FACULDADE DE TECNOLOGIA SENAC GOIÁS
Tecnologia em Segurança da Informação

Aldo Filho
Jordan Hugs
Liniker Lettierre
Rony Carneiro

Uso de ferramentas de Segurança

Francisco Xavier Calaça

GOIÂNIA,
2016

Aldo Filho
Jordan Hugs
Liniker Lettierre
Rony Carneiro

Uso de ferramentas de Segurança

Relatório apresentado como requisito parcial para obtenção de aprovação na disciplina Segurança em Sistemas Operacionais, no curso de Segurança da Informação, na Faculdade de Tecnologia Senac Goiás.
Francisco Xavier Calaça

GOIÂNIA,
2016

SUMÁRIO

1 INTRODUÇÃO.....4
2 DESENVOLVIMENTO.....4
2.1 Firewall.....4
2.2 AntiVírus.....4
2.3 Graylog.....4
2.4 VeraCrypt.....4
2.5 Windows Active Directory.....5
2.6 Proxy.....5
3 CONCLUSÃO.....5
4 REFERÊNCIAS BIBLIOGRÁFICAS.....5

1 INTRODUÇÃO

Para mantermos os pilares da Segurança da Informação (Integridade, Confidencialidade, Disponibilidade), conforme prescrito na Política de Segurança da Informação da VDM CORP. serão implementados procedimentos que mitiguem a possibilidade de perca/roubo de dados e registre qualquer acesso a todos os sistemas da empresa.

2 DESENVOLVIMENTO

2.1 Firewall

A nossa primeira barreira contra os ataques externos é um firewall. Será instalado na empresa o tipo de firewall NGFW(Next Generation Firewall) que faz a análise de todos os pacotes, a vantagem deste tipo de firewall é que além dele atuar como um firewall tradicional fazendo analises de porta, IP's ele consegue verificar se o pacote que está sendo trafegado é realmente daquela aplicação/protocolo.

2.2 Antivírus

O Antivírus é a barreira de proteção contra os ataques externos e internos, este software que protege nossos usuários, graças a ele vírus mais genéricos e (dependendo da fabricante do mesmo) vírus mais perigosos são efetivamente detectados e removidos. O programa antivírus será instalado para mitigar as chances de infecção de worms, trojans e outros tipos de ameaças.

2.3 Graylog

Serviço de monitoramento dos servidores, com o intuito de descobrir e reduzir os problemas rapidamente e proativamente. O graylog suporta grandes quantidades de informações e consegue manipula-las com extrema rapidez, nesta ferramenta podemos fazer vários tipos de filtros nos logs para disponibilizarmos as informações realmente importantes para um administrador de redes.

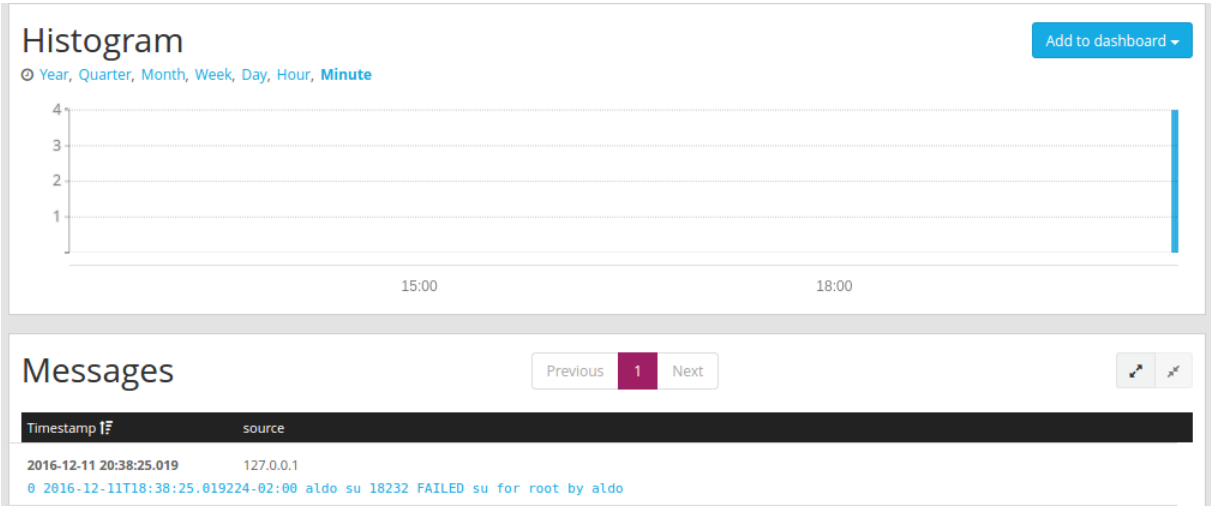

Figura 1. Autenticação do usuário root.

2.4 VeraCrypt

Veracrypt é um software que utiliza OTFE(On-the-fly-encryption) e cria um disco virtual criptografado. On-the-fly-encryption significa que o dado é encriptado logo depois de ser salvo e descriptografado logo após ser carregado, sem nenhuma intervenção dos usuários. Todos os computadores da empresa precisam ter uma partição criptografada para armazenar todos os dados sensíveis da empresa, após o uso do disco criptgrafado os usuários devem desmontar a partição para evitar de um atacante conseguir acessá-la caso ele consiga acesso ao computador de algum usuário.

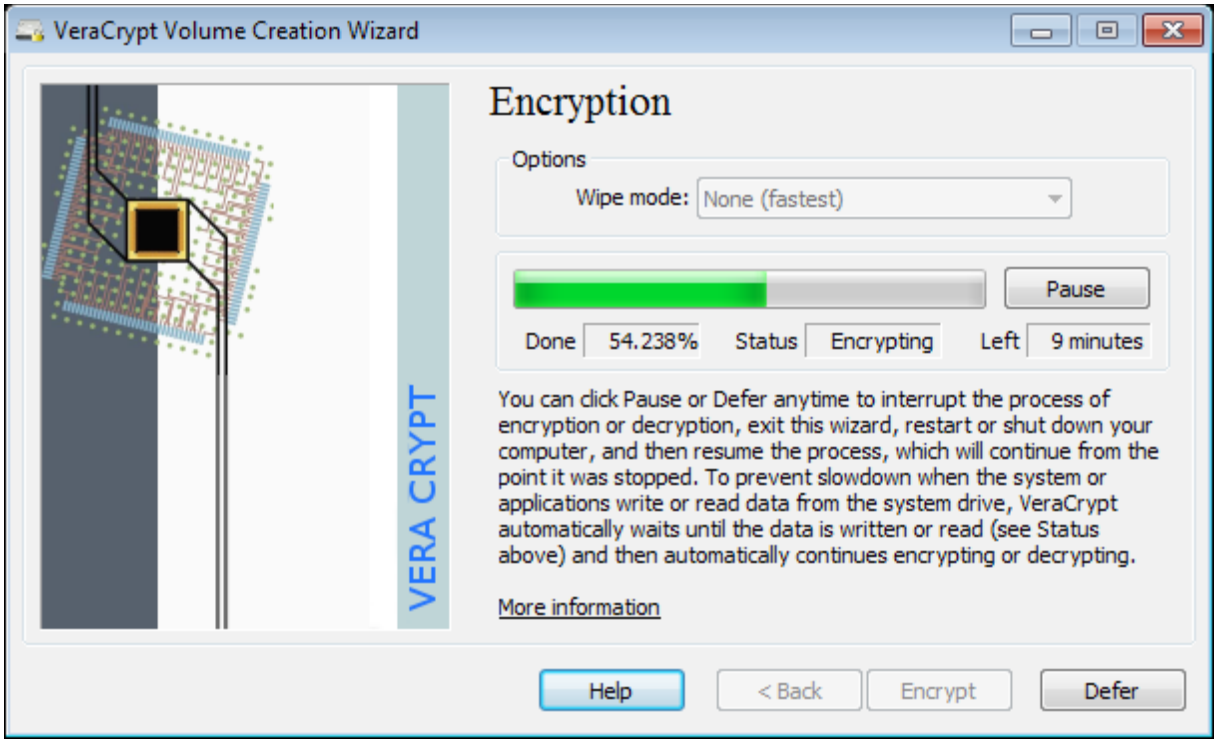

Figura 2. Encriptação do disco.

2.5 Windows Active Directory

A ferramenta Active Directory nos permite controlar o domínio ao qual o usuário está cadastrado, com isto, é possível que um usuário siga as diretrizes estabelecidas na PSI, como por exemplo a política de senhas, ela pode ser facilmente implementada utilizando a GPO (Diretiva de Grupo).

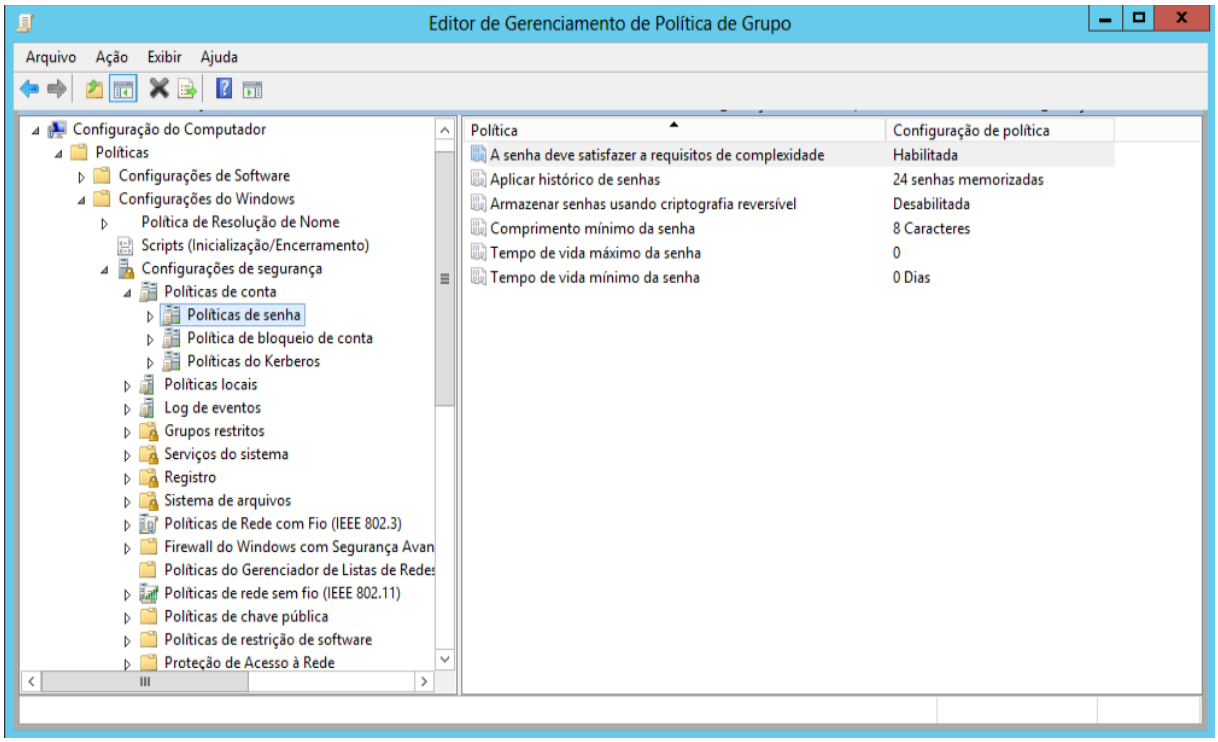

Figura 3. Diretriz da Política de senha.

Além disto os usuário do domínio serão autenticados através do SSO(Single Sign-On) possibilitando que os usuários não precisem se preocupar com várias senhas, pois ele será autenticado e autorizado no sistema para acessar as demais aplicações da empresa.

2.6 Proxy

O serviço de proxy é importante para a organização pois ele consegue além de bloquear os sites especificados é possível bloquear também os tipos de arquivos como .exe, .mp4, .jpg que iriam ser baixados. A implementação de um proxy na empresa, é vital para o monitoramento de todos os sites acessados pelos os usuários.

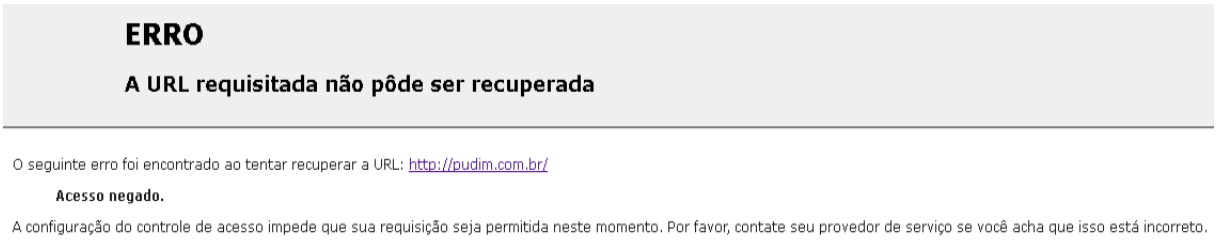

Figura 4. Bloqueio de URL da ferramenta Squid.

3 CONCLUSÃO

O uso de ferramentas de segurança é de extrema importância para se utilizar em uma empresa, atender suas necessidades, monitorar, proteger, e reduzir o risco de incidentes de segurança.

4 REFERÊNCIAS BIBLIOGRÁFICAS

https://veracrypt.codeplex.com/wikipage?title=Introduction
http://docs.graylog.org/en/2.1/