FACULDADE DE TECNOLOGIA SENAC GOIÁS
Tecnologia em Segurança da Informação

Aldo Filho
Jordan Hugs
Liniker Lettierre
Rony Carneiro

PLANEJAMENTO DE SEGURANÇA

Olegário Correa da Silva Neto

GOIÂNIA,
2016

Aldo Filho
Jordan Hugs
Liniker Lettierre
Rony Carneiro

PLANEJAMENTO DE SEGURANÇA

Relatório apresentado como requisito parcial para obtenção de aprovação na disciplina de Planejamento de Segurança da Informação, no Curso de Tecnologia em Segurança da Informação, na Faculdade de Tecnologia Senac Goiás.

Olegário Correa da Silva Neto

GOIÂNIA,
2016

SUMÁRIO

1 INTRODUÇÃO

A camada de aplicação é um termo utilizado em redes de computadores para designar a sétima camada do modelo OSI. É responsável por prover serviços para aplicações de modo a separar a existência de comunicação em rede entre processos de diferentes computadores. Também é a camada número cinco do modelo TCP/IP que engloba também as camadas de apresentação e sessão no modelo OSI. Ela contém os protocolos de nível mais alto como SMTP, SSH, HTTP, DHCP.

2 PROTOCOLO HTTP

O protocolo HTTP, além de não oferecer criptografia, também não garante que os dados não possam ser interceptados, coletados, modificados ou retransmitidos e nem que você esteja se comunicando exatamente com o site desejado. Por estas características, ele não é indicado para transmissões que envolvem informações sigilosas, como senhas, números de cartão de crédito e dados bancários, e deve ser substituído pelo HTTPS, que oferece conexões seguras.

O protocolo HTTPS utiliza certificados digitais para assegurar a identidade, tanto do site de destino como a sua própria, caso você possua um. Também utiliza métodos criptográficos e outros protocolos, como o SSL (Secure Sockets Layer) e o TLS (Transport Layer Security), para assegurar a confidencialidade e a integridade das informações.

Sempre que um acesso envolver a transmissão de informações sigilosas, é importante certificar-se do uso de conexões seguras. Para isso, você deve saber como identificar o tipo de conexão sendo realizada pelo seu navegador Web e ficar atento aos alertas apresentados durante a navegação, para que possa, se necessário, tomar decisões apropriadas.

3 PROTOCOLO SSH

Para que o serviço SSH funcione de forma mais segura possível será necessário a realização do seguinte passos:

1 - Adicionar um Banner para informar que o acesso é restrito

2 - Modificar porta padrão.

Modificando a porta padrão ira dificultar que os *Scan* detecte em qual porta está sendo rodado o SSH, assim evitando possíveis ataques de *Brute Force*.

3- Utilizar somente protocolo SSH versão 2.

-A versão 1 do SSH possui diversas falhas detectadas que foram corregidas na versa 2

-Atualmente por padrão o SSH já vem configurado para utilizar somente a versão 2, por precaução verificar o protocolo utilizado

4- Desabilitar login como root.

-O usuário root tem controle total do sistema, caso um atacante consiga as credenciais de acesso do root ele terá controle total do sistema

5- Permitir acesso via SSH para usuários específicos

-Não é necessário que todos os usuários do sistema tenham acesso via SSH. Limitando o acesso será reduzido as brechas.

6- Limitar conexões não autenticadas e Reduzir o tempo de espera para login.

-Para que quando o servidor receba um ataque pelo SSH ele não fique sobrecarregado de conexões falsas

7- Habilitar somente o uso de chaves com passphrase

-Autenticação por via de Login e senha são suscetíveis a ataques de *Brute Force*, ou até mesmo de uma pessoa ver a senha no momento em que ela está sendo digitada, utilizando a autenticação por meio de chave não tem este problema, o atacante vai precisar do arquivo da chave que está no computador do administrador, junto com a passphrase com apenas uma das duas não é possível se conectar ao servidor

8-Aumentar a força da senha

-Uma passphrase pode ser uma senha normal de 8 a 12 caracteres, até uma frase complexa, não utilizar senhas obvias é o principal, uma boa senha consiste em letras maiúsculas e minúsculas, número e caracteres especiais.

4 PROTOCOLO SMTP

Soluções para que o SMTP trabalhe de forma mais segura, faremos os seguintes passos:

-Autenticação dos usuários

Permitir somente os usuários autenticados no sistema possam utilizar o serviço de e-mail, isto vai evitar que nosso servidor seja considerado open relay.

-Configuração do SSL

Implementação do serviço de segurança para o SMTP que não possui nenhuma medida de criptografia, evitando assim a circulação de pacotes com texto puro.

-Desabilitar o VRF:

O comando VRFY se torna um risco ao servidor de e-mail dado que um atacante possa usar o VRFY para checar se a conta do usuário e caixa de correio estão disponíveis.

5 PROTOCOLO DHCP

Existem alguns problemas famosos existentes no DHCP, e é necessário utilizar algumas práticas ao se utilizar o servidor DHCP.

O DHCP é um protocolo não autenticado.

Quando um usuário se conecta à rede, ele não precisa fornecer credenciais para ter concessão à rede. Um usuário não autenticado pode então obter uma concessão para qualquer cliente DHCP sempre que um servidor DHCP estiver disponível para fornece-la.

DHCP Starvation

Este ataque consiste em alocar todos os endereços IP disponíveis no servidor DHCP, onde o atacante de forma simples, através de um broadcast usando requisições DHCP com endereços MAC falsos, obtém sucesso. Isso leva à negação de serviço na rede para os clientes habituais, abrindo uma brecha para os atacantes configurarem um servidor DHCP falso, e através dele envia informações falsas para os clientes, como por exemplo, dando-lhes o seu próprio endereço IP, se passando por default gateway. A partir do momento que os clientes aceitarem as novas configurações DHCP todo o tráfego da rede passara pela máquina do atacante, tornando assim muito fácil o monitoramento das informações.

Contras-Medidas

-Configure Manualmente em todos os clientes da rede os endereços de servidores DNS.

-Mantenha o servidor DHCP atualizado com os últimos pacotes de segurança do Sistema Operacional utilizados.

-Faça alterações nas senhas de acesso padrão do servidor e crie uma diretriz de segurança que faça sua alteração em períodos estabelecidos.

-Desabilite serviços e usuários não necessários.

-Crie rotinas de monitoramento da rede para aumentar a chance de detecção de servidores clandestinos na rede. (Olhando logs do servidor DHCP para localizar ips e MAC's não conhecidos ou autenticados.

-Para redes Wi-Fi, utilize criptografia WPA2 e mantenha roteadores e pontos de acesso atualizados

Dynamics ARP Inspection

O Dynamic ARP inspection é um recurso de segurança que valida os pacotes ARPs na rede. Intercepta, grava as operações que ocorrem na rede e descarta os pacotes ARP com ligações inválidas IP-para-MAC. Isso protege mais a rede de ataques Man-inThe-Middle.

O Dynamic ARP inspection faz com que apenas os ARP request e response válidos sejam retransmitidos. O switch executa as seguintes atividades:

• Intercepta todo ARP request and response nas portas não confiáveis;

• Verifica se cada um desses pacotes interceptados tem uma ligação válida de endereço IP-para-MAC antes de atualizar o cache ARP local ou encaminhar o pacote para o destino adequado;

• Descarta pacotes ARP inválidos;

6 CONCLUSÃO

Tendo em vista os aspectos analisados, conclui-se que o protocolo de comunicação HTTP (Hyper Text Transfer Protocol) não é seguro pois não tem criptografia com base no ataque Man In The Middle, sendo assim todo tráfego na rede pode ser observador por atacantes, comprometendo a confidencialidade do serviço, e tem como solução a configuração do SSL habilitado da porta 80 HTTP para a porta 443 HTTPS.

O SSH (Secure Shell) é uma ferramenta com tráfego criptografado, que permite controles via terminal, execução de aplicativos gráficos, realização de transferências de arquivos e também é capaz de encapsular outros protocolos, por exemplo o VNC por tunelamento criptografado. O protocolo responde diferentes tipos de ataques já conhecidos, e detecta quando o servidor foi trocado por outra máquina com o objetivo de obter as credenciais e detectar injeções de dados na comunicação e também permite a detecção de ataques de MAN-IN-THE MIDDLE. É Suscetível a Brute-Force, porém, esse ataque é vetado devido ao uso de chaves assimétricas, uma chave é denominada de chave pública quando ela permite apenas encriptar os dados, a outra chave é denominada chave privada, que permite apenas desencriptar as informações criptografadas da primeira chave.

O SMTP (Simple Mail Transferer Protocol) é um MTA (Agente de Transferência de Mensagem) é um protocolo padrão que permite que faz a transferência de e-mail através da internet utilizando o TCP/IP. Utiliza do código ASCII o que torna os protocolos mais fáceis de testar, desenvolver e depurar. Na internet, a mensagem de correio eletrônico é entregue quando a máquina de origem estabelece uma conexão TCP com a porta 25 da máquina de destino, mas o SMTP utiliza também a porta 587.

Caso o servidor esteja disponível para receber a mensagem o cliente anunciará de quem veio a mensagem e para quem ela está indo. O servidor realiza e, se esse receptor existir no local de destino, o servidor sinaliza ao cliente para enviar mensagem. Em seguida, o cliente enviará e o servidor confirmará. Depois de todas as mensagens tiverem sido trocadas a conexão será encerrada.

O SMTP foi projetado na ideia de “cooperação” e “confiança” entre os servidores. E por não ter sido projetado para o uso global o SMTP possui graves problemas sobre a segurança, como não implementação da autenticação, facilitando o envio de spam e também que as mensagens transmitidas não possuem criptografia. Para resolução do problema de mensagens em texto se implementa o SSL (Secure Socket Layer) que criará uma conexão criptografada com os servidores, e outra solução é a implementação do envio de mensagens somente por pessoas autenticadas no servidor.

O DHCP (Dynamic Host Configuration Protocol) é um protocolo utilizado por dispositivos conectados a uma rede para obter as configurações de rede, configurações que incluem endereço IP, máscara de sub-rede, gateway padrão, e os endereços IP dos servidores de DNS, tudo a partir de um servidor executando o software do servidor DHCP.

Ao ligarem-se à rede, os clientes fazem um pedido para a rede, fazendo solicitação da informação de configuração. O pedido é recebido pelo servidor de DHCP, que responderá fornecendo a informação solicitada. Sendo um protocolo normalizado, clientes com diferentes sistemas operativos poderão interagir com este serviço, independentemente da plataforma na qual ele esteja implementado.

Como o DHCP não é um protocolo autenticado, faz-se a implementação de uma tabela ARP fixa, com IPS ligados a endereços MAC.

7 REFERÊNCIAS BIBLIOGRÁFICAS

Gabritech: Tipos de Ataques por camada

http://gabritech.blogspot.com.br/2009/10/tipos-de-ataques-por-camada-camada-de.html

Acesso em 14 de junho de 2016

Abusing, & Exploiting DHCP

http://pt.slideshare.net/JamesHemmings/abusing-dhcp

Acesso em 15 de junho de 2016

Blog LabCisco: DHCP Snooping na Mitigação de Servidores Falsos

http://labcisco.blogspot.com.br/2013/01/dhcp-snooping-na-mitigacao-de.html

Acesso em 15 de junho de 2016

DHCP Starvation

https://brenn0.wordpress.com/2015/01/24/dhcp-starvation-ataque-de-negacao-de-servico-em-rede-local/

Acesso em 15 de junho de 2016

Informações de segurança do DHCP

https://technet.microsoft.com/pt-br/library/cc780347(v=ws.10).aspx

Acesso em 14 de junho de 2016

Configuração do cliente SSH - Dominando o SSH

http://www.hardware.com.br/tutoriais/dominando-ssh/pagina3.html

Acesso em 11 de junho de 2016

http e https – seguranca com https

https://juancarloscunha.wordpress.com/2009/06/02/http-e-https-seguranca-com-https-diferenca-entre-http-e-https/

Acesso em 15 de junho de 2016

Cartilha de Segurança -- Uso seguro da Internet

http://cartilha.cert.br/uso-seguro/

Acesso em 15 de junho de 2016

Setup Postfix with SMTP-AUTH and TLS on CentOS

https://blog.tinned-software.net/setup-postfix-with-smtp-auth-and-tls-on-centos/

Acesso em 14 de junho de 2016

Oque é protocolo HTTPS (Andamento) - Perguntas e Respostas HiperContas

https://www.hipercontas.com.br/perguntas.php?&id=300

Acesso em 14 de junho de 2016

HowTos/Https - CentOS Wiki

https://wiki.centos.org/HowTos/Https

Acesso em 15 de junho de 2016

Morimoto, Carlos Eduardo, Servidores Linux, Guia Prático/Carlos Eduardo Morimoto. – Porto Alegre: Sul Editores, 2015

Protocolo TCP/IP / Behrouz A. Forouzan, Sophia Chung Fegan; revisão técnica Flávio Soares Corrêa da Silva, Roerto Hirata Jr; tradução João Eduardo Nóbrega Tortello. – São Paulo: McGraw-Hill, 2008.

Redes de Computadores / Andrew S. Tanenbaum e David Wetherall ; tradução Daniel Vieira ; revisão técnica Isaías Lima. – São Paulo: Pearson Prentice Hall, 2011