Enumeração de serviços de diretório e LDAP

O Lightweight Directory Access Protocol (LDAP) é usado para interagir e organizar banco de dados. LDAP é comumente usado porque é um padrão aberto e um grande número de fornecedores usam em seus próprios produtos, em muitos casos, serviços de diretórios como o Active Directory da Microsoft. Tenha em mente que você pode ter outros serviços interagindo com LDAP e, portanto, informações estarem sendo vazadas para outros sem a sua aprovação.

Se você fazer suas anotações durante a fase de escaneamento, você pode lembrar de ter achado alguma porta 389 aberta. Se você achou esta porta aberta durante o scan, você pode ter achado um alvo interessante. Esta porta está associada com o LDAP, no qual você pode achar um serviço de diretório ou algo semelhante.

O LDAP é muito usado com o Active Directory ou OpenLDAP, mas na prática, este protocolo é usado pelas empresas que são armazens de um grande volume de dados.

Um diretório é um banco de dados, mas os dados são organizados de forma hierárquica ou lógica. Outra forma de olhar para este desenho é pensar como uma organização de dados assim como ocorrer em um sistema operacional, com arquivos e pastas. Para facilitar e tornar mais eficiente o acesso estes dados, você pode usar um serviço de DNS para aumentar a velocidade das consultas.

Serviços de diretórios criados para usar o LDAP:

- Active Directory
- Novell eDirectory
- OpenLDAP
- Open Directory

- Oracle iPlanet

Em muitos casos, as consultas realizadas através do LDAP no banco de dados tendem a vazar dados sensíveis que o atacante pode tirar vantagem. Muitos serviços de diretórios oferecem formas de proteger estas consultas através de criptografia ou outros mecanismos, os quais são ativados por padrão ou devem ser ativados pelo administrador.

Ferramentas que permitem a enumeração de sistemas e serviços com LDAP ativo são:

- JXplorer
- LDAP Admin Tool
- LDAP Account Manager
- LEX (The LDAP Explorer)
- Active Directory Explorer
- LDAP Administration Tool
- LDAP Search
- Active Directory Domain Services Management Pack
- LDAP Browser/Editor
- Nmap (using an NSE script)

JXplorer

JXplorer é uma ferramenta popular e grátis para navegação LDAP usada para ler e buscar por qualquer diretório LDAP ativo. É necessário uma máquina virtual Java instalada para execução.

Algumas funcionalidades dele são:

- Suporta as operações padrão LDAP (add, delete, modify);
- Pode copiar e deletar a estrutura da árvore;
- Autenticação SSL e SASL;
- Serviços de segurança plugáveis;
- Multiplataforma, incluindo Windows, Linux, Solaris, HPUX, BSD e AIX;
- Exibição dos dados tipo HTML;

Evitando enumeração LDAP

LDAP pode ser difícil de proteger contra a enumeração, mas é possível. A parte difícil de proteger o LDAP é que, se você fechar portas ou filtrar o tráfego relacionado ao LDAP, você poderia facilmente afetar o desempenho de sua rede, impedindo que os clientes consultem um diretório ou outro serviço crítico. Sem recomendar qualquer produto de terceiros, a maneira mais fácil de iniciar o processo de proteger as informações acessadas via LDAP é fazer uso das permissões e configurações de segurança presentes em seu serviço de diretório.

Sugestões de livros: