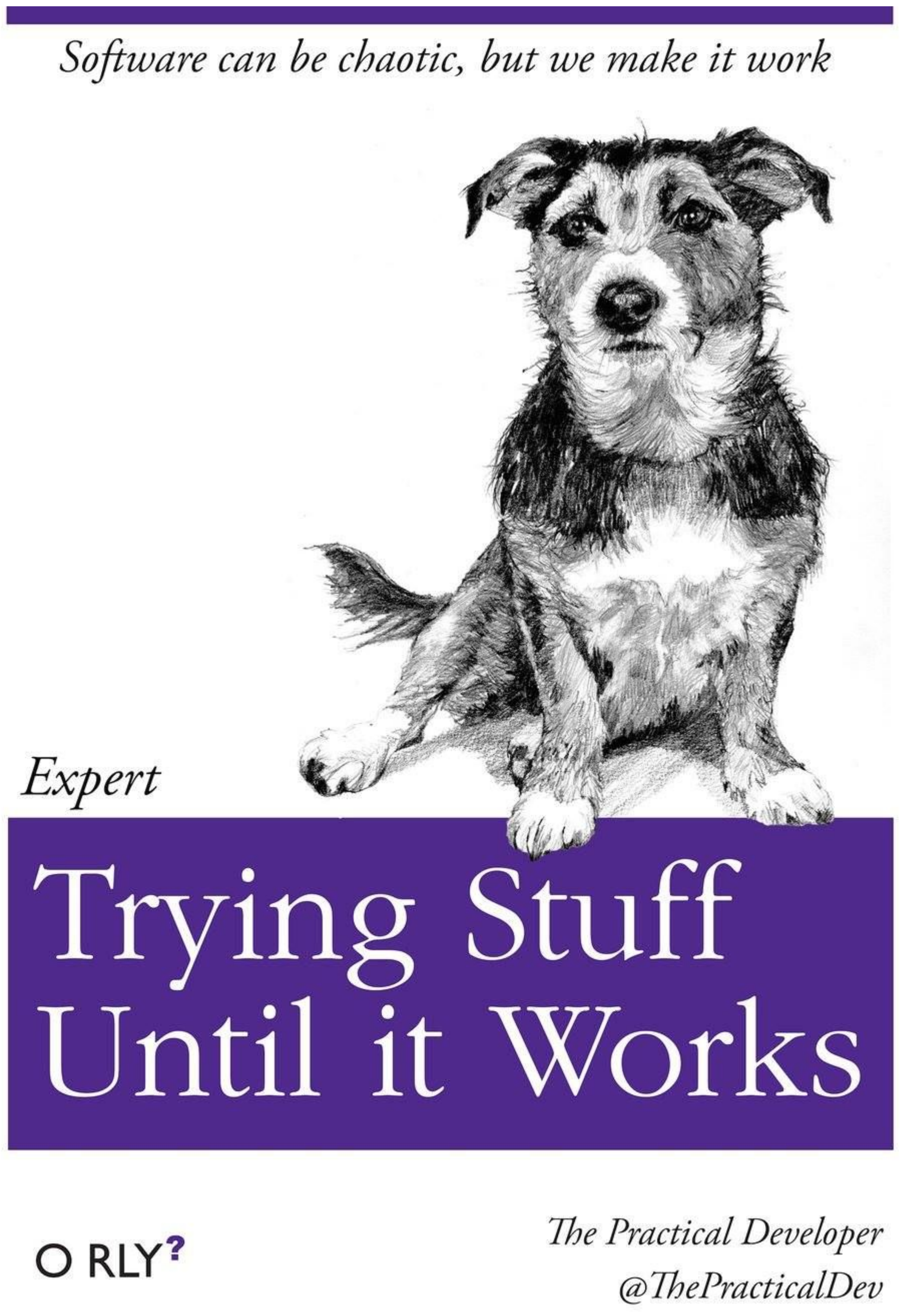
- Email filtering is best done on the mail server due to transport encryptions
- Email should be filtered on the SMTP port if you run your own mail server, as well as the Submission port
- If you use remote email services, you have to filter on the POP/IMAP ports and cannot do much in transit with the SSL-enabled POP/IMAP traffic
- With remote services, you often must rely on the email service provider for your email security and protection
- Remote email accessed using web interfaces is covered by web filtering for http

DIY UTM - Email Solution Example

- Various email filtering tools have come and gone, it tends to be a david and goliath situation, i.e. the number of people trying to misbehave far outnumber the number of people and organizations defending - burnout and financial viability are very real factors in the longevity of any particular defender
- Aside from keeping the software functional on new OS releases, the allowlists, blocklists, and signature lists can be challenging to maintain on your own
- See the Ubuntu server guide for recommendations on setting up postfix/dovecot with amavis/clamav/spamassassin
- Other distro vendors will have their own recommendations

Software Appliance UTM Examples

- pfsense can be configured with packages to handle much of the UTM capability but requires more administrative oversight than a commercial solution
- Sophos offers 2 flavours of software appliance UTM solution and is highly regarded
- The Sophos software appliance used to be available for a home/test network with a full-featured unlimited license on a single machine, but they have gone to trial software models
- Sophos also offers an install image you can put on your own PC-compatible hardware as well as their own custom-built ready-to-use hardware preloaded and licensed
- Other solution vendors have similar options available


Software can be chaotic, but we make it work
Expert
Trying Stuff Until it Works
O RLY?
The Practical Developer
@ThePracticalDev

UTM Lab

- e2guardian install
- clamav setup
- utm web proxy testing