Enumeração com SNMP

O Simple Network Management Protocol (SNMP) é um mecanismo útil para enumerar sistemas alvos durante um pentest. Ele é usado para auxiliar na gestão de dispositivos como roteadores, hubs e switches.

Existem 3 versões atualmente:

SNMPv1 – Esta versão do protocolo foi introduzida e padronizada como um mecanismo para gerenciar dispositivos de rede. Enquanto ele veio para fazer muitas tarefas de forma padronizada, ele deixou a desejar em outras coisas que vieram ser resolvidas nas versões posteriores. Como um pentester, basta saber que esta versão não tem nenhum mecanismo de segurança.

SNMPv2 – Esta versão introduziu novas funções de gestão, assim como de segurança. Pelo desenho, ele é compatível com sua versão anterior, a v1.

SNMPv3 – É a versão mais recente do protocolo, a qual trouxe uma ênfase maior em segurança. A segurança está focada em duas áreas:

Autenticação que é usada para garantir que as capturas sejam lidas apenas pelo seu destinatário.

Privacidade criptografa o payload da mensagem SNMP para garantir que não possa ser lida por usuários não autorizados.

SNMP é um protocolo da camada de Aplicação que funciona através do UDP. O protocolo é multiplataforma, o que significa que pode ser acessado pelos SO modernos, incluindo o Windows, Linux e Unix. O principal requisito para SNMP é que a rede seja TCP/IP.

A enumeração SNMP para um hacker ético consiste em alavancar as fraquezas do protocolo para revelar contas de usuários e

dispositivos que estejam executando no protocolo. Para entender melhor isto, vamos nos aprofundar em alguns componentes do sistema SNMP. Basicamente temos dois componentes: o agente SNMP e a estação de gestão SNMP. O agente fica localizado no dispositivo monitorado ou gerenciado, enquanto a estação de gestão se comunica com os agentes.

Nos equipamentos empresariais mais modernos, como roteadores e switches, possuem um agente SNMP embutido em seu sistema.

O sistema funciona da seguinte forma:

1. A estação de gerenciamento SNMP envia uma solicitação ao agente;
2. O agente recebe a solicitação e envia uma resposta.

As mensagens enviadas e recebidas funcionam definindo ou lendo variáveis em um dispositivo. Além disso, o agente usa artifícios para deixar a estação de gerenciamento saber se alguma coisa ocorreu, como falha ou reinicialização, que precisa ser resolvido.

Management Information Base

O Management Information Base (MIB) é um banco de dados que contém descrições de objetos de rede que podem ser gerenciados através do SNMP. MIB é a coleção hierárquica e organizada da informação. Ele provê uma representação padronizada das informações e armazenamento do agente. Elementos MIB são reconhecidos usando identificadores de objetos. O object identifier (OID) é um nome numérico dado ao objeto e começa na raíz da árvore MIB. Ele pode identificar unicamente o objeto presente na hierarquia MIB.

Os objetos gerenciados pelo MIB incluem objetos escalares que definem uma instância de objeto único e objetos tabulares que definem grupos de instâncias de objetos relacionados. Os

identificadores de objeto incluem o tipo do objeto, como contador, sequência ou endereço; Nível de acesso, como leitura ou leitura/escrita; Restrições de tamanho; E informações de alcance. O MIB é usado como um livro de códigos pelo gerenciador SNMP para converter os números OID em uma tela legível por humanos.

Por padrão, SNMP tende a ter duas senhas usadas tanto para configurar e ler a informação de um agente:

- String da comunicadade para leitura:
  - Configuração do dispositivos ou sistema que pode ser visto com a ajuda desta senha;
  - Estas strings são públicas;
- String de comunidade para leitura/escrita:
  - Configuração no dispositivo que pode ser trocada ou editada usando esta senha;
  - Estas strings são privadas.

Apesar destas strings poderem ser trocadas, elas também podem ser deixadas de forma padrão. Atacantes podem e irão aproveitar esta oportunidade de erro. Um atacante pode usar a senha padrão para modificar ou visualizar informações de um dispositivo ou sistema. Como um hacker ético, você tentará usar o serviço para enumerar as informações de um dispositivo para ataques futuros.

Veja o que pode ser extraído através do SNMP:

- Recursos de rede como os hosts, roteadores e dispositivos;
- Compartilhamentos de arquivos;
- Tabelas ARP;
- Tabela de roteamento;
- Informações específicas do dispositivo;
- Estatísticas de tráfego;

Ferramentas de enumeração SNMP incluem o SNMPUtil e o IP Network Browser da SolarWinds.

SNScan

É um utilitário feito para detectar dispositivos em uma rede com SNMP ativo. Ele irá ajudar a localizar e identificar dispositivos que sejam vulneráveis a ataques SNMP. SNScan fareja em portas específicas (ex.: UDP 161, 193, 391 e 1993) e procura por nomes padrões de comunicadades (públicas e privadas) e as definidas pelo usuário. Nomes de comunidades definidas pelo usuário podem ser usadas para avaliar de forma mais eficiente a presença de dispositivos com SNMP ativo em redes complexas.

Sugestões de livros: