a11y.text tomcat_administration The tomcat_administration module scans a range of IP addresses and locates the Tomcat Server administration panel and version. msf > use auxiliary/admin/http/tomcat_administration

msf auxiliary(tomcat_administration) > show options

Module options (auxiliary/admin/http/tomcat_administration):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target address range or CIDR identifier
RPORT	8180	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
THREADS	1	yes	The number of concurrent threads
TOMCAT_PASS		no	The password for the specified username
TOMCAT_USER		no	The username to authenticate as
VHOST		no	HTTP server virtual host

To configure the module, we set the RHOSTS and THREADS values and let it run against the default port. msf auxiliary(tomcat_administration) > set RHOSTS 192.168.1.200-210
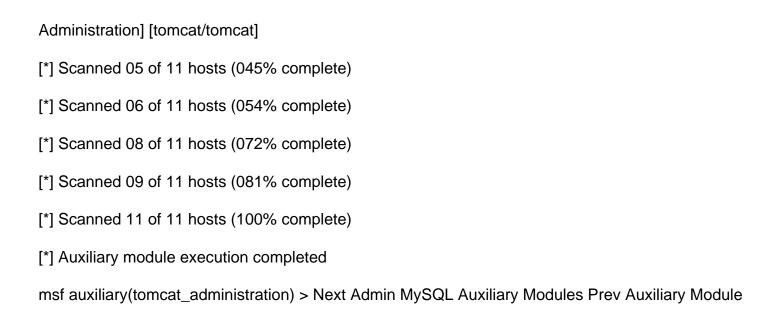
RHOSTS => 192.168.1.200-210

msf auxiliary(tomcat_administration) > set THREADS 11

THREADS => 11

msf auxiliary(tomcat_administration) > run

[*] http://192.168.1.200:8180/admin [Apache-Coyote/1.1] [Apache Tomcat/5.5] [Tomcat Server

Administration] [tomcat/tomcat]

[*] Scanned 05 of 11 hosts (045% complete)

[*] Scanned 06 of 11 hosts (054% complete)

[*] Scanned 08 of 11 hosts (072% complete)

[*] Scanned 09 of 11 hosts (081% complete)

[*] Scanned 11 of 11 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(tomcat_administration) > Next Admin MySQL Auxiliary Modules Prev Auxiliary Module

Reference