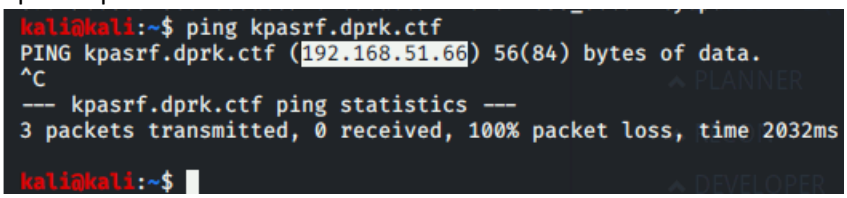
Question

Intelligence suggests that the Kiringul People's Army Strategic Rocket Forces (KPASRF) is the group responsible for running the nuclear missile program. Perhaps we can find a way into their network by one of their Internet-facing websites?

What is the IP address of the KPASRF public website, kpasrf.dprk.ctf?

Ping kpasrf.dprk.ctf

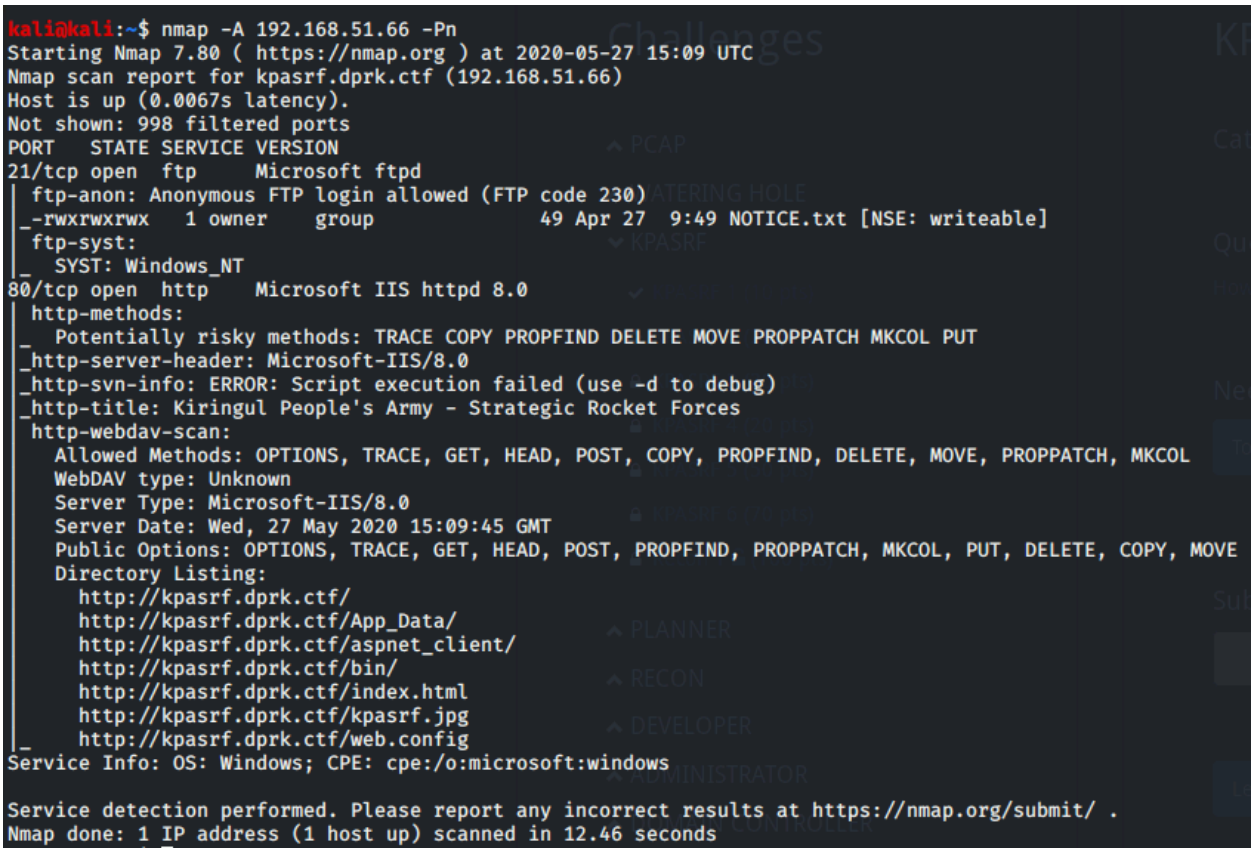


Flag: 192.168.51.66

Question

How many TCP ports are open on this IP address?

Nmap the ipaddress

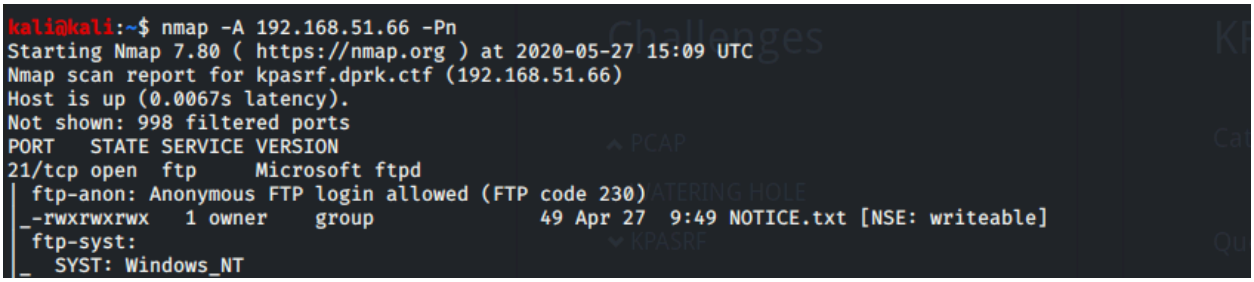


Flag: 2

Question

Enumerate the FTP service for vulnerabilities.

What is a valid username that can upload files to the server?

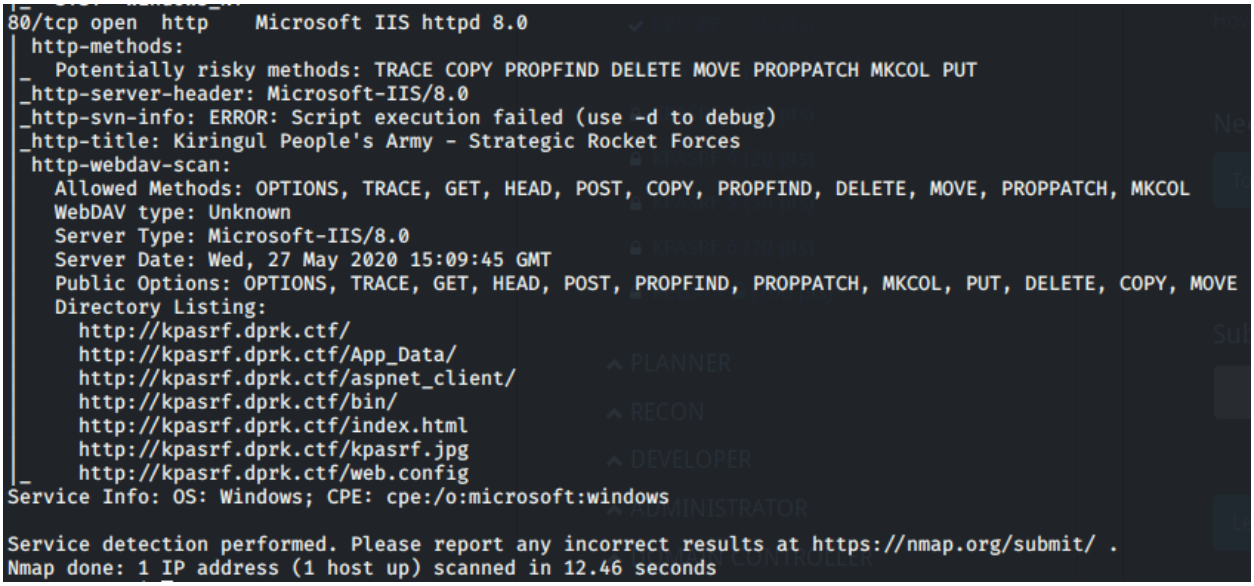


Flag: Anonymous

Question

Let's enumerate the web server for vulnerabilites.

What version of IIS is the web server running?



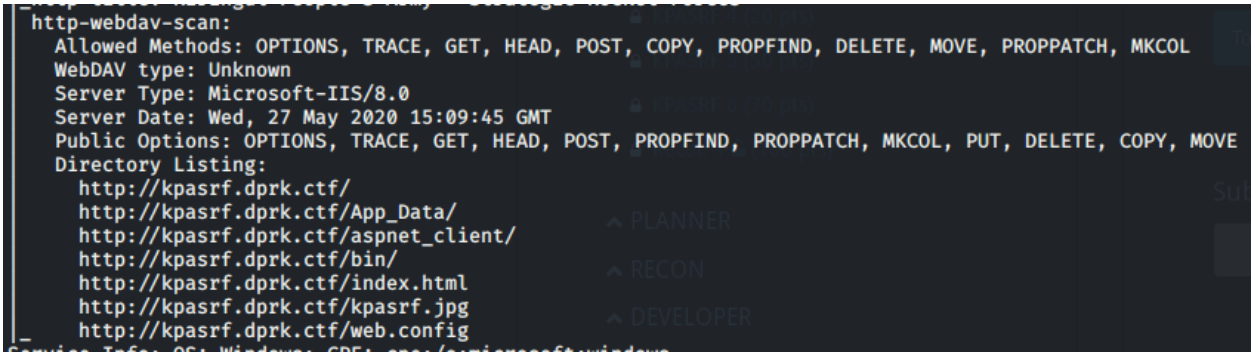
```
80/tcp open  http    Microsoft IIS httpd 8.0
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND DELETE MOVE PROPPATCH MKCOL PUT
|_http-server-header: Microsoft-IIS/8.0
|_http-svn-info: ERROR: Script execution failed (use -d to debug)
|_http-title: Kiringul People's Army - Strategic Rocket Forces
| http-webdav-scan:
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, POST, COPY, PROPFIND, DELETE, MOVE, PROPPATCH, MKCOL
|   WebDAV type: Unknown
|   Server Type: Microsoft-IIS/8.0
|   Server Date: Wed, 27 May 2020 15:09:45 GMT
|   Public Options: OPTIONS, TRACE, GET, HEAD, POST, PROPFIND, PROPPATCH, MKCOL, PUT, DELETE, COPY, MOVE
|   Directory Listing:
|     http://kpasrf.dprk.ctf/
|     http://kpasrf.dprk.ctf/App_Data/
|     http://kpasrf.dprk.ctf/aspnet_client/
|     http://kpasrf.dprk.ctf/bin/
|     http://kpasrf.dprk.ctf/index.html
|     http://kpasrf.dprk.ctf/kpasrf.jpg
|_    http://kpasrf.dprk.ctf/web.config
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.46 seconds
```

Flag: 8

Question

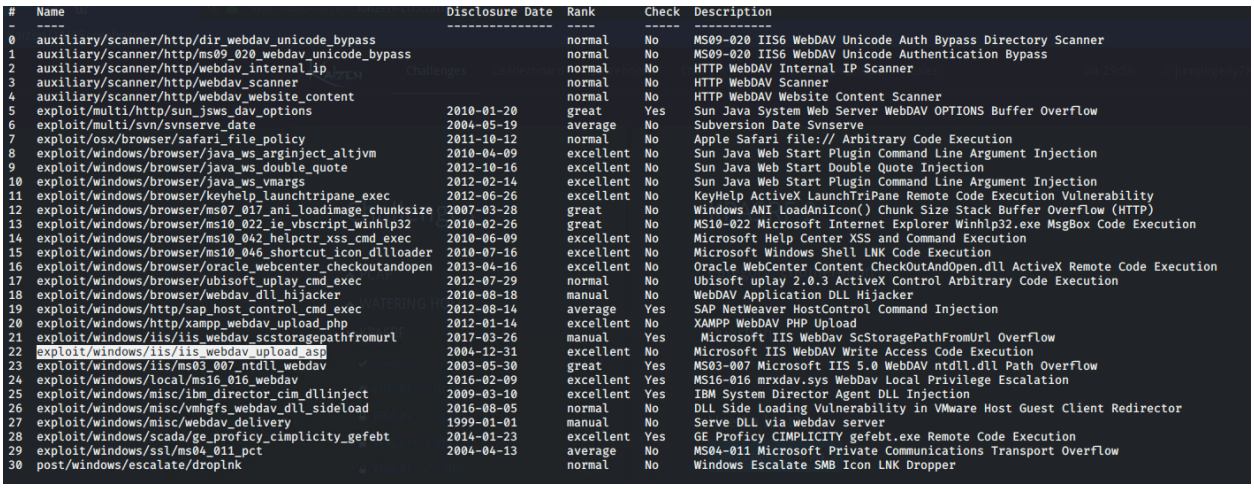
What administration module is enabled on this webserver, which could allow a remote user to upload or modify files?



Flag: webdav

Question

What is the name of a Metasploit module that could exploit one of the discovered flaws in this webserver?



#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/dir_webdav_unicode_bypass		normal	No	MS09-020 IIS6 WebDAV Unicode Auth Bypass Directory Scanner
1	auxiliary/scanner/http/ms09_020_webdav_unicode_bypass		normal	No	MS09-020 IIS6 WebDAV Unicode Authentication Bypass
2	auxiliary/scanner/http/webdav_internal_ip		normal	No	HTTP WebDAV Internal IP Scanner
3	auxiliary/scanner/http/webdav_scanner		normal	No	HTTP WebDAV Scanner
4	auxiliary/scanner/http/webdav_website_content		normal	No	HTTP WebDAV Website Content Scanner
5	exploit/multi/http/sun_jsws_dav_options	2010-01-20	great	Yes	Sun Java System Web Server WebDAV OPTIONS Buffer Overflow
6	exploit/multi/svn/svnserve_date	2004-05-19	average	No	Subversion Date Svnserve
7	exploit/osx/browser/safari_file_policy	2011-10-12	normal	No	Apple Safari file:// Arbitrary Code Execution
8	exploit/windows/browser/java_ws_arginject_altjvm	2010-04-09	excellent	No	Sun Java Web Start Plugin Command Line Argument Injection
9	exploit/windows/browser/java_ws_double_quote	2012-10-16	excellent	No	Sun Java Web Start Double Quote Injection
10	exploit/windows/browser/java_ws_vmargs	2012-02-14	excellent	No	Sun Java Web Start Plugin Command Line Argument Injection
11	exploit/windows/browser/keyhelp_launchtripane_exec	2012-06-26	excellent	No	KeyHelp ActiveX LaunchTriPane Remote Code Execution Vulnerability
12	exploit/windows/browser/ms07_017_ani_loadimage_chunksize	2007-03-28	great	No	Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (HTTP)
13	exploit/windows/browser/ms10_022_ie_vbscript_winhlp32	2010-02-26	great	No	MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution
14	exploit/windows/browser/ms10_042_helpctr_xss_cmd_exec	2010-06-09	excellent	No	Microsoft Help Center XSS and Command Execution
15	exploit/windows/browser/ms10_046_shortcut_icon_dllloader	2010-07-16	excellent	No	Microsoft Windows Shell LNK Code Execution
16	exploit/windows/browser/oracle_webcenter_checkoutandopen	2013-04-16	excellent	No	Oracle WebCenter Content CheckOutAndOpen.dll ActiveX Remote Code Execution
17	exploit/windows/browser/ubisoft_uplay_cmd_exec	2012-07-29	normal	No	Ubisoft uplay 2.0.3 ActiveX Control Arbitrary Code Execution
18	exploit/windows/browser/webdav_dll_hijacker	2010-08-18	manual	No	WebDAV Application DLL Hijacker
19	exploit/windows/http/sap_host_control_cmd_exec	2012-08-14	average	Yes	SAP NetWeaver HostControl Command Injection
20	exploit/windows/http/xampp_webdav_upload_php	2012-01-14	excellent	No	XAMPP WebDAV PHP Upload
21	exploit/windows/iis/iis_webdav_scstoragepathfromurl	2017-03-26	manual	Yes	Microsoft IIS WebDav ScStoragePathFromUrl Overflow
22	exploit/windows/iis/iis_webdav_upload_asp	2004-12-31	excellent	No	Microsoft IIS WebDAV Write Access Code Execution
23	exploit/windows/iis/ms03_007_ntdll_webdav	2003-05-30	great	Yes	MS03-007 Microsoft IIS 5.0 WebDAV ntdll.dll Path Overflow
24	exploit/windows/local/ms16_016_webdav	2016-02-09	excellent	Yes	MS16-016 mrxdav.sys WebDav Local Privilege Escalation
25	exploit/windows/misc/ibm_director_cim_dllinject	2009-03-10	excellent	Yes	IBM System Director Agent DLL Injection
26	exploit/windows/misc/vmhgfs_webdav_dll_sideload	2016-08-05	normal	No	DLL Side Loading Vulnerability in VMware Host Guest Client Redirector
27	exploit/windows/misc/webdav_delivery	1999-01-01	manual	No	Serve DLL via webdav server
28	exploit/windows/scada/ge_proficy_cimplicity_gefebt	2014-01-23	excellent	Yes	GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
29	exploit/windows/ssl/ms04_011_pct	2004-04-13	average	No	MS04-011 Microsoft Private Communications Transport Overflow
30	post/windows/escalate/droplnk		normal	No	Windows Escalate SMB Icon LNK Dropper

Flag: exploit/windows/iis/iis_webdav_upload_asp