LD Scanning

Clube dos Mercenários

http://cdm.hacking.la

Por: Jerry Slater jerryslater@bol.com.br **14/03/2003**
http://jerryslater.host.sk

Fatos:

Desde o início sempre ficou visível o abismo que existe entre a comunidade underground e o pessoal da segurança. Com o passar dos anos muitos acreditavam que esse abismo iria diminuir ou até mesmo acabar, mas o que aconteceu foi justamente o oposto. A distância entre esses dois universos ficou cada vez maior, tanto em termos éticos, quanto técnicos.

O caráter financeiro da profissão de Analista de Segurança atraiu a atenção de muitos, que partiram desenfreadamente para essa ramificação. Com o excedente número de profissionais, o mercado para esse ramo começa a se tornar saturado, pessoas completamente despreparadas abraçam o "*security world*" levados apenas pela ganância e não pelo simples impulso que um hacker têm dentro de si, a curiosidade. Com isso redes mais inseguras foram surgindo, falsas soluções foram nascendo e trazendo consigo a surreal sensação de segurança. Mas o processo de seleção natural começa a agir, quem não conseguir evoluir vai ficar no meio do caminho e acabar sendo excluído.

Técnica:

Recentemente escrevi um texto para o CdM (Clube dos Mercenários) sobre o básico de Port Scanning. Notei que hoje muitas redes procuram proteger-se de um scaneamento, pois esse, na maioria das vezes, é o passo inicial de um ataque. Inibindo o ponto de partida muitos procuram um outro alvo mais fraco que não

exija muito trabalho. Ferramentas foram desenvolvidas para anular o ponto 0 usando vários meios como:

- Enviando informações falsas sobre a rede alvo;
- Barrando tráfego entre a rede alvo e o atacante.

Isso acontece por que muitos executam um Port Scanning de suas próprias máquinas ou através de um bounce e isso acaba não mudando muito no resultado.

Percebi que a melhor opção para se scanear um rede é usando Port Scanning Distribuited, pois o mesmo é capaz de passar por firewalls e até mesmo ferramentas de segurança e ainda torna dificílima da tarefa de encontrar o responsável pelo scaneamento. Mas para isso seria necessário acesso a “muitos” hosts para se executar.

É preciso acesso a vários hosts para se executar um Port Scanning Distribuited?

Minhas resposta é **NÃO**.

Imagine uma rede com 5 máquinas e 1 servidor, todos com IP’s reais. Conseguindo acesso a apenas 1 das máquinas da rede eu posso usar o resto dos hosts para executar um Port Scanning Distribuited sem sequer tentar invadí-los. Como?

Utilizando IP Spoofing + Sniffing.

Vamos utilizar aqui como exemplo o SYN Scan.

Sabemos que o pacote inicial para o estabelecimento de um conexão entre dois hosts possui a flag SYN ativa.
O SYN scan consiste em o atacante enviar um pacote com essa flag ativada para várias portas do host alvo. Se o alvo responder com um pacote com as flags SYN + ACK ativadas significa que a porta está aberta.

O Port Scanning LD consiste em, com acesso a 1 host da rede o atacante instalaria um sniffer e enviaria pacotes com os IP’s do resto da rede para seu alvo e com o sniffer ele conseguiria capturar a resposta do alvo aos hosts spoofados..:)

Com isso a regra mais utilizada por firewalls e ferramentas de segurança seria quebrada e com acesso a apenas 1 host um atacante poderia scanear qualquer rede sem problemas.

Um problema pode ser visto, o alvo saberia de qual REDE veio o ataque, mas isso seria algo a se considerar se o atacante estiver em uma rede pequena. Imagine o atacante com acesso a um backbone... o modo como um Analista de

Segurança poderia tentar se defender era bloqueando a comunicação entre a REDE e o alvo, mas com acesso a um backbone isso seria muito inviável.

Há quem pense: “Então eu vou bloquear os pacotes com a flag SYN ativada!”
Então acostume-se com a solidão...:)

Qualquer outra forma de Half-Open ou Stelath scan pode ser utilizada.

Em breve estarei disponibilizando o código para implementação dessa técnica.

Agradecimentos:

Agradeço primeiramente a Jeová Deus, a minha amada esposa que sempre está ao meu lado. Aos meus amigos, principalmente ao meu velho amigo Nash Leon e a todo pessoal do #mercenaries.

[ ]’s

Jerry Slater.