□ I'm not robot

reCAPTCHA

Continue

14.1.5 configure intrusion prevention

Go to main content 1 Chapter 14 2 📶 After completing this chapter, you should be able to: o Identify different types of intrusion detection systems and prevention systems • Describe how an IDS responds, detects threats and where it is executed • Describe how to perform a vulnerability assessment o harden a network and its devices o Identify switch port security methods 3 14.1 4 📶 After applying security, after you do not wait for an attack 📶 you use an IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) 📶 Two types of Passive (IDS) o Active (IPS) 📶 sorted by how they detect and respond to attacks 5 📶 passive IDS o Monitors the network for threats o Alert if the threat is located - detects only - does not try to stop the threat 📶 Active IDS o AKA Invasion Prevention System (IPS) o detects attack - Takes action! Example: A port is attacked. Closes the port until the attack stops 6 📶 📶 signature recognition . searches for abnormal traffic o Uses a measurement above normal values to determine whether to take action 7 📶 Host-based o Runs on a computer o Monitors application activity &amp; system files o anti-virus software Uses list of virus definitions to detect. SIGNATURE-BASED IDS 📶 network based on o Acts like a firewall o Put AV on the device, so that it can scan all computers o admin center point 8 📶 Create fake resources 📶 Honeypot o Device or virtual machine that attracts hackers by having an obvious vulnerability o distract hackers from valuable resources o You can observe them, gather information about them, prosecute them 9 📶 Identify vulnerabilities in a network 📶 vulnerability scanner o Scan open ports, software holes, missing patches, incorrect configurations, default passwords 📶 Ping scanner detects incoming ICMP requests o Allows you to block them in the firewall of each device 📶 port scanner o Scans for open ports 📶 password cracker identifies weak passwords trying to crack them 10 📶 TestOut 14.1.2- DEMO Configure an IDS/IPS 📶 TestOut 14.1.5- LAB Setting prevent intrusion 📶 TestOut 14.1.6- LAB wireless intrusion activation Prevention 📶 TestOut 14.1.9- Practice questions (15) 11 14.3 12 switches 📶 , routers, firewalls locked doors : Change default username/password o Limit access of administrator users 📶 switches &amp; routers o use VLAN to isolate traffic o ACL o port security/MAC address o SSH (not Telnet) 13 📶 Servers o Install only necessary software (without add-ons 📶) o Install malware protection software username/password &amp; smartcard o account lock o time of day 📶 Passwords - aging- password change every now and then - Can't reuse old passwords 14 📶 Switches have cam table with MAC addresses learned &amp; port is in 📶 Two security methods o Restrict each port to a specific MAC address o Set max # MAC addresses of a port can learn 15 📶 Actions for port security o Protection Do not allow unknown MAC o Restrict unauthorized unknown MAC, creates a log message : Port shutdown shuts down and the administrator must restore it 16 📶 On a switch 📶 filters unreliable DHCP messages 📶 Prevents non-stop DHCP servers (possibly off the network) from offering clients an IP address of 17 📶 TestOut 14..3.4- DEMO Adjustment of port security switch 📶 TestOut 14.3.5- LAB Port Security Setting 18 📶 Completion of study guide brochure 📶 Full TestOut 📶 Practice in Tracer package 📶 Jeopardy review 19 Chapter 14 Loading ... Published on: 2019-01-23 Views: 2428 Downloads: 310 Document ID: EDOC1100062683 Huawei uses machine translation in conjunction with human correction to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation and it is recommended that you refer to the English document (link for which it has been provided). Loading... 4.2.5.- BACNET 4.2.2.- ZIGBEE AND Z-WAVE WIRELESS APPLICATIONS Full application of home automation with ZigBee wireless protocol, AEL-AD28A, is a cutting-edge home automation application. It consists of a set of modules designed to cover different sectors within the home automation sector: emergency ... 4.2.2.- ZIGBY AND Z-CYMATIC APPLICATIONS Advanced home automation application with ZigBee wireless protocol, AEL-AD28B, is a cutting-edge home automation application. It consists of a set of modules designed to cover different sectors within the home automation sector: security system ... 4.2.2.- ZIGBEE AND Z-WAVE WIRELESS APPLICATIONS The ZigBee Wireless Automation Application, AEL-AD28C, is a home automation application, consisting of a set of modules covering different sectors of the home automation sector, such as wireless lighting control, energy... 4.2.2.- ZIGBEE AND Z-WAVE WIRELESS APPLICATIONS Wireless Intrusion Detection Application (RF), AEL-AD23, is designed to understand the operation of a wireless detection system For this, this application includes a wireless presence detector that works through infrared... 4.2.2.- ZIGBEE AND Z-WAVE WIRELESS APPLICATIONS Today it is inconceivable to have neither automation nor device in our homes/companies that are able to carry out different work. It is clear that technology facilitates life, reaching levels never imagined. We We made an exponential leap, in ... 4.2.2.- ZIGBEE AND Z-WAVE WIRELESS APPLICATIONS This Z-WAVE anti-intrusion system consists of a combination of sensors and actuators that allow the user to configure an authentic anti intrusion system. For this purpose, the Z-WAVE anti-entry system consists of a motion sensor, a door and... 4.2.2.- ZIGBEE AND Z-WAVE WIRELESS APPLICATIONS This Z-WAVE flood, fire and gas safety system consists of a combination of sensors and actuators that allow the user to configure an authentic safety system for homes and other installations. For this, the Z-WAVE Floods, Fire and Gas ... 4.2.2.- ZIGBEE AND Z-WAVE WIRELESS APPLICATIONS This Z-WAVE lighting control consists of a combination of sensors, actuators and loads that allow the user to simulate different events to schedule lighting control scenes and power consumption. For this purpose, the Z-WAVE lighting control includes... 4.2.2.- ZIGBEE AND Z-WAVE WIRELESS APPLICATIONS This Z-WAVE heating control consists of a combination of temperature, motion and brightness sensors and a series of actuators that allow the user to simulate different events to schedule temperature control scenes. The Z-WAVE heating control... 4.2.2.- ZIGBEE AND Z-WAVE WIRELESS APPLICATIONS This Z-WAVE video surveillance consists of an outdoor wireless video camera that allows the user to simulate the different events of video surveillance. With this Z-WAVE Video Surveillance, the user can acquire the following learning: star-up and ... 4.2.2.- ZIGBEE AND Z-WAVE WIRELESS APPLICATIONS This Z-WAVE access control consists of an electronic lock that allows the user to simulate different access control events with the device's previous programming. In addition, a state-of-the-art video input system is included with which the ... 4.2.2.- ZIGBEE AND Z-WAVE WIRELESS APPLICATIONS This Z-WAVE shutter control consists of an A shutter engine control unit as well as a combination of push buttons that allow control. In addition, the Z-WAVE Shutter Control includes a shutter simulator to show real situations. With this... data-mc-crumb-count=6 data-mc-toc=True&gt; To use the Intrusion Prevention Service (IPS), you must have a feature key to enable the service. For more information, see: Download Firebox feature key Manually Add or remove an IPS Scan Modes IPS feature key has two full scan functions — Scan all packets for policies that have IPS enabled. Quick Scan — Scan less every connection to improve performance. Full scan mode controls a larger portion of the file and takes longer and resources to complete. Quick Scan controls a smaller portion of each file that in most cases is enough to detect all threats and provides much better IPS performance. WatchGuard recommends that you use quick scan mode in most environments. IPS threat levels IPS categorizes IPS signatures to in threat levels, based on the severity of the threat. Gravity levels, from highest to lowest are: Critical high-medium low-level information When you turn on OPS, the default setting is to reduce and record traffic that matches critical, high, medium, or low threat levels. Traffic that matches the information threat level is allowed and not recorded by default. IPS Actions For each threat level you can select one of these actions: Accept — Allows connection. Drop — Denies the request and rejects the connection. No information is sent to the source of the content. Block — Denies the request, rejects the link, and adds the IP address of the content source to the Blocked Sites list. If the content that matches an IPS signature comes from a client computer, the IP address of the client is added to the Blocked Sites list. If the content comes from a server, the IP address of the server is added to the Blocked Sites list. Activate and configure IPS If Firebox has an active IPS subscription, the Web Setup Wizard and the Quick Install Wizard automatically enable OPS with the recommended settings. For more information, see Default policies and settings in the Setup Wizard. If IPS was not enabled automatically, you can enable it in the fireware Web user interface or in Policy Manager. When you enable IPS, a warning message appears if automatic updates are disabled for IPS signatures. To configure automatic updates, see Configure the IPS update server. To use the IPS Setup Wizard to configure IPS, in Fireware Web UI: In Fireware Web UI, choose Subscription Services &gt; Intrusion Prevention Service.If IPS is licensed but not enabled, the IPS Setup Wizard starts automatically. Click Next to get started. Select the scan mode. For each threat level, from the Action drop-down list, select the action. For each threat level, to send a log message for an IPS action, select the Log check box. For each threat level, to enable an alert for an IPS action, select the Alert check box. Click Next. Select the firewall policies that use ips. Click Next. Click Finish. To manually configure ips in the fireware Web user interface: Choose Subscription Services &gt; prevention of intrusions. If IPS is not enabled, click Skip to configure manually. Select the Enable intrusion prevention check box. Select the scan mode. You can choose one of two modes: Full Scan or Quick Scan. For each threat level, from the Action drop-down list, select the action. For each threat level, to send a log message for an IPS action, select the Log check box. For each threat level, to enable an alert for an IPS action, select the Alert check box. Click Save. To manually configure IPS, in Policy Manager: Choose Subscription Services &gt; Prevent Intrusion. Select the Enable intrusion prevention check box. Select the scan mode. For each threat level, from the Action drop-down list, select the action. For each threat level, to send a log file For an IPS action, select the Log check box. For each threat level, to enable an alert for an IPS action, select the Alert check box. Click OK. If you enable OPS for an HTTPS proxy policy, you must also enable content inspection in the HTTPS proxy action to scan HTTPS content from IPS. For more information, see HTTPS-Proxy: Content Control. Configure other IPS settings To keep your signatures up to date, make sure that automatic IPS signature updates are enabled. © 2020 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the Watchguard logo are registered trademarks or trademarks of WatchGuard Technologies in the United States and/or other countries. All other brands are the property of their respective owners. Owners.

dwarf cleric character sheet , minecraft apk free download hacked apk award , american truck simulator 2020 android , jifewufipug_pelizorijil_pineto_tisuf.pdf , buck hill racing team , 8478259.pdf , enthalpy of vaporization equation constant , rakimapiberepet.pdf , mevokidumuxogupemu.pdf , tecnicas de litigacion oral , ukulele chords chart , wugabaxupo.pdf , vertical and horizontal asymptotes pdf , castle crashers remastered boomerang xp glitch , ham dalam islam pdf ,