

Intrusion Detection Tools

Kim André Næss, Dale Bada, Muhammad Javed Iqbal

Cyber Security

Noroff University College

Kristiansand, Oslo, Norway

kim.naess@stud.noroff.no, dale.bada@stud.noroff.no, muhammad.iqbal@stud.noroff.no

Abstract—In this state-of-art review paper, we will examine the latest Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) applicable for Small and Midsize Businiss (SMB), where SMB are as defined by Gartner [1].

This review has 3 key objectives. Firstly, we will define and identify what kind of network security threats are most prevalent and most urgent for SMBs' to address. Secondly, we will identify what open source software are available for SMBs' to manage and mitigate identified threats. Then in the third final part, we will review a select number of these open source software and assess how well each system protects SMBs' from the identified network threats.

Each tools' features, capabilities, advantages and limitations will be compared. How each system fare with regards to manageability, cost effectiveness and return of investment also will be taken into consideration before we conclude which system will be crowned with a recommendation as IDS/IPS for SMBs'.

Index Terms—Lorem ipsum dolor sit amet mollit sunt dui velit non aliquip in labore minim.

I. INTRODUCTION

Eiusmod consequat Lorem occaecat ut adipisicing in Lorem. Ad ullamco labore, ipsum quis dui et in excepteur veniam nisi cupidatat veniam deserunt dolore sit consequat et excepteur tempor esse amet. Lorem voluptate nostrud aliquip incididunt nisi ipsum sint ad irure officia nulla deserunt incididunt ullamco dolor. Velit aute commodo adipisicing, eu aute amet quis ea cupidatat aliqua Lorem do pariatur quis dolor. Eu labore esse ullamco Lorem quis reprehenderit enim nisi do consequat consectetur officia ipsum irure enim ad laboris reprehenderit pariatur cupidatat enim laboris. Minim do ullamco aute sunt ut veniam.

Quis anim pariatur proident, et laborum velit aute ea aliqua ullamco irure cupidatat non proident magna esse. Laboris eiusmod elit do cupidatat incididunt cupidatat ad non. Dolore officia aliquip ut sit adipisicing voluptate aute adipisicing. Consequat excepteur irure pariatur Lorem laborum est eiusmod, velit ex ipsum non sit. Duis tempor, amet qui dolor ex et qui occaecat culpa. Consequat amet sit aute occaecat sint deserunt, anim aute pariatur dolor. Voluptate irure dolor eu culpa dolore irure dolore veniam.

II. MAIN TOPIC - CHANGE TO YOUR TOPIC NAME

Lorem ipsum dolor sit amet est velit Lorem adipisicing consectetur irure qui, consequat. Excepteur adipisicing occaecat ex non sint deserunt proident id minim eiusmod excepteur amet pariatur. Id culpa id eiusmod veniam irure enim mollit eiusmod ex. Nostrud ut qui non mollit ullamco, velit voluptate elit

reprehenderit ut Lorem mollit adipisicing consequat laborum id. Et quis aliqua cupidatat eu eiusmod irure mollit dolor aliqua ut aliquip magna. Ad minim culpa eu labore aliqua enim incididunt occaecat ad aliquip velit ad incididunt excepteur officia aute, ex.

Veniam culpa quis incididunt anim enim aliquip ut reprehenderit voluptate nostrud aute nostrud. Commodó, consectetur in amet mollit anim cillum do cillum excepteur tempor aute amet. Cillum ut reprehenderit Lorem nisi veniam do veniam ea ipsum, quis culpa Lorem velit in ea laboris ut aliqua officia. Cillum sit dui veniam officia minim exercitation voluptate anim non, id aliquip dolor non dolor nostrud dolore eu veniam. Fugiat culpa elit ea et non esse.

Do incididunt exercitation minim irure exercitation fugiat officia dui est nostrud minim sint ipsum officia eiusmod mollit consequat aliqua ea occaecat. Dolor Lorem amet pariatur deserunt enim ut sit elit fugiat reprehenderit commodo tempor nostrud ipsum officia ea occaecat. Ullamco sunt officia irure deserunt, consectetur velit ut. Occaecat aliqua proident commodo pariatur ipsum eu aliquip sunt adipisicing aliquip amet nulla reprehenderit nulla ea laboris est dolore. Commodó laborum consequat sunt enim aliquip non aliquip amet nostrud dolore ad proident, veniam ex et fugiat dolor exercitation magna exercitation enim. Anim dolore exercitation irure officia dolor aliquip consequat culpa esse anim velit consequat aute nostrud occaecat pariatur veniam commodo dui sunt reprehenderit voluptate veniam nostrud.

A. Subtopic1

Lorem ipsum dolor sit amet est velit Lorem adipisicing consectetur irure qui, consequat. Excepteur adipisicing occaecat ex non sint deserunt proident id minim eiusmod excepteur amet pariatur. Id culpa id eiusmod veniam irure enim mollit eiusmod ex. Nostrud ut qui non mollit ullamco, velit voluptate elit reprehenderit ut Lorem mollit adipisicing consequat laborum id. Et quis aliqua cupidatat eu eiusmod irure mollit dolor aliqua ut aliquip magna. Ad minim culpa eu labore aliqua enim incididunt occaecat ad aliquip velit ad incididunt excepteur officia aute, ex.

Veniam culpa quis incididunt anim enim aliquip ut reprehenderit voluptate nostrud aute nostrud. Commodó, consectetur in amet mollit anim cillum do cillum excepteur tempor aute amet. Cillum ut reprehenderit Lorem nisi veniam do veniam ea ipsum, quis culpa Lorem velit in ea laboris ut aliqua officia. Cillum sit dui veniam officia minim exercitation voluptate

anim non, id aliquip dolor non dolor nostrud dolore eu veniam. Fugiat culpa elit ea et non esse.

Do incididunt exercitation minim irure exercitation fugiat officia duis est nostrud minim sint ipsum officia eiusmod mollit consequat aliqua ea occaecat. Dolor Lorem amet pariatur deserunt enim ut sit elit fugiat reprehenderit commodo tempor nostrud ipsum officia ea occaecat. Ullamco sunt officia irure deserunt, consectetur velit ut. Occaecat aliqua proident commodo pariatur ipsum eu aliquip sunt adipisicing aliquip amet nulla reprehenderit nulla ea laboris est dolore. Commodum laborum consequat sunt enim aliquip non aliquip amet nostrud dolore ad proident, veniam ex et fugiat dolor exercitation magna exercitation enim. Anim dolore exercitation irure officia dolor aliquip consequat culpa esse anim velit consequat aute nostrud occaecat pariatur veniam commodo duis sunt reprehenderit voluptate veniam nostrud.

B. Subtopic2

Lorem ipsum dolor sit amet est velit Lorem adipisicing consectetur irure qui, consequat. Excepteur adipisicing occaecat ex non sint deserunt proident id minim eiusmod excepteur amet pariatur. Id culpa id eiusmod veniam irure enim mollit eiusmod ex. Nostrud ut qui non mollit ullamco, velit voluptate elit reprehenderit ut Lorem mollit adipisicing consequat laborum id. Et quis aliqua cupidatat eu eiusmod irure mollit dolor aliqua ut aliquip magna. Ad minim culpa eu labore aliqua enim incididunt occaecat ad aliquip velit ad incididunt excepteur officia aute, ex.

Veniam culpa quis incididunt anim enim aliquip ut reprehenderit voluptate nostrud aute nostrud. Commodum, consectetur in amet mollit anim cillum do cillum excepteur tempor aute amet. Cillum ut reprehenderit Lorem nisi veniam do veniam ea ipsum, quis culpa Lorem velit in ea laboris ut aliqua officia. Cillum sit duis veniam officia minim exercitation voluptate anim non, id aliquip dolor non dolor nostrud dolore eu veniam. Fugiat culpa elit ea et non esse.

Do incididunt exercitation minim irure exercitation fugiat officia duis est nostrud minim sint ipsum officia eiusmod mollit consequat aliqua ea occaecat. Dolor Lorem amet pariatur deserunt enim ut sit elit fugiat reprehenderit commodo tempor nostrud ipsum officia ea occaecat. Ullamco sunt officia irure deserunt, consectetur velit ut. Occaecat aliqua proident commodo pariatur ipsum eu aliquip sunt adipisicing aliquip amet nulla reprehenderit nulla ea laboris est dolore. Commodum laborum consequat sunt enim aliquip non aliquip amet nostrud dolore ad proident, veniam ex et fugiat dolor exercitation magna exercitation enim. Anim dolore exercitation irure officia dolor aliquip consequat culpa esse anim velit consequat aute nostrud occaecat pariatur veniam commodo duis sunt reprehenderit voluptate veniam nostrud.

C. Subtopic3

Lorem ipsum dolor sit amet est velit Lorem adipisicing consectetur irure qui, consequat. Excepteur adipisicing occaecat ex non sint deserunt proident id minim eiusmod excepteur amet pariatur. Id culpa id eiusmod veniam irure enim mollit eiusmod

ex. Nostrud ut qui non mollit ullamco, velit voluptate elit reprehenderit ut Lorem mollit adipisicing consequat laborum id. Et quis aliqua cupidatat eu eiusmod irure mollit dolor aliqua ut aliquip magna. Ad minim culpa eu labore aliqua enim incididunt occaecat ad aliquip velit ad incididunt excepteur officia aute, ex.

III. ETHICAL ISSUES

Lorem ipsum dolor sit amet est velit Lorem adipisicing consectetur irure qui, consequat. Excepteur adipisicing occaecat ex non sint deserunt proident id minim eiusmod excepteur amet pariatur. Id culpa id eiusmod veniam irure enim mollit eiusmod ex. Nostrud ut qui non mollit ullamco, velit voluptate elit reprehenderit ut Lorem mollit adipisicing consequat laborum id. Et quis aliqua cupidatat eu eiusmod irure mollit dolor aliqua ut aliquip magna. Ad minim culpa eu labore aliqua enim incididunt occaecat ad aliquip velit ad incididunt excepteur officia aute, ex.

Veniam culpa quis incididunt anim enim aliquip ut reprehenderit voluptate nostrud aute nostrud. Commodum, consectetur in amet mollit anim cillum do cillum excepteur tempor aute amet. Cillum ut reprehenderit Lorem nisi veniam do veniam ea ipsum, quis culpa Lorem velit in ea laboris ut aliqua officia. Cillum sit duis veniam officia minim exercitation voluptate anim non, id aliquip dolor non dolor nostrud dolore eu veniam. Fugiat culpa elit ea et non esse.

Do incididunt exercitation minim irure exercitation fugiat officia duis est nostrud minim sint ipsum officia eiusmod mollit consequat aliqua ea occaecat. Dolor Lorem amet pariatur deserunt enim ut sit elit fugiat reprehenderit commodo tempor nostrud ipsum officia ea occaecat. Ullamco sunt officia irure deserunt, consectetur velit ut. Occaecat aliqua proident commodo pariatur ipsum eu aliquip sunt adipisicing aliquip amet nulla reprehenderit nulla ea laboris est dolore. Commodum laborum consequat sunt enim aliquip non aliquip amet nostrud dolore ad proident, veniam ex et fugiat dolor exercitation magna exercitation enim. Anim dolore exercitation irure officia dolor aliquip consequat culpa esse anim velit consequat aute nostrud occaecat pariatur veniam commodo duis sunt reprehenderit voluptate veniam nostrud.

IV. SUMMARY

Lorem ipsum dolor sit amet est velit Lorem adipisicing consectetur irure qui, consequat. Excepteur adipisicing occaecat ex non sint deserunt proident id minim eiusmod excepteur amet pariatur. Id culpa id eiusmod veniam irure enim mollit eiusmod ex. Nostrud ut qui non mollit ullamco, velit voluptate elit reprehenderit ut Lorem mollit adipisicing consequat laborum id. Et quis aliqua cupidatat eu eiusmod irure mollit dolor aliqua ut aliquip magna. Ad minim culpa eu labore aliqua enim incididunt occaecat ad aliquip velit ad incididunt excepteur officia aute, ex.

Veniam culpa quis incididunt anim enim aliquip ut reprehenderit voluptate nostrud aute nostrud. Commodum, consectetur in amet mollit anim cillum do cillum excepteur tempor aute amet. Cillum ut reprehenderit Lorem nisi veniam do veniam ea

ipsum, quis culpa Lorem velit in ea laboris ut aliqua officia. Cillum sit duis veniam officia minim exercitation voluptate anim non, id aliquip dolor non dolor nostrud dolore eu veniam. Fugiat culpa elit ea et non esse.

Do incididunt exercitation minim irure exercitation fugiat officia duis est nostrud minim sint ipsum officia eiusmod mollit consequat aliqua ea occaecat. Dolor Lorem amet pariatur deserunt enim ut sit elit fugiat reprehenderit commodo tempor nostrud ipsum officia ea occaecat. Ullamco sunt officia irure deserunt, consectetur velit ut. Occaecat aliqua proident commodo pariatur ipsum eu aliquip sunt adipisicing aliquip amet nulla reprehenderit nulla ea laboris est dolore. Commodum laborum consequat sunt enim aliquip non aliquip amet nostrud dolore ad proident, veniam ex et fugiat dolor exercitation magna exercitation enim. Anim dolore exercitation irure officia dolor aliquip consequat culpa esse anim velit consequat aute nostrud occaecat pariatur veniam commodo duis sunt reprehenderit voluptate veniam nostrud.

V. CONCLUSION

Lorem ipsum dolor sit amet est velit Lorem adipisicing consectetur irure qui, consequat. Excepteur adipisicing occaecat ex non sint deserunt proident id minim eiusmod excepteur amet pariatur. Id culpa id eiusmod veniam irure enim mollit eiusmod ex. Nostrud ut qui non mollit ullamco, velit voluptate elit reprehenderit ut Lorem mollit adipisicing consequat laborum id. Et quis aliqua cupidatat eu eiusmod irure mollit dolor aliqua ut aliquip magna. Ad minim culpa eu labore aliqua enim incididunt occaecat ad aliquip velit ad incididunt excepteur officia aute, ex.

Veniam culpa quis incididunt anim enim aliquip ut reprehenderit voluptate nostrud aute nostrud. Commodum, consectetur in amet mollit anim cillum do cillum excepteur tempor aute amet. Cillum ut reprehenderit Lorem nisi veniam do veniam ea ipsum, quis culpa Lorem velit in ea laboris ut aliqua officia. Cillum sit duis veniam officia minim exercitation voluptate anim non, id aliquip dolor non dolor nostrud dolore eu veniam. Fugiat culpa elit ea et non esse.

Do incididunt exercitation minim irure exercitation fugiat officia duis est nostrud minim sint ipsum officia eiusmod mollit consequat aliqua ea occaecat. Dolor Lorem amet pariatur deserunt enim ut sit elit fugiat reprehenderit commodo tempor nostrud ipsum officia ea occaecat. Ullamco sunt officia irure deserunt, consectetur velit ut. Occaecat aliqua proident commodo pariatur ipsum eu aliquip sunt adipisicing aliquip amet nulla reprehenderit nulla ea laboris est dolore. Commodum laborum consequat sunt enim aliquip non aliquip amet nostrud dolore ad proident, veniam ex et fugiat dolor exercitation magna exercitation enim. Anim dolore exercitation irure officia dolor aliquip consequat culpa esse anim velit consequat aute nostrud occaecat pariatur veniam commodo duis sunt reprehenderit voluptate veniam nostrud.

APPENDIX A: CITATION EXAMPLES

Items are shown in "main.bib" file

An article [2] - The required fields here are author, title, journal, and year; all others can be omitted if you do not have the corresponding information. Note as well that author names should be separated by "and".

A book [3] - The required fields are author, title, publisher, and year.

A series [4] - Series are cited as books with an additional field.

Someone's thesis [5] - The required fields are author, title, publisher, and year. You may also cite master's theses using the *mastersthesis* entry type.

Some technical report [6] - The required fields are author, title, publisher, and year.

A collection [7] - The required fields are author, title (of the article within the book), book- title (name of the book containing the article), and year.

Visited website [8] - For websites, note the specific formatting of the howpublished field. Be sure to include the date of access as shown. Also, keep in mind that certain characters common in urls, such as underscores, must be escaped (preceded by a backslash, ex.

Accepted for publication [9] - To show that an article has been accepted for publication but not yet published, include the line note = (in press).

Submitted for publication [10] - cited as published with an additional field.

Not published [11] - If a manuscript has not yet been published or submitted for publication, you may still cite it. Include a note to this effect.

Conversation [12] - Occasionally, an important item that does not exist in the literature will be discussed with your mentor. When this happens, you may cite the conversation with your mentor.

REFERENCES

- [1] Gartner, "Definition of small and midsize business - it glossary — gartner." [Online]. Available: <https://www.gartner.com/en/information-technology/glossary/smbs-small-and-midsize-businesses>
- [2] A. B. Cummings, D. Eftekhary, and F. G. House, "The accurate determination of college students' coefficients of friction," *Journal of Sketchy Physics*, vol. 13, no. 2, pp. 46–129, 2003.
- [3] I. J. Kuss, *On the Importance of Kissing Up to Your Boss*, 5th ed. Cambridge MA: Dilbert Books, 1995.
- [4] L. M. Napster, *Mathematical Theory of Efficient Piracy*, ser. Lecture Notes in Mathematics. New York NY: Springer Verlag, 1998, vol. 3204.
- [5] O. P. Qwerty, "History of the goofy layout of keyboards," Ph.D. dissertation, NUC, Podunk IN, 1996.
- [6] R. Swearingen, "Morphology and syntax of british sailors' english," NUC, New York NY, Tech. Rep., 1985.
- [7] T. Upsilon, "Obscure greek letters and their meanings in mathematics and the sciences," in *Proceedings of the seventh international trivia conference*, V. W. Xavier, Ed. Philadelphia PA: Last Resort Publishers, 1987, pp. 129–158.
- [8] J. Tetazoo, "A brief guide to recreational pyromania," Available at <http://www.blowinglotsofweirdstuffup.com/guide.html> (2005/06/12).
- [9] J. Mentor, "Behavior of small animals on fire," (in press).
- [10] —, "Behavior of small animals on fire," 2012, unpublished Manuscript.
- [11] —, "Behavior of small animals on fire," 2012, unpublished Manuscript.
- [12] S. Freud, Personal conversation, July 2012.