Laboratório - Tratamento de Incidentes

# Objetivos

Aplique seus conhecimentos sobre procedimentos de tratamento de incidentes de segurança para formular perguntas sobre determinados cenários de incidentes.

# Histórico/Cenário

A resposta a incidentes de segurança do computador tornou-se uma parte vital de qualquer organização. O processo para lidar com um incidente de segurança pode ser complicado e envolver muitos grupos diferentes. Uma organização deve ter padrões para responder a incidentes na forma de políticas, procedimentos e listas de verificação. Para responder adequadamente a um incidente de segurança, o analista de segurança deve ser treinado para entender o que fazer e também deve seguir todas as diretrizes descritas pela organização. Há muitos recursos disponíveis para ajudar as organizações a criar e manter uma política de tratamento de resposta a incidentes de computador. A Publicação Especial NIST 800-61r2 é citada especificamente nos tópicos do exame Noções Básicas de Operações de Segurança Cibernética da Cisco (200-201 CBROPS).

# Instruções

## Infestação por worm e agente de negação de serviço distribuído (DDoS)

Estude o cenário a seguir e discuta e determine as perguntas de tratamento de resposta a incidentes que devem ser feitas em cada estágio do processo de resposta a incidentes. Considere os detalhes da organização e do CSIRC ao formular suas perguntas.

Este cenário é sobre uma pequena empresa de investimento familiar. A organização tem apenas um local e menos de 100 funcionários. Em uma manhã de terça-feira, um novo worm é lançado; ele se espalha por meio de mídia removível e pode se copiar para abrir compartilhamentos do Windows. Quando o worm infecta um host, ele instala um agente DDoS. Foi várias horas depois que o worm começou a se espalhar antes que as assinaturas de antivírus ficassem disponíveis. A organização já havia incorrido em infecções generalizadas.

A empresa de investimento contratou uma pequena equipe de especialistas em segurança que muitas vezes usam o modelo de diamante de manipulação de incidentes de segurança.

**Preparação:**

Digite suas respostas aqui.

**Detecção e análise:**

Digite suas respostas aqui.

Contenção, erradicação e recuperação:

Digite suas respostas aqui.

Atividade pós-incidente:

Digite suas respostas aqui.

## Acesso não autorizado a registros de folha de pagamento

Estude o seguinte cenário. Discuta e determine as perguntas de tratamento de resposta a incidentes que devem ser feitas em cada estágio do processo de resposta a incidentes. Considere os detalhes da organização e do CSIRC ao formular suas perguntas.

Este cenário é sobre um hospital de médio porte com vários escritórios satélites e serviços médicos. A organização tem dezenas de locais que empregam mais de 5000 funcionários. Devido ao tamanho da organização, eles adotaram um modelo CSIRC com equipes distribuídas de resposta a incidentes. Eles também têm uma equipe de coordenação que cuida da equipe de operações de segurança e os ajuda a se comunicar uns com os outros.

Em uma quarta-feira à noite, a equipe de segurança física da organização recebe uma chamada de um administrador de folha de pagamento que viu uma pessoa desconhecida sair do escritório, correr pelo corredor e sair do prédio. O administrador deixou sua estação de trabalho desbloqueada e sem vigilância por apenas alguns minutos. O programa de folha de pagamento ainda está conectado e no menu principal, como estava quando ela o deixou, mas o administrador percebe que o mouse parece ter sido movido. A equipe de resposta a incidentes foi solicitada a adquirir evidências relacionadas ao incidente e determinar quais ações foram realizadas.

As equipes de segurança praticam o modelo de cadeia de eliminação e entendem como usar o banco de dados VERIS. Para uma camada extra de proteção, eles terceirizaram parcialmente a equipe para um MSSP para monitoramento 24 horas por dia, 7 dias por semana.

Preparação:

Digite suas respostas aqui.

Detecção e análise:

Digite suas respostas aqui.

Contenção, erradicação e recuperação:

Digite suas respostas aqui.

Atividade pós-incidente:

Digite suas respostas aqui.

Fim do documento6