Web Application Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

HTTP Method Testing with Nmap, Metasploit

Metasploit – scanner/http/options

```
msf> use auxiliary/scanner/http/options
msf auxiliary(options) >
msf auxiliary(options) > show options

Module options (auxiliary/scanner/http/options):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        Use a proxy chain
   RHOSTS   192.168.1.11     yes       The target address range o
   RPORT    80               yes       The target port
   THREADS  1                yes       The number of concurrent t
   VHOST                     no        HTTP server virtual host

msf auxiliary(options) > run

[*] 192.168.1.11 allows POST,OPTIONS,GET,HEAD methods
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(options) >
msf auxiliary(options) >
```

Nmap: http-methods.nse

```
PentesterAcademy# nmap --script=http-methods.nse 192.168.1.11 -n -p 80

Starting Nmap 6.25 ( http://nmap.org ) at 2013-09-02 07:26 EDT
Nmap scan report for 192.168.1.11
Host is up (0.00046s latency).
PORT   STATE SERVICE
80/tcp open  http
|_http-methods: POST OPTIONS GET HEAD

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
PentesterAcademy#
PentesterAcademy#
PentesterAcademy# nmap --script=http-methods.nse --script-args=http-methods.retest=1 192.168.1.11 -n -p 80

Starting Nmap 6.25 ( http://nmap.org ) at 2013-09-02 07:27 EDT
Nmap scan report for 192.168.1.11
Host is up (0.0033s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-methods: POST OPTIONS GET HEAD
| POST / -> HTTP/1.1 200 OK
|
| OPTIONS / -> HTTP/1.1 200 OK
|
| GET / -> HTTP/1.1 200 OK
|
|_HEAD / -> HTTP/1.1 200 OK

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
PentesterAcademy#
```

Verb Tampering

```
msf> use auxiliary/scanner/http/verb_auth_bypass
msf auxiliary(verb_auth_bypass) >
msf auxiliary(verb_auth_bypass) > show options

Module options (auxiliary/scanner/http/verb_auth_bypass):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   PATH     /                yes       The path to test
   Proxies                   no        Use a proxy chain
   RHOSTS                    yes       The target address range
   RPORT    80               yes       The target port
   THREADS  1                yes       The number of concurrent
   VHOST                     no        HTTP server virtual host

msf auxiliary(verb_auth_bypass) >
```

```
nmap --script=http-method-tamper.nse  192.168.1.11 -n -p 80
```