



# Self Service Penetration Testing

Matthew Cook

<http://escarpment.net/>

# Introduction

**Matthew Cook**  
**Senior IT Security Specialist**

**Loughborough University**  
**Computing Services**

**<http://escarpment.net/>**

# Self Service Penetration Testing

- The Loughborough University Context
  - Penetration Testing
  - Available Tools
  - Methodology
  - Trial System
  - Conclusions
- 

# The Loughborough University Context

- Had no formal IT Security Staff until Autumn 2003
- Most services provided centrally
- Some local services provided on various platforms
- Default open policy with:  

```
wc -l firewall_rules  
1061 firewall_rules
```
- Limited NIDS implementation

# The Loughborough University Context...

- Providing secure installation documentation
- Providing best-practice guides
- Providing Operating system cook-books

Most commonly asked question:

Can you check if my machine is secure?

# Penetration Testing

- A method of evaluating the external security of a machine.
- Services are evaluated to identify weakness, flaws, vulnerabilities and the absence of patches.
- Checks are usually preformed without a local account from a network connected machine.
- More often called 'Security Assessment'

# Penetration Testing...

## External LAN Penetration Testing:

- Complete external viewpoint
- Evaluates the security of the entire site
- Supposed to act like a hacker, social engineering?
- Black or white-box testing
- Does not expose the problems of internal machine compromises

# Penetration Testing...

## Internal LAN Penetration Testing:

- Often taken as a white-box approach
- Identifying the security of hosts
- No protection from the firewall
- Identify Wireless points?
  - NetDisco with MAC Address lists
  - War Driving

# Available Tools

## Nessus:

- Open Source
- Nmap Port Scanner
- 2165 Current plug-ins
- Updates on a close to daily basis
- Modular and easily configured
- Huge number of clients and command line driven

# Available Tools...

## Retina:

- Payware
- Licenses Nmap port scanner
- Regular updates
- Scheduling
- Excellent reporting options

# Available Tools...

## ISS System Scanner

- Payware
- Regular updates
- System baseline creation
- Good reporting options
- Scriptable using TCL

# Available Tools...

## CANVAS:

- Payware
- >50 Exploits
- Multiple OS's
- Actual penetration testing
- No false positives
- Limited use



# Available Tools...

## GFiLANguard:

- Payware
- Regular updates
- Focuses heavily on Windows platform
- User, Groups, Share security
- Patch checking

# Available Tools...

## CORE Impact:

- Payware
- Updates to vulnerabilities and exploits
- Tries to exploit vulnerabilities
- Actual penetration testing
- Excellent report generation

# Methodology

To provide an answer to the question:  
Can you check if my machine is secure?

- Staff Time
- Diversion from critical work
- Constantly fire fighting
- Not the best use of resources

# Methodology...

- Decided to use Nessus for its scripting ability and native Linux/Unix based client.
- Decided to have a web based front end to enable users to provide machine details.
- Users can only scan the machine they initiate the connection from.
- Request a username/password from AD

# Methodology...

- Results from Nessus will be emailed to the user.
- A guide to interpreting the results will be produced.
- Modify the .desc files to provide more information.
- Update Nessus plug-ins via cron on a daily basis.
- Use more advanced tools across the network and on specific hosts.

# Trial System

## Hardware:

- DELL 2650
- Dual 3Ghz Processors
- 2Gb Ram
- Approx 300Gb RAID 5 array

A tad overkill, but future proof...

# Trial System...

- Fedora Core 2 (Tettnang)
- Kernel 2.6.6
- Updates via yum
- `exclude=kernel*` in `/etc/yum.conf`
- Apache 2.0.49
- Exim 4.34

# Trial System...

## Authentication:

- Mod\_IMAP or Mod\_auth for Apache
- PAM Kerberos link to Active Directory
- REMOTE\_ADDR checked
  - Loughborough Netblock
  - Not a web cache
- Only address a scan can be preformed against!

# Trial System...

## Collected Details:

- Username
  - Email address
  - Machines IP address
- 
- Possibility of building a database of requests and machine data?

# Trial System...

- Web based CGI creates a shell script and embeds the IP address from the headers and the email address collected from the form.
- Script saved into `/pentest/requests` directory.
- Cron moves contents into `/pentest/active` directory, sets permissions and executes a queue runner.
- Queue runner executes the scripts.

# Trial System...

- Scripts are named after the IP address of the machine that is to be scanned.
- Scripts contain five components:
  - Log intended actions
  - Pipe IP address to `/pentest/active/<ip>.txt`
  - Execute the command line Nessus
  - Mail the results from `/pentest/results/<ip>.txt`
  - Delete the script

# Trial System...

- Defaults are set on a Nessus server which is running on a port bound to loopback.

```
/usr/local/bin/nessus -q  
127.0.0.1 1241 <user>  
<password>  
/pentest/active/<ip>.txt  
/pentest/results/<ip>.txt
```

# Conclusions

- Worked really well
- Entirely script based (I'm not a programmer!)
- Requests for more human friendly results.
  - Parse results in Perl
  - Improve .desc files and feedback
- Expand tool set including DoS attacks and actual machine penetration attacks.

# Conclusions...

Is it really Penetration Testing?

Well no, not at the moment, but with all buzzwords it takes time to correct people? Hacker/Cracker?

Does it work, is it useful?

I stopped getting asked to check machines.

Users can proactively check their machines.

# Conclusions...

## Futures?

- Improved results
- Database of machines with periodic checking
- Automatic checks from Network based Tripwire
- Machine details provided for administrators; IP Address, MAC Address, DNS Name, WINS workstation, username, workgroup, dhcp details and last active network device/port.

# Conclusions...

Giving the users the tools...

- Nessus Accounts for IT Support Staff
- CD Based Linux Distros
  - Knoppix STD
  - Professional Hacker's Linux Assault Kit
- Actual exploits – Metasploit Project

# Conclusions...

- Should the project should be re-titled:  
Machine vulnerability testing?
- Actual Penetration Testing will be performed by IT Security staff.
- Education of users is paramount!



# Questions

<http://escarpment.net/>