MANAGING
CYBER SECURITY
AS A BUSINESS RISK

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

Introduction to Penetration testing

CYBER SECURITY EVENT

netLabs!UG

Agenda

CYBER SECURITY EVENT

- The business case – Data Protection, where is it going ?
- Vulnerability scanning -vs- Penetration testing
- What exactly is Penetration testing ?
- The steps involved in carrying out a pen-test
- Kali GNU/Linux toolkit

Data Protection, where is it going

- General Data Protection Regulation (GDPR)
  - Control to citizens of their personal data
  - Simplify the regulatory environment for business
  - Data breach notification obligation within 72 hours
    - Sanctions
      - €20,000,000 (84,000,000,000 UGx)
      - 4% of the annual worldwide turnover
  - Right to erasure ("Right to be forgotten")
  - Data portability
  - Data protection by 'Design' and by 'Default'

Ref: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*

Data Protection, where is it going

CYBER SECURITY EVENT

- Data Protection and Privacy Bill, 2016
  - Principles of Data Protection
  - Data Collection and Processing
    - Consent, protection of privacy
  - Security of Data - breach notification to NITA-U
  - Rights of subjects
    - Access, prevent processing, etc..
  - Sanctions
    - Individuals: 4,800,000 UGx and/or 10 years prison
    - Corporations: All individuals involved

Ref: *Uganda Data Protection and Privacy bill 2016, First Reading, 20 Apr, 2016*

Data Protection, Recommendations

CYBER SECURITY EVENT

- Robust **Data Breach Incident Management Policy**
- **Pseudonymisation** of personal data
  - Separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately
- **Encryption** of data
- **Assess** applications and critical infrastructure for security vulnerabilities and the effectiveness of security controls
  - Vulnerability Testing
  - Penetration Testing
  - Control Testing

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

Vulnerability scanning
- vs -
Penetration testing

CYBER SECURITY EVENT

netLabs!UG

Vulnerability Scan

CYBER SECURITY EVENT

- **Objective**: The process includes identification, ranking and reporting of vulnerabilities that may compromise the system.
- **Plan the scan**: Recommended quarterly scans or after any significant changes have been made to the system.
- **Duration**: Vulnerability scans take a short period of time; typically scanning can be completed within a day.
- **Functionality**: An automated scan which produces a report which is then analysed by a data security firm.
- **Reports**: Vulnerabilities are typically ranked in accordance with the CVSSv3.

Ref: *PCI Data Security Standard (PCI DSS)*

Penetration Testing

CYBER SECURITY EVENT

- **Objective**: To discover and exploit exposures within the network (internal or external) in order to gain access to sensitive information or resources.
- **Plan the scan**: It is recommended that pen-test are conducted annually or after any significant changes made to the system.
- **Duration**: Pen-testing takes more time, and differs depending on the nature of the testing, the size, and the complexity of the environment.
- **Functionality**: Manual test process which includes reconnaissance, discovery and exploitation phases. The output delivers a comprehensive report.

REF: *PCI Data Security Standard (PCI DSS)*

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

The Penetration test (pen-test)

CYBER SECURITY EVENT

netLabs!UG

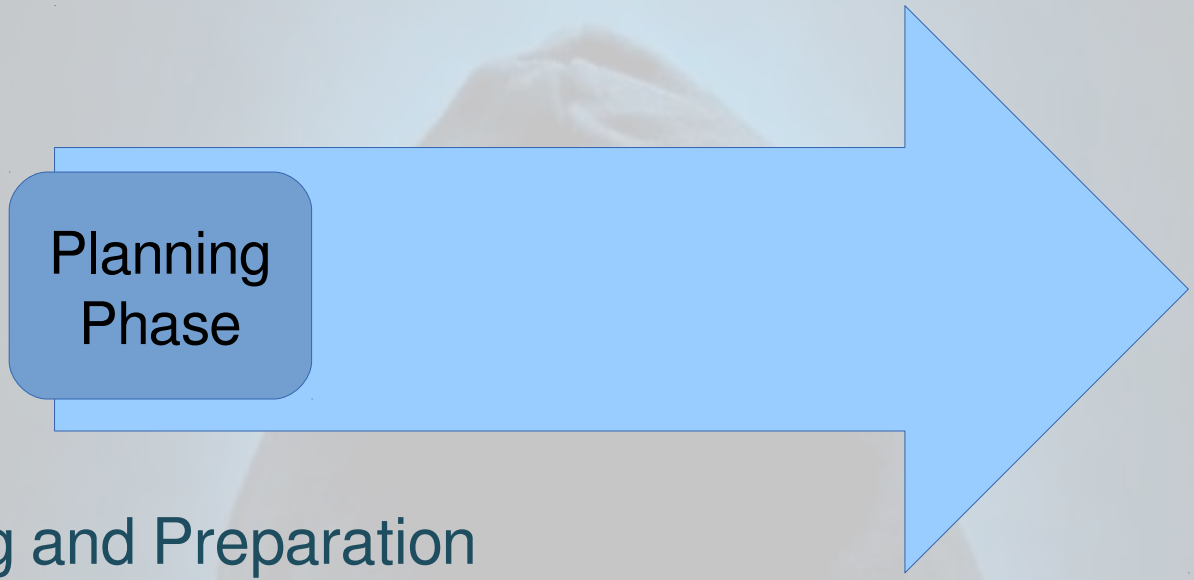
What is Penetration testing

CYBER SECURITY EVENT

- Pen-testing should be:
  - Proactive
  - Authorised
  - Evaluation of IT infrastructure
  - Safely attempting to exploit system
    - Expose vulnerabilities
    - Improper configurations
    - Risky end-user behaviour

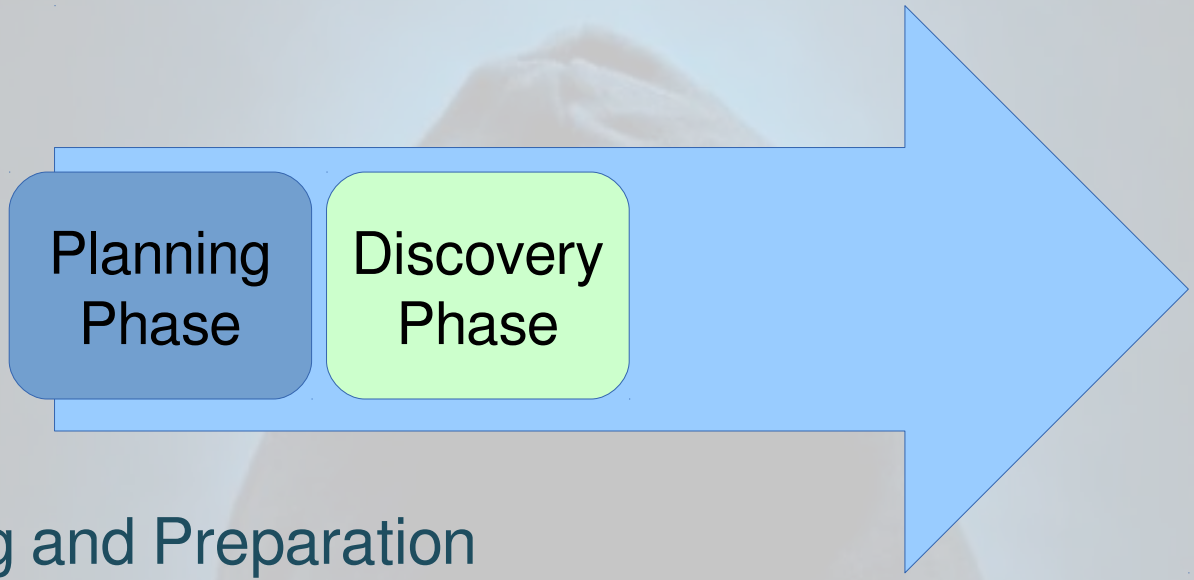
What steps are used to carry out a pen-test

CYBER SECURITY EVENT



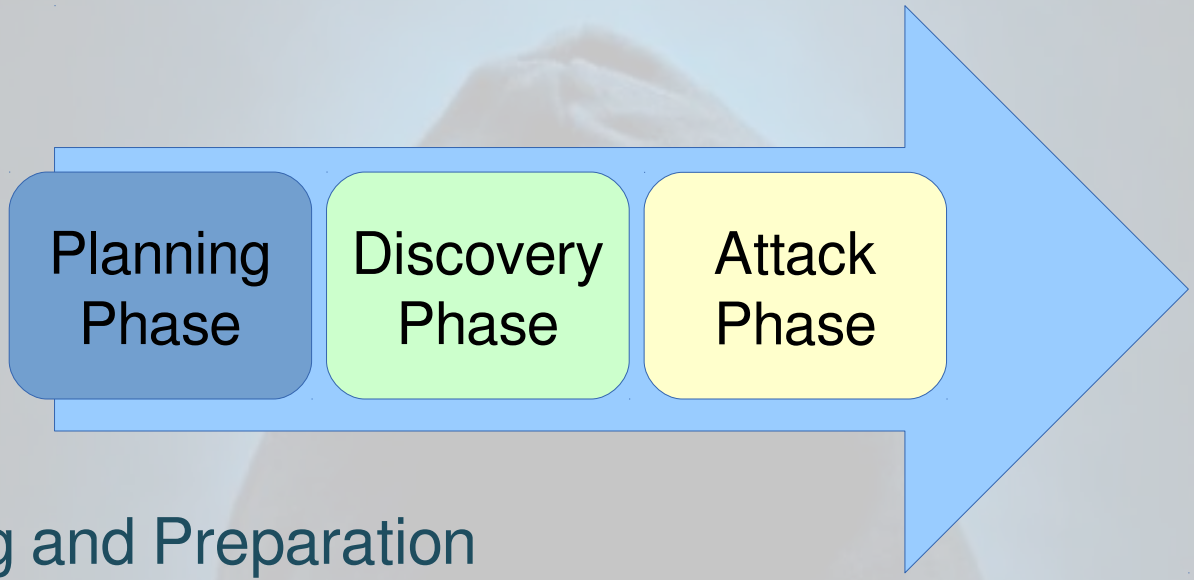
- Planning and Preparation

What steps are used to carry out a pen-test



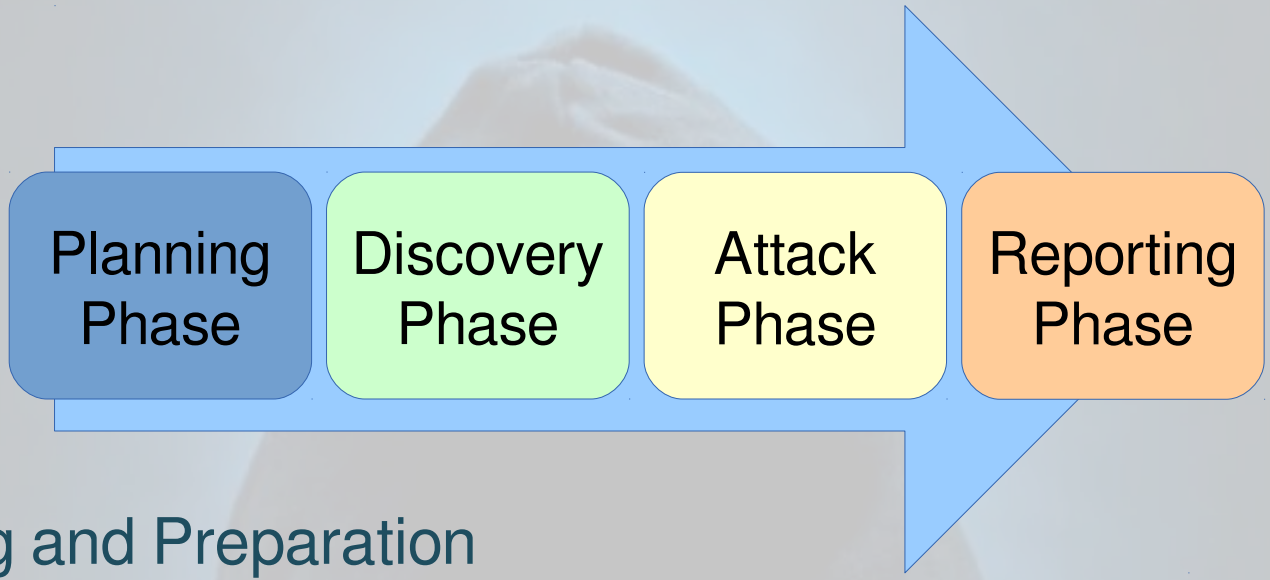
- Planning and Preparation
- Information Gathering and Analysis
- Vulnerability Detection

What steps are used to carry out a pen-test



- Planning and Preparation
- Information Gathering and Analysis
- Vulnerability Detection
- Penetration attempt

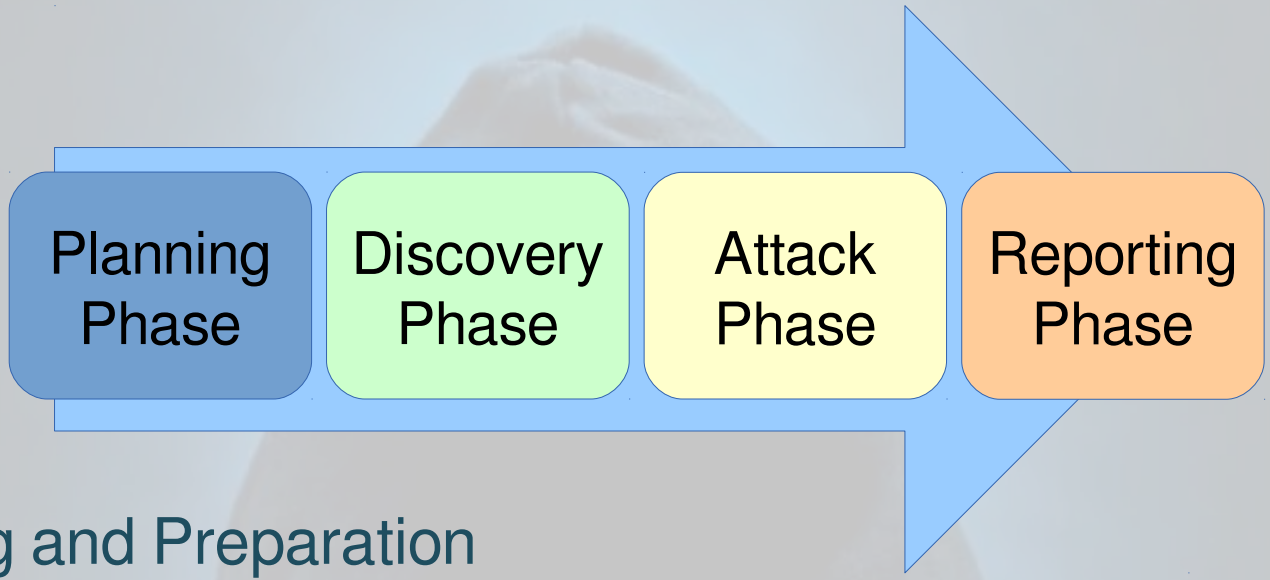
What steps are used to carry out a pen-test



- Planning and Preparation
- Information Gathering and Analysis
- Vulnerability Detection
- Penetration attempt
- Analysis and Reporting

What steps are used to carry out a pen-test

CYBER SECURITY EVENT



- Planning and Preparation
- Information Gathering and Analysis
- Vulnerability Detection
- Penetration attempt
- Analysis and Reporting
- Cleaning up

Planning and Preparation

CYBER SECURITY EVENT

- **Kick-off meeting**
  - Clear objective for pen-test
  - Timing and duration allowed for the pen-tests
  - Personnel involved
  - Are staff being informed of the tests?
  - Network and computers involved
  - Operational requirements during the pen-test
  - How the results are to be presented

Planning and Preparation

CYBER SECURITY EVENT

- **Pen-test Plan**
  - Detailed plan
  - Confidentiality Statement
  - Acceptance Sign-off Sheet

AMI Penetration Test Plan

Version 1.0

Primary Author:
Justin Searle, Utilisec

Contributers:
Galen Rasche, EPRI
Andrew Wright, N-Dimension Solutions
Scott Dinnage, N-Dimension Solutions

Reviewers:
NESCOR Team 3 Members and Volunteers
Annabelle Lee, EPRI

Introduction

This security test plan template was created by the National Electric Sector Cybersecurity Organization Resource (NESCOR) to provide guidance to electric utilities on how to perform penetration tests on AMI systems. Penetration testing is one of the many different types of assessments utilities can perform to assess their overall security posture. While NESCOR recommends that utilities engage in all other forms of security assessment, NESCOR created this document to help utilities plan and organize their AMI penetration testing efforts. For a list of other types of Smart Grid security assessments, please see NESCOR's whitepaper titled "Guide to Smart Grid Assessments." For a list of other NESCOR Penetration Test Plan documents that cover other systems such as Wide-Area Monitoring, Protection, and Control (WAMPAC), Home Area Network (HAN), or Distribution Management, please see NESCOR's website or contact one of the persons listed above.

The objective of the NESCOR project is to establish an organization that has the knowledge and capacity to enhance the effort of the National Electric Sector Cybersecurity Organization (NESCO) by providing technical assessments of power system and cybersecurity standards to meet power system security requirements; provide recommendations for threats and vulnerabilities; and participate in testing emerging security technologies in labs and pilot projects.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NESCOR, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

1

Pen-test example headings

- **Getting Started**
  - Pre-testing Checklist
  - Documentation Review
  - Authentication Tests
  - Concurrent Sessions
- **Encrypted Login**
  - POST
  - Time Out
  - Password Change Processes
  - Password Autocomplete
  - Locked on Failed Attempts
  - Session Management
- **Insecure Cookies**
  - Session Fixation
  - File Upload Security
- **Virus upload test**
  - Executable Test
  - Bypass Client-side Authentication test
  - Web Directory Test
  - Including Dangerous Objects Tests
- **Developer Comments**
  - Third-party Libraries
  - Unlicensed Code
  - High Value Directories
  - Testing for Back-up Files.
- **Testing Your SSL**
  - GlobalSign

Ref: *NIST (2015). SP 800-115: Technical Guide to Information Security Testing and Assessment.*
NIST (2014). SP 800-53A Revision 4: Building Effective Assessment Plans.
NESCOR (2012). AMI Penetration Test Plan Security test plan template.
PCI DSS (2012). Penetration Testing Guidance.

Information gathering and analysis

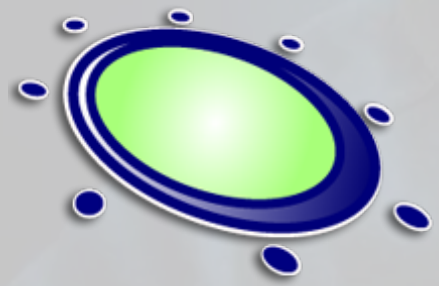
CYBER SECURITY EVENT

- Gathering of as much information as possible as a reconnaissance is essential.
  - What does the network look like?
  - What devices are on the network?
  - Who works at the company?
  - What does the organogram of the company look like?

Vulnerability detection

CYBER SECURITY EVENT

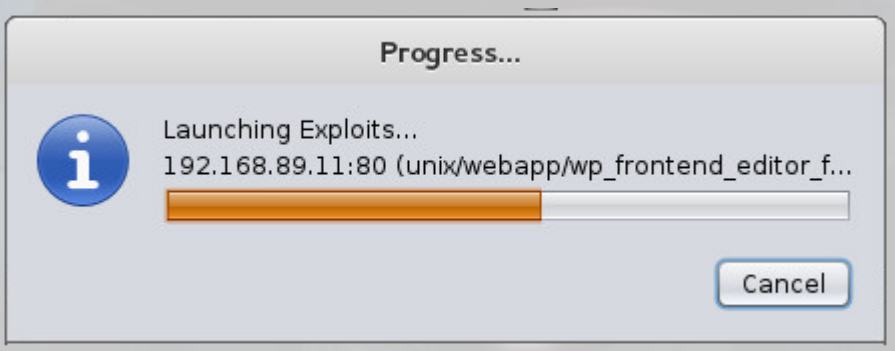
- Once a picture of the target organisation has been compiled a scan of vulnerabilities is the next step:
  - fierce
  - nmap/Zenmap
  - OpenVAS
  - Metasploit/Armitage
  - OWASP ZAP



Penetration attempt

CYBER SECURITY EVENT

- Identifying the best targets from the machines showing vulnerability is important particularly if the time given is short.
- IT personnel nomenclature to use functional names like MAILSVR or FTPSERVER etc…
- Define the list of machines that are to be given special additional treatment.
- Try password cracking tools, dictionary, brute force and hybrid attacks.



Analysis and Reporting

CYBER SECURITY EVENT

- A detailed report must be furnished to the client at the conclusion of the tests. It should include:
  - A summary of successful pen-tests.
  - A list of all information gathered during the pen-test.
  - A complete list and description of vulnerabilities found.
  - A suggested list of next steps to close the vulnerabilities and increase security at the client company.

RESTRICTED PENETRATION TEST REPORT

Vulnerability Details

External DNS Server Allows Zone Transfer

Impact	Risk	Likelihood	Fix Effort
Medium	Medium	High	Low

Summary of Problem:

A DNS server responsible for the example.com domain responds to DNS zone transfer requests from any source. This allows an attacker to enumerate all example.com subdomains and their IP addresses.

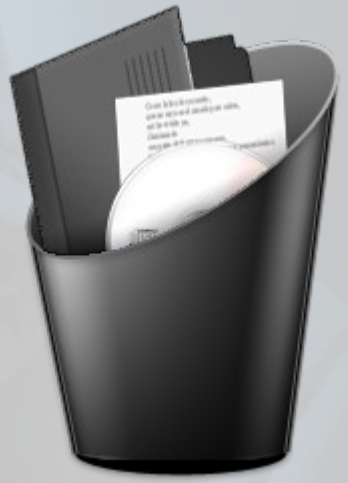
Affected Asset(s):

ns1. example.com

Tidy up

CYBER SECURITY EVENT

- During the pen-testing a detailed list of steps taken should be maintained.
- Pen-testers work with the client staff ensure that the steps have not left any residual issues:
  - entries in configuration files
  - new users
  - groups
  - etc...



CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

KALI™ GNU/Linux

CYBER SECURITY EVENT

netLabs!UG

Kali GNU/Linux

- The GNU/Linux operating system includes a vast array of tools for each step of the pen-testing activity.
- Derived from Debian GNU/Linux, distribution specifically designed for digital forensics and penetration testing.
- It is maintained and funded by Offensive Security Ltd.
- Pre-installed with over 600 penetration-testing programs.

Ref: *Kali GNU/Linux distribution. Offensive Security [online]. Available: https://www.kali.org*

File Machine View Input Devices Help

Applications Places Wed 16:35 1

Information Gathering and Analysis

- DNS tools discover non-contiguous IP space and host-names
- Scan the IP space with **nmap** or **zenmap** to discover services

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# nmap -Pn 192.168.89.1
  Starting Nmap 6.40 (http://nmap.org)
  at 2015-11-03 11:41 EAT
  Nmap scan report for 192.168.89.1
  Host is up (0.00086s latency).
  Not shown: 65530 closed ports
  PORT      STATE SERVICE
  21/tcp    open  ftp
  22/tcp    open  ssh
  23/tcp    open  telnet
  80/tcp    open  http
  2000/tcp  open  cisco-sccp
  8291/tcp  open  unknown

  Nmap done: 1 IP address (1 host up)
  scanned in 6.00 seconds
```

Scan Tools Profile Help

Target: 192.168.89.1 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.89.1

Hosts Services

OS Host

192.168.89.1

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 192.168.89.1 Details

```
Starting Nmap 6.40 ( http://nmap.org ) at 2015-11-03 11:48
EAT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 11:48
Scanning 192.168.89.1 [1 port]
Completed ARP Ping Scan at 11:48, 0.22s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 11:48
Completed Parallel DNS resolution of 1 host. at 11:48,
0.00s elapsed
Initiating SYN Stealth Scan at 11:48
Scanning 192.168.89.1 [1000 ports]
Discovered open port 80/tcp on 192.168.89.1
Discovered open port 22/tcp on 192.168.89.1
Discovered open port 21/tcp on 192.168.89.1
Discovered open port 23/tcp on 192.168.89.1
Discovered open port 2000/tcp on 192.168.89.1
Discovered open port 8291/tcp on 192.168.89.1
Completed SYN Stealth Scan at 11:48, 1.42s elapsed (1000
total ports)
Initiating Service scan at 11:48
Scanning 6 services on 192.168.89.1
Completed Service scan at 11:50, 131.10s elapsed (6
services on 1 host)
Initiating OS detection (try #1) against 192.168.89.1
NSE: Script scanning 192.168.89.1.
Initiating NSE at 11:50
```

Ref: *Nmap: the Network Mapper - Free Security Scanner [online]. Available: https://nmap.org.*
Zenmap - Official cross-platform Nmap Security Scanner GUI [online]. Available: https://nmap.org/zenmap/.

Right Ctrl

Vulnerability detection and penetration

- Many penetration tools available:

File Machine View Input Devices Help

Applications Places Wed 16:35

OpenVAS Webclient

Report: Results 1 - 14 of 14 (total: 14) PDF 52 %

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qod=70 l

Vulnerability	Severity	QoD	Host	Location	Actions
OS fingerprinting	0.0 (Log)	70%	192.168.89.1	general/tcp	
FTP Banner Detection	0.0 (Log)	80%	192.168.89.1	21/tcp	
Services	0.0 (Log)	75%	192.168.89.1	21/tcp	
SSH Protocol Versions Supported	0.0 (Log)	95%	192.168.89.1	22/tcp	
SSH Server type and version	0.0 (Log)	80%	192.168.89.1	22/tcp	
Services	0.0 (Log)	75%	192.168.89.1	22/tcp	
Detect Server type and version via Telnet	0.0 (Log)	80%	192.168.89.1	23/tcp	
Services	0.0 (Log)	75%	192.168.89.1	23/tcp	
Services	0.0 (Log)	75%	192.168.89.1	80/tcp	
Web mirroring	0.0 (Log)	80%	192.168.89.1	80/tcp	
Directories used for CGI Scanning	0.0 (Log)	75%	192.168.89.1	80/tcp	
wapiti (NASL wrapper)	0.0 (Log)	75%	192.168.89.1	80/tcp	
Check for Telnet Server	0.0 (Log)	80%	192.168.89.1	2000/tcp	
Detect Server type and version via Telnet	0.0 (Log)	80%	192.168.89.1	2000/tcp	

(Applied filter:sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qod=70 levels=hmlg autofp=0 notes=1 overrides=1 first=1 rows=100 delta_states=gn) 1 - 14 of 14 (total: 14)

Ref: *OpenVAS - Open Source vulnerability scanner and manager [online]. Available: http://www.openvas.org/.*

Right Ctrl

File Machine View Input Devices Help

Applications Places Wed 16:35 1

OpenVAS Webclient

Result Details

Task: Immediate scan of IP 192.168.89.1

ID: 64cec0e9-ef7e-4b95-b1d9-3ff113f22676

Vulnerability		Severity	QoD	Host	Location	Actions
Services		0.0 (Log)	75%	192.168.89.1	23/tcp	

Summary

This plugin attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 and set the results in the plugins knowledge base.

Vulnerability Detection Result

```
A telnet server seems to be running on this port
```

Log Method

Details: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

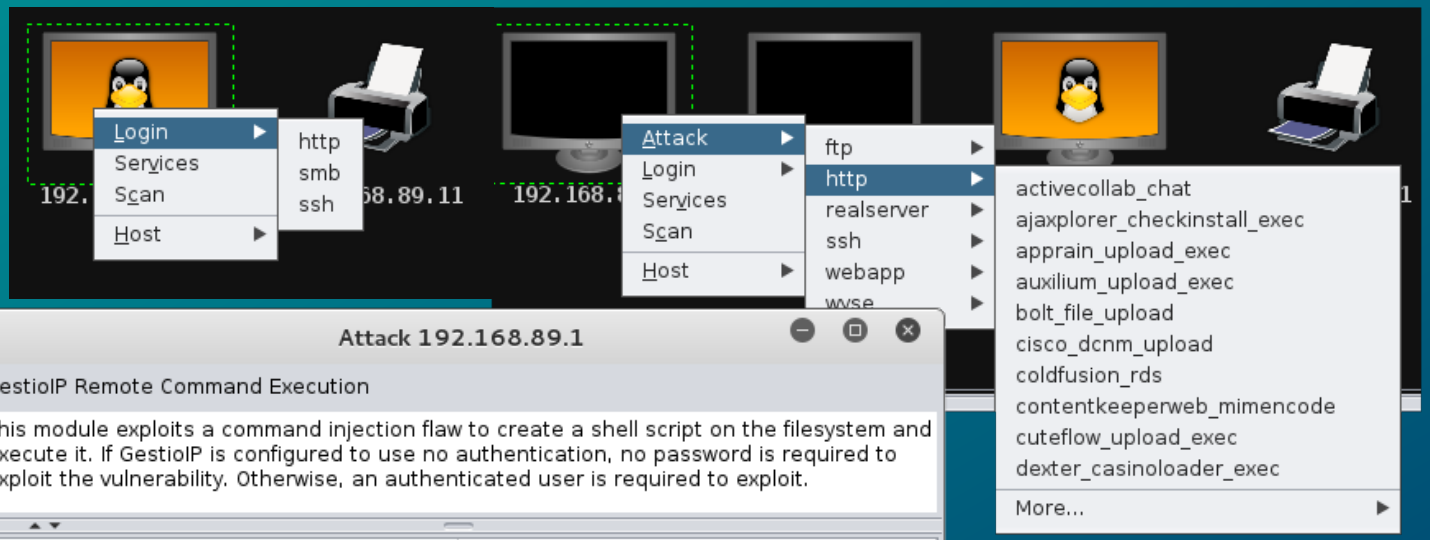
Version used: $Revision: 69 $

Right Ctrl

File Machine View Input Devices Help

Applications Places Wed 16:35

Metaspoilt - Scanning, Attack vectors, Attack



Ref: *Metasploit Unleashed. Offensive Security [online]. Available: https://www.offensive-security.com/metasploit-unleashed/.*
Armitage - Cyber Attach Managem,ent for Metasploit [online]. Available: http://www.fastandeasyhacking.com/.

Right Ctrl

OWASP ZAP

- Tool for finding vulnerabilities in web applications.

Untitled Session - 20151008-151403 - OWASP ZAP 2.4.1

File Edit View Analyse Report Tools Online Help

Standard mode

Sites | Quick Start | Request | Response

Contexts
Default Context
Sites

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://www.obriain.com Select...

Attack Stop

Progress: Spidering the URL to discover the content

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:

Configure your browser: Plug-n-Hack

Or point your browser at: http://localhost:8080/pnh/?apikey=2srn4rt71u2kaeim1c77e6geti

History | Search | Alerts | Output | Spider

New Scan Progress: 0: http://www.obriain.com 39% Current Scans: 1 | URIs Found: 26

Processed	Method	URI	Flags

Alerts 0 1 3 0 Current Scans 0 0 0 1 0 0 0

Ref: *OWASP Zed Attack Proxy Project [online]. Available: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project.*

File Machine View Input Devices Help

Applications Places Wed 16:35

OWASP ZAP Results

History | Search | Alerts | Output | Spider | Active Scan

- Alerts (5)
  - Directory Browsing (5)
  - X-Frame-Options Header Not Set (63)
  - Private IP Disclosure (9)
  - Web Browser XSS Protection Not Enabled (63)
  - X-Content-Type-Options Header Missing (63)

X-Frame-Options Header Not Set

URL: http://www.obriain.com

Risk: Medium

Confidence: Medium

Parameter:

Attack:

Evidence:

CWE Id: 0

WASC Id: 0

Description:

X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Other Info:

Solution:

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use

Reference:

http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

Alerts 0 2 3 0 Current Scans 0 1 0 0 0 0 0

Right Ctrl

Detection Systems

CYBER SECURITY EVENT

- **p0f** – Passive Reconnaissance fingerprinting tool:
  - Passively extracts information from packets on the network
- Port Scan Attack Detector (**psad**):
  - Detects, alerts, and optionally blocks port scans and suspect traffic
- Passive Asset Detection System (**pads**):
  - Using the network traffic it builds an asset list of devices on the network

Summary

CYBER SECURITY EVENT

- A pen-test is an authorised simulated attack on a computer and network systems to discover security weaknesses, potentially gaining access to the system's features and data:
  - Identifies the target systems
  - Reviews available information
  - Undertakes simulated attacks to determine if a system is vulnerable to attack
  - Security issues uncovered are reported to the system owner
  - Identify countermeasures to reduce risk.
- Penetration tests are a component of a full security audit

MANAGING CYBER SECURITY AS A BUSINESS RISK

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

Thank you

CYBER SECURITY EVENT

netLabs!UG