Proposta de um Modelo de Ferramenta de Administração e Segurança Computacional

Robson Gomes de Melo, Paulo Lício de Geus

[1]Instituto de Computação - Universidade Estadual de Campinas (UNICAMP)
Caixa Postal 6176 - 13083-970 - Campinas - SP - Brasil

{robinho,paulo}@las.ic.unicamp.br

1. Introdução

Não é novidade que a administração e segurança de redes e sistemas computacionais são tarefas primordiais às organizações, principalmente nos cenários atuais. Na tentativa de auxiliar os administradores, algumas ferramentas computacionais buscam assistí-los no momento de configuração de um serviço ou dispositivo de forma segura. No entanto, torna-se extremamente complexa a administração/configuração, mesmo com o auxílio dessas ferramentas, em situações onde a presença física do administrador nos ambientes a serem configurados seja inviável.

Esse trabalho propõe um modelo de ferramenta para auxilio à administração e segurança, baseado em um ambiente de interface gráfica de acesso remoto via WEB, capaz de realizar configurações remotas em máquinas da rede e de eliminar a necessidade da presença física do administrador no ambiente que se configura.

2. Ferramentas de Configuração de Segurança

Segundo [Nakamura and de Geus 2007], dados tempo, recursos e a motivação, um intruso pode violar praticamente qualquer sistema. Mesmo que se conte com todos os recursos e procedimentos tecnológicos atualmente disponíveis para a segurança computacional, não se pode garantir 100% de proteção. Também, como mencionado por [Bishop 2003], a principal estratégia dos profissionais de segurança é de utilizar os recursos disponíveis para dificultar e tentar minimizar as possibilidades de incidentes. Dentre tais recursos pode-se contar com técnicas, procedimentos e uso de ferramentas, enfim praticamente qualquer tipo de ação que adcione bloqueios sucessivos à progressão de ataques.

Nas tarefas de configuração de sistemas, serviços e redes de computadores, a utilização de ferramentas automatizadas de configuração se apresenta como solução atrativa para evitar as vulnerabilidade causadas por uma administração manual, que pode sofrer de desatenção ou mesmo despreparo. Como demonstrado por [de Albuquerque et al. 2005], abordagens que ofereçam abstração, integração e ferramentas de suporte ao gerenciamento da configuração de mecanismos de segurança são fundamentais para tornar o processo de configuração menos sujeito a erros e mais efetivo.

3. Proposta do Modelo de Ferramenta

Projetou-se uma ferramenta central de administração e segurança computacional, com ênfase em serviços de segurança como *filtro de pacotes, IDS* e outros, que também tenham sua configuração implementada por arquivos textos. A arquitetura do modelo, suas camadas/módulos de funcionamento, como o modo de utilização, podem ser vistos nas

Figuras 1 e 2. O funcionamento dos módulos segue uma estrutura independente: o processo se inicia com o módulo de conexão, que acessa a máquina remota a ser configurada e obtém o arquivo de configuração do serviço desejado. Posteriormente o módulo coordenador é acionado e realiza o primeiro tratamento no arquivo de configuração, eliminando comentários e linhas em branco. Na sequência, o módulo conversor recebe esse arquivo pré-tratado e realiza uma conversão de seus valores para o formato *XML*, identificando em cada linha do arquivos quais dados se referem aos parâmetros, delimitadores e valores (estrutura encontrada na maioria dos arquivos de configuração). Após essa conversão, o módulo formulário cria formulários Web que são incorporados na interface gráfica do sistema. Essa interface gráfica por sua vez aplica técnicas de validação dos campos do formulário, como também possibilita o acesso remoto através de um navegador de internet para qualquer máquina da rede, eliminando a necessidade da presença física do administrador na máquina que se configura, como também na rede onde ela se encontra.

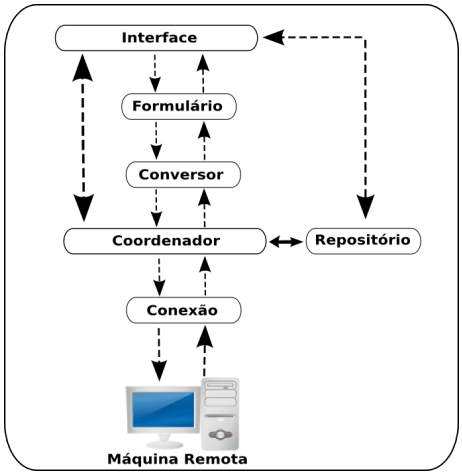

Figure 1. Arquitetura da Ferramenta

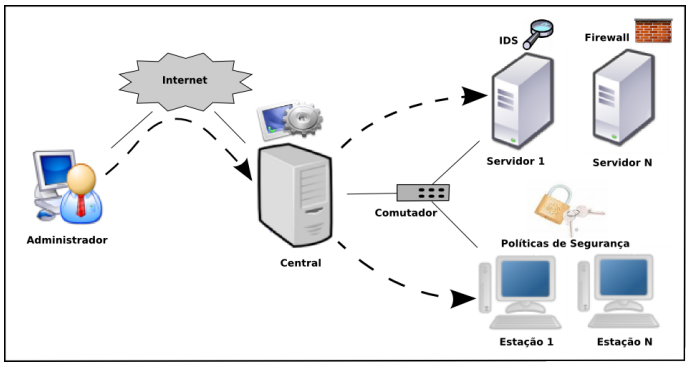

Figure 2. Modo de utilização da Ferramenta

4. Conclusão

Com esse modelo de ferramenta para administração e segurança computacional, é possível imaginar um cenário onde a presença física do administrador não seja mais um empecilho para manter serviços ou dispositivos configurados de forma adequada e segura. Graças ao modelo utilizado, o administrador desfruta da segurança de dados provida por *https*, da portabilidade que um navegador de internet permite e ainda pode evitar muitas falhas de operação de sistemas e serviços computacionais, devido à automatização do processo por meio de formulários que garantem sintaxe rígida de comandos.

References

Bishop, M. (2003). *Computer Security: Art and Science*. Addison Wesley Professional.

de Albuquerque, J. P., de Geus, P. L., Isenberg, H., and Krumm, H. (2005). Gerenciamento baseado em modelos da configuração de sistemas de segurança em redes de larga escala. *V Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*.

Nakamura, E. T. and de Geus, P. L. (2007). *Segurança de Redes em Ambientes Cooperativos*, volume 2. Novatec.