Camping Without Any Tools

Living Off the Land with Native Binaries

By:
Dylan Makowski
What does “Living Off The Land” mean?

- Many times during engagements, you will find that you have a particular access, but not a robust toolkit

- During these situations, you need to use what you can in order to get either better access, or to pivot somewhere else

- Both *nix and Windows machines have their own sets of binaries that come shipped with them that have some alternate uses that can help out any operator
Windows Binaries

- Certutil.exe
- MpCmdRun.exe
- Rundll32.exe
- Regsvr32.exe
Unix Binaries

- Docker
- file
- Dmesg
- whois
Certutil.exe

• Legitimate Windows binary shipped with almost ever version of Windows

• Used for displaying certificate information and configuring Certificate Services

• This can also be used to download binaries from a remote source

• This can also be used encode and decode data to/from base64
MpCmdRun.exe

• Binary that is shipped with Windows Defender (heh!)
• This is normally used to manage certain settings within Defender
• This can be used to download files from a remote host
Rundll32.exe

• Just as it sounds, a native Windows binary that is used to execute dll files

• It can execute any dll on disk, signed or not (but be mindful of AV, this is a common technique used by toolsets such as MSF)

• Not only dll’s, this can also run arbitrary JS
Regsvr32.exe

- Another native binary that is used to register a dll that uses COM classes. It will create a registry entry for the CLSID’s (Class IDs) for the COM dll.

- This can be used to execute .sct scripts by utilizing the scripting library found within scrobj.dll

- Not only will this execute scripts, but these scripts will be able to open other binaries (i.e. calc.exe) and bypass any allowlists that are in place
docker

• The docker binary allows you to control docker containers within the host operating system (i.e. start, stop, pull images, etc)

• With such a robust binary, this is open to allow a lot of nifty things, such as breaking out of restrictive environments, read/write files, and if there are sudo privileges, the ability to drop into a root shell and access the host filesystem

• Note: not native, but more and more common
file

- Binary that is shipped with most Unix systems that will determine the filetype of any file
- Providing sudo access to this binary seems pretty benign, but there is a feature of file that allows you provide a list of file names to examine
- This option will attempt to read all the files within a file-list, but it will verbosey list out the contents of the file, even if there are not real files on disk
dmesg

• A binary shipped with most unix systems, used to read the system message buffer. Used to troubleshoot low level system issues such as hardware and firmware

• It is common for system administrators to have sudo access to this binary to help troubleshoot systems

• If you provide a particular parameter, it will drop you into a default pager (which is usually less), which then you can break out of into a shell
whois

• A common binary to help lookup domain records on an IP

• This is usually a pretty benign binary that queries IANA whois server for information, but can be used by attackers to exfil data out of a target network, or download files onto a target

• This is done by specifying a remote host you control as the whois server, and then using file data as the query data, which will send the contents to/from the target