Como eu configuro o ESA para saltar o anti-Spam e/ou a exploração anti-vírus para meus remetentes confiados?

Índice

Pergunta:

Como eu configuro o ESA para saltar o anti-Spam e/ou a exploração anti-vírus para meus remetentes confiados?

AsyncOS oferece três ferramentas principais que você pode usar para saltar o anti-Spam ou a verificação anti-vírus para ver se há seus remetentes mais confiados. Note por favor que o ESA não recomenda a verificação anti-vírus de salto a qualquer hora, mesmo para ver se há seus remetentes mais confiados, devido ao potencial para a infecção inadvertida com os vírus. O seguinte é um exame das três maneiras que você pode saltar o anti-Spam que verifica para ver se há algum subconjunto de seu fluxo de mensagem.

A primeira ferramenta disponível a você é as políticas do fluxo de correio da tabela do acesso host (CHAPÉU). Usando políticas do fluxo de correio, você pode identificar remetentes pelo endereço IP de Um ou Mais Servidores Cisco ICM NT (usando endereços IP de Um ou Mais Servidores Cisco ICM NT numéricos ou nomes de DNS PTR), pela contagem de SenderBase, ou por um whitelist do DNS local ou a lista negra. Uma vez que você identificou remetentes como confiado dentro de um grupo do remetente no CHAPÉU, você pode então marcar esse grupo do remetente para saltar a exploração do anti-Spam.

Por exemplo, deixe-nos supõem que você quis identificar um parceiro de negócios específico, EXAMPLE.COM, que não deve ter o anti-Spam que verifica em seu correio. Você teria que encontrar registros dos endereços IP de Um ou Mais Servidores Cisco ICM NT (ou do DNS Pointer) do mail server SCU.COM. Neste caso, deixe-nos supõem que EXAMPLE.COM tem os server do correio que terão endereços IP de Um ou Mais Servidores Cisco ICM NT com registros PTR DNS de "smtp1.mail.scu.com" a "smtp4.mail.scu.com." para recordar neste caso que nós estamos olhando o registro PTR (chamado às vezes reverso DNS) para os server do correio; isto não não tem nada fazer com o Domain Name que os povos em SCU.COM usarão para correio que parte.

Você poderia criar um grupo novo do remetente (ou para usar um grupo existente do remetente, tal como o WHITELIST) com o grupo do remetente de Policies>Overview>Add do correio. Deixe-nos criar um chamado “NotSpammers”. Depois que você submeteu esta página, você estará retornado à tela de Policies>Overview do correio, onde você terá a oportunidade de adicionar uma política nova para este grupo do remetente. Se você clica sobre “adicionar a política,” você estará dado a oportunidade de criar uma política nova. Neste caso, nós queremos cancelar somente a política padrão em uma área: Detecção do Spam. Dê à política um nome e ajuste o comportamento da conexão para ser “aceitam,” enrole então para baixo a seção da detecção do Spam e ajustado esta política para saltar a verificação do Spam. Submeta essa política nova, e

não a esqueça “comprometem mudanças.”

Um abordagem alternativa é usar políticas do correio recebido para saltar a exploração do anti-Spam. A diferença entre o CHAPÉU e as políticas do correio recebido é que o CHAPÉU está baseado inteiramente na informação IP no remetente: o endereço IP de Um ou Mais Servidores Cisco ICM NT verdadeiro, o endereço IP de Um ou Mais Servidores Cisco ICM NT como refletido no DNS, a contagem de SenderBase (que é baseada no endereço IP de Um ou Mais Servidores Cisco ICM NT) ou uma entrada do whitelist ou da lista negra DNS baseada no endereço IP de Um ou Mais Servidores Cisco ICM NT. As políticas do correio recebido são baseadas na informação do envelope da mensagem: quem a mensagem é ou quem a mensagem é. Isto significa que são susceptíveis a ser enganado por alguém que encarna um remetente de mensagem. Contudo, se você quer saltar simplesmente todo o anti-Spam que verifica para ver se há o correio recebido que vem dos povos que têm os endereços email que terminam em “@example.com,” você poderia fazer aquele também.

Para criar tal política, vá enviar a política de Policies>Add do correio de Policies>Incoming. Isto deixá-lo-á adicionar uma política que defina um grupo de remetentes (ou de receptores). Uma vez que você define a política do correio recebido, aparecerá na tela da vista geral (políticas do correio de Policies>Incoming do correio). Você pode então clicar sobre a coluna do “Anti-Spam” e editar os ajustes específicos para o anti-Spam para este usuário particular.

Os ajustes do Anti-Spam para uma política particular têm lotes das opções, mas neste caso, nós queremos simplesmente saltar a verificação do anti-Spam. Note aqui uma outra diferença entre a política e políticas Chapéu-baseadas do correio recebido: o CHAPÉU pode deixou-o somente saltar ou não saltar a exploração do anti-Spam, quando as políticas do correio recebido tiverem o controle muito maior. Por exemplo, você poderia escolher quarantine o Spam de determinados remetentes, e suprime do Spam de outros remetentes.

A terceira opção para a exploração de salto do anti-Spam está em filtros da mensagem. (Nota que os filtros satisfeitos não podem ser usados para esta porque os filtros satisfeitos ocorrem depois que a exploração do anti-Spam tem ocorrido já). Uma das ações em filtros da mensagem é “faixa clara-spamcheck.” O filtro da mensagem abaixo saltará o anti-Spam que verifica para ver se há remetentes que têm um endereço IP particular ou que vêm de um Domain Name particular:

```
SkipSpamcheckFilter:
    se ((== '192.168.195.101' do IP remoto) ou
         (correio-\ @example do == do “\ .com$"))
    {
        faixa clara-spamcheck();
    }
```