Sessão 10: Auditoria de segurança da informação

1) Auditoria com Nessus

Instale e configure o Nessus, conforme apresentado na parte teórica. Realize uma auditoria a partir da estação cliente, objetivando analisar os dois servidores presentes na rede de servidores. Oriente o Nessus a analisar a rede inteira.

1. Baixe o pacote do Nessus no endereço: http://www.nessus.org/download/ Escolha a versão para Linux Debian 32 bits. Foi disponibilizada no diretório home do usuário root da sua máquina virtual uma versão do Nessus. Caso não seja possível o download da versão mais atual, essa versão pode ser utilizada.
2. Instale o pacote na máquina virtual KALI com o comando: `# dpkg –i /root/Nessus-4.4.0-debian5_i386.deb`
3. Faça o registro no site do projeto com o perfil de licença HomeFeed. Esse perfil é o suficiente para o propósito desta atividade. Para fazer o registro, acesse: http://www.nessus.org/register/ Cadastre um e-mail válido, para o qual será enviado o número da licença.
4. Inicie o servidor Nessus com o comando: `# /etc/init.d/nessusd start`
5. Acesse o console de gerência do Nessus, a partir de um navegador web da máquina física: https://172.16.G.30:8834 Certifique-se de que existe regra de exceção no firewall para permitir essa conexão e não esqueça de seguir os passos indicados pelo instalador web, em especial o passo que solicita a digitação do registro do Nessus. Se você digitar o número de registro e por algum motivo o Nessus não conseguir conexão à internet, poderá ser necessário gerar outra chave de registro.
6. Com o console aberto, crie uma nova Policy, com o nome “padrao”. Marque todas as opções de Port Scanners disponíveis. Em Credentials, aceite as configurações padrão. Habilite todos os filtros, clicando no botão Enable All. No restante das opções, aceite os valores padrão.
7. No console do Nessus, crie um novo Scan com os parâmetros:

- Nome: RedeDMZ
- Type: Run Now
- Policy: Padrao
- Scan Targets: 172.16.G.0/24
- Clique no botão Launch Scan.

1. Analise o relatório gerado pelo Nessus no menu Reports. Foi possível encontrar os hosts da rede DMZ? Quais serviços foram encontrados

2) Auditoria sem filtros de pacotes

Agora retire todas as regras do firewall e refaça a auditoria com uso no Nessus a partir da estação

cliente, objetivando os dois servidores presentes na rede DMZ. Oriente o Nessus para analisar apenas os dois endereços IPs, para agilizar o processo.

1. Desabilite todas as regras no firewall do host FWGW1. Pode ser utilizado o seguinte comando: `# iptables-restore < /etc/iptables.down.rules`
2. Acesse o console de gerência do Nessus, a partir de um navegador web da máquina física: https://172.16.G.30:8834 Certifique-se de que existe regra de exceção no firewall para permitir essa conexão.
3. Com o console aberta, crie uma nova Policy, com o nome "VerificaIDS". Marque as opções de Port Scanners, TCP Scan e SYN Scan, escolha Port Scan Range 80,443. Em Credentials, aceite as configurações padrão. Habilite apenas os filtros relacionados a servidores web, clicando no botão Disable All e habilitando apenas as famílias de regras CGI abuses e Web Servers. No restante das opções, aceite os valores padrão.
4. Abra uma sessão Shell no host FWGW1 e deixe listando todos alertas do Snort, com o comando: `# tail –f /var/log/snort/alert`
5. No console do Nessus, crie um novo Scan com os parâmetros:

- Nome: WebDMZ
- Type: Run Now
- Policy: VerificaIDS
- Scan Targets: 172.16.G.10,172.16.G.20
- Clique no botão Launch Scan.

1. Verifique os logs do Snort. Foi registrada alguma tentativa de explorar falhas em serviços web?

3) Auditoria do IDS

Insira as regras de bloqueio de firewall criadas no capítulo3 e realize a auditoria novamente. Caso tenha realizado a auditoria com as regras retiradas, insira-as agora e realize nova auditoria. Compare os dois relatórios e verifique o que mudou. Altere parâmetros no Nessus e verifique as mudanças nos resultados.

4) Utilizando o Nikto

A ferramenta Nikto é um scanner de vulnerabilidades especializado, ou seja, desenvolvido para análise um determinado serviço. Nesta atividade pede-se para executar o Nessus e o Nikto contra o servidor Windows 2008 e comparar o relatório gerado. Os passos abaixo explicam como instalar e executar o Nikto.

1. Baixe o Nikto no Servidor LinServer e descompacte-o:

```
# wget -c http://www.cirt.net/nikto/nikto-current.tar.gz
# tar -xzpf nikto-current.tar.gz
# cd nikto-2.1.4
```

2. Agora vamos executar a atualização do Nikto: `# ./nikto.pl -update`
3. Agora vamos disparar o Nikto contra o servidor Windows 2008 que possui o serviço HTTP instalado: `# ./nikto.pl -h 172.16.G.20 -o /tmp/relatorio.txt` Acesse o arquivo /tmp/relatorio.txt e veja as vulnerabilidades encontradas. Pesquise no Google sobre algumas das vulnerabilidades indicadas e como você poderia corrigi-las.

5) Auditoria em Microsoft Windows

1. Instale o pacote de auditoria da Microsoft MBSA no host físico:
   - http://www.microsoft.com/technet/security/tools/mbsahome.mspx
   - http://technet.microsoft.com/en-us/security/cc184923
2. Execute-o na sua estação de trabalho e na sua rede local. Que benefícios este programa pode fornecer para a segurança da informação?