

# Solaris

[+] Solaris vulnerabilities:

Solaris 7:

sadmind_exec	SADMIND -	weakness in default security settings - allows root - rootdown.pl
**ttyprompt	TELNET -	buffer overflow in solaris login - manual through telnet client
sendmail_exec	LPD -	line printer daemon buffer overflow - allows root
heap_noir	DTSPCD -	CDE common desktop environment heap overflow TCP port 6112, runs with root
ypupdated_exec	YPUPDATED -	weakness in handling of the command shell - allows root
kcms_readfile	kcms / ttdbserverd	remote file read (only in msf2)

Solaris 8:

sadmind_exec	SADMIND -	weakness in default security settings - allows root - rootdown.pl
**ttyprompt	TELNET -	buffer overflow in solaris login - manual through telnet client
sendmail_exec	LPD -	line printer daemon buffer overflow - allows root
heap_noir	DTSPCD -	CDE common desktop environment heap overflow TCP port 6112, runs with root
ypupdated_exec	YPUPDATED -	weakness in handling of the command shell - allows root.
no exploit - adm_build_path	SADMIND -	stack buffer overflow in adm_build_path() function.
kcms_readfile	kcms / ttdbserverd	remote file read (only in msf2)

solaris 9:

sadmind_exec	SADMIND -	weakness in default security settings - allows root - rootdown.pl
ypupdated_exec	YPUPDATED -	weakness in handling of the command shell - allows root.
sadmind_adm_build_path	SADMIND -	stack buffer overflow in adm_build_path() function.
kcms_readfile	kcms / ttdbserverd	remote file read (only in msf2)

Solaris 10:

fuser	TELNET -	authentication bypass through -f command - can be manually exploited
ypupdated_exec	YPUPDATED -	weakness in handling of the command shell - allows root.

Solaris 11:

fuser	TELNET -	authentication bypass through -f command - can be manually exploited
-------	----------	--

[+] Adding solaris user:

```
useradd -u 0 -o pentestuser
passwd -d pentestuser
```

[+] In addition, familiarise yourself with rpcinfo, nfsshell, showmount, 'mount -t nfs'.