**Atividade: Aplicar técnicas de proteção do sistema operacional**

**Cenário**

Você é analista de segurança cibernética do yummyrecipesforme.com, um site que vende receitas e livros de receitas. Um padeiro descontente decidiu publicar as receitas mais vendidas do site para o público acessar gratuitamente.

O padeiro executou um ataque de força bruta para obter acesso ao host. Eles inseriram repetidamente várias senhas padrão conhecidas para a conta administrativa até adivinharem corretamente a senha correta. Após obterem as credenciais de login, eles puderam acessar o painel de administração e alterar o código-fonte do site. Eles incorporaram uma função javascript no código-fonte que solicitava aos visitantes que baixassem e executassem um arquivo ao visitar o site. Após executar o arquivo baixado, os clientes são redirecionados para uma versão falsa do site onde as receitas do vendedor passam a estar disponíveis gratuitamente.

Várias horas após o ataque, vários clientes enviaram e-mails para o suporte técnico do yummyrecipesforme. Eles reclamaram que o site da empresa os havia solicitado a baixar um arquivo para atualizar seus navegadores. Os clientes alegaram que, após executar o arquivo, o endereço do site mudou e seus computadores pessoais passaram a funcionar mais lentamente.

Em resposta a esse incidente, o proprietário do site tenta fazer login no painel de administração, mas não consegue, então entra em contato com o provedor de hospedagem do site. Você e outros analistas de segurança cibernética têm a tarefa de investigar esse evento de segurança.

Para resolver o incidente, você cria um ambiente sandbox para observar o comportamento suspeito do site. Você executa o analisador de protocolo de rede tcpdump e digita a URL do site, yummyrecipesforme.com. Assim que o site é carregado, você é solicitado a baixar um arquivo executável para atualizar seu navegador. Você aceita o download e permite que o arquivo seja executado. Você então observa que seu navegador o redireciona para um URL diferente, greatrecipesforme.com, que foi projetado para se parecer com o site original. Porém, as receitas que sua empresa vende agora são postadas gratuitamente no novo site.

Os logs mostram o seguinte processo:

1. O navegador solicita uma resolução DNS do URL yummyrecipesforme.com.
2. O DNS responde com o endereço IP correto.
3. O navegador inicia uma solicitação HTTP para a página da web.
4. O navegador inicia o download do malware.
5. O navegador solicita outra resolução DNS para greatrecipesforme.com.
6. O servidor DNS responde com o novo endereço IP.
7. O navegador inicia uma solicitação HTTP para o novo endereço IP.

Um analista sênior confirma que o site foi comprometido. O analista verifica o código-fonte do site. Eles percebem que o código javascript foi adicionado para solicitar aos visitantes do site que baixem um arquivo executável. A análise do arquivo baixado encontrou um script que redireciona os navegadores dos visitantes de yummyrecipesforme.com para greatrecipesforme.com.

A equipe de segurança cibernética relata que o servidor web foi impactado por um ataque de força bruta. O padeiro insatisfeito conseguiu adivinhar a senha facilmente porque a senha do administrador ainda estava definida como a senha padrão. Além disso, não havia controles para evitar um ataque de força bruta.

Seu trabalho é documentar detalhadamente o incidente, incluindo identificar os protocolos de rede usados ​​para estabelecer a conexão entre o usuário e o site. Você também deve recomendar uma ação de segurança a ser tomada para evitar ataques de força bruta no futuro.

**Passo 1: Acesse o modelo**

Arquivo “*Relatório de incidente de cibersegurança*”

**Passo 2: Acessar os materiais de suporte**

Arquivo “*2 SUPORTE Log de tráfego DNS & HTTP”*

Arquivo “3 SUPORTE Como ler tráfego de log DNS & HTTP”

**Passo 3: Identifique o protocolo de rede envolvido no incidente**

Imagine que você é um dos analistas de segurança cibernética nesse cenário e tem a tarefa de escrever um relatório de incidente para esse evento de segurança. Usando o arquivo de log DNS e HTTP produzido com tcpdump, determine qual protocolo de rede é identificado nas capturas de pacotes durante a investigação. Você usará o que aprendeu sobre as quatro camadas do modelo TCP/IP e quais protocolos ocorrem em cada camada. Se necessário, você pode revisar o vídeo e ler sobre o modelo TCP/IP para usar como guia em sua resposta. Em seguida, revise o log de tráfego DNS e HTTP e registre qual protocolo você identificou na primeira seção do modelo de relatório de incidente de segurança.

**Passo 4: Documente o incidente**

Resuma o incidente na segunda seção do relatório. Forneça o máximo de detalhes e fatos possíveis em sua documentação. Ao escrever a documentação, certifique-se de:

* Evite usar linguagem emocional forte (bom, terrível, horrível, etc.).
* Inclua o máximo possível de fatos sobre o problema, incluindo onde o incidente ocorreu, como aconteceu, se alguém o testemunhou, como foi descoberto, etc.
* Indique suas fontes de informações e evidências.

Escrever documentação precisa e detalhada para incidentes de segurança cibernética pode servir como ponto de referência para outros analistas de segurança cibernética. Além disso, a documentação de qualidade pode ser usada para educar outros funcionários sobre as medidas de segurança cibernética tomadas na empresa quando ocorrem incidentes e pode ajudar as empresas a cumprir diversas auditorias de segurança.

**Etapa 5: recomende uma solução para ataques de força bruta**

Depois de documentar o incidente, escreva uma recomendação para ajudar sua organização a prevenir ataques de força bruta no futuro.

Alguns dos métodos de segurança comuns usados ​​para prevenir ataques de força bruta incluem:

* Exigindo senhas fortes
* Aplicando autenticação de dois fatores (2FA)
* Monitorando tentativas de login
* Limitando o número de tentativas de login

Selecione uma medida de segurança e explique por que ela é eficaz na seção três do modelo de relatório de incidentes de segurança.

Quanto mais medidas de segurança estiverem em vigor, menor será a probabilidade de um agente mal-intencionado conseguir aceder a informações confidenciais.

**O que incluir em sua resposta**

Certifique-se de atender aos seguintes critérios em sua atividade concluída:

* Cite um protocolo de rede identificado durante a investigação
* Documente o incidente
* Recomende uma medida de segurança

**Exemplo Concluído**

Arquivo “*Security incident report exemplar*”

Arquivo “*The Exemplar Explained - Security incident report exemplar*”

**Avaliação do Exemplo**

Compare o exemplar com sua atividade concluída. Revise seu trabalho usando cada um dos critérios do exemplar. O que você fez bem? Onde você pode melhorar? Use suas respostas a essas perguntas para orientá-lo à medida que avança no curso.

**Nota**: O exemplo representa uma possível explicação para os problemas que os usuários finais enfrentam. O seu provavelmente será diferente em alguns aspectos. O importante é que você identificou os protocolos de rede envolvidos e criou um relatório. Em sua função como analista de segurança, você e sua equipe documentariam qualquer problema que ocorresse na rede e apresentariam soluções para ajudar a evitar que os mesmos problemas ocorressem no futuro. Documentação de boa qualidade pode economizar tempo para você e sua organização e potencialmente gerenciar o ataque desde o início.

Primeiro, analise o log de tráfego DNS e HTTP para identificar um protocolo de rede. Em seguida, documente o incidente de segurança cibernética. Por fim, recomende uma medida de segurança que sua organização poderia implementar para evitar ataques de força bruta no futuro. A criação deste processo, por sua vez, ajudará a melhorar a postura de segurança da organização.

O exemplar é acompanhado da atividade e apresenta um exemplo de documentação profissional que inclui o seguinte:

* Um protocolo de rede identificado durante a investigação
* Documentação do incidente
* Uma medida de segurança recomendada