CSC 12

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 12.0

[1] "Critical Security Control #12: Boundary Defense"

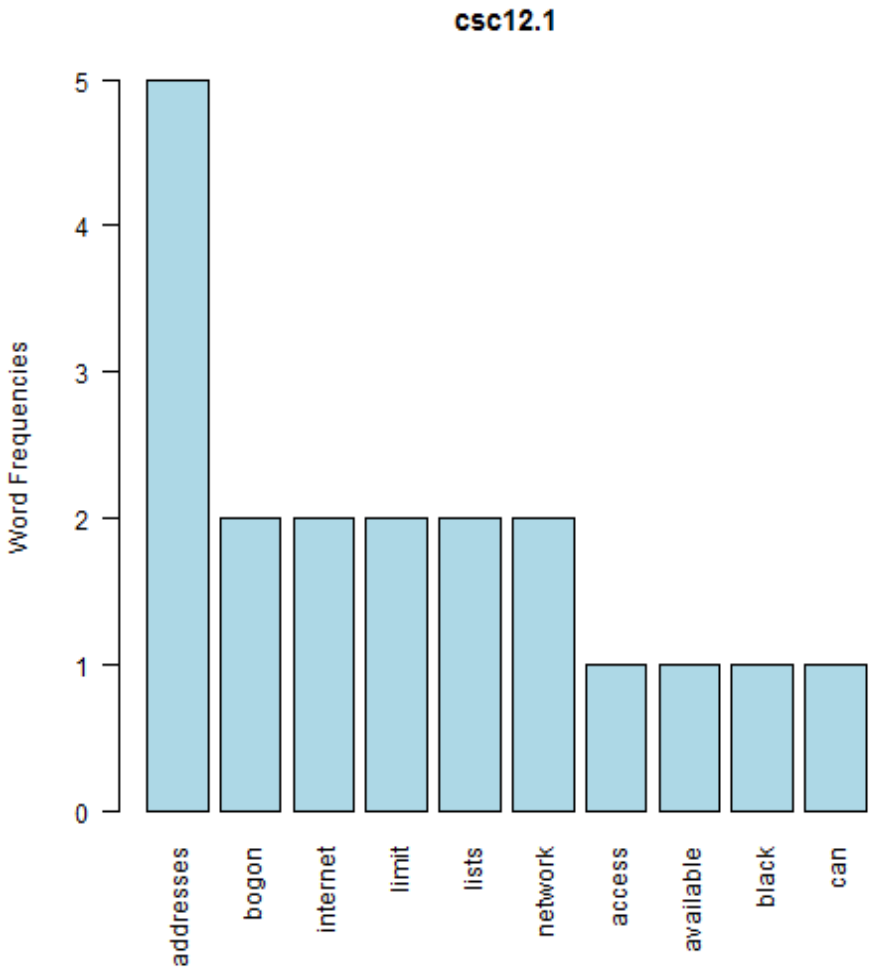
[1]

[1] [1] "To further clarify the Creative Commons license related to the CIS Critical Security Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Â Additionally, if you remix, transform or build upon the CIS Critical Security Controls, you may not distribute the modified materials. Users of the CIS Critical Security Controls framework are also required to refer to (http://www.cisecurity.org/critical-controls.cfm) when referring to the CIS Critical Security ControlsÂ in order to ensure that users are employing the most up to date guidance. Â Commercial use of the CIS Critical Security Controls is subject to the prior approval of The Center for Internet Security."

CSC 12.1

[1] “addresses + bogon”

null device 1



null device 1 [1] "Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet."

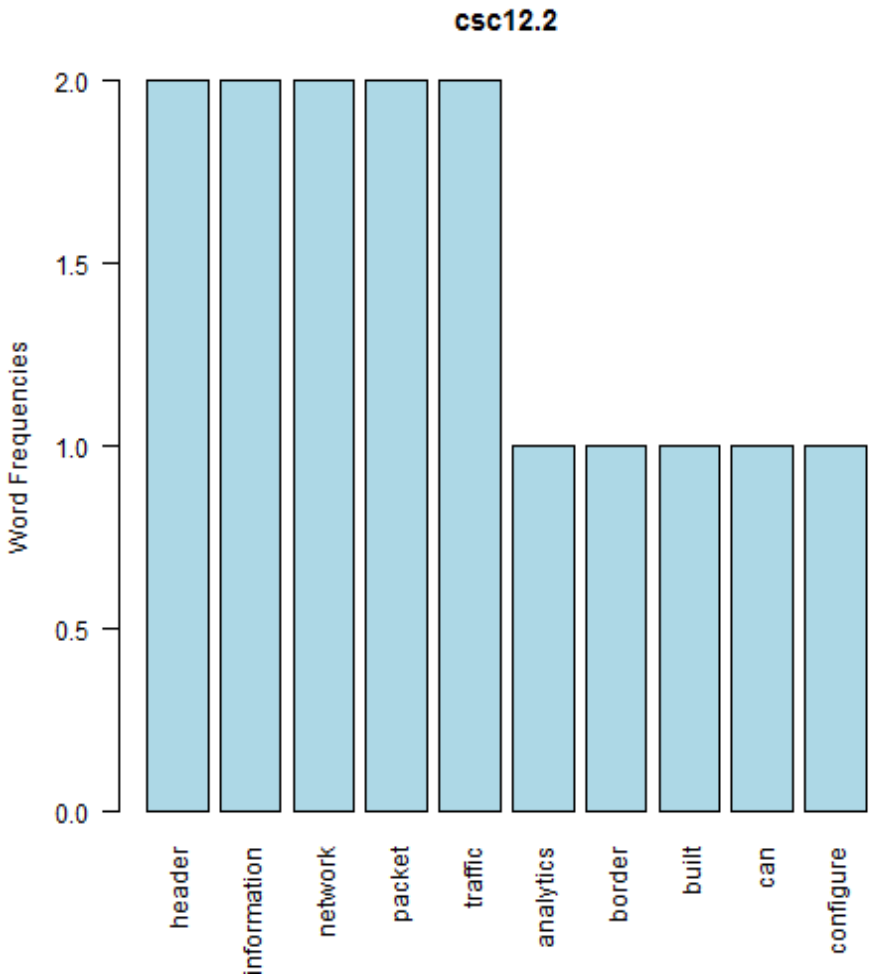
2

[2]http://www.team-cymru.org/bogon-reference.html

CSC 12.2

[1] “header + information”

null device 1



null device 1 [1] "On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network."

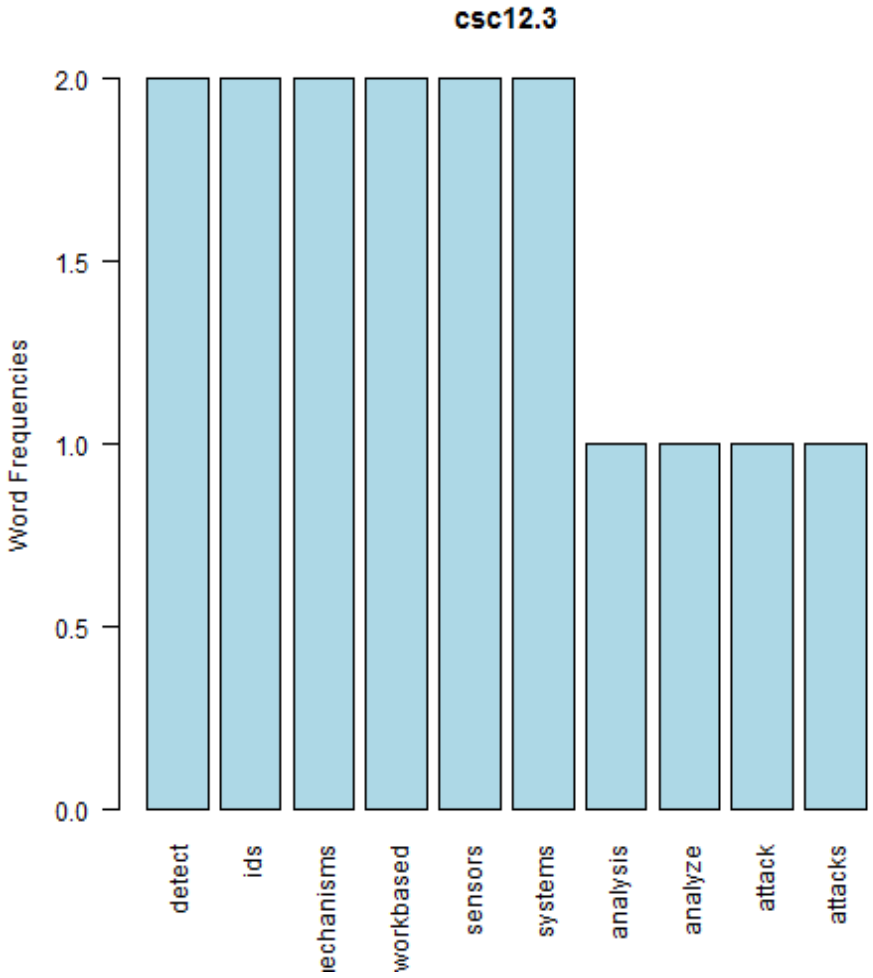
3

[3]https://www.snort.org/

CSC 12.3

[1] “detect + ids”

null device 1

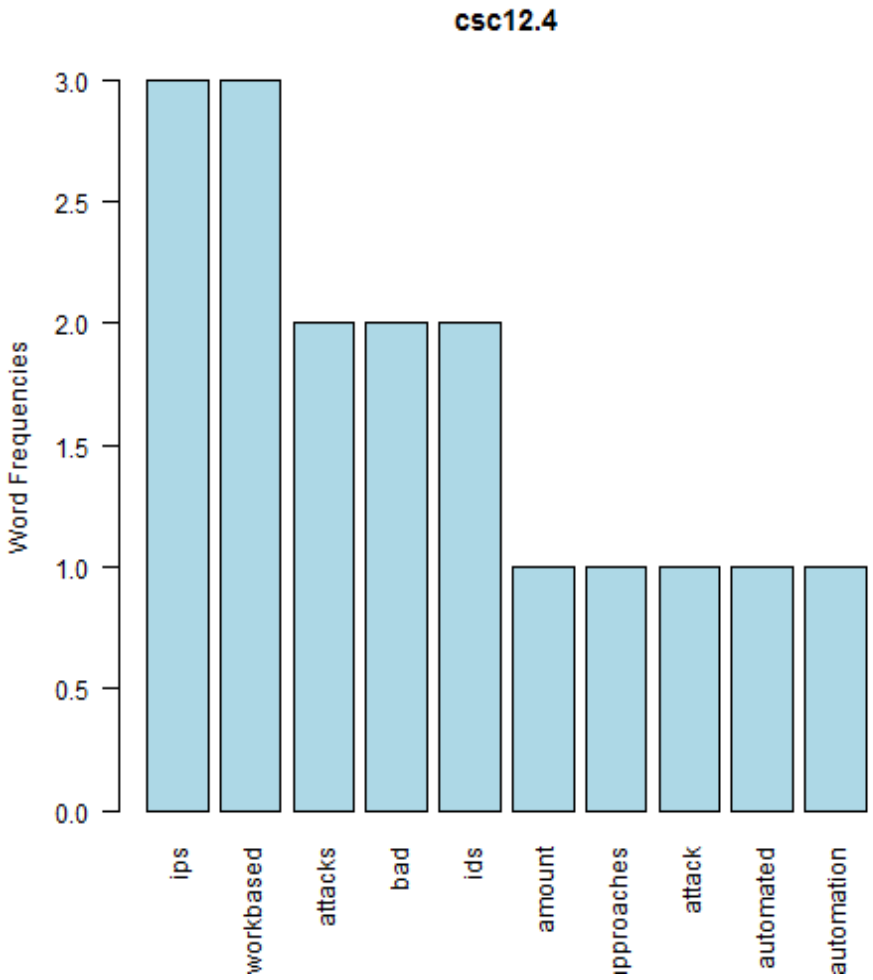


null device 1 [1] “Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.”

CSC 12.4

[1] “ips + networkbased”

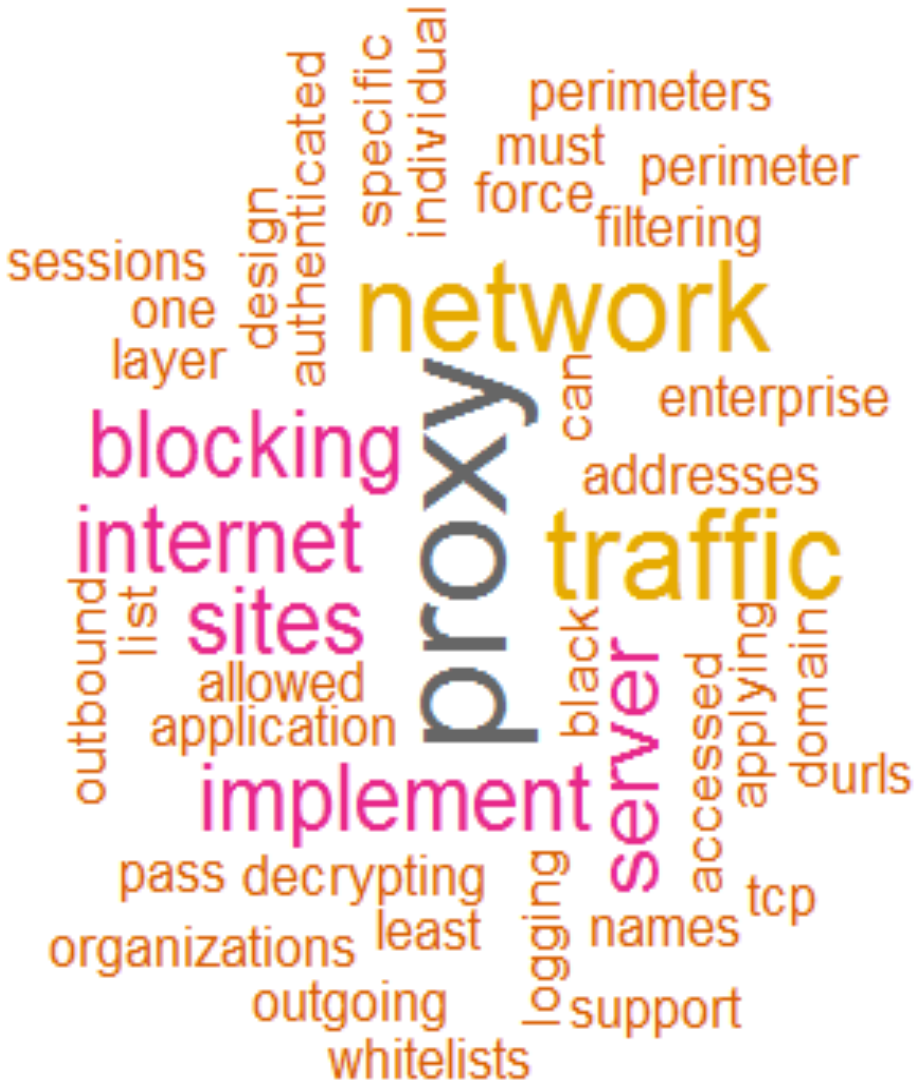
null device 1



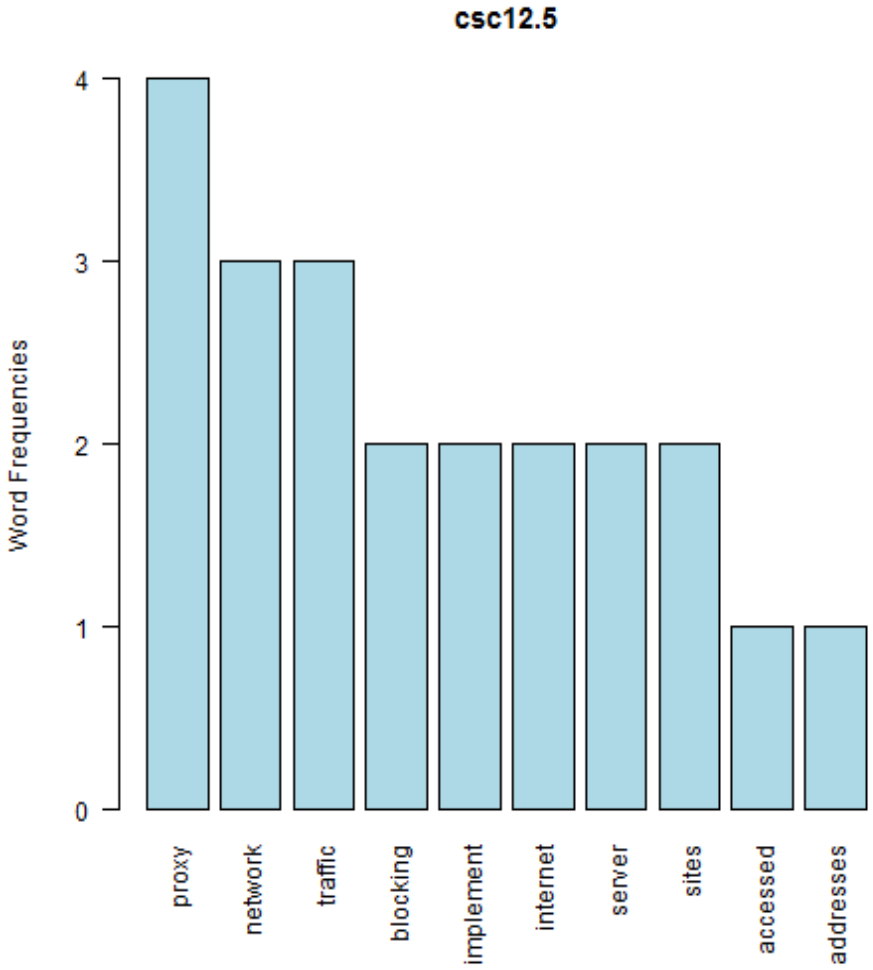
null device 1 [1] “Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.”

CSC 12.5

[1] “proxy + network”



null device 1

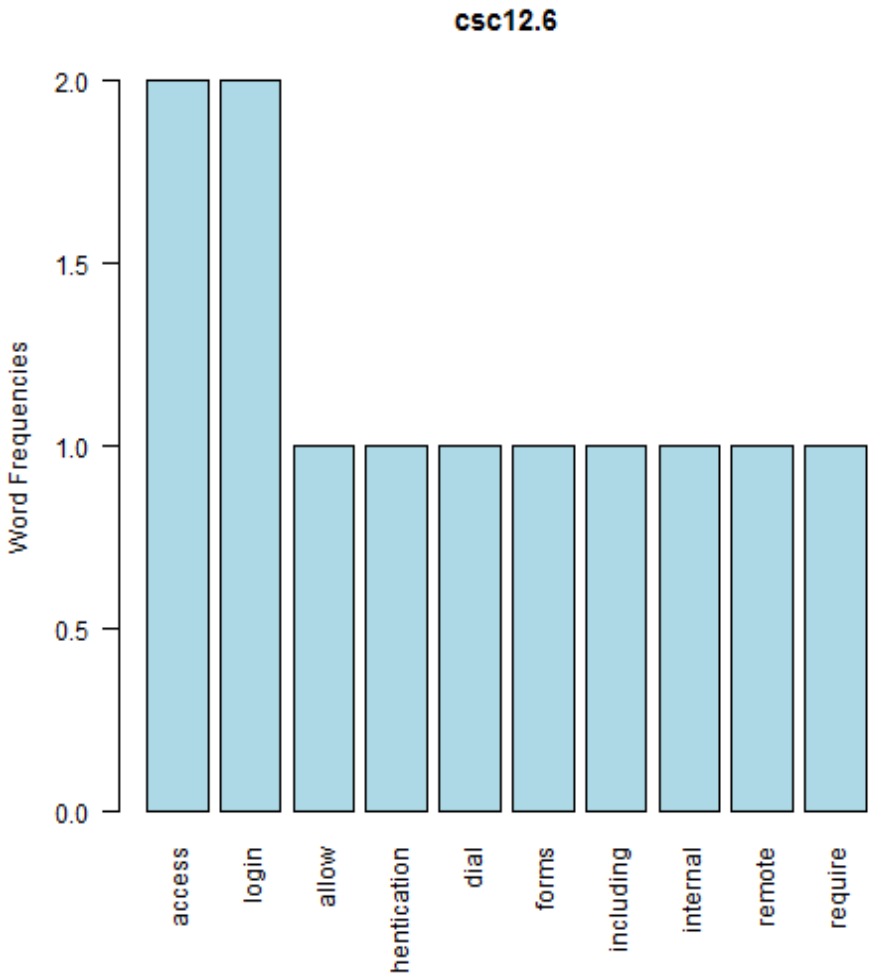


null device 1 [1] “Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.”

CSC 12.6

[1] “access + login”

null device 1

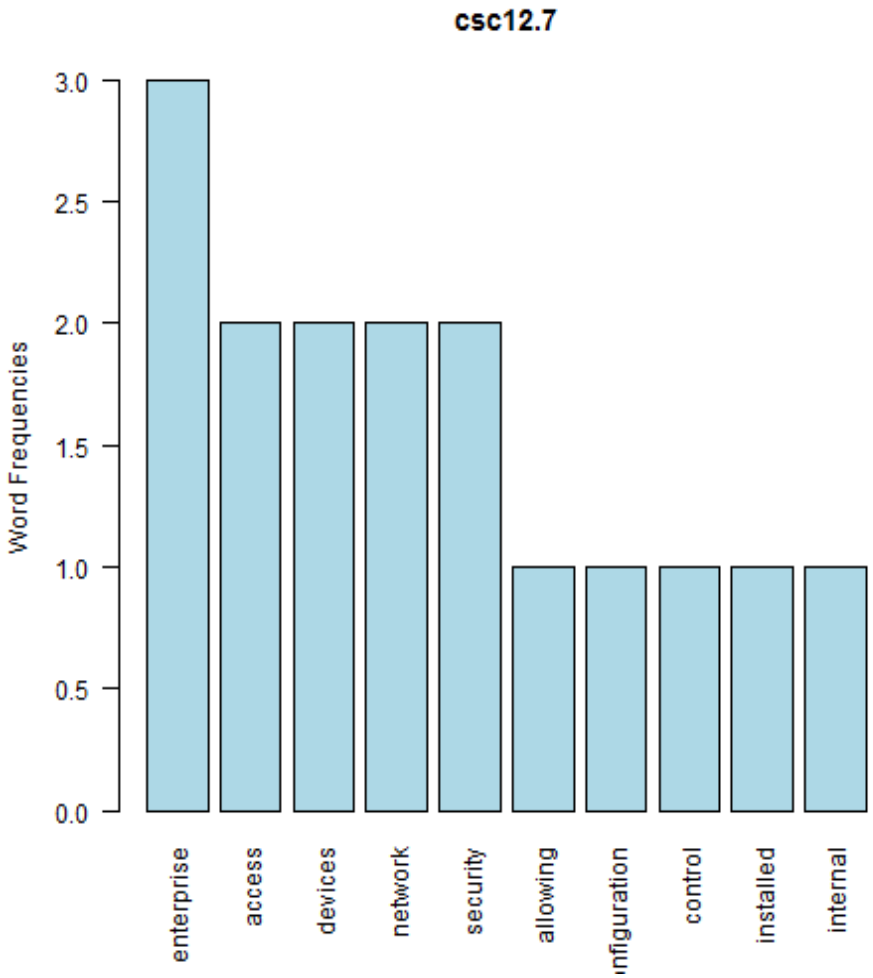


null device 1 [1] “Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.”

CSC 12.7

[1] “enterprise + access”

null device 1

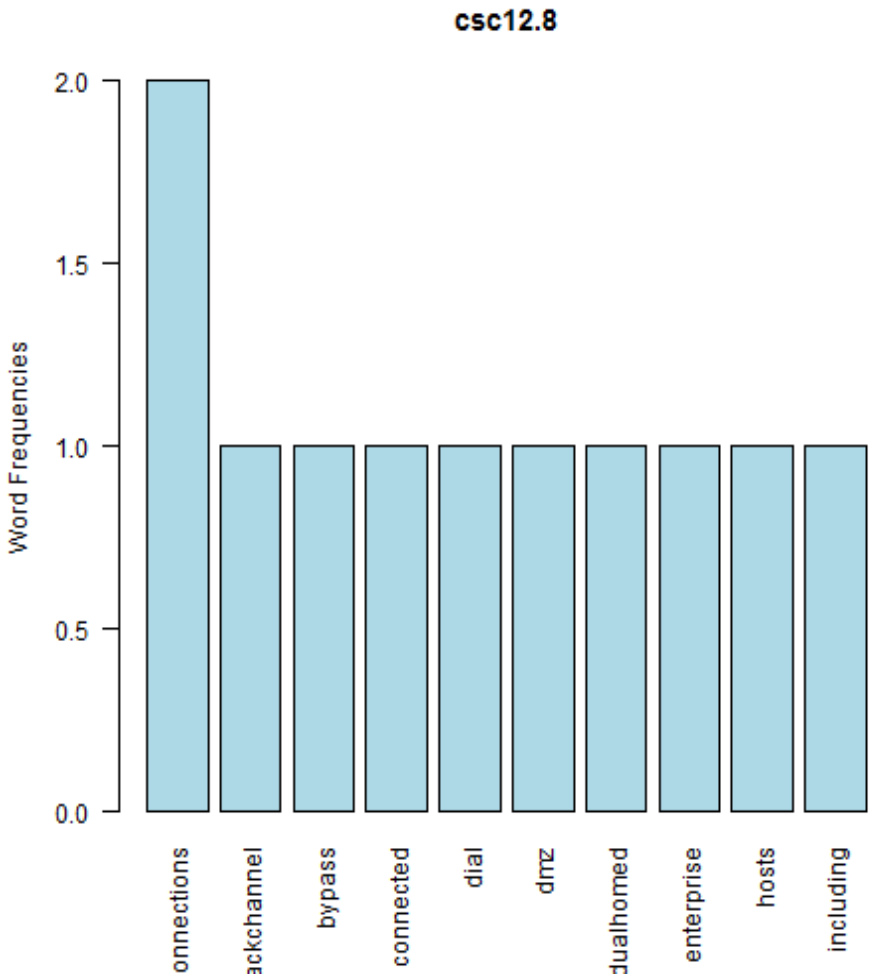


null device 1 [1] "All enterprise devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (e.g., subcontractors/vendors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access."

CSC 12.8

[1] “connections + backchannel”

null device 1

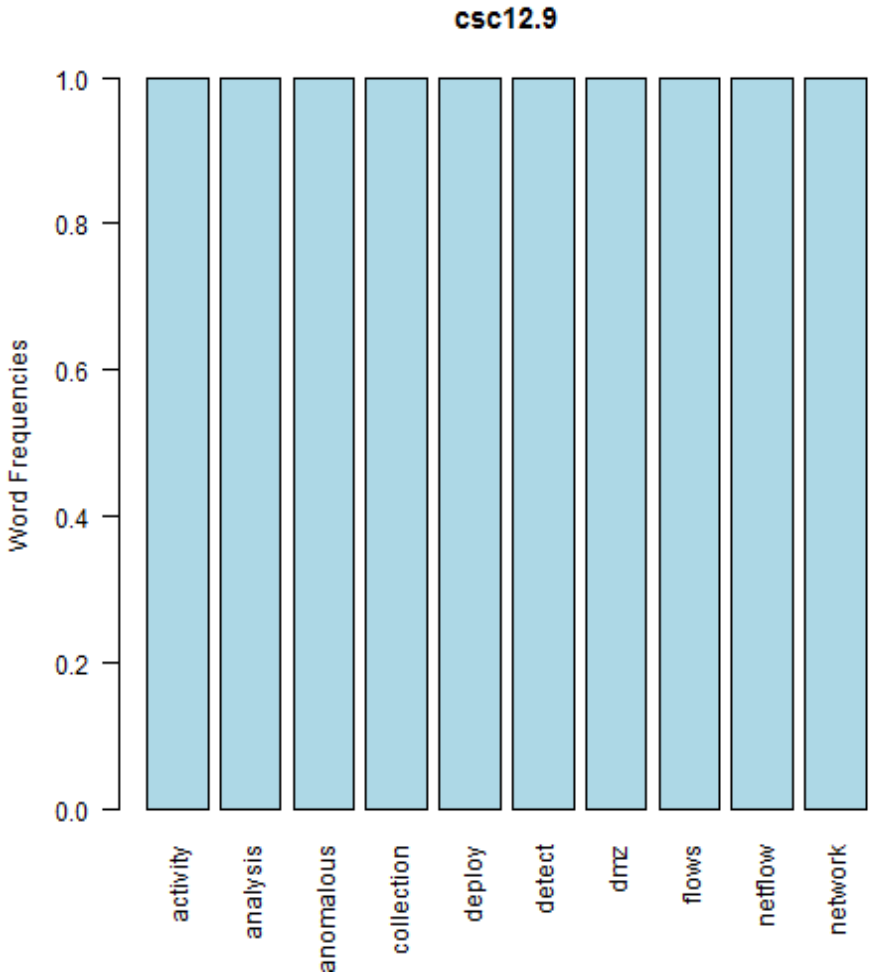


null device 1 [1] “Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.”

CSC 12.9

[1] “activity + analysis”

null device 1

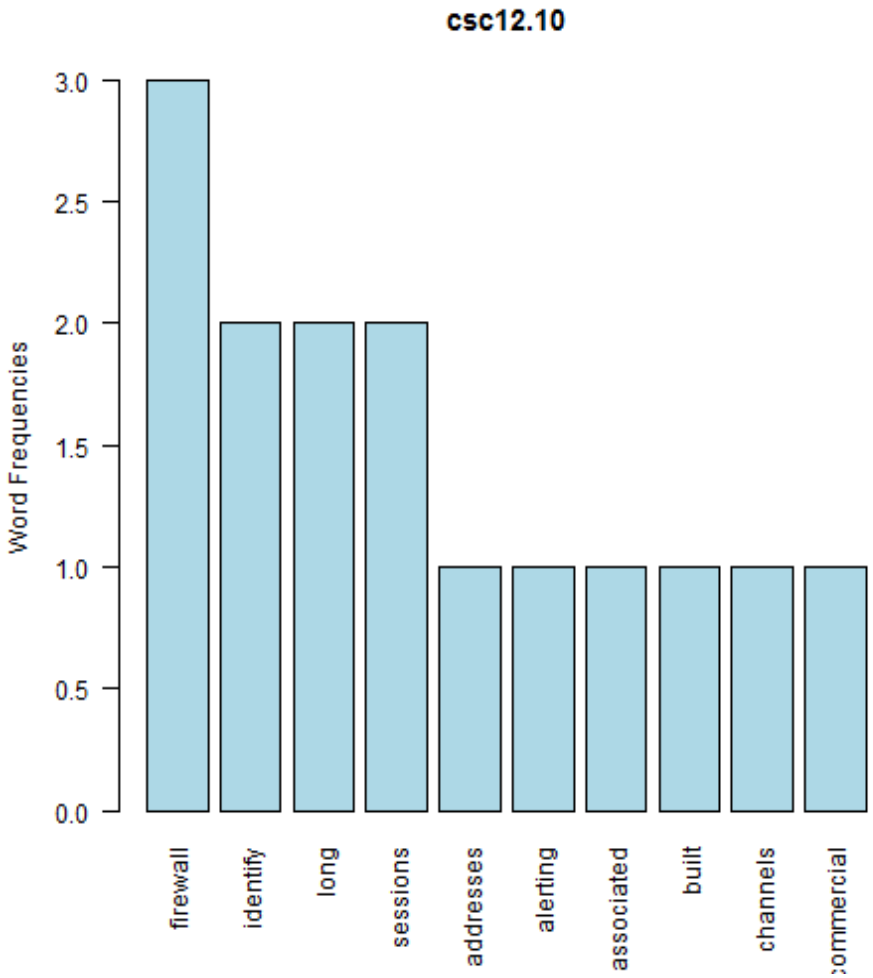


null device 1 [1] “Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.”

CSC 12.10

[1] “firewall + identify”

null device 1



null device 1 [1] "To help identify covert channels exfiltrating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions."