



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

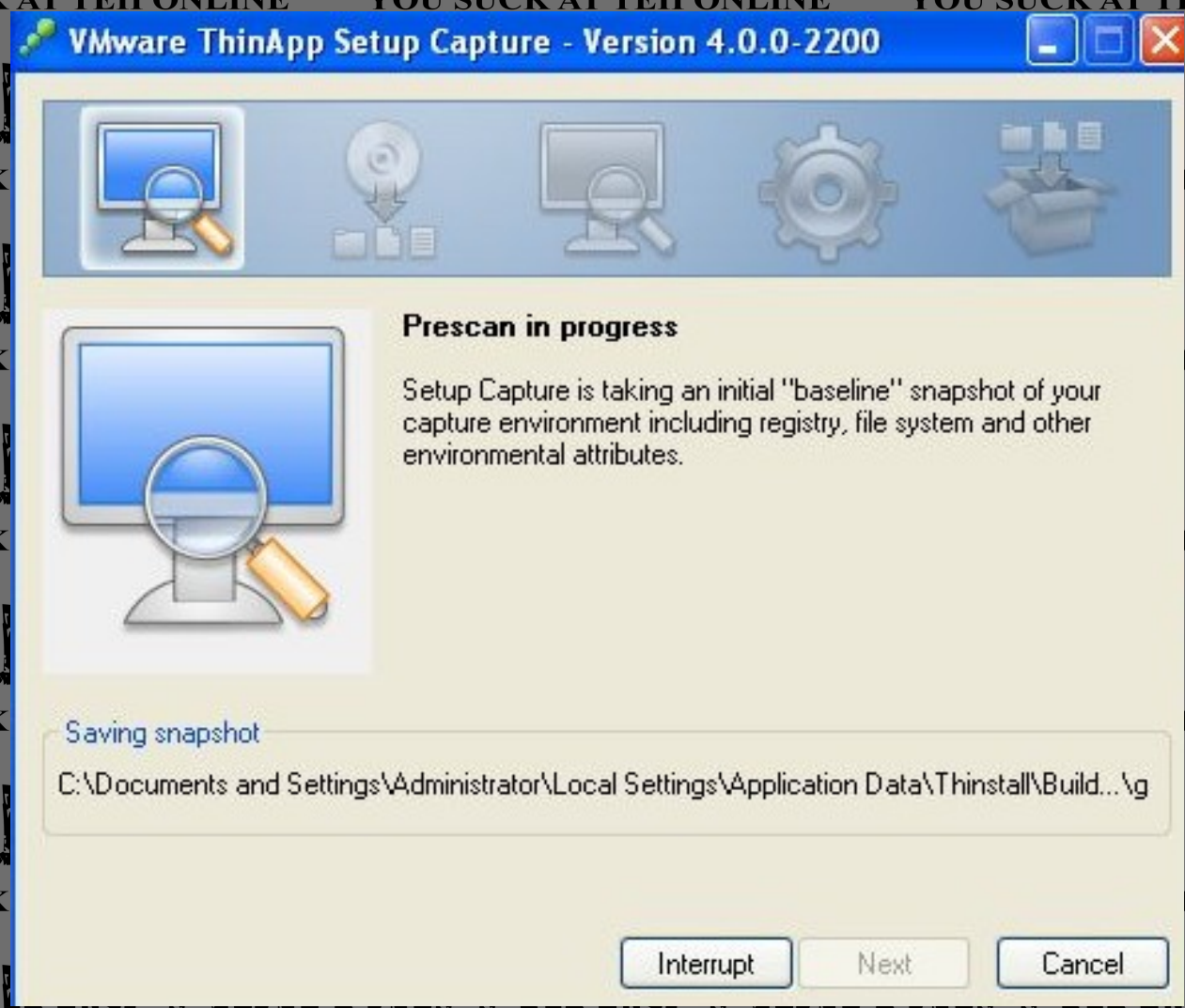
- REG SNIFF/PATCH

The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains various icons, with numbers 1 through 6 highlighting specific icons: 1 (Search), 2 (Filter), 3 (Tools), 4 (Options), 5 (Process Monitor), and 6 (File Manager). The main display area is a table with the following data:

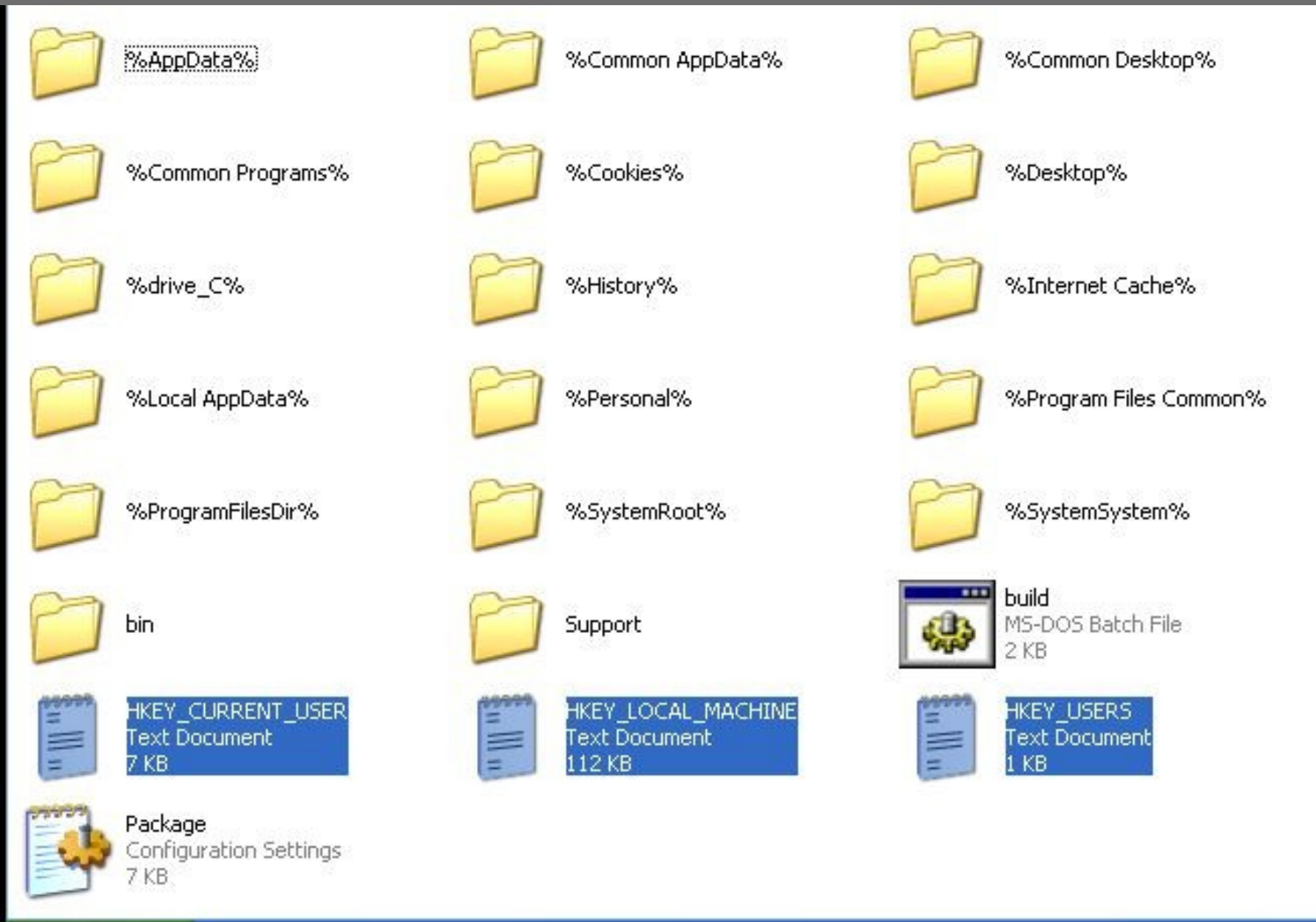
Seq...	Time ...	Process Name	PID	Operation	Path
12254	16:32:03...	svchost.exe	1008	RegCreateKey	HKLM\System\CurrentControlSet\Control
12259	16:32:03...	svchost.exe	1008	RegSetValue	HKLM\System\CurrentControlSet\Control

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
```

demo w3af

Wizards New Save Clear Pause Multiple Exploit Manual Request Fuzzy Request Encode/Decode Compare Proxy

Scan config Log Results Exploit

Vulnerabilities Information Error

[06/23/09 12:29:07] Cross Site Scripting was found at: "http://zero.webappsecurity.com/plink.asp", using HTTP [06/23/09 12:29:07] Cross Site Scripting was found at: "http://zero.webappsecurity.com/plink.asp", using HTTP [06/23/09 12:29:07] Cross Site Scripting was found at: "http://zero.webappsecurity.com/plink.asp", using HTTP [06/23/09 12:29:07] Starting sqlj plugin execution. [06/23/09 12:29:08] A SQL error was found in the response supplied by the web application, the error is (only a id 849. [06/23/09 12:29:08] A SQL error was found in the response supplied by the web application, the error is (only a id 849. [06/23/09 12:29:11] SQL injection in a Microsoft SQL database was found at: "http://zero.webappsecurity.com/220&password=&graphicOption=standard". The modified parameter was "login". The vulnerability was found in the [06/23/09 12:29:11] An unidentified web application error was found at: "http://zero.webappsecurity.com/login1.a it to the w3af developers. The vulnerability was found in the request with id 50. [06/23/09 12:29:11] Finished scanning process.

Audit progress: 0.0 % - E Not run

Vulns

w3af - Web Attack and Audit Framework - Vulnerability Report

File Edit View History Bookmarks Tools Help

File:///C:/Documents and Settings/Us... w3af - Web Attack and Audit Fra...

w3af target URL's

URL

Type	Port	Issue
Vulnerability	tcp/80	Cross Site Scripting was found at The sent post-data was: "...txtN vulnerability affects ALL browsers
Vulnerability	tcp/80	Cross Site Scripting was found at POST. The sent post-data was:

demo.testfire.net

Foundstone SASS tools

OWASP WebGoat

OWASP SiteGenerator

testasp.acunetix.com

testphp.acunetix.com

testaspnet.acunetix.com

zero.webappsecurity.com

crackme.cenzic.com