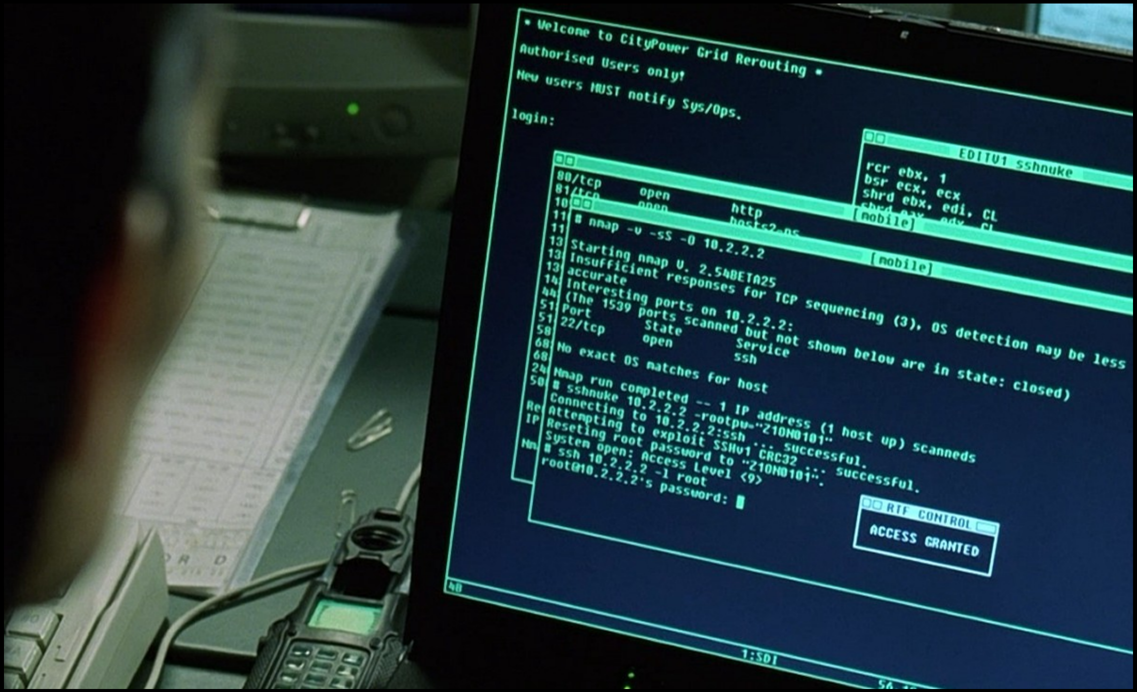
The Nmap Scripting Engine

Making Nmap work for you!



```
* Welcome to CityPower Grid Rerouting *
Authorised Users only!
New users MUST notify Sys/Ops.

login:
```

```
# nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection may be less
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z10N0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:
```

Who am I...?

DUNGEONS & DRAGONS

SHADOWRUN

dash 9 SECURITY

NMAP.ORG

GIAC CERTIFIED INCIDENT HANDLER GCIH

GIAC CERTIFIED PENETRATION TESTER GPEN

TENABLE Network Security®

My blog...

- SkullSecurity.org
  - Random research, rants, etc.
  - Nmap dev news
  - Password database
- I post updates to Twitter
  - https://twitter.com/iagox86

My job...

- Tenable Network Security
  - Makers of the Nessus vulnerability scanner
  - I do research, reverse engineering
  - Giving talks
  - Plugins:
    - ms10-070 remote
    - ms10-075 remote
    - Padding oracle checks
    - ActiveSync audit (not yet released)

My other job...

- Dash9Security.com
  - Vulnerability assessment
  - Penetration testing
  - Training
  - Etc.
- Local to Winnipeg, for now

Nmap script – intro

- Written in Lua
  - Awesome embedded language
- Come with Nmap
  - Look for files called '*.nse' and '*.lua'
  - /usr/local/share/nmap/scripts
  - /usr/share/nmap/scripts
  - c:\Program Files\Nmap
- Expand Nmap's capabilities
  - Extended version scanning, discovery, vulnerability checks, etc

Running scripts – Commandline

```
nmap --script=default 192.168.1.0/24

nmap --script=http-enum nmap.org

nmap --script=smb-enum-users
    --script-args=smbuser=ron,smbpass=123456
    192.168.1.2

nmap --script=safe www.skullsecurity.org

nmap --script=“(default or ftp-*) and not *http*”
    10.*.*.*
```

Expression can be arbitrarily complex Lua

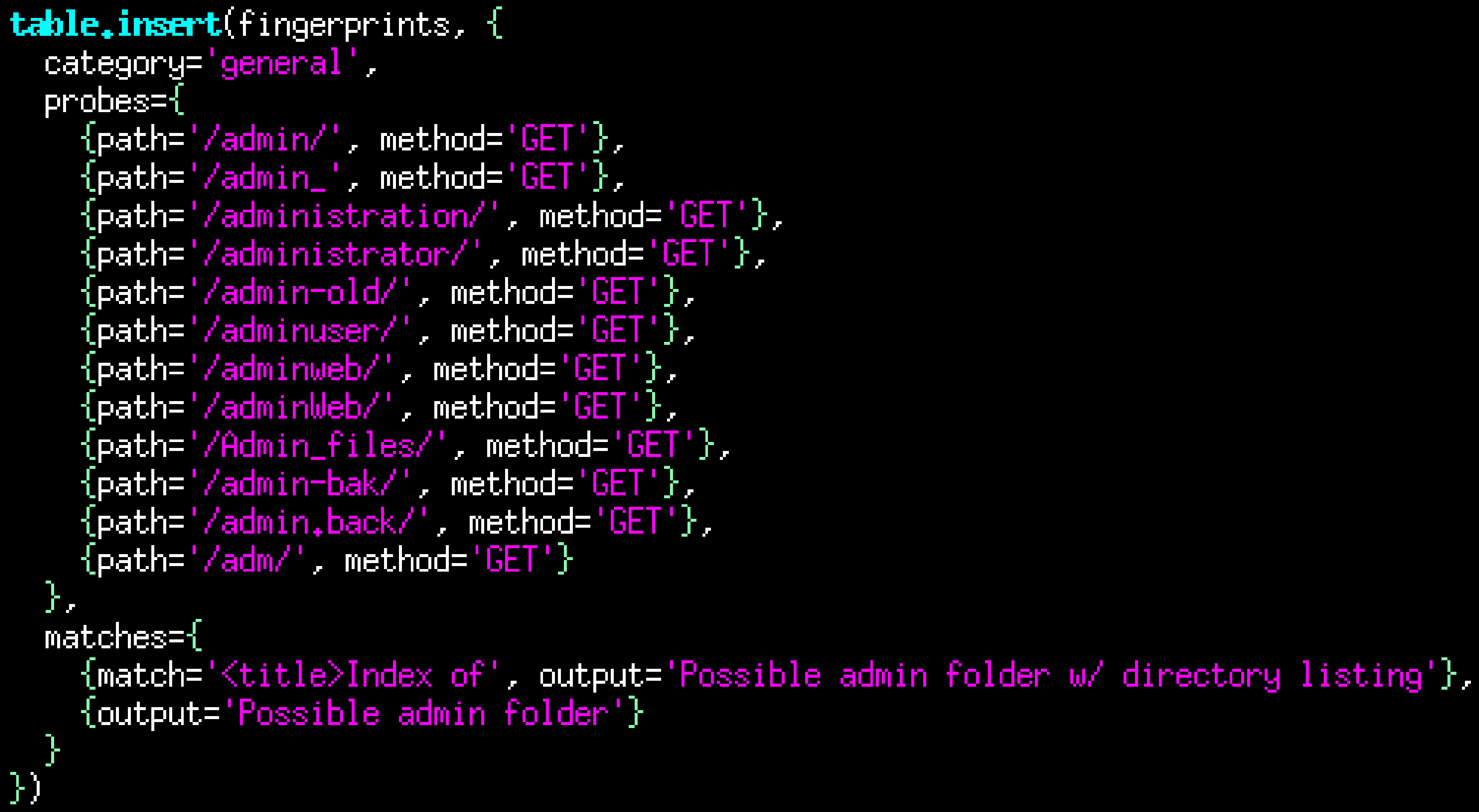
Nmap script – find them

- NSEDoc - http://nmap.org/nsedoc
- Use the Zenmap GUI
- Find them on the filesystem
- Use categories
  - --script=default
  - --script=intrusive
- DEMO!

New script: http-enum.nse

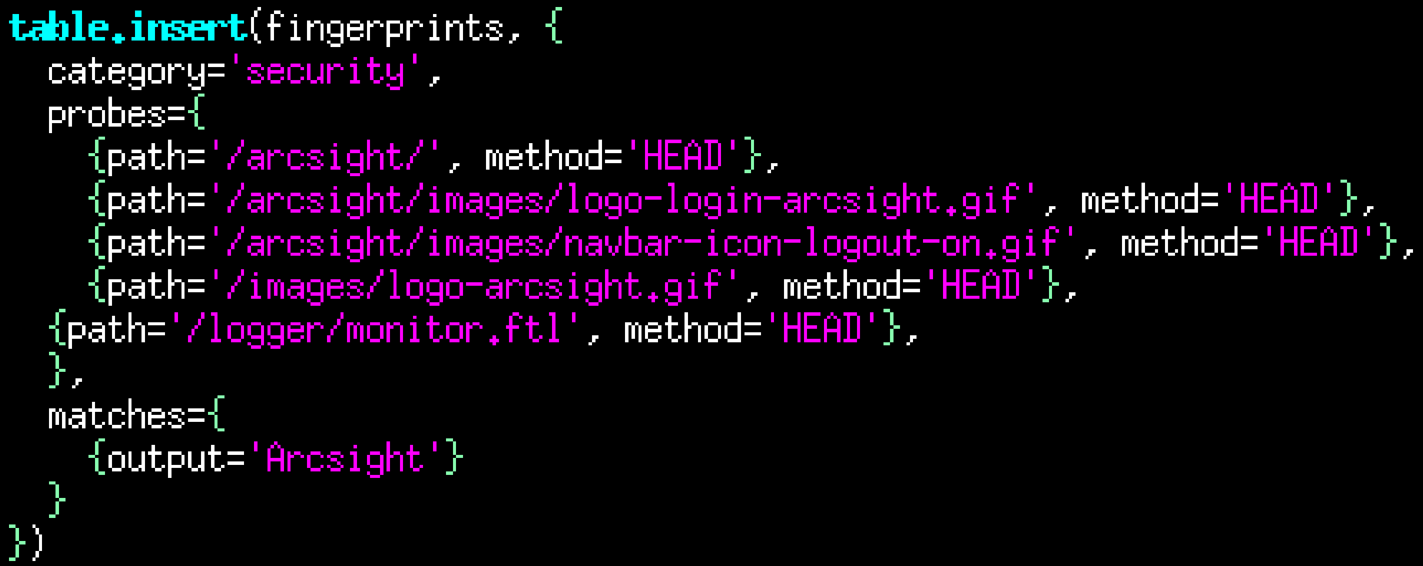
- Web application discovery, fingerprinting
- Powerful, lua-based format
  - nselib/data/http-fingerprints.lua
- Call to arms: we need fingerprints!
  - For more information: http://www.skullsecurity.org

http-enum – Example 1



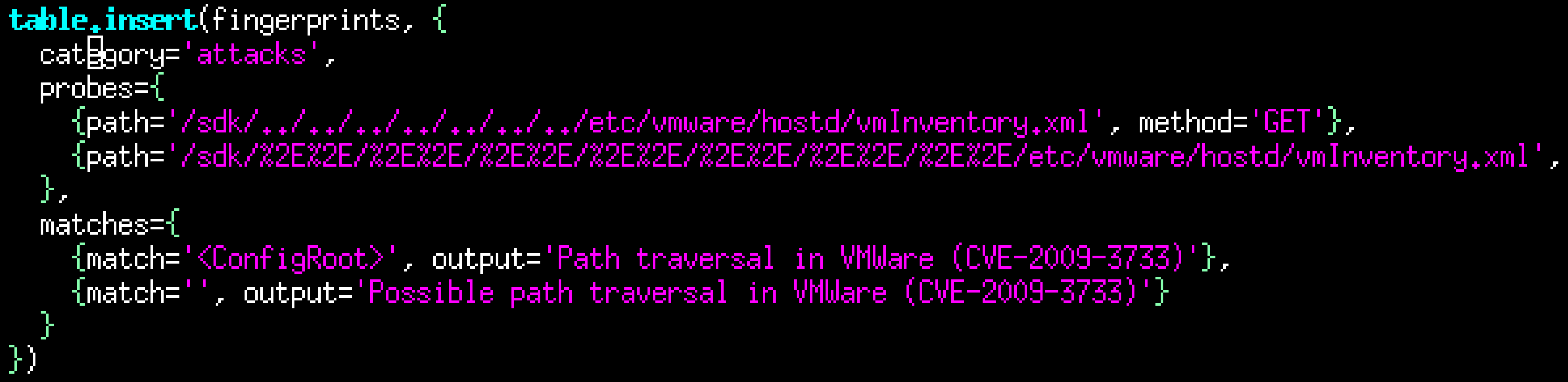
```
table.insert(fingerprints, {
  category='general',
  probes={
    {path='/admin/', method='GET'},
    {path='/admin_', method='GET'},
    {path='/administration/', method='GET'},
    {path='/administrator/', method='GET'},
    {path='/admin-old/', method='GET'},
    {path='/adminuser/', method='GET'},
    {path='/adminweb/', method='GET'},
    {path='/adminWeb/', method='GET'},
    {path='/Admin_files/', method='GET'},
    {path='/admin-bak/', method='GET'},
    {path='/admin.back/', method='GET'},
    {path='/adm/', method='GET'}
  },
  matches={
    {match='<title>Index of', output='Possible admin folder w/ directory listing'},
    {output='Possible admin folder'}
  }
})
```

http-enum – Example 2



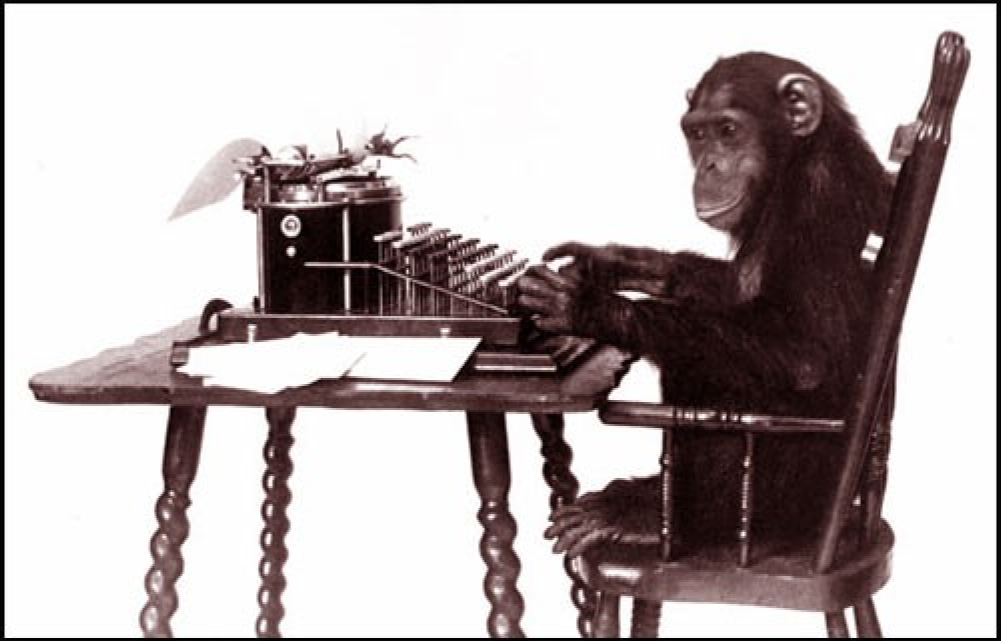
```
table.insert(fingerprints, {
  category='security',
  probes={
    {path='/arcsight/', method='HEAD'},
    {path='/arcsight/images/logo-login-arcsight.gif', method='HEAD'},
    {path='/arcsight/images/navbar-icon-logout-on.gif', method='HEAD'},
    {path='/images/logo-arcsight.gif', method='HEAD'},
  {path='/logger/monitor.ftl', method='HEAD'},
  },
  matches={
    {output='Arcsight'}
  }
})
```

http-enum – Example 3



```
table.insert(fingerprints, {
  category='attacks',
  probes={
    {path='/sdk/../../../../../../../etc/vmware/hostd/vmInventory.xml', method='GET'},
    {path='/sdk/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/etc/vmware/hostd/vmInventory.xml',
  },
  matches={
    {match='<ConfigRoot>', output='Path traversal in VMWare (CVE-2009-3733)'},
    {match='', output='Possible path traversal in VMWare (CVE-2009-3733)'}
  }
})
```

Writing scripts



Lua

- Scripting language
- Best known for World of Warcraft
- Easy to learn

Lua

```
local var = 3
if(var > 6) then
  io.write(“Something is weirdt\n”);
end

for i=1, 10, 1 do
  io.write(string.format(“The value is %d\n”, i))
end

function max(a, b)
  if(a > b) then
    return a
  else
    return b
  end
end
```

Every script needs...

- Some documentation
  - A description
  - One or more categories
- A 'rule' function
  - Always called; determines whether or not the script should execute
- An 'action' function
  - Run when the script executes

“rule” function

- Every script requires one or more rules:
  - portrule – runs for every matching port
  - hostrule – runs for every matching host
  - prerule – runs before the scan
  - postrule – runs after the scan

```
portrule = function(host, port)
 return (port.number > 1024 and host.ip ~= '127.0.0.1')
end
```

“shortport” Library

- Simplifies portrules

```
require 'shortport'

-- Run for every http server
portrule = shortport.http

-- Run for every server with port '22' or ssh
portrule = shortport.port_or_service(22, 'ssh')
```

“action()” function

- action() function
  - Every time one of the 'rule' functions returns true, the action() function is called.
  - Return value of action() is displayed to user
    - See stdnse.format_output()

Output...

- Plain string
  - Return the string from action(), done
- Table data: use 'tab' nselib:
  - http://nmap.org/nsedoc/lib/tab.html
- Structured data or error message: use stdnse.format_output()
  - http://nmap.org/nsedoc/lib/stdnse.html#format_output
- When in doubt, if it's more than one line, use stdnse.format_output(),

Arguments to scripts

- Getting arguments from users:
  - stdnse.get_script_args(...)
  - Takes any number of arguments, returns that many values (some may be nil if the user didn't set them)

```
local arg1, arg2 = stdnse.get_script_args(
  'script-name.arg1',
  'script-name.arg2')

-- Pick a default value for arg1 if it's not set
arg1 = arg1 or 'default_value'

-- Return an error if arg2 isn't set
if(not(arg2)) then
  return stdnse.format_output(false,
    “script-name.arg2 has to be set!”)
end
```

The Nmap registry

- Stores data between scripts/ports (not persistent)
  - `nmap.registry.data = 'This can be accessed by other scripts'`

```
-- script 1
local discovered_mac = smb.get_mac_address(host)
if(discovered_mac) then
  nmap.registry['mac_address'] = discovered_mac
End
```

```
-- script 2
local mac_address = nmap.registry['mac_address']
if(mac_address) then
  return “We already knew the mac: ” .. mac_address
end
```

sample-script.nse

- Written as a template
- Found on 'docs' folder of Nmap source
- Implements best practices
- All new scripts should be based on it

Where to get help...

- Read other scripts
- NSELib online documentation
  - http://nmap.org/nsedoc
- Mailing list
  - nmap-dev@insecure.org
- IRC channel
  - #nmap on irc.freenode.net
  - Be patient!

Testing

- Nmap has a 'random scan' feature
  - -iR
- Scan 100,000 hosts with your script:
  - nmap -iR 100000 --script=myscript.nse
- Legality is questionable
- My friend 'bob' does it all the time, has had great success

Submitting a script

- Make sure it's documented, bug free, useful, novel, etc.
- Make sure it works with latest svn version of Nmap
- Email it to nmap-dev@insecure.org
    - Fix any suggested changes
        - Repeat

Writing scripts demo!

- Demo!

Conclusion

- Hopefully you learned how to write Nmap scripts!
- Your mission:
  - Write an .nse script for your favourite service/attack/etc
  - Write an http fingerprint for http-enum.nse
  - Submit them to nmap-dev@insecure.org

Questions

- Ron Bowes
  - Email: ron@skullsecurity.net
  - Web/blog: http://www.skullsecurity.org
  - IRC: irc.freenode.net #skullsecurity
  - Or, I'm in town all week!