1.Ferramentas de segurança

Na sua rede corporativa, provavelmente há várias ferramentas de segurança diferentes. Você pode ter firewalls de próxima geração, sistemas de prevenção de intrusões e scanners de vulnerabilidades executando verificações regulares. Essas ferramentas geram uma grande quantidade de informações, mas cada uma tem um formato próprio para descrever eventos e vulnerabilidades. O desafio é que um firewall, um sistema de prevenção de intrusões e um scanner de vulnerabilidades podem identificar a mesma falha, mas usando nomes, descrições e classificações diferentes.

Para resolver esse problema, a indústria criou o **Security Content Automation Protocol (SCAP)**. Esse protocolo é mantido pelo **National Institute of Standards and Technology (NIST)**, e mais informações podem ser encontradas em **scap.nist.gov**. O SCAP permite consolidar vulnerabilidades em uma linguagem padronizada que todos os dispositivos entendem. Assim, se um firewall, um sistema de prevenção de intrusões e um scanner de vulnerabilidades identificarem a mesma falha, o SCAP garante que todos reconheçam essa vulnerabilidade como sendo exatamente a mesma.

Isso permite que diferentes ferramentas de segurança trabalhem juntas, automatizando a detecção e a correção de vulnerabilidades na rede. Por exemplo, um scanner de vulnerabilidades pode identificar um dispositivo com uma falha e enviar essa informação para um sistema de gerenciamento, que então pode automatizar o envio de um patch para corrigir o problema, sem necessidade de intervenção manual. Esse processo é especialmente útil quando há centenas ou milhares de dispositivos que precisam de atualizações frequentes em diferentes sistemas operacionais.

Com todos os dispositivos de segurança falando a mesma linguagem, a comunicação entre eles se torna mais eficiente, facilitando a automação da correção de falhas. Processos que antes exigiam intervenção manual agora podem ser automatizados, como a detecção de vulnerabilidades, o envio de alertas e a aplicação de patches para manter os sistemas em conformidade.

Ao longo do tempo, foram desenvolvidas diversas **melhores práticas de segurança** para diferentes sistemas operacionais e aplicativos. Isso significa que é possível seguir um conjunto de diretrizes para configurar um sistema operacional da forma mais segura possível. O mesmo se aplica a aplicativos, conexões com provedores de nuvem e outros elementos do ambiente de TI.

Por exemplo, um benchmark de segurança para um dispositivo móvel pode incluir diretrizes como desativar capturas de tela, impedir gravações de tela, bloquear chamadas de voz quando o sistema está bloqueado e forçar a criptografia de backups. A combinação dessas práticas cria um ambiente seguro logo após a instalação do sistema.

Uma biblioteca extensa de benchmarks de segurança está disponível no **Center for Internet Security (CIS)**, acessível pelo site **cissecurity.org**.

Manter dispositivos seguros é um desafio, pois novas vulnerabilidades são descobertas constantemente. Cada vez que um sistema se conecta à rede ou um usuário faz login, é comum que verificações sejam realizadas para garantir a conformidade com as políticas de segurança. Em alguns casos, um agente de segurança é instalado previamente no dispositivo para monitoramento contínuo. Em outros, uma verificação sob demanda pode ser feita sem a necessidade de instalação permanente.

Os agentes instalados nos dispositivos garantem monitoramento constante, verificando a conformidade com as políticas de segurança. No entanto, isso requer atualizações frequentes do agente e das regras de segurança. Já as verificações sem agente ocorrem quando um dispositivo se conecta à rede, executando verificações temporárias e removendo-se automaticamente após a análise.

Outra ferramenta essencial de segurança é o **SIEM (Security Information and Event Management)**, um sistema que consolida logs de dispositivos como firewalls, switches e servidores em um único banco de dados. Com o SIEM, é possível correlacionar eventos de diferentes fontes, como acessos a VPNs, uso de aplicativos e regras de firewall bloqueadas. Esse tipo de análise permite criar relatórios detalhados sobre atividades suspeitas e realizar investigações forenses sobre incidentes de segurança.

Sistemas operacionais modernos incluem **antivírus e antimalware** para detectar ameaças como cavalos de Troia, worms e vírus de macro. Embora os termos antivírus e antimalware sejam frequentemente usados de forma intercambiável, ambos se referem a softwares projetados para proteger contra códigos maliciosos.

Para impedir a transferência de dados sensíveis para fora da rede, muitas empresas utilizam **Data Loss Prevention (DLP)**. **Esse tipo de ferramenta monitora o tráfego em tempo real e bloqueia informações confidenciais**, como números de cartão de crédito, registros médicos e dados de identidade. O DLP pode ser aplicado não apenas em redes locais, mas também em ambientes de nuvem e dispositivos móveis.

Muitos dispositivos já possuem sistemas de monitoramento embutidos, que coletam informações por meio do **Simple Network Management Protocol (SNMP)**. **Esse protocolo permite que dispositivos reportem métricas como uso de banda, status da CPU e tráfego de rede**. Os dados são armazenados em uma **Management Information Base (MIB)** e acessados por meio de identificadores numéricos chamados **Object Identifiers (OID)**. O SNMP geralmente opera na porta **UDP 161** e pode ser configurado para gerar alertas chamados **SNMP traps**, enviados para um sistema de gerenciamento quando certos limites são atingidos.

Além do SNMP, outro protocolo amplamente utilizado para monitoramento de tráfego é o NetFlow, que permite analisar padrões de comunicação entre dispositivos. O NetFlow coleta informações sobre os fluxos de dados e pode ser usado para identificar padrões anômalos de tráfego na rede. A análise de NetFlow é feita por meio de **probes** que coletam informações de tráfego e enviam para um **coletor de NetFlow**, responsável por gerar relatórios detalhados sobre o uso da rede.

Outra ferramenta essencial para a segurança da rede é o **scanner de vulnerabilidades**, que identifica falhas potenciais nos dispositivos sem explorar as brechas ativamente. Esses scanners podem executar varreduras externas para simular o que um atacante veria ao tentar acessar a rede. Como essas varreduras coletam grandes volumes de informações, é importante revisar os resultados para descartar falsos positivos e priorizar a correção das vulnerabilidades críticas.

Ao analisar os resultados de uma varredura, é comum encontrar vulnerabilidades classificadas por nível de risco, desde falhas críticas até alertas informativos. Por exemplo, um scanner pode detectar um problema com o gerador de números aleatórios de um servidor, o que permitiria que um atacante obtivesse acesso remoto ao sistema. Também pode identificar sistemas operacionais sem suporte, que não recebem mais atualizações de segurança e representam um risco significativo.

As varreduras de vulnerabilidades devem ser realizadas regularmente para evitar que falhas críticas permaneçam na rede por longos períodos. A correção dessas vulnerabilidades deve seguir um plano de gerenciamento de riscos, garantindo que os sistemas sejam mantidos seguros sem causar interrupções nos serviços.