Terceiro Trabalho de Introdução à Segurança Computacional

[Worm, ataque com mecanismo de propagação]

Rafael Ravedutti Lucio Machado
Universidade Federal do Paraná
Curitiba, Paraná
rrlm13@inf.ufpr.br

ABSTRACT

Este artigo provê informações relativas ao terceiro trabalho de Introdução à Segurança Computacional. O objetivo do trabalho é o desenvolvimento de um worm, o qual deve realizar o ataque com um código explorador (exploit) em um servidor WuFTPD junto com um mecanismo de força bruta para que possa ser espalhado e executado para diferentes máquinas adjacentes recursivamente.

Keywords

worm; bruteforce; spread; scanner; segurança; computacional

1. INTRODUÇÃO

Os worms são programas com a capacidade de realizar ataques e se difamar sobre uma rede inteira de computadores. Com uma coleção de ataques por exploração (exploits), escaneadores de rede (port scanners) e mecanismos para quebra de senhas (força bruta e dicionário, por exemplo) os worms procuram diversas formas de adentrar nos servidores e, ao fazê-lo, procuram se replicar em seus servidores adjacentes até que uma rede inteira (ou boa parte dela) seja comprometida. Neste trabalho foi desenvolvido um modelo simples de worm dividido em 5 módulos (worm, exploit, spread, bruteforce e scanner).

2. FUNCIONAMENTO

Conforme mencionado anteriormente, o worm desenvolvido é composto por 5 módulos, os módulos nesta seção serão abordados separadamente:

2.1 Scanner

O scanner da rede é o mesmo desenvolvido no trabalho 1. Seu objetivo é escanear os endereços especificados via linha de comando, com uma ressalva: neste trabalho, se não forem especificados parâmetros, cada rede pertencente a cada interface de rede da máquina (ifconfig -a) será utilizada como faixa de entrada, dos hosts 1 ao 255 (este funcionamento não está presente no binário para arquitetura i686 devido à incompatibilidade de bibliotecas).

Como mencionado no artigo do primeiro trabalho, o scanner pode acabar não obtendo todos os serviços de todos os hosts, o que acaba por diminuir a precisão do worm, porém nos testes efetuados não foram reproduzidos problemas deste gênero.

2.2 Bruteforce

O ataque de força bruta é o mesmo desenvolvido no trabalho 2, porém este foi aprimorado para que se possa executar em paralelo usando pthreads. Contudo, sua performance foi melhorada além de conter funções específicas para testes de conexão FTP.

2.3 Exploit

O código explorador foi encontrado na web (1) e modificado para que não se comporte como um programa separado, mas como uma biblioteca de funções. Para isto, fora desenvolvida a função remote_exploit, que utiliza (de forma mais sucinta) os mesmos procedimentos da função principal contida no exploit (que foi removida), porém sem receber entradas via linha de comando e retornando o file descriptor obtido após a exploração (o qual é usado para injetar comandos na máquina alvo).

2.4 Spread

O mecanismo para o worm se espalhar foi feito estudando e respeitando os comandos do protocolo FTP. Após o login obtido via força bruta, são enviados ao servidor os comandos para informar que o arquivo a ser transferido é um binário e posteriormente um comando para entrar no modo passivo. Após o comando para o modo passivo, o servidor retorna o endereço e a porta a ser efetuada a conexão para transmissão dos dados, então é feita a conexão e os binários do worm (x86_64 e i686) são transferidos para a máquina alvo.

2.5 Worm

O corpo do worm é o que fica reponsável por utilizar e orquestrar os outros módulos da maneira adequada. Primeiro é feito a varredura da rede, depois aleatoriamente é selecionado o método para transferir o worm para o servidor alvo (em caso de falha de um dos métodos mencionados, o outro método referente à mesma etapa é utilizado). Os métodos usados são: (1) força-bruta, onde se obtêm as cre-

ACM ISBN 978-1-4503-2138-9.
DOI: 10.1145/1235

denciais do servidor FTP e então o acessa para fazer upload dos binários, e (2) exploit, onde utilizando o código de exploração é criado um usuário na máquina alvo com uma senha já conhecida, este usuário então é usado para se conectar via FTP e fazer upload dos binários.

Em seguida, de acordo com a decisão anterior, o método de execução remota do worm é realizado. Os possíveis métodos são: (1) telnet, onde se utiliza um script usando o programa expect para se conectar no servidor alvo via Telnet e então executar o worm, e (2) exploit, onde se executa o worm através da sessão remota como root obtida pelo código de exploração. Não foi possível executar o comando expect nas máquinas alvos disponibilizadas devido à carência de seu binário e suas bibliotecas, portanto este método tende a não funcionar quando as mesmas atuam como atacantes (o que implica no uso do código explorador).

3. RESULTADOS

Com base nos testes efetuados, o worm foi copiado com sucesso para as máquinas alvos e posteriormente executado nas mesmas, as quais realizam uma varredura nas máquinas adjacentes e prosseguem atacando. Estes casos foram observados no resultado final.

Vale ressaltar que cada máquina alvo irá se encontrar em sua própria varredura, durante os testes foi possível verificar que não há problemas de conflito na cópia do arquivo (i.e. a transferência dos binários quando uma máquina ataca a si mesma não afeta o processo do worm em execução) e que este fato ajuda a máquina a continuar varrendo e espalhando o worm para eventuais máquinas que surgirem na rede.

4. CONCLUSÃO

Pôde-se concluir que o worm conclui seu objetivo. Eventualmente foram pensados em criar um pseudo servidor HTTP e utilizar na máquina alvo um comando para baixar os binários do worm (wget ou curl), porém a parte prática não foi realizada. Diversas outras técnicas foram pensadas mas acabaram por não serem implementadas devido à inviabilidade ou apenas por falta de necessidade.

5. REFERÊNCIAS

[1] https://www.exploit-db.com/exploits/348/