



Mississippi State  
UNIVERSITY

# CySA+

## Cybersecurity Analyst

CCI  
Post Office Box 9627  
Mississippi State, MS 39762



Mississippi State University Center for Cyber Innovation



# CySA+

## Part 4 Security Architectures



# Tool Sets

## Chapter 15



# Outline

- **Prevention Tools**
- **Collective Tools**
- **Analytical Tools**
- **Exploitative Tools**
- **Forensic Tools**
- **Quiz**



# Preventative Tools

- **Preventative tools**
  - **Are tools that help prevent incidents**
  - **Gives the user the ability to create defensive perimeters around and application, host, or network**
  - **Recommended**
    - **Protective layers should be proportional to the value of the asset**



# Preventative Tools

- **Firewalls**
  - **Definition**
    - Are systems that follow specific sets of rules
    - Used to restrict the flow of network data
  - **Enforces an organization's security policies**
    - Provides high-level directives on acceptable and unacceptable actions pertaining to assets
  - **Access control list**
    - Are the firewall policy or rule set for the IP addresses, ranges allowed, and ports that can be accessed



# Preventative Tools

- **Firewalls**
  - **Stateless Packet Filtering**
    - Firewall only checks listed parameters
  - **Stateful Packet Filtering**
    - Firewall only checks listed parameters but keeps track of the state connection between endpoints
  - **Application-level firewall**
    - Firewall only allows packets that understands the application.
  - **Next-Generation Firewall**
    - Firewall similar to Application-level firewall and addition of an intrusion prevention system engine



# Preventative Tools

- **Firewall Tools**
  - **Next-Generation Firewall (NGFW)**
    - **Lead by three companies called Check point, Cisco, and Palo Alto due to having the largest shares**
  - **NGFW Tools**
    - **Check Point**
    - **Cisco**
    - **Palo Alto**





# Preventative Tools

- **Check point**
  - Known for creating the stateful packet inspection firewall
  - Does not quickly implement innovative features, but when implemented they perform well
  - Considered one of the market leaders due to there strong research and development arm
  - Strong reputation from complex deployments in larger organizations and niche use cases.
    - **Example:**
      - Organization is large and the required upgrades are complex. Check point would help with transitioning of the upgrades including regulatory compliance.



# Preventative Tools

- **Cisco**
  - **NGFW solutions are only available in Cisco-only deployments**
  - **Solutions are marketed as Cisco ASA with FirePOWER services**
    - **Represent a (subscription based) FirePOWER service on a traditional ASA firewall**
  - **Compared to other traditional firewall features and protection, Cisco is in the lead**
  - **Compared with the two other leading NGFW**
    - **Cisco is not as innovative, but its total cost of ownership makes up for this**



# Preventative Tools

- **Palo Alto**
  - **The industry leader in NGFW innovation**
    - **Frequently releases new feature ahead of its competitors**
  - **Examples of innovation**
    - **Cloud-based malware detection**
    - **Wild-fire subscription**
      - **Is integrated with their threat intelligence cloud**
  - **Product Line:**
    - **The integration into the threat intelligence cloud is a major theme within Palo Alto's product line**
    - **Results: Better protection against unknown threats and faster detection times**
    - **Con: Due to the innovations Palo Alto's solutions are more expensive than competitors**



Vendor	Platform Type	Key Features	Price	Best For...
Check Point	Hardware, software, and cloud	Integrated mobile security, endpoint protection, cloud-based sandboxing, and threat intelligence feeds	Mid to High	Balanced, mature approach between traditional SPI and NGFW, regulatory compliance
Cisco	Hardware and cloud	Behavioral IOCs and virtual firewalls	Mid	Traditional SPI firewall functionality with NGFW add-ons, TCO, heterogeneous cloud environments
Palo Alto	Hardware, software, and cloud	Endpoint protection, automatic IOC generation/sharing, threat intelligence feeds, and cloud-based malware detection	High	All-in-one state-of-the-art solution, if price is no object

## Preventative Tools

The figure above is a comparison of the NGFW tools



# Preventative Tools

- **Intrusion detection system (IDS)**
  - System that captures network traffic
  - Compares traffic to a set of rules/heuristics
  - Generates a type of notification if there is any evidence of unauthorized activity
- **Intrusion Prevention System (IPS)**
  - Is an IDS that attempts to prevent the intrusions it detects
    - Special class of IDS that retains all the IDS features and adds responsive capabilities
- Both systems can be network or host based



# Preventative Tools

- **BRO**
  - **Is an IDS**
    - Can be used as an IPS with its powerful scripting language
  - **This (IDS) does two task**
    - It captures all events while labeling them neither good nor bad
    - Uses scripts to analyze all the events for
      - Anomalies related security events
      - Signatures that indicate a security incident
  - **Scripts**
    - Scripts can be used to stop threats by
      - Sending a warning messages
      - Changing configurations on a system
  - **Strengths**
    - Records everything
    - Service is free



# Preventative Tools

- **Snort**
  - **Is an IDS**
    - More frequently used as an IPS than BRO
    - Is open source
  - **Its scripting language is not as powerful as Bro's but**
    - Is powerful enough to stop any signature network threat
  - **Key Difference**
    - Snort cannot look for anomalous behaviors
    - Snort does not automatically log all network activity
      - This may be useful to companies with limited storage



# Preventative Tools

- **Sourcefire**
  - **Is an IPS**
    - Comes with commercial support
  - **Was acquired by Cisco in 2013**
    - Firepower IPS was integrated into Cisco products
    - Requires an annual license fee
    - Licensing model increases with the number of hosts being supported
  - **Small organizations**
    - Is affordable if Cisco firewalls already owned can support Sourcefire Firepower





Tool	Developer	OS/UI	Key Features	Pricing	Best For...
Bro	Vern Paxson	Linux, BSD, and Mac OS	Rule and heuristic based.	Open source	Auditing, network forensics, anomaly-based detection, and malware analysis
Snort	Martin Roesch	Linux, BSD, Mac OS, and Windows	Rule based. Rule language is very popular. Extensive rule sets.	Open source	Ease of use, multiplatform support, and finding trained operators
Sourcefire	Cisco	Adaptive Security Appliance (ASA)	Tight integration with Cisco products. Based on Snort.	Commercial	Implementing next-generation IPS and integrating with Cisco environments

## Preventative Tools

The figure above compares three IDS/IPS Tools



# Preventative Tools

- **Host-Based Intrusion Prevention Systems (HIPS)**
  - **Is an IPS**
    - Only inspects and responds
    - Monitors the traffic in and out of a host's network interface
  - **Protection is only available on one device**
    - Allows the HIPS to become finely tuned to traffic and pattern of specific host
    - Incorporates behavioral or heuristic approaches
    - Does not rely on only signatures
  - **Flaws**
    - Need the appropriate time, money, or personnel to properly install and maintain
    - Requires a large amount of supervision during the anomaly-based training phase
      - Can cause a loss of productivity due to HIPS incorrectly classifying traffic as malicious but can be reduced by ensuring your solution includes monitoring capabilities and centralized management.



# Preventative Tools

- **Antimalware (antivirus software)**
  - **Can detect and neutralize malicious software such as**
    - **Worms, Trojan horses, and Viruses.**
  - **Majority of commercially available antimalware software is rule based**
    - **New malware definition files are being downloaded from the vendor on a weekly basis**
  - **Identifies malware that is already know to the vendor**
    - **Cannot detect new or old malware that has been modified**
    - **No antimalware product offer 100 percent protection**
    - **Not difficult to develop malware to be invisible to any one product**



# Preventative Tools

- **Enhanced Mitigation Experience Toolkit (EMET)**
  - **Is a free Microsoft product**
    - **Enhances the protection of Windows systems against a variety of threats mainly unknown or zero-day threats**
    - **As of July 2018 EMET has reached end of life**
      - **EMET features are key parts of Windows 10**
  - **EMET Key Features**
    - **Data Execution Prevention (DEP)**
      - **Prevents buffer overflows by**
        - » **Labeling the data space as non-executable**
        - » **Prevents data from being written to code space**
    - **Address Space Layout Randomization (ASLR)**
      - **Makes it harder to determine the location of the targeted instruction/data**
    - **Control Flow Guard (CFG)**
      - **Reduces the risk of return-oriented programming (ROP) by**
        - » **Preventing any flows that are not mapped from the virtual map created by CFG.**



# Preventative Tools

- **Web Proxies**
  - Is a system that intercepts and forwards web traffic between clients and servers
  - Commonly used for content filtering
    - Can block unacceptable web traffic
    - Monitor bandwidth-usage statistics
    - Block restricted website usage
    - Screen traffic for specified keywords
    - Provide logs with detailed information pertaining to sites users have visited
  - Proxy Servers:
    - Can be configured to act as a caching server
      - Keeps local copies of frequently requested resources.
        - » Allows organizations to reduce their upstream bandwidth usage and cost while increasing performance.



# Preventative Tools

- **Web Proxies**
  - **Supports HTTPS traffic**
    - **Requires examining the contents of a conversation**
      - Is encrypted and is usually private to the user
      - Ensure policies are in place that are clear to the user this can happen
    - **Certificate Authority (CA)**
      - The Proxy's CA must be trusted by the client
        - » If not trusted the browser will prompt the user with a certification warnings every time
- **Web Application Firewall (WAF)**
  - **Reduces external traffic to a protected server**
  - **Configured to protect specific apps or web apps**
    - **Can determine which URLs, directories, parameters that are acceptable and which are suspicious**
      - Traditional firewall are unable to do this



# Preventative Tools

- **SecureSphere**
  - **One of the market-leading Web application firewalls**
    - **Know for its dynamic profiling feature**
  - **Dynamic Profiling**
    - **Automatically learns protected applications' behaviors structure, and normal behavior of the user**
    - **Can exchange found threat sources and indicators of new attacks**
      - **Utilizes threat intelligence system in the cloud**
      - **Helps reduce the vulnerability to attacks and actors that have been seen elsewhere**
  - **Pricing**
    - **Tens of thousands of dollars per appliance**



# Preventative Tools

- **ModSecurity**
  - Is an open source toolkit for web application logging, control, and monitoring
  - Originally developed as an Apache server module
    - Has been adopted to work with Microsoft Internet Information Server (IIS) and Nginx
  - Can leverage OWASP Core Rule Set (CRS)
    - CRS is a set of detection rules for the most common web application attacks
    - CRS is developed by the OWASP for ModSecurity
  - Features
    - Able to aggregate multiple rule matches to trigger a higher-level alert
    - Supports traditional rule-based detection
    - ModSecurity would be a low-cost solution





# Preventative Tools

- **Nginx Anti XSS and SQL Injection (NAXSI)**
  - Is an open source web server developed to outperform Apache in high demand environments
    - Has a small rule set that identifies the features of 99% of know web application attacks
  - Implements a deny by default policy
    - It is important to tune NAXSI implementation
      - Requires whitelists
      - Semi-supervised self-learning
      - Can potentially generate its own whitelists
  - Might be the best fit for performance during rapid growth and limited funds



<b>Tool</b>	<b>Developer</b>	<b>OS/UI</b>	<b>Key Features</b>	<b>Pricing</b>	<b>Best For...</b>
SecureSphere	Imperva	Appliance and cloud	Dynamic profiling and threat intelligence feeds	Commercial	Larger organizations
ModSecurity	Trustwave	BSD, Linux, and Windows	Integration with OWASP CRS and rule- and anomaly-based detection	Open source	Apache servers
NAXSI	NBS System	BSD and Linux	High performance, with a focus on whitelisting	Open source	Nginx servers and busy sites

## Preventative Tools

In the figure above is a comparison of the monitoring tools just discussed



# Collective Tools

- **Security information and Event Management (SIEM)**
  - **This type of tool performs four basic functions**
    - **Collect, store, analyze, and report**
  - **The CySA+ will focus only six SIEM tools**
    - **Unified Security Management Platform**
    - **Arc Sight**
    - **Kiwi Syslog**
    - **Open Source Security Information Manager (OSSIM)**
    - **QRadar**
    - **Security Intelligence Platform**



# Collective Tools

- **Unified Security Management (USM) Platform**
  - **Is a proprietary extension of OSSIM**
    - **Along with the OSSIM capabilities USM includes**
      - Data analytics and visualizations
      - Log management
      - Phone and email support
      - Documentation and a knowledgebase
      - A full day of training
  - **This product has a lot to offer for a reasonable ticket price**



# Collective Tools

- **ArcSight**
  - **SIEM solution that combines security analytics from multiple tools to have better threat analysis**
    - **Provides both user behavior analytics (UBA) and DNS malware analytics**
  - **Has an open architecture**
    - **It can interface with other systems like Hadoop and Kafka**
  - **This product would be idea for a growing business**
    - **A large enough business could utilize the offered big data analytics**



# Collective Tools

- **Kiwi Syslog**
  - **Monitor, archive, and alerts on syslog events**
    - **Not typically used as a SIEM tool**
    - **Does have SIEM related features such as**
      - **Prioritizing and alerting on messages**
  - **Designed to help**
    - **Monitor performance**
    - **Regulatory compliance issues**
    - **Identify compromises**
  - **Would not be sufficient as a standalone SIEM**
    - **Would be a good solution if your main challenge was integrating Windows and Linux log files**



# Collective Tools

- **Open Source Security Information Manager (OSSIM)**
  - **Is the basis for USM platform**
  - **Is a collection of components**
    - **For vulnerability assessment it has OpanVAS**
    - **For network-based intrusion detection it has Suricata**
    - **For host-based intrusion detection and file integrity monitoring it has OSSEC**
    - **All components are integrated into a web-based interface**
  - **If your organization has a limited budget OSSIM might be a good fit**
    - **Would have to invest in training your security staff to use the free platform**



# Collective Tools

- **QRadar**
  - **IBM's SEIM solution**
  - **Supports incident response**
    - **Integrates NetFlows, packet captures, and event logs**
  - **Correlates offense events**
    - **These correlated events are more likely to indicate a security compromise**
    - **Analysts can see all**
      - **Network and log data supporting the security compromise**
      - **Affected hosts**
      - **All relevant vulnerabilities**
  - **Good fit for an organizations that wants a tight integration between the SEIM and response process**





# Collective Tools

- **Security Intelligence Platform (SIP)**
  - Started off as a log files analysis engine but has developed into a SIEM
  - Has two products
    - **Splunk Enterprise**
      - Provides event and log collection, indexing, and analysis
    - **Splunk Enterprise Security**
      - Provides traditional SEIM features
  - Depending on the organizations needs
    - **Splunk is a competitive solution**



# Collective Tools

The figure to the right is a comparison of the six mentioned SIEM tools

Tool	Developer	OS/UI	Key Features	License	Best For...
Unified Security Management Platform	AlienVault	Hardware or virtual appliance	Integration of SIEM, discovery, vulnerability assessment, and intrusion detection into one platform	Commercial	Big needs on tight budgets, AWS and Azure integration, and low cost
ArcSight	HP Enterprise	Hardware or virtual appliance	Third-party integration, high degree of customization, and event correlation	Commercial	Midsized or larger organizations needing full incident investigation support
Kiwi Syslog	SolarWinds	Windows	Centralized monitoring/storing of syslog, Windows events, and SNMP traps	Commercial	System event and SNMP monitoring and compliance
OSSIM	AlienVault	Virtual appliance	Integration of SIEM, discovery, vulnerability assessment, and intrusion detection into one platform	Open source	Big needs but no budget
QRadar	IBM	Hardware or virtual appliance, IaaS	Correlation of NetFlow and log events	Commercial	Scalability and availability
Security Intelligence Platform	Splunk	Hardware or virtual appliance, SaaS	Machine learning as well as diverse log file searching and analysis	Commercial	Diverse data sources and sophisticated analysis



# Network Scanning

- **Network Scanning**
  - Is used to determine what is listening and what is responding on a network
- **Horizontal Network Scan**
  - Sends messages to a set of host addresses
  - This determines which addresses correspond to responding systems
- **Vertical Network Scan**
  - Sends messages to a set of protocol/port combinations
  - This determines which ports are listening for client connection attempts



# Network Scanning

- **Nmap**
  - **Is a command-line interface (CLI) tool**
  - **It send specially crafted messages and then examines the responses**
    - **Determines what hosts are active on the network**
    - **Determines what ports are listening**
    - **Determines the operating system, hostname, and patch level of some systems**
  - **Here are a few graphical user interface (GUI) Nmap tools**
    - **Zenmap (Windows)**
    - **NmapFE (Linux)**
    - **Xnmap (Mac OS)**



# Network Scanning

- **Packet Capture**
  - Also known as sniffers are used for troubleshooting and incident response
    - Sniffers can also be used for logging and auditing purposes
  - Network Packet Capture tools
    - Wireshark
    - Tcpdump
    - Aircrack-ng



# Network Scanning

- **Wireshark**
  - **Is a GUI-based packet analyzer**
  - **TShark**
    - **Wireshark's command-line interface tool**
      - Useful for scripting a packet capture
      - Can be used when connecting over SSH
    - **Can view captured traffic in the GUI**
  - **PCAP file format**
    - **Can view PCAP files from other packet capture tools**
  - **Can run on**
    - **BSD, Linux, Mac OS, and Windows**



# Network Scanning

- **Tcpdump**
  - **Is a command-line interface tool**
    - Can save captures as PCAP files
    - Not as easy to read traffic capture as in Wireshark
  - **Is a standard distribution on**
    - BSD, Linux, and Mac OS
  - **Windump**
    - Is a Windows version of tcpdump



# Network Scanning

- **Aircrack-ng**
  - Is an open source wireless network security tool
  - Can audit the security of WLANs during
    - Attacks on WPA keys, replay attacks, deauthentication, and establishment of fake APs
  - Can be used to capture packets over the wireless network
    - With some effort can capture packets over a wired network
  - This is a good operation for an organization that needs a wireless security solution





# Command-line Utilities

- **A Security Analyst must be familiar with several CLI tools**
  - **Here are a few that are required for the CySA+ exam**
    - **Netstat**
    - **Ping**
    - **Traceroute**
    - **Ifconfig**
    - **Nslookup**
    - **OpenSSL**
  - **Outside of the scope of the exam, time should be taken to work with these tools**



# Command-line Utilities

- **Netstat**
  - **Offers useful features making it a popular tool**
    - Provides information on the status of network connections and listening sockets
    - Provide interface statistics
    - Provides protocol statistics (E.g. IP and ICMP)
  - **Is by default on Linux, Mac OS, and Windows**
- **Ping**
  - **Sends four (Windows) or continuous (other OSs) ICMP echo requests to an indicated host**
    - Depending on the target, it will send back an ICMP echo reply message for each received
  - **Provides the total time for the exchange (Round-Trip)**
    - Will compare the time the request was sent with the time the response was received
    - Provides indicator of the latency to/from that target



# Command-line Utilities

- **Traceroute**
  - **Network tool used to**
    - **Display possible routes of packets**
    - **Measures the transit delays of packets**
  - **Uses the time to live (TTL) field of an IP packet**
    - **This utility increments the TTL which starts at 1**
      - **In a sequence of messages to the same host the TTL is incremented**
      - **The receiving host will decrement the TTL on an arriving packet**
    - **By incrementing the TTL each consecutive host between the source and the destination is forced to reveal its IP address**
  - **Is a utility for Linux, and Mac OS**
    - **Tracert is the same utility for Windows**



# Command-line Utilities

- **Ifconfig**
  - **CLI tool**
    - Used to see the IP address of a host
    - Provides other IP parameter such as netmask, default gateway, and MAC address
  - **Is a CLI tool for Linux and Mac OS**
    - Ipconfig is the CLI tool for Windows
  - **Major difference between ifconfig and ipconfig**
    - Ifconfig can be used to configure the interfaces
    - Ipconfig only allows the user to see the parameters



# Command-line Utilities

- **Nslookup**
  - **Stands for name sever lookup**
    - **Is the CLI of the DNS**
  - **CLI tool**
    - **Used to query the domain name system (DNS)**
    - **Can obtain domain name or IP address mapping**
    - **Allows the user to resolve the IP address corresponding to a fully qualified domain name (FQDN) of a host**
    - **Can interrogate the target server and obtain other data records**
      - **E.g. email and canonical name**



# Command-line Utilities

- **OpenSSL**
  - **Is an open source software library**
    - **Allows software system to communicate securely**
    - **Includes both**
      - **Secure Socket Layer (SSL) functionality**
      - **Transport Layer Security (TLA) functionality**
  - **Is a library that includes a CLI**
    - **Can generate and validate certificates**
    - **Can generate, sign and verify MD5 and SHA hashes**
    - **Encrypt and decrypt data**
    - **Establish secure connections to remote servers**



# Analytical Tools

- **Vulnerability Scanning**
  - Provides a view of your network from the adversary's eyes and identifies weaknesses of these systems
    - Can identify software flaws and misconfigurations
    - Can suggest countermeasures or compensating controls
  - **Vulnerability Scanning Tools**
    - QualysGuard
    - Nessus
    - OpenVAS
    - Nexpose
    - Nikto
    - Microsoft Baseline Security Analyzer



# Analytical Tools

- **QualysGuard**
  - **Has a Software as a Service (SaaS) model**
    - Provides several cloud-based vulnerability assessment and management products
    - Assessments of internal scans are reported to Qualys server
  - **Web-base UI**
    - Can access all network discovery, mapping, asset prioritization , scheduling, vulnerability assessment reporting, and remediation tracking tasks
  - **Can generate detailed reports**
    - Comes with several report templates





# Analytical Tools

- **Nessus**
  - **Has a library of over 80,000 plug-ins**
    - All used for scanning for vulnerabilities
  - **Web-based UI**
    - Provides an easy way for the user to configure assessments and view the results
    - Can generate reports and provide remediation suggestions
  - **Vulnerability Discovery**
    - When a vulnerability is discovered a severity level is assigned
    - Provides technical details about the discovery such as
      - Method used to identify the vulnerability
      - Databases references
  - **Assess Compliance**
    - Has a library of compliance checks
    - Can be used to schedule compliance scans to automatically run periodically



# Analytical Tools

- **OpenVAS**
  - Has a library of nearly 50,000 network vulnerability tests (NVTs)
    - Is a free product and relies on community support
  - **OpenVAS Manager**
    - Used to configure and access OpenVAS Scanner
    - Can schedule and run vulnerability scans



# Analytical Tools

- **Nexpose**
  - **Designed to**
    - **Manage the entire vulnerability lifecycle**
    - **Scan and catalog vulnerabilities**
    - **Integrate directly into Metasploit**
  - **Dashboard**
    - **Network-connected device will appear in the dashboard**
    - **Can view details of the scan**
      - Shows the site-wide vulnerability charts
      - Breaks all discoveries down by CVSS score
      - Rates all vulnerabilities by how exploitable they might be
    - **Can generate reports containing**
      - Summary of the network
      - An overview of both devices and vulnerabilities



# Analytical Tools

- **Nikto**
  - **CLI tool**
    - **Web server vulnerability scanner**
    - **Can quickly assess software and configuration vulnerabilities**
    - **Must specify a target host with any additional options**
  - **Reports**
    - **Can be saved in a variety of ways including HTML**
    - **Provides a summery of the command issued**
    - **Provides information about the tested servers**
    - **Provides hyperlinks to relevant resources and their vulnerability data**



# Analytical Tools

- **Microsoft Baseline Security Analyzer**
  - **Windows Tool**
    - Can identify missing security patches
    - Can identify software misconfigurations in Windows operating system
    - Can only be used for assessing Windows endpoints and servers
    - Design for
      - Windows Vista, XP, 7, and 8
      - Windows Server 2003, 2008, and 2012
  - **Can Scan for**
    - Vulnerabilities related to passwords
    - Server and database misconfigurations
    - Missing security updates
  - **Reporting**
    - Provides information about the test results and links to possible solutions



Tool	Developer	OS/UI	Type	Pricing	Best For...
QualysGuard	Qualys	Browser based	Cloud-based vulnerability scanning and management	Paid	Continuous monitoring of large networks
Nessus	Tenable	Browser based	Vulnerability scanner and manager	Paid	Continuous monitoring of large enterprises
OpenVAS	Greenbone Networks	Browser based	Vulnerability scanner and manager	Free	Continuous monitoring of large enterprises
Nexpose	Rapid7	Browser based	Vulnerability scanner and manager	Free Paid	Vulnerability identification and exploitation
Nikto	CIRT.net	Command line	Web server scanner	Free	Identifying web server flaws and misconfigurations
Microsoft Baseline Security Analyzer	Microsoft	Windows	Endpoint and server scanner	Free	Identifying missing security updates and misconfigurations in Windows environments

## Analytical Tools

In the figure above is a comparison of the vulnerability scanning tools



# Monitoring Tools

- **Network monitoring**
  - **Provides visibility of our Network**
    - Through packet capture, watching traffic, or examining for unusual connections
    - This is required to prevent attacks and improve usability
  - **Tools**
    - MRTG
    - Nagios
    - Orion
    - Cacti
    - Netflow Analyzer



# Monitoring Tools

- **Multi Router Traffic Grapher (MRTG)**
  - **Is a cross-platform, network measuring tool**
    - **Produces graphs and statistics**
      - Relies on Simple Network Management Protocol (SNMP) exchanges
  - **Offered as free software under GNU General Public License**
    - **Developed in Perl**
    - **Is lightweight and is very fast**
    - **Capable of storing traffic logs for years**
      - Without significant increase in log storage requirements
- **Cacti**
  - **Is a free front-end network logging and graphing tool**
    - **Is based on MRTG**
    - **Its strength is in its speed in ingesting and visualizing logging data**
  - **Popular tool for web administrators**





# Monitoring Tools

- **Nagios**
  - **Is a monitoring and alerting platform**
  - **Nagios Core**
    - **Open source option**
    - **Does not provide as much control over the dashboards, graphs and reports**
  - **Nagios XI**
    - **Commercial option**
    - **Provides advanced configuration of the dashboards, graphs, and reports**
  - **Both options provide**
    - **Quick access of to the network assets**
    - **Details of each device are hyperlinked directly from the dashboard**



# Monitoring Tools

- **Orion**
  - **Performs protocol analysis to determine what kinds of data is moving from nodes**
  - **Provides the foundation of SolarWinds suite of products**
    - **Orion is the base framework for NetFlow Traffic Analyzer tool**
- **NetFlow Analyzer**
  - **An analysis tool for network traffic**
    - **Relies on NetFlow data to give administrators a full view of their network**
    - **Provides basic bandwidth monitoring and service identification**
    - **Provides traffic-shaping features which can identify curb bandwidth abuse**
  - **Can be used to for network forensics and security-specific capabilities**



<b>Tool</b>	<b>Developer</b>	<b>OS/UI</b>	<b>Type</b>	<b>Pricing</b>	<b>Best For...</b>
MRTG	Tobi Oetiker	Windows, Linux, Mac, and Novell Netware	Network graphing	Free	Simple graphs
Nagios	Nagios	Browser based	Infrastructure monitoring and analytics	Free or Paid	Monitoring host resources, services, and network infrastructures
Orion	SolarWinds	Windows and Linux	Monitoring platform	Paid	Continuous monitoring of large enterprise networks
Cacti	The Cacti Group, Inc.	Browser based	Network graphing	Free	Detailed graphs
Netflow Analyzer	ManageEngine	Windows and Linux	Traffic monitoring and analytics	Paid	Gaining real-time visibility on traffic in large networks

## Monitoring Tools

The figure above gives a comparison of the monitoring tools



# Interception Proxy

- **Interception Proxies**

- **Can be used to collect, modify, or block certain types of data**

- **Sits in between the user and the requested resource**
- **Provides insight into user behavior**

- **Tools**

- **Burp Suite**
- **ZAP**
- **Vega**



# Interception Proxy

- **Burp Suite**
  - Is an integrated web application testing platform
    - Used to map and analyze a web apps vulnerabilities
    - Can manually inspect every request passing through the user server
  - Does offer point-and-click web-scanning features in the paid version
- **Zed Attack Proxy (ZAP)**
  - OWASP's flagship project
    - ZAP is placed in between the user's browser and the web application
  - ZAP's features include
    - Can inspect user request and modify the contents



# Interception Proxy

- **Vega**
  - **Is a cross-platform interception proxy**
  - **Features provided are**
    - **Automated scanning**
    - **Injection discovery**
    - **Cross-site scripting vulnerability discovery**
  - **Can launch quick attacks with a provided target**
  - **Results will include**
    - **Short description of the discovery**
    - **Why it is important**
    - **How best to remediate**



Tool	Developer	OS/UI	Type	Pricing	Best For...
Burp Suite	PortSwigger	Linux, Mac, and Windows	Web application testing	Free or Paid	Analysts who require feature-rich toolset for custom security testing
ZAP	OWASP	Linux, Mac, and Windows	Web application testing	Free	Web developers, penetration testers, and network and security engineers
Vega	Subgraph	Linux, Mac, and Windows	Web application testing	Free	Security analysts seeking automation and API availability

## Interception Proxy

In the figure above is a comparison of the interception proxy tools



# Exploitative Tools

- **Exploitation Frameworks**
  - **Provides security teams with tools**
    - **Needed to replicate attacks**
    - **Validate vulnerabilities**
  - **Usually has a range of pen-testing options**
    - **Provides well-known vulnerabilities, exploits and security tools**
  - **Tools**
    - **Metasploit**
    - **Nexpose**





# Exploitative Tools

- **Metasploit**
  - The framework provides an easy way for security professionals to
    - Assess system vulnerabilities
    - Determine exploitability
  - Several interfaces and professional options available with a paid license
    - Each version ships with hundreds of exploits and payloads referred to as modules, which contain the relevant code and reference data
  - Main strength is versatility it provides with modular design
    - Exploits can be combined with payloads to take advantage of flaws and execute code in a single effort






# Exploitative Tools















- **Nexpose**
  - **Vulnerability discovery and management tool**
  - **Integrates extremely well within Metasploit**
    - **Choice for security analysts wanting to pivot quickly from analysis to exploitation without leaving the interface**
    - **Useful in determining and prioritizing exploitable vulnerabilities on the network and reducing the burden of managing reports across the two systems**







- **Nexpose vulnerabilities listing sorted by known exploits, found during routine scan**

VULNERABILITIES 

> Apply Filters (0 applied)

Title			CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
ISC BIND: Assertion Failure in buffer.c While Building Responses to a Specifically Constructed Request (CVE-2016-2776)			7.8		255 Tue Sep 27 2016	Mon Feb 20 2017	Critical	2	 Exclude
lighttpd: Denial of Service - endless loop in parsing Connection header (CVE-2012-5533)			5		174 Fri Nov 23 2012	Thu Nov 24 2016	Severe	1	 Exclude
Default or Guessable SNMP community names: public			10		913 Tue Dec 31 1996	Tue Dec 03 2013	Critical	1	 Exclude
SMB signing disabled			7.3		814 Sun Oct 31 2004	Wed Jul 11 2012	Severe	8	 Exclude
SMB signing not required			6.2		806 Sun Oct 31 2004	Wed Jul 11 2012	Severe	8	 Exclude
X.509 Certificate Subject CN Does Not Match the Entity Name			7.1		761 Thu Aug 02 2007	Tue Jan 27 2015	Severe	6	 Exclude
CIFS NULL Session Permitted			7.5		755 Tue Dec 31 1996	Thu Jan 05 2017	Critical	2	 Exclude
Default or Guessable SNMP community names: admin			7.5		755 Tue Dec 31 1996	Tue Dec 03 2013	Critical	1	 Exclude
SNMP credentials transmitted in cleartext			7.5		748 Mon Feb 11 2002	Wed Jun 18 2014	Critical	1	 Exclude
No password for Grub			4.6		743 Thu Dec 31 1998	Tue Apr 12 2016	Severe	1	 Exclude

Showing 1 to 10 of 52 |  Export to CSV

Rows per page: 10   1 of 6 



<b>Tool</b>	<b>Developer</b>	<b>OS/UI</b>	<b>Type</b>	<b>Pricing</b>	<b>Best For...</b>
Metasploit	Rapid7	Linux, Mac, and Windows	Exploitation framework	Free or Paid	Penetration testers and network security engineers
Nexpose	Rapid7	Browser based	Vulnerability scanner and manager	Free or Paid	Vulnerability identification and exploitation

## Exploitative Tools

In the figure above is a comparison of the exploitation frameworks



# Exploitative Tools

- **Fuzzers**

- **A technique used to discover software flaws**

- **Input random data into the software**
    - **If there is a fall the software will be unstable or will crash**
    - **Errors usually can help point out the root cause**

- **Tools**

- **Untidy**
    - **Peach Fuzzer**
    - **Microsoft SDL fuzzers**



# Exploitative Tools

- **Untidy**
  - Popular Extensible Markup Language (XML) fuzzer
  - Used to test web application clients and servers
    - Takes valid XML and modifies it before inputting it into the application
  - Now a part of the Peach Fuzzer project



# Exploitative Tools

- **Peach Fuzzer**

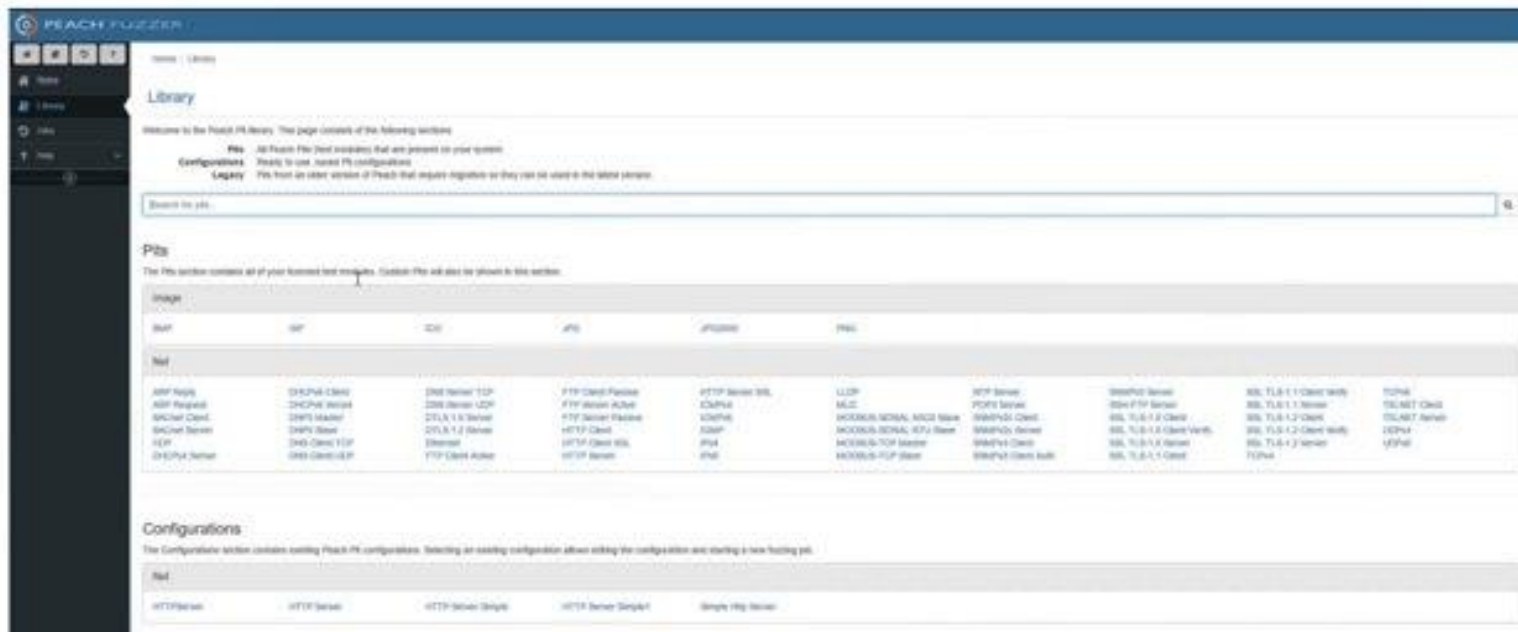
- **Fuzzing suite capable of testing a wide range of targets**
- **Uses XML-based modules, called pits, to provide all the testing information needed to run the fuzz**
  - **Pits are configurable based on the testing needs**
  - **Before conducting a fuzz test, user must specify the type of test, the target, and any monitoring settings desired**





# Exploitative Tools

- Peach library of fuzz testing modules available during a test below



# Exploitative Tools

- **Microsoft SDL Fuzzers**
  - Microsoft released two types of standalone fuzzers designed to be used in the verification phase of the Security Development Lifecycle (SDL):
    - **Minifuzz file fuzzer and Regex Fuzzer**
      - Microsoft has since dropped support and no longer provides these applications for download



Tool	Developer	OS/UI	Type	Pricing	Best For...
Untidy	PortSwigger	Linux, Mac, and Windows	XML fuzzer	Free	Discovering vulnerabilities in web clients and servers
Peach Fuzzer	OWASP	Browser based	Automated fuzzing platform	Free or Paid	Fuzzing binaries, embedded systems, and IoT devices
Microsoft SDL fuzzers	Microsoft	Windows	Regex and file fuzzer	Free	Basic file and regular expression fuzzing capabilities

## Exploitative Tools

In the figure above is a comparison of fuzzers



# Forensic Tools

- **Forensic Suites**
  - **Provides a range of tools**
    - **Tools to uncover hidden data**
    - **Tools to automatically document the evidence analysis progression**
  - **Here are a few Forensic Suites**
    - **EnCase**
    - **FTK**
    - **Helix**
    - **Cellebrite**



# Forensic Tools

- **Encase**

- Suite includes tools for forensic acquisition, analysis, and report generation
- Evidence File format is among the most common types of forensic imaging formats, due in part to its high portability
  - Imaged volume's data, metadata, and hashes are all included in a single file
- Very popular in law enforcement and government
  - Easy-to-use GUI
  - Chain-of-custody features



# Forensic Tools

- **FTK**
  - **AccessData's Forensic Toolkit**
  - **For investigators needing to create forensic images of hard drives**
  - **Built in logging features make the process of documentation easier for forensic analysis**
    - **Investigators looking to preserve details of the analysis itself**
  - **One of the more popular tools is the FTK Imager**
    - **Data previews and volume imaging tool**



# Forensic Tools

- **Helix**
  - **Allows analysts to fully image all internal devices, including physical memory and hard disks**
    - **Helix3 Pro is the latest multiplatform forensic suite offered by e-fense**
    - **Based on the open source Knoppix live boot utility**
  - **Also includes utilities for mobile device analysis, offering the same nondestructive imaging features**



# Forensic Tools

- **Cellebrite**

- **UFED user can extract encrypted, deleted, or hidden data from select mobile phones**
  - **Also provides evidence preservation using write blocking during the data extraction procedure**
- **Their Universal Forensic Extraction Device (UFED) is a handheld hardware device**
  - **primarily marketed to law enforcement and military communities**





<b>Tool</b>	<b>Developer</b>	<b>OS/UI</b>	<b>Type</b>	<b>Pricing</b>	<b>Best For...</b>
EnCase	Guidance Software	Windows	Digital forensic suite	Paid	Digital forensics collection as well as analysis and reporting
FTK	AccessData	Windows	Forensic imaging suite	Free or Paid	File discovery and volume replication
Helix	e-fense	Windows and Linux	Digital forensic suite	Free or Paid	Nondestructive forensic analysis
Cellebrite Universal Forensic Extraction Device (UFED)	Cellebrite	Cross-platform	Mobile forensic suite	Paid	Data extraction and analysis of mobile devices

## Forensic Tools

In the figure above is a comparison of forensic suites



# Hashing

- **Hashing tools**
  - **Is used to verify the integrity of files**
    - **Creates a value of a fixed size regardless of the input**
    - **If one bit in the input is changed the output value will be or should be completely different**
      - **The idea is to make it obvious if that the data has been modified**
  - **Tools**
    - **Md5sum**
      - **Computes a value of 128-bits long given any input of varying size**
    - **Shasum**
      - **Computes a value of 160-bits long given any inout of varying size**



<b>Tool</b>	<b>Developer</b>	<b>OS/UI</b>	<b>Type</b>	<b>Pricing</b>	<b>Best For...</b>
md5sum	Ulrich Drepper, Scott Miller, and David Madore	Linux, Mac, and Windows	MD5 message digest	Free	Generating MD5 message digests
shasum	Mark Shelor	Linux, Mac, and Windows	SHA message digest	Free	Generating SHA message digests

## Hashing

In the figure above is a comparison of hashing tools



# Password Cracking

- **Password Cracking Tools**
  - **Common target for OS password files**
    - **Windows**
      - Security Accounts Manager (SAM) file is the database of user passwords
    - **Modern Linux environment**
      - User information is stored in /etc/passwd file
      - Password hashes are stored in /etc/shadow file
    - **These files are protected by cryptographic methods**
      - Given the right tools it is possible to break into these files
  - **Tools**
    - **John the Ripper**
    - **Cain and Able**



# Password Cracking

- **John the Ripper**
  - **Is an open source password-cracking tool**
    - **Developed for UNIX but has variations for other Oss**
  - **CLI tool**
    - **Runs attacks with wordlists like rockyou.txt**
    - **Runs attacks by brute force**
      - **Tries many different combinations in the character space**
    - **Supports auto-detection of password hash types**
      - **A protective measure used to prevent unauthorized viewing of the password file**
    - **Paid version expands on the selection of hashes supported**



# Password Cracking

- **Cain and Abel**
  - **Windows password-cracking tool**
  - **Can operate on**
    - **Sniffed network traffic**
    - **Locally acquired password hashes**
  - **Does support**
    - **Wordlists and brute-force attacks**
      - **rockyou.txt**
    - **Rainbow tables**
      - **Used to speed up its analysis**
  - **Not supported by OSs newer than Windows Vista**



<b>Tool</b>	<b>Developer</b>	<b>OS/UI</b>	<b>Type</b>	<b>Pricing</b>	<b>Best For...</b>
John the Ripper	Alexander Peslyak	Linux, Mac, and Windows	Password recovery tool	Free or Paid	Custom password cracking
Cain and Abel	Massimiliano Montoro	Windows	Password recovery tool	Free	Dictionary, brute force, and cryptanalysis attacks

## Password Cracking

In the figure above is a comparison of password crackers



# Imaging

- **Imaging Tools**
  - **Copy data from a source regardless of the file system**
    - **Meaning that a hard drive running on Windows or Linux will be copied the same way using the same utility**
  - **Allows for an entire contents of a drive to be duplicated to a single file in a remote destination**
    - **Includes a file system's slack and free space**
      - **Fragments of deleted files may reside in slack space**
  - **dd**
    - **Is the easiest way to get a bit-for-bit copy of a hard drive**





# Quiz

## Chapter 15



# Question #1

- **1. You are concerned about your ability to block zero-day exploits before they enter your network. Which of the following tools would best allow you to do this?**
  - A. Wireshark**
  - B. Imperva's SecureSphere**
  - C. Metasploit**
  - D. PaloAlto Networks NGFW**



# Answer #1

- **D**
  - **Next-Generation Firewalls (NGFWs), such as those made by Palo Alto Networks, can connect to threat intelligence feeds to quickly identify new attacks and share those with others with similar firewall**
  - **They also have the ability to run applications in a sandbox to determine whether they are benign or malicious before allowing them into the network**



## Question #2

- **2. What class of tools is best able to receive information from a variety of platforms, aggregate it into a data store, generate alerts, and allow users to query the data?**
  - A. Interception proxy**
  - B. SIEM**
  - C. Fuzzer**
  - D. HIPS**



# Answer #2

- **B**
  - Security information and event management (SIEM) systems are designed to collect, store, analyze, and report security information and events



# Question #3

- **3. Which of the following is an example of a vulnerability scanner?**
  - A. Bro
  - B. NAXSI
  - C. OpenVAS
  - D. Helix



# Answer #3

- **C**
  - **OpenVAS (in addition to Qualys, Nessus, Nexpose, Nikto, and Microsoft Baseline Security Analyzer) is a vulnerability scanner with which you should be familiar**



# Question #4

- **4. To what class of tools does Metasploit belong?**
  - A. Vulnerability scanners**
  - B. Interception proxies**
  - C. Password crackers**
  - D. Exploitation frameworks**





# Answer #4

- **D**
  - **Metasploit is the most widely used open source exploitation framework**



# Scenario for Questions 5-7

- **Your company's internal development team just developed a new web application for deployment onto the public-facing web server. You are trying to ensure that it conforms to best security practices and does not introduce any vulnerabilities into your systems**



# Question #5

- **5. Which would be the best tool to use if you want to ensure that the web application is not transmitting passwords in cleartext?**
  - A. Nikto**
  - B. FTK**
  - C. Burp Suite**
  - D. Aircrack-ng**



# Answer #5

- **C**
  - **Burp Suite is an integrated web application testing platform often used to map and analyze a web application's vulnerabilities**
  - **It is able to intercept web traffic and allow analysts to examine each request and response**



# Question #6

- **6. Having tested the web application against all the input values you can think of, you decide to try random data to see if you can force instability or crashes, Which is the best tool for this purpose?**
  - A. Untidy**
  - B. Cellebrite**
  - C. Cain and Abel**
  - D. Qualys**



# Answer #6

- **A**
  - The class of tools that tests applications by bombarding them with random values is called fuzzing tools
  - Untidy, Peach Fuzzer, and Microsoft's Regex Fuzzer are all examples covered in this chapter



# Question #7

- **7. You discover a vulnerability that causes the application to crash whenever it receives a password of length 256 or greater. This is the only flaw you find, and you are under immense pressure to get the app online. The development team will need a week to fix the issue. Assuming you are already using it, which of the following security tools might allow you to mitigate the risk and allow the app to go online by tomorrow?**
  - A. AlienVault**
  - B. Sourcefire**
  - C. Nessus**
  - D. Metasploit**



# Answer #7

- **B**
  - Sourcefire is an intrusion prevention system that can be configured to block traffic to your web server containing the problematic password values
  - None of the other tools listed is an IPS or could reasonably be expected to perform the task at hand





# Scenario for Questions 8-10

- You are an analyst at a large organization and are tracking a fairly large sophisticated adversary who appears to have compromised some hosts on your network. This actor's tactics, techniques, and procedures (TTPs), gleaned from a threat intelligence feed, include consolidating files on an internal, compromised host, compressing them onto one file, encrypting them, and then sending them to an external server. The internal aggregator runs a server on TCP port 1337.



# Question #8

- **8. Using which of the following tools might you best determine if any of your internal hosts are listening on port 1337?**
  - A. Snort
  - B. Wireshark
  - C. nmap
  - D. netstat



# Answer #8

- **C**
  - Though any of the options listed might work in certain specific conditions, nmap is the best answer because you can use it to quickly and remotely check all hosts on your network
  - Snort and Wireshark would only be able to identify the server(s) if they captured traffic to/from it
  - Netstat would require you to remotely log into all hosts and see if port 1337 was listening, which is very time-consuming way to check a large network



# Question #9

- **9. You find a host running an illicit server on port 1337 and move it to an isolated virtual local area network (VLAN) to prevent further data loss. The next step is to find any other compromised hosts that might be trying to communicate with the rogue server. You quickly provision a new Linux host with the same hostname and IP address and then start a web server on port 1337. Which tool might let you track compromised hosts trying to connect to that socket?**
  - A. tcpdump**
  - B. ifconfig**
  - C. nslookup**
  - D. SHASum**



# Answer #9

- **A**
  - Tcpdump can be configured to capture only traffic destined for a given port on the local host, which would over time collect the source IP addresses of any other compromised hosts
  - Tcpdump can capture packets and save them to a remote shared file, which would allow you to monitor it for changes instead of manually checking time and again



# Question #10

- **10. You want to make a forensic image of the isolated server's hard drive and then ensure the integrity of all the copied data. Which combination of tools is best suited for these tasks? (Choose two)**
  - A. mv
  - B. cp
  - C. md5sum
  - D. dd
  - E. shasum



# Answer #10

- **D, E**
  - The **dd** utility is often used to make a bit-for-bit forensic copy of secondary storage devices such as hard disk drives
  - In order to ensure the integrity of the data, you could use either **md5sum** or **shasum**, but the latter is preferred, particularly if you use **SHA-256** or better
  - The **cp** (copy) command or **mv** (move) command could conceivably be used to copy or move specific files, respectively, but certainly neither would be able to make a forensic duplicate of a disk or file system



# References

1. **Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.**

