Network Discovery

Monitoring and Log Management

Network Discovery

- Network discovery involves examining a network to determine what services are accessible and what machines are present
- Discovery can be passive or active
- Active discovery can be simple and non-intrusive or more complex and potentially intrusive
- Intrusive discovery can trigger network defenses, and may also debilitate or crash network services
- With respect to logging and monitoring, we are mostly looking for unauthorized use of our network, and authorized uses which may need to be incorporated into our logging and monitoring strategies

Passive Discovery

- Passive discovery refers to identifying network actors without interacting with them
- The simplest form is to examine logs and view reports from network monitoring software with the goal of extracting endpoint identification - log examination can be very incomplete
- wireshark/tshark's reporting tools can provide much more detail for a specific traffic capture, endpoints,{tcp,udp} and endpoint,{ip,ipv4,ipv6} reports show all users of the network in a given capture or can be run live
- Filtering known good traffic when reviewing these reports can help bring unexpected traffic into view
- Always best to capture traffic, then analyze captured traffic - live reports may reveal something worth investigating but traffic is no longer visible

Active Discovery

- Hosts which participate in the network they are attached to transmit and receive packets
- If they are not configured to ignore ICMP echo requests (pings), they can easily be discovered by tools which ping IP addresses on our network
- Machines configured to ignore pings can usually be detected easily by sending other types of packets which should get either a positive or negative response, such as TCP SYN or ACK
- Network scanning tools take advantage of this when doing scans, nmap/zenmap is good for this and supports many types of scans although some may trigger network defenses if present
- Your monitoring tools should alert you when a scan is being done on your network
- Be sure you know what kind of scan your tools will run before you try to interpret their output
- In cases where the intruder is trying to hide or mask their presence, it may be helpful to do a packet capture when scanning to see what responses may have been generated by the scan that the scanning tool was not designed to observe, analyze, or report (e.g. port-knocking and alerting responses)

HIDS and NIDS

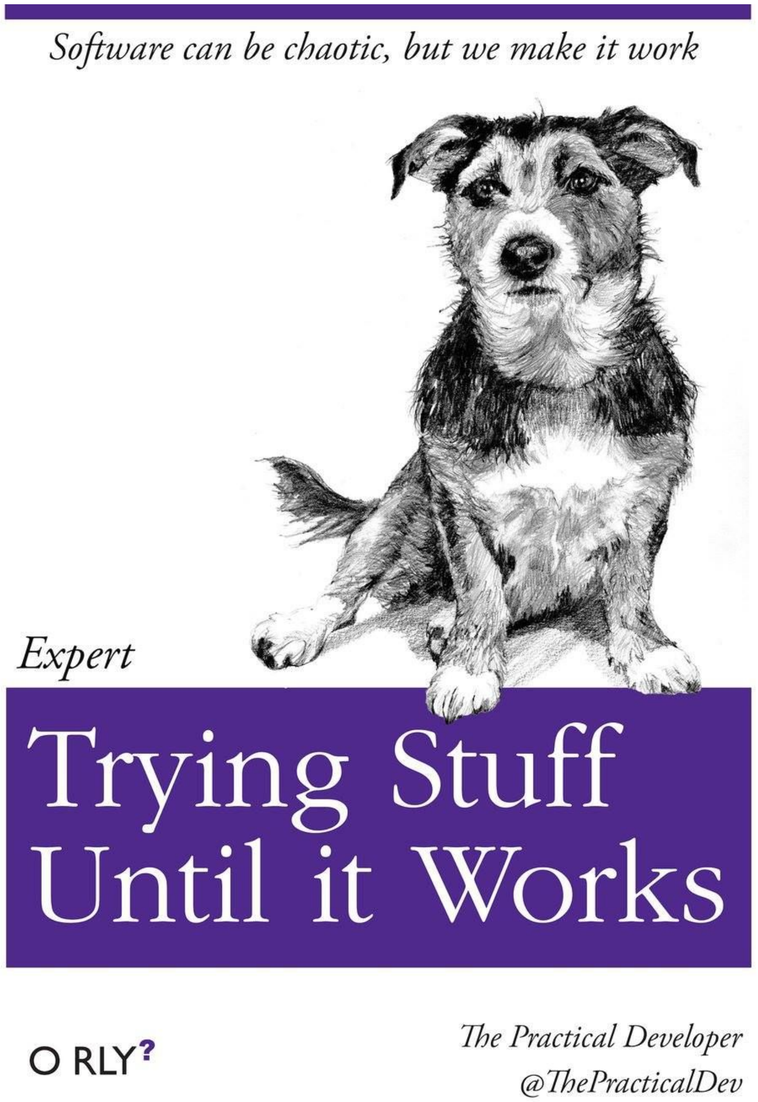
- On any networked machine we manage, there is expected activity for that machine/user/application combination
- Host-based Intrusion Detection Systems (HIDS) are software tools that use historical data stored in logs and monitoring systems to analyze the past activity of a host to determine if the activity is unexpected (due to type of activity, result of activity, actors involved, etc.)
- HIDS software is run on a host to determine if the host is being abused, used to send unwanted traffic, abuse the network, or provide access to bad actors - some include filesystem analysis components
- Network-based Intrusion Detection Systems (NIDS) are software tools that analyze the live activity on a network to determine if the activity is unexpected (due to source, destination, protocols, volume, etc.)
- NIDS software is typically run on monitoring hosts, not end-user desktops but may use agent programs placed around the network(s) being observed
- HIDS and NIDS together can form a good view of activity on a network

IDS vs. IPS

- NIDS or HIDS software that analyzes activity can potentially take action based on rulesets
- Rules may be signature-based or anomalous activity detection-based or both
- When the IDS software takes action to block or prevent future recurrence, we call it intrusion prevention software (IPS)
- HIDS software is also known as security information management (SIM) software
- NIDS software is also known as security event management (SEM) software
- IPS software that performs both SIM and SEM is also known as security information and event management (SIEM) software and can be part of an incident response strategy

Advanced Automated Threat Detection

- HIDS, NIDS, IPS, and SIEM software suites are non-trivial to install and manage
- Most packages such as Snort, Splunk, OSSEC, Samhain, etc. come with a base configuration that must be tailored to your application environment in order to be effective at identifying events that actually require investigation
- Commercial packages such as Splunk, Papertrail, ManageEngine's Eventlog Analyzer, etc. can be set up by the vendor for fees and can be supported under contract
- All of them run on top of the services we have learned to set up and maintain in this course, such as logging, netflow, and snmp and most presume you already have those things in place



Network Discovery Lab

- nmap/zenmap
- wireshark/tshark