FACULDADE DE TECNOLOGIA SENAC GOIÁS

TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Alunos:
Cristhian Lopes de Souza
Matheus do Carmo
Matheus Oliveira
Pablo de Almeida

SERVIÇOS IP

Professor: Dinailton

Goiânia, 10 de dezembro de 2016

HTTP

HTTP (porta padrão: 80) O HTTP não oferece uma conexão segura, porque as informações navegam na rede de forma clara. O protocolo HTTP é um protocolo da camada de aplicação responsável por apresentar ao usuário de forma acessível os dados fornecidos por um servidor, como os dados trafegados do HTTP não são criptografados isso facilita visualização de dados interceptados perdendo a confidencialidade dos dados.

Para solucionar o problema de segurança foi adicionado uma camada de segurança que última chave pública e chave privada para criptografa os dados, esses certificados são emitidos por unidades certificadoras confiáveis.

Com essa nova camada de segurança o protocolo HTTP passa a ser chamado de HTTPS, onde o "s" significa seguro. O protocolo HTTPS é utilizado, em regra, quando se deseja evitar que a informação transmitida entre o cliente e o servidor seja visualizada por terceiros, como por exemplo no caso de compras online.

SSH

Desde 1995 após ter sido vítima de um ataque que capturou a senha, o SSH passou a ser criptografado tornando-o um protocolo de acesso remoto seguro, com isso o serviço passou a garantir confidencialidade, integridade, autenticidade, porém um grande problema surgiu, como o SSH é um serviço IP e vem habilitado na maioria dos sistemas operacionais administradores de rede passaram a utilizar senhas repetidas e fracas facilitando um ataque por forca bruta. Outro problema é permitir que usuário de acesso root tenha permissão para fechar conexões remota.

O arquivo de configuração do serviço SSH, SSHD.CONFIG, possui um campo em que o administrador especifica qual usuário tem permissão ***AllowUsers*** de acesso enquanto na linha
DenyUsers é possível especificar quais não podem fazer a conexão remota ou definir ***PermitRootLogin*** como ***no*** com esse procedimento impossibilita o usuário root de autenticar via SSH.

Definir a senha com um padrão que utilize letras maiúsculas e minúscula com números e caracteres especiais cria um grau de dificuldade maior para ser quebrada e por fim redefinir a porta padrão do serviço que por default é a porta 22.

Depois de realizar as devidas modificações é necessário reiniciar o serviço para serem aplicadas.

SMTP

Simple Mail Transfer Protocol (abreviado SMTP. Traduzido do inglês, significa "Protocolo de transferência de correio simples") é o protocolo padrão para envio de e-mails através da Internet. Ele foi padronizado pela RFC 821.

É um protocolo relativamente simples, baseado em texto simples, onde um ou vários destinatários de uma mensagem são especificados (e, na maioria dos casos, validados) sendo, depois, a mensagem transferida.

Esse protocolo usa por padrão a porta 25 numa rede Transmission Control Protocol (ou 465 para conexão criptografada via SSL). No Brasil, porém, desde 2013, provedores e operadoras de internet passaram a utilizar a porta 587, como medida de segurança para diminuir o número de spams.

A resolução DNS de um servidor SMTP de um dado domínio é possibilitada por sua entrada MX (Mail eXchange).

DHCP

A base de protocolo DHCP não inclui qualquer mecanismo de autenticação. Por isso, é vulnerável a uma variedade de ataques. Estes ataques se dividem em três categorias principais:

- Fornecimento de informações falsas a clientes por servidores DHCP não autorizados;
- Acesso aos recursos da rede por clientes não autorizados;
- Ataques exaustivos aos recursos da rede advindos de clientes DHCP mal-intencionados.

Porque o cliente não tem como validar a identidade de um servidor DHCP, servidores DHCP não autorizados podem ser operados em redes, prestação de informações incorretas aos clientes DHCP. Isso pode servir tanto como um ataque de negação de serviço, impedindo o cliente de ter acesso a conectividade de rede. Porque o servidor DHCP fornece o cliente DHCP com endereços IP do servidor, como o endereço IP de um ou mais servidores DNS, um atacante pode convencer um cliente DHCP para fazer pesquisas através de seu DNS seu próprio servidor DNS, e pode, portanto, fornecer suas próprias respostas a consultas DNS do cliente. Por sua vez, permite que o atacante para redirecionar o tráfego de rede através de si, permitindo-lhe escutar as conexões entre os servidores de rede do cliente e ele entra em contato, ou simplesmente para substituir os servidores de rede com o seu próprio. Porque o servidor DHCP não tem nenhum mecanismo seguro para autenticar o cliente, os clientes podem obter acesso não autorizado aos endereços IP de apresentação de credenciais, tais como identificadores do cliente, que pertencem a outros clientes DHCP. Isso também permite que os clientes DHCP para esgotar o DHCP armazenamento de servidor de endereços IP-, apresentando novas credenciais cada vez que ele pede um endereço, o cliente pode consumir todos os endereços IP disponíveis em um link de rede particular, impedindo outros clientes DHCP da obtenção de serviços. DHCP fornece alguns mecanismos para mitigar esses problemas.

- O Relé de Agente de Informações extensão protocolo Option (RFC 3046) permite que os operadores de rede para conectar marcas a mensagens DHCP uma vez que estas mensagens chegam na rede de confiança do operador de rede. Esta tag é então usado como um token de autorização para controlar o acesso do cliente aos recursos da rede. Porque o cliente não tem acesso à rede a montante do agente de retransmissão, a falta de autenticação não impede que o operador do servidor DHCP de confiar no token de autorização.

- Outro ramal, autenticação para DHCP mensagens (RFC 3118), fornece um mecanismo para autenticação de mensagens DHCP. Infelizmente RFC 3118 não viu a adopção generalizada por causa dos problemas de gerenciamento de chaves para um grande número de clientes DHCP.

Bibliografias

A confexão de trabalho teve colaboração de inúmeros sites destacando-se entre eles:

https://pt.wikipedia.org
https://www.google.com.br