Faculdade de Tecnologia Senac Goiás
Segurança da Informação

ALDO BRITO DA COSTA FILHO
LEVI SOUZA
MATHEUS MARÇAL RAMPIN
MATHEUS OLIVEIRA RODRIGUES

PROJETO INTEGRADOR

PROFESSOR OLEGÁRIO

Goiânia
2015

DESCRIÇÃO DA ATIVIDADE

Fazer um levantamento e elaborar uma planilha, de requisitos de Hardware e Software necessários para executar o processo de Hardening dos servidores contra os ataques de Man-In-The-Middle, nas plataformas Linux e Windows e justificar a escolha.

Requisitos Mínimos para Windows Server 2012 R2

Processador	De 64 bits e 1,4 GHz
Memoria RAM	512 MB
Disco Rígido	32 GB
REDE	Adaptador Gigabit (10/100/1000baseT) Ethernet
Unidade de DVD (caso pretenda instalar o sistema operacional usando mídia de DVD)	
Monitor Super VGA (1024 x 768) ou com resolução superior	
Teclado e mouse Microsoft® (ou outro dispositivo apontador compatível)	
Acesso à Internet (tarifas podem ser aplicadas)	

Requisitos para Servidor Red Hat

	Mínimo	Recomendado
Processador	Intel Core, 2.4GHz, 512K de cache ou equivalente	Intel multi-core, 2.4GHz dual processor, 512K de cache ou equivalente
Memoria	2 GB	8 GB
Disco Rígido	5 GB de armazenamento para a instalação base do Red Hat Enterprise Linux	
Um mínimo de 30 GB de armazenamento por canal de software (incluindo os canais filho e Base) no diretório /var/satellite/ configurável na instalação		
Recomendado - uma SAN externa para backups mais confiáveis		

OBS.: O uso de CPU's mais rápidas, e mais RAM e de disco rígidos de maior capacidade aumenta a escalabilidade e o desempenho dos servidores DNS, que usam cerca de 100 BYTES de RAM para cada registro de recurso. Esse número, pode ser obtido com a exame de cada zona do snap-in DNS, permite que vocẽ calcule o quanto de memória é necessário.

Softwares - Linux:

Stunnel:

É um software de segurança que permite criptografar conexões TCP dentro do protocolo SSL.

Iptables:

Sistema de controle de filtros para protocolos ipv4. Para montar as regras do firewall.

Bind 9:

As versões 4 e 8 do BIND tinham uma série de vulnerabilidades de segurança e, por isso, o seu uso é hoje fortemente desencorajado. Uma das motivações para reescrever o BIND, e lançar o BIND 9, foi disponibilizar um sistema mais seguro.

Arpon:

É um software que faz o protocolo ARP seguro afim de previne contra o MITM (Man in the Middle) que tem como forma de ataques “ARP Spoofing”, “ARP Cache Poisoning” e ARP Poison Routing (APR).

Arp Watch:

Ferramenta para monitorar a atividade em uma rede ethernet, importante ferramenta contra ataques de “Arp Spoofing” e “Arp Poisoning”.

Softwares – Windows:

TLS/SSL:

O cliente compara o atual **DNS name of server** com o **DNS name of certificate**.

SSH Tunneling:

O SSH possui as mesmas funcionalidades do TELNET, com a vantagem da criptografia na conexão entre o cliente e o servidor.

VPN:

Uma VPN é uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados.

ARP Freeze:

É uma ferramenta para prevenção contra MITM (Man in the Middle), permite configuração estática da tabela ARP.