CSC 20

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 20.0

[1] "Critical Security Control #20: Penetration Tests and Red Team Exercises"

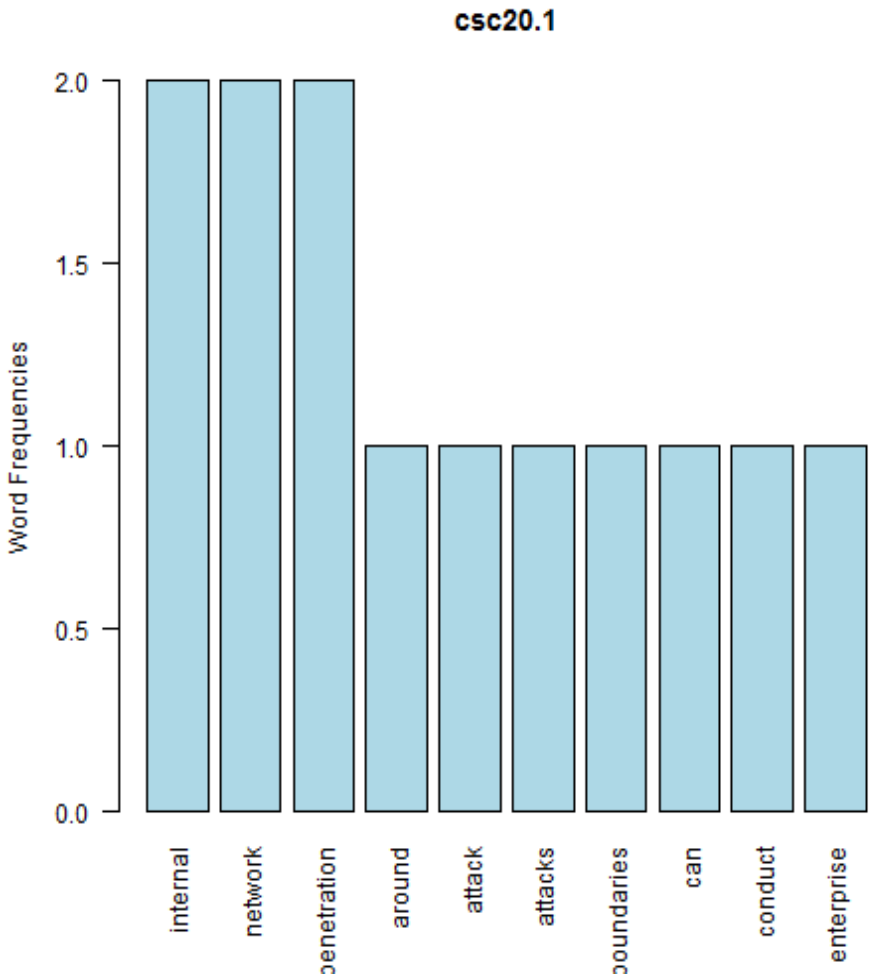
[1]

[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 20.1

[1] “internal + network”

null device 1

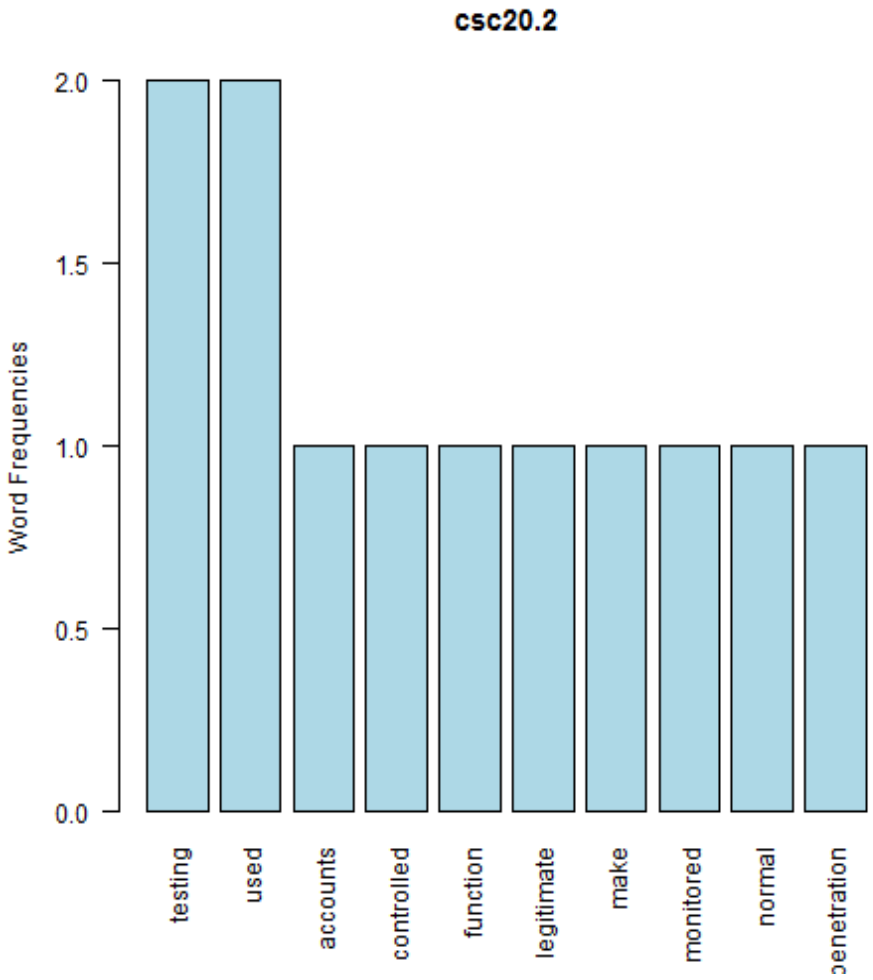


null device 1 [1] "Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks."

CSC 20.2

[1] “testing + used”

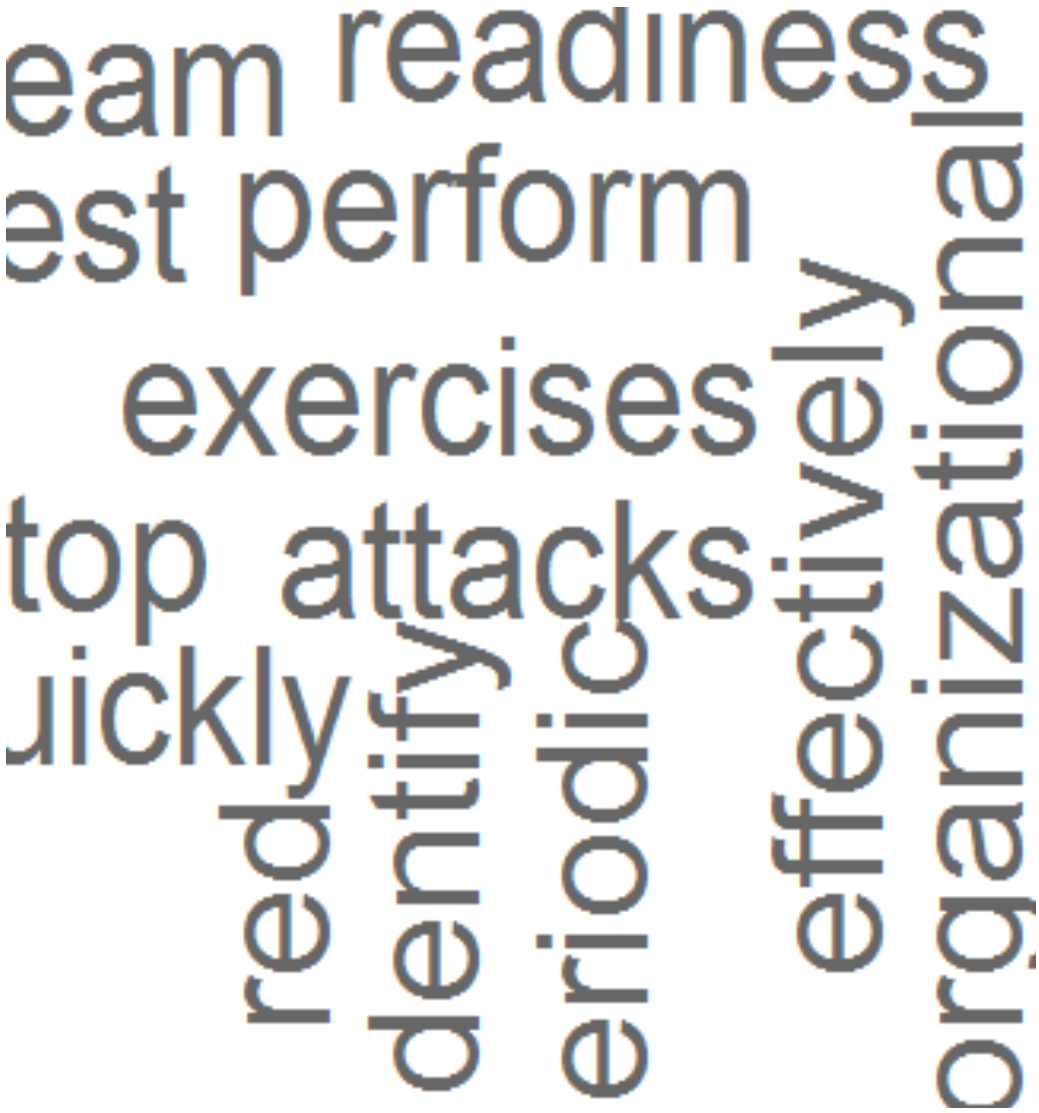
null device 1



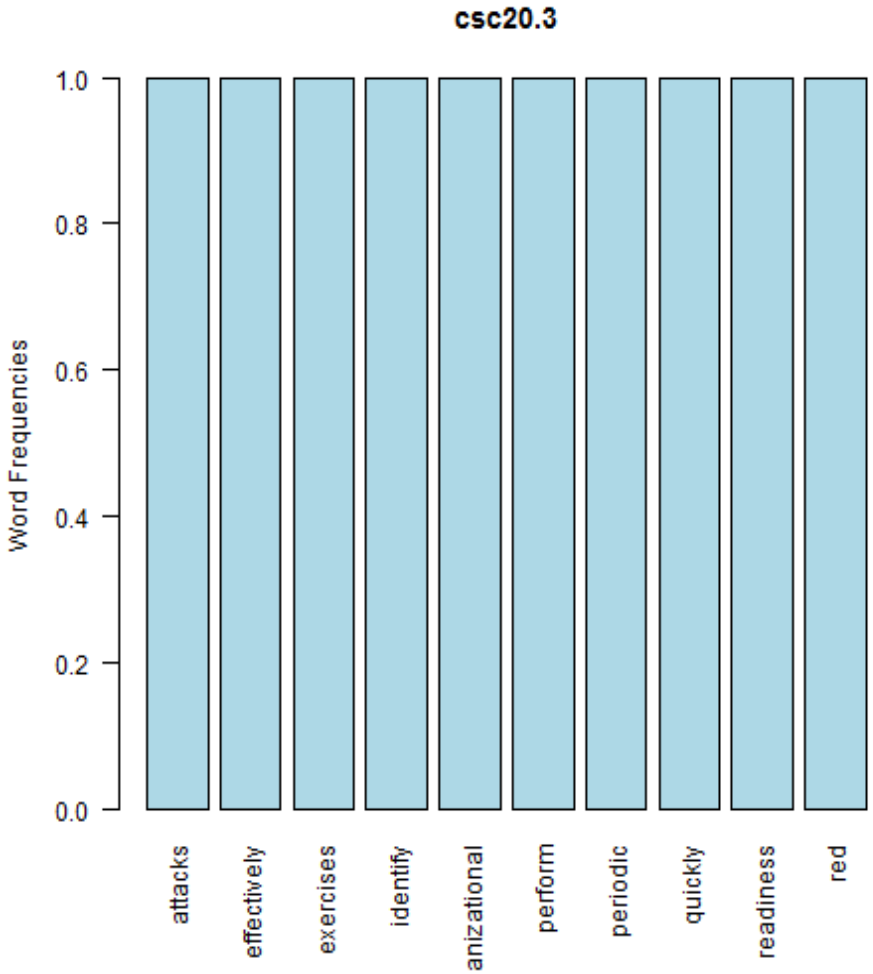
null device 1 [1] "Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over."

CSC 20.3

[1] “attacks + effectively”



null device 1

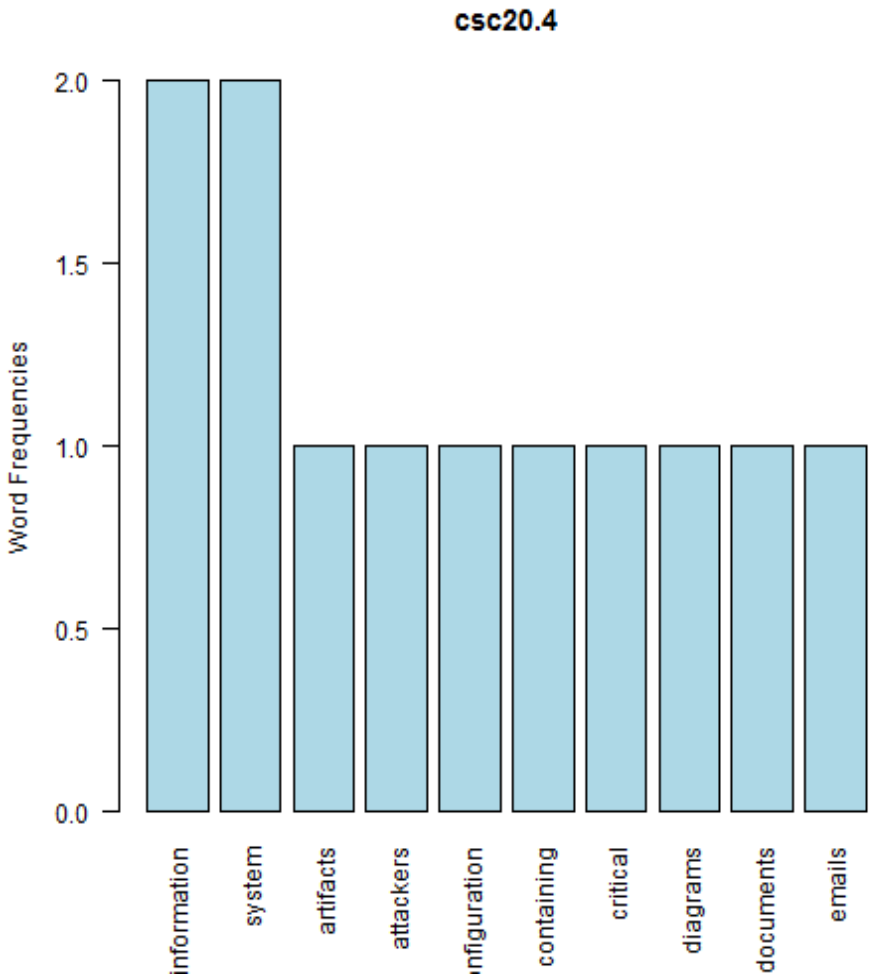


null device 1 [1] “Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.”

CSC 20.4

[1] “information + system”

null device 1

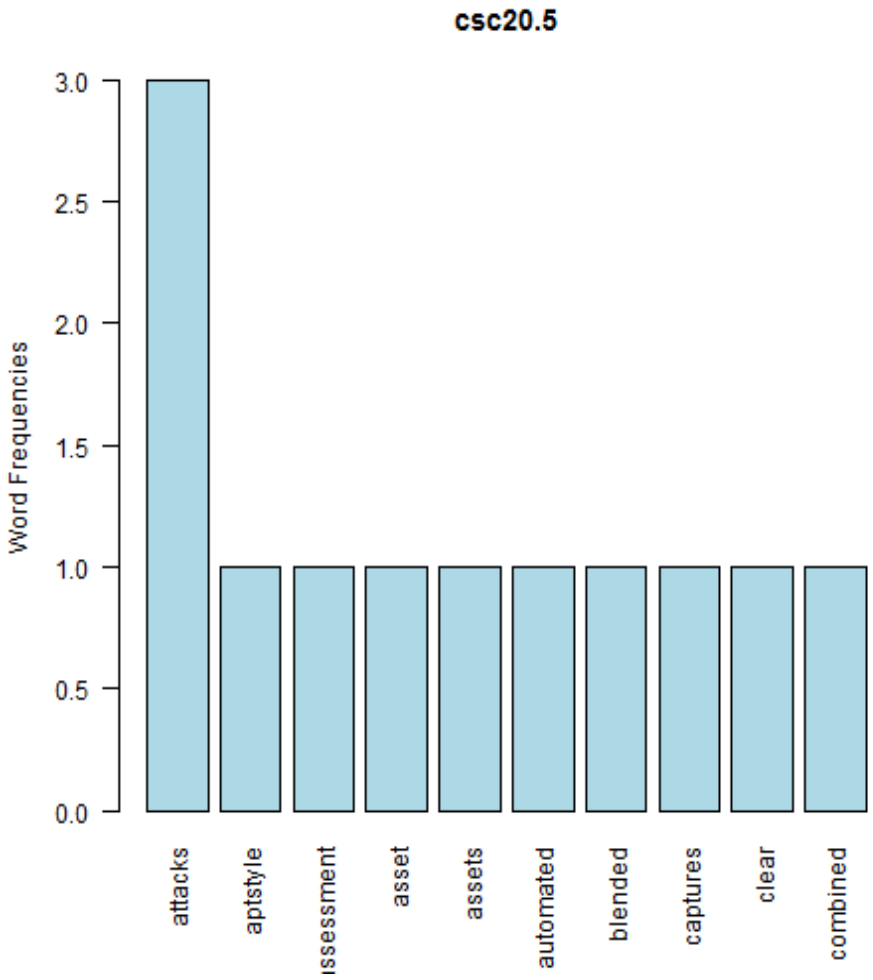


null device 1 [1] “Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.”

CSC 20.5

[1] “attacks + aptstyle”

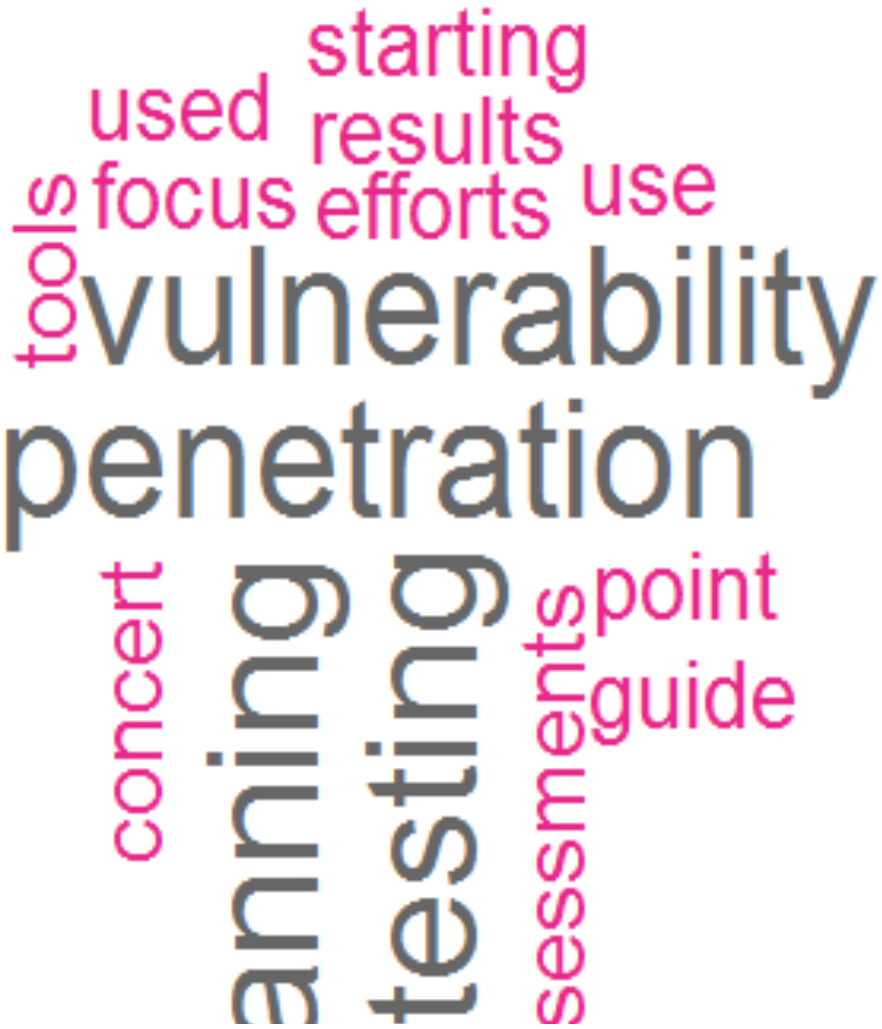
null device 1



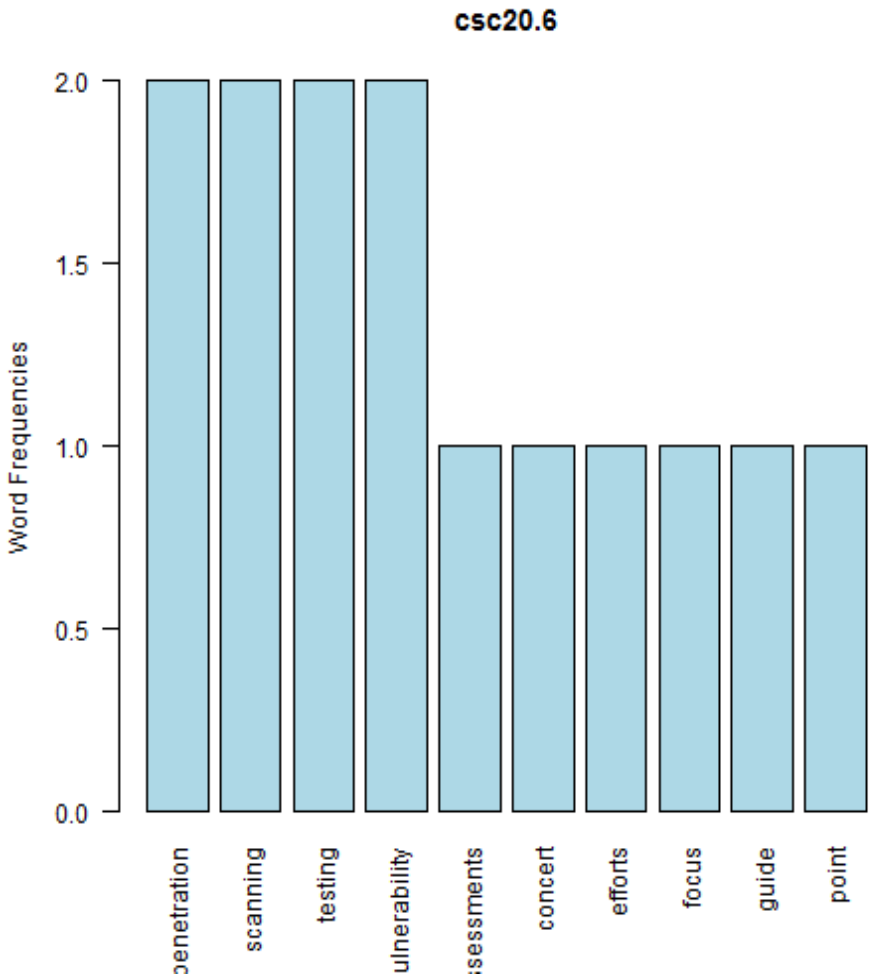
null device 1 [1] “Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectorsâ ”often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.”

CSC 20.6

[1] “penetration + scanning”



null device 1

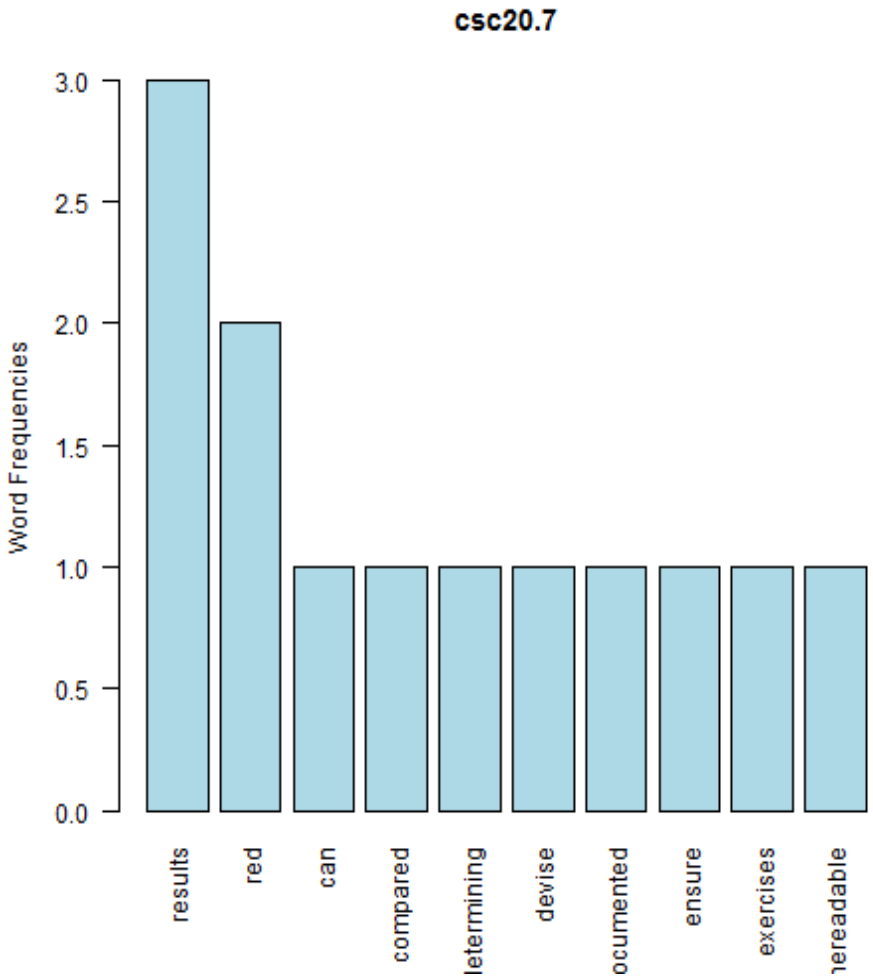


null device 1 [1] “Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.”

CSC 20.7

[1] “results + red”

null device 1

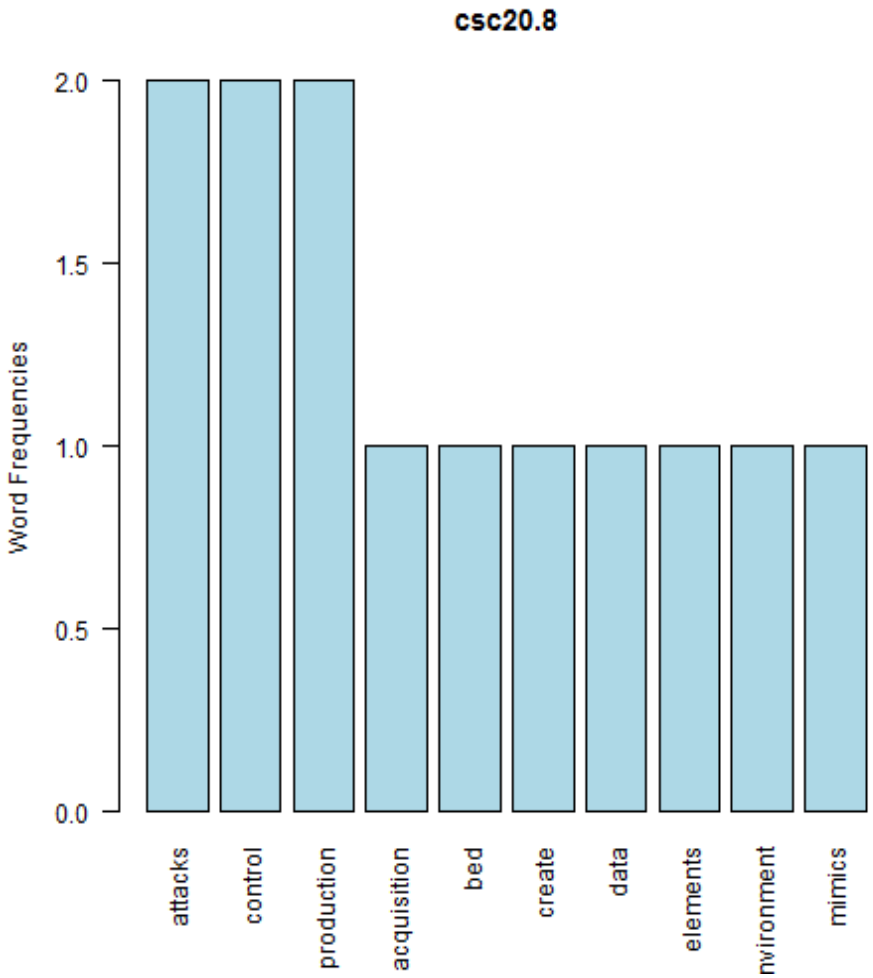


null device 1 [1] "Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time."

CSC 20.8

[1] “attacks + control”

null device 1



null device 1 [1] “Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.”