Universidade de Aveiro
Mestrado em Cibersegurança

Exame Teórico de Ep. Especial de Segurança em Redes de Comunicações
13 de Setembro de 2021

Duração: 1h45m. Sem consulta. Justifique cuidadosamente todas as respostas.

1. Explique as diferentes fases e possíveis vetores de ataque para o roubo de dados numa sistema de base de dados numa empresa. Apresente possíveis mecanismos de defesa. (4.0 valores)

Tendo em conta que um **vetor de ataque** representa a abordagem escolhida pelo atacante para realizar um ataque a uma determinada máquina ou sistema, este vetor encontra-se dividido em múltiplas fases.

A fase inicial é a de **descoberta**, onde o atacante estuda a empresa-alvo e as relações humanas dentro da mesma, de modo a identificar o alvo mais vulnerável. Normalmente, são utilizadas redes sociais, tanto virtuais como físicas, para esta fase de pesquisa, resultando na abordagem de pessoal que não está diretamente relacionado com a gestão de topo da empresa em análise, mas que ainda assim possui algumas credenciais de acesso, constituindo um alvo mais desprotegido que pode garantir acesso a informações mais restritas.

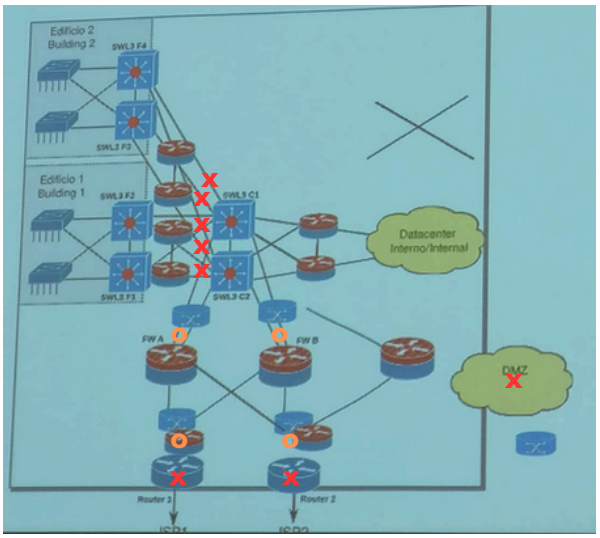
Segue-se a fase de **infiltração**, onde o atacante lança o ataque ao alvo selecionado, através do envio de um e-mail com link (phishing), por exemplo, ou uma mensagem nas redes sociais, induzindo a vítima a inserir as suas credenciais da empresa ou a instalar um software que permita o acesso remoto ao dispositivo. Embora mais raro, é também possível considerar o acesso direto à máquina alvo através de distrações do pessoal de serviço, deixando-a momentaneamente desprotegida e vulnerável, permitindo que alguém consiga aceder ao dispositivo ou inserir uma pen USB que extraia ou descarregue dados, obtendo credenciais e/ou outros tipos de informações sensíveis.

Posteriormente, sucede a fase de **propagação**, onde, uma vez infiltrado na rede, o atacante tenta disseminar-se pela mesma, procurando acesso a mais recursos através de metodologias como a exploração de credenciais e vulnerabilidades, bem como o spoofing de utilizadores e serviços.

No caso de ataques via e-mail, é essencial a existência de sistemas de **filtragem** para bloquear mensagens provenientes de fontes maliciosas, embora a implementação correta destes sistemas seja bastante complexa e desafiante. Além disso, deve haver monitorização relativa a anomalias na comunicação, como a interação entre máquinas que anteriormente nunca comunicaram entre si, para identificar possíveis roubos de dados. Também é possível controlar as formas de upload e download de dados, comparando-as com valores anteriores através de algoritmos predefinidos para avaliar a situação.

Relativamente a mensagens enviadas através de outras aplicações de comunicação, a monitorização depende em grande parte do bom senso do utilizador, o que deixa uma margem considerável para erros e falhas. Para evitar estes ataques, devem ser implementados mecanismos de segurança diretamente nas máquinas e nos sistemas, tais como honeypots, definição de regras de firewall e a implementação de serviços de deteção e prevenção de intrusões.

2. Uma empresa pretende colocar na sua infraestrutura de rede um conjunto de servidores HTTPS (portos TCP 443 e TCP 8888) acessíveis do exterior com vários serviços Web da empresa. Proponha uma solução de proteção da rede que permita (i) controlar os fluxos de tráfego de acesso aos serviços e (ii) proteger a infraestrutura contra ataques de negação de serviço distribuídos (DDoS). Assuma que a empresa apenas tem uma infraestrutura de encaminhamento de tráfego IP e que possui utilizadores internos que precisam de aceder à Internet (4.5 valores)



Para que o fluxo de trafego de acesssos aos serviços seja controlado, então é necessário que os servidores públicos ligados às firewalls. Ou seja, a posição das firewalls deve ser mudada, enquanto que de momento estas estão implementadas dentro dos edificios, deverão passar a ser implementadas antes dos mesmos, e ainda mais perto do acesso à internet, junto aos R1 e R2 (x).

Atualmente, estão implementadas apenas duas firewalls stateful. Estas firewalls A e B, por serem stateful, armazenam constantemente todos os dados relativos aos estados atuais das comunicações correntes. No caso de um ataque DDoS, as firewalls irão sincronizar todos os fluxos do ataque até atingirem o limite de capacidade. No entanto, ao sincronizarem, não partilham a carga de trabalho, pois ambas possuem as mesmas informações, o que não é suficiente para proteger o sistema contra um ataque DDoS.
Para aumentar a capacidade de processamento e melhorar a defesa contra ataques, podemos aplicar mais firewalls e desligar o sincronismo entre elas. Em seguida, podemos utilizar load balancers (o, em cima e em baixo das firewalls) para distribuir o tráfego de forma equilibrada, garantindo que o tráfego seja sempre encaminhado através do mesmo caminho sem sobrecarregar as firewalls. Desta forma, o tráfego é melhor gerido e a infraestrutura de segurança torna-se mais robusta.
Além disso, dado que a DMZ depende de uma firewall, é devemos definir explicitamente quem pode ou não aceder à DMZ, bem como os comportamentos que determinarão se o tráfego de um determinado IP deve ser bloqueado ou permitido.

3. Proponha uma solução de interligação entre múltiplos polos de uma empresa que providencie confidencialidade para o tráfego de videoconferência e tráfego de sincronismo de base de dados entre elas (e apenas a esse tráfego). (4.0 valores)

Para garantir a confidencialidade nas comunicações entre múltiplos polos, deve ser utilizado IPSEC-ESP. Considerando a existência de múltiplos pontos de comunicação, deve ser implementado um túnel multiponto protegido por IPSEC-ESP, assegurando assim a confidencialidade dos dados transmitidos. No entanto, é igualmente necessário garantir que esta comunicação é utilizada exclusivamente para o serviço de videoconferência. Para tal, deverão ser definidos routemaps específicos.

4. Admitindo que numa rede empresarial existem múltiplas fichas Ethernet em espaços públicos ou semi-públicos e terminais Wi-Fi, proponha uma solução integrada de controle do acesso de máquinas à rede. (3.0 valores)

A norma IEEE 802.1X, que proporciona autenticação para dispositivos que desejam conectar-se a uma LAN, será configurada para realizar a autenticação, autorização e contabilidade dos dispositivos que tentam aceder a rede. Esta norma, em conjunto com um servidor RADIUS (Remote Authentication Dial-In User Service) integrado com LDAP (Lightweight Directory Access Protocol) para verificar as credenciais dos utilizadores e dispositivos, oferece uma solução eficaz para este propósito.

Será também necessário adicionar exceções às regras da firewall implementadas para permitir estas verificações.

5. Numa rede empresarial pretende-se implementar um sistema de deteção de intrusões (IDS) que permita detetar as máquinas comprometidas por uma BotNet. Os elementos da BotNet podem a qualquer momento efetuar uma das seguintes atividades: (i) comunicar diretamente entre si para sincronismos de ações, (ii) receber comandos do exterior da rede via ligações HTTPS e (iii) participar no envio de e-mail em quantidades elevadas (Spam) usando o servidor da empresa. Explique como o sistema pode ser integrado na arquitetura de uma rede empresarial e proponha um possível conjunto de regras para a deteção de comunicações ilícitas. (4.5 valores)

Para implementar um sistema de deteção de intrusões (IDS) numa rede empresarial e identificar máquinas comprometidas por uma BotNet, é necessário considerar que os elementos da BotNet podem comunicar diretamente entre si para sincronizar ações, receber comandos do exterior via ligações HTTPS e enviar grandes quantidades de e-mails de spam utilizando o servidor da empresa.

O IDS deve ser estrategicamente posicionado para monitorizar tráfego entre diferentes segmentos da rede, incluindo VLANs e comunicações externas. Sugere-se a colocação de sensores IDS nos pontos de entrada e saída da rede, entre VLANs e nos servidores críticos, como o servidor de e-mail.

Para detetar comunicações ilícitas, pode-se estabelecer as seguintes regras: (i) Monitorizar o aumento do tráfego direto entre máquinas em VLANs distintas, registando a matriz de tráfego para calcular a percentagem de comunicação entre cada par de máquinas. Utilizar estatísticas SNMP para detetar variações anómalas no volume de tráfego interno e estabelecer alertas para aumentos significativos na comunicação direta entre dispositivos. (ii) Filtrar e analisar o tráfego HTTPS nas firewalls, focando-se em volumes de tráfego incomuns e comunicações com países não habituais. Criar eventos de alerta para tentativas de comunicação com endereços IP desconhecidos ou provenientes de países raramente comunicantes com a empresa, monitorizando estes eventos em tempo real para identificar padrões de comando e controlo. (iii) Implementar sistemas de monitorização da frequência de envio de e-mails nos servidores de e-mail, utilizando SNMP para recolher estatísticas de utilização. Estabelecer alertas para variações abruptas na frequência de envio de e-mails, como uma máquina que passa a enviar e-mails de hora a hora para a cada 3 segundos. Verificar se os e-mails enviados utilizam domínios legítimos da empresa e analisar a localização geográfica dos servidores de destino, investigando qualquer desvio significativo dos padrões normais de envio.

A integração de um IDS numa rede empresarial para detetar máquinas comprometidas por uma BotNet requer uma abordagem multifacetada, com sensores estrategicamente posicionados e regras específicas para identificar comportamentos anómalos, assegurando a monitorização contínua e a análise detalhada do tráfego para identificar e mitigar a atividade maliciosa de forma eficaz.