Aiming at Higher Network Security Levels Through Extensive

PENETRATION TESTING

Anestis Bechtsoudis

http://bechtsoudis.com

abechtsoudis *(at)* ieee.org

Athena Summer School 2011

Course Goals

- Highlight modern network and system security complexity
- Importance of conducting security tests
- Penetration testing systematic methodology applicable both to amateurs & professionals
- Tools arsenal – Open/Close/Free/Commercial
- Motivation to adopt security procedures and response teams to your working environments

Overview

- Introduction
- Definition
- Purpose
- Methodology
- Live Demo
- Conclusions

Introduction

Information & **C**ommunication **T**echnology

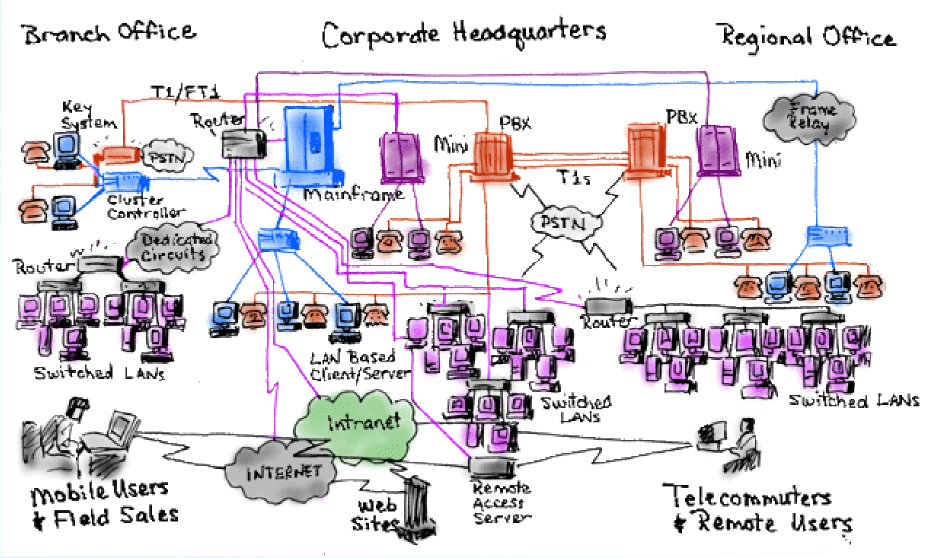
Security

Introduction

- Modern enterprise infrastructures adopt:
  - Multilayer network architectures
  - Scalable web services
  - Custom applications
  - Heterogeneous server platform environments

- Complex architectures result in large security demands

Introduction



Introduction

- Attackers have formed teams and formulated their hacking procedures

Introduction

- Most companies & institutes adopt just an up-to-date security policy
- Take into faith that vendor’s fixes will keep their systems safe
- This approach is not adequate for a truly proactive security planning

Introduction

- What about mis-configured settings or network infrastructure design flaws?
- Do ICT Security administrators really know whether and where they are vulnerable?
- Are managers and administrators willing to pay the cost?

Aiming to Higher Security Levels

Penetration Testing

==

Ethical Hacking

What is Penetration Testing?

- Systematic probing of a *system* to find vulnerabilities that an attacker could exploit
  - *System*: computer/server, application, network device, smart card, rfid etc.
- Emphasis on how deep one can get into a system
- Must not be confused with audits

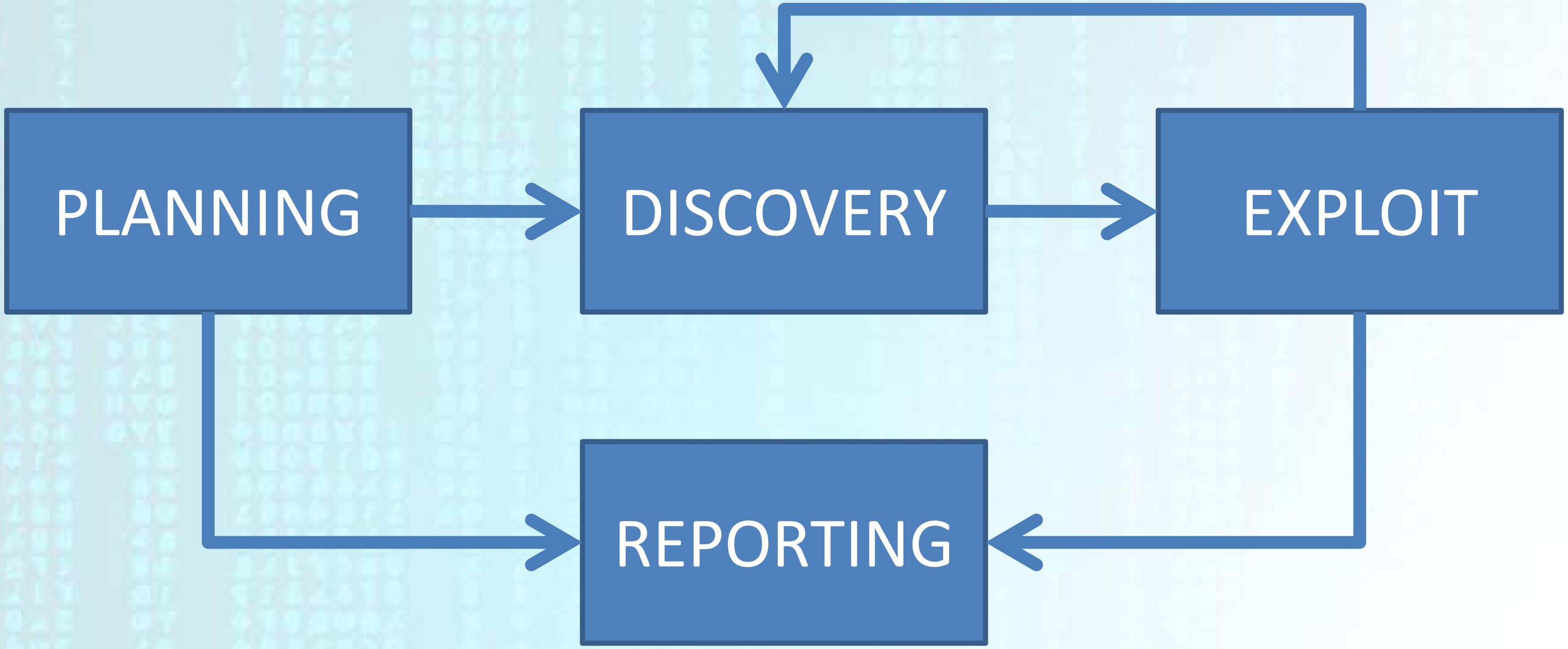
Pen-testing Classes

- What kind of attack does the organization want to simulate?
  - ➢**Black-Box**: No (or little) knowledge about the systems -> external attacker
  - ➢**White-Box**: Complete knowledge about the systems -> internal attack

Why pen-testing?

- Find vulnerabilities and fix them
- Test systems before going on-line
- Locate employees’ naïve or intentional changes
- Train & test organization’s ICT response and incident handling teams
- Marketing

Methodology



Planning

- Define the scope
- Sign management approvals, documents and agreements (like NDA)
- Define a strategy taking into account all the limitations:
  - Time
  - Legal restrictions
  - Down-time

Discovery

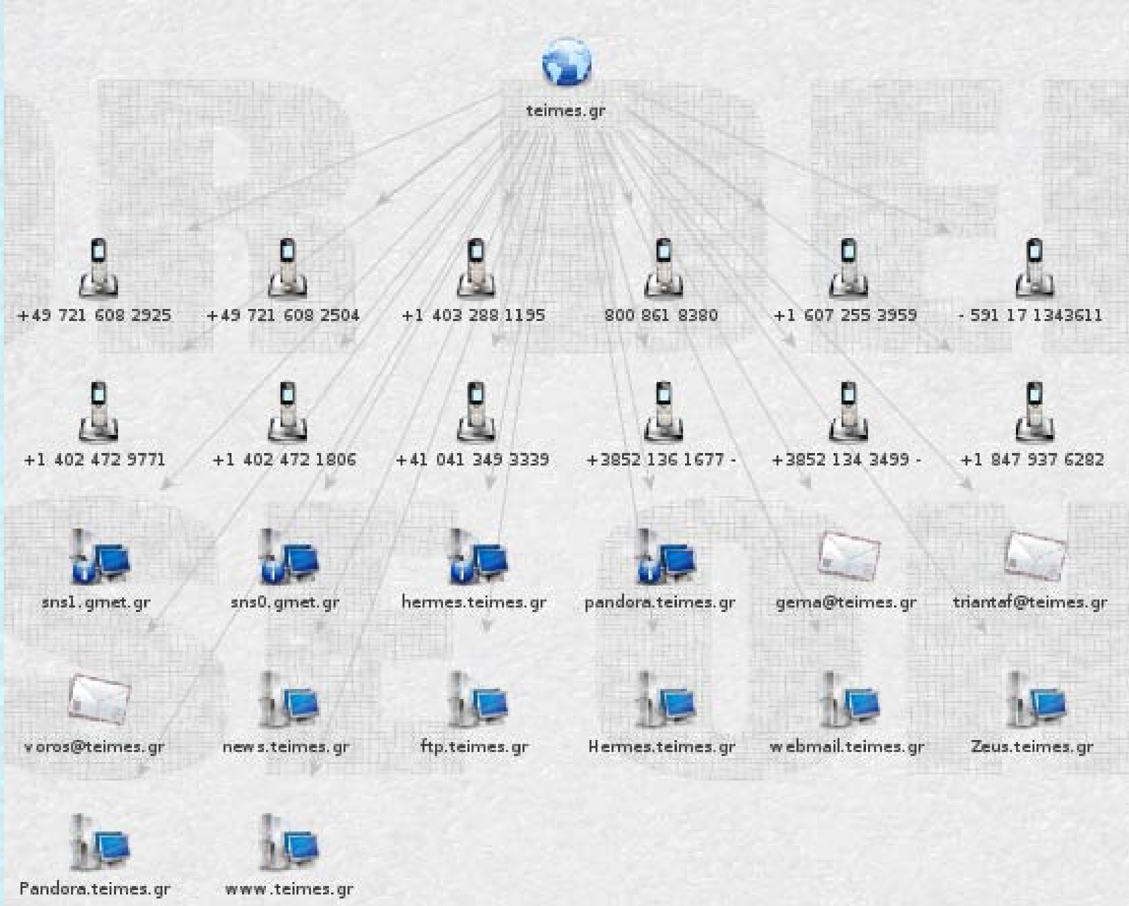
- *“Knowing is half the battle”*
- Information gathering phase – As much as possible
- Further categorized to:
  - Footprinting – Non-intrusive
  - Scan & Enumeration – Intrusive
  - Vulnerability Analysis – Both

Discovery -> Footprinting

- Searching the internet and querying public repositories.
  - Whois databases
  - Domain registrars
  - Mailing lists
  - Public documents
  - Social Networking
  - Text dump sites
  - …

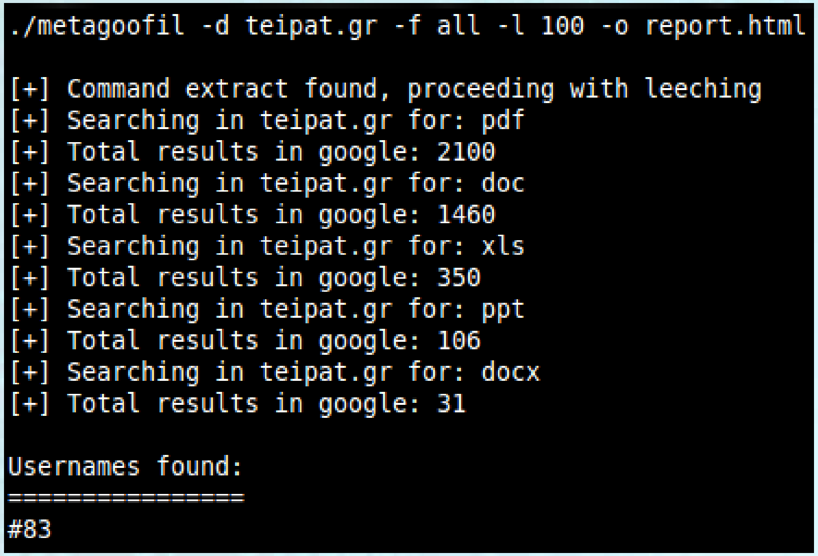
Discovery -> Footprinting -> Tools

Maltego: Information Reconnaissance Toolkit

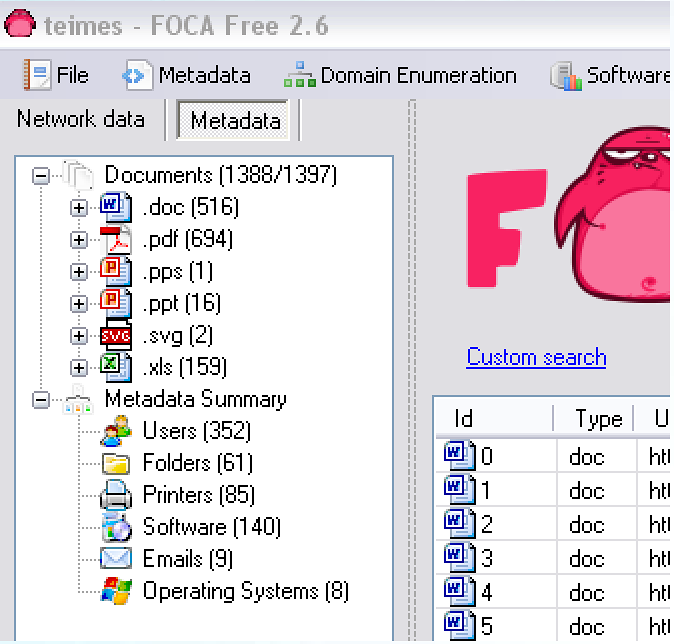


Discovery -> Footprinting -> Tools

File metadata enumeration



```
./metagoofil -d teipat.gr -f all -l 100 -o report.html

[+] Command extract found, proceeding with leeching
[+] Searching in teipat.gr for: pdf
[+] Total results in google: 2100
[+] Searching in teipat.gr for: doc
[+] Total results in google: 1460
[+] Searching in teipat.gr for: xls
[+] Total results in google: 350
[+] Searching in teipat.gr for: ppt
[+] Total results in google: 106
[+] Searching in teipat.gr for: docx
[+] Total results in google: 31

Usernames found:
================
#83
```



teimes - FOCA Free 2.6

- Documents (1388/1397)
  - .doc (516)
  - .pdf (694)
  - .pps (1)
  - .ppt (16)
  - .svg (2)
  - .xls (159)
- Metadata Summary
  - Users (352)
  - Folders (61)
  - Printers (85)
  - Software (140)
  - Emails (9)
  - Operating Systems (8)

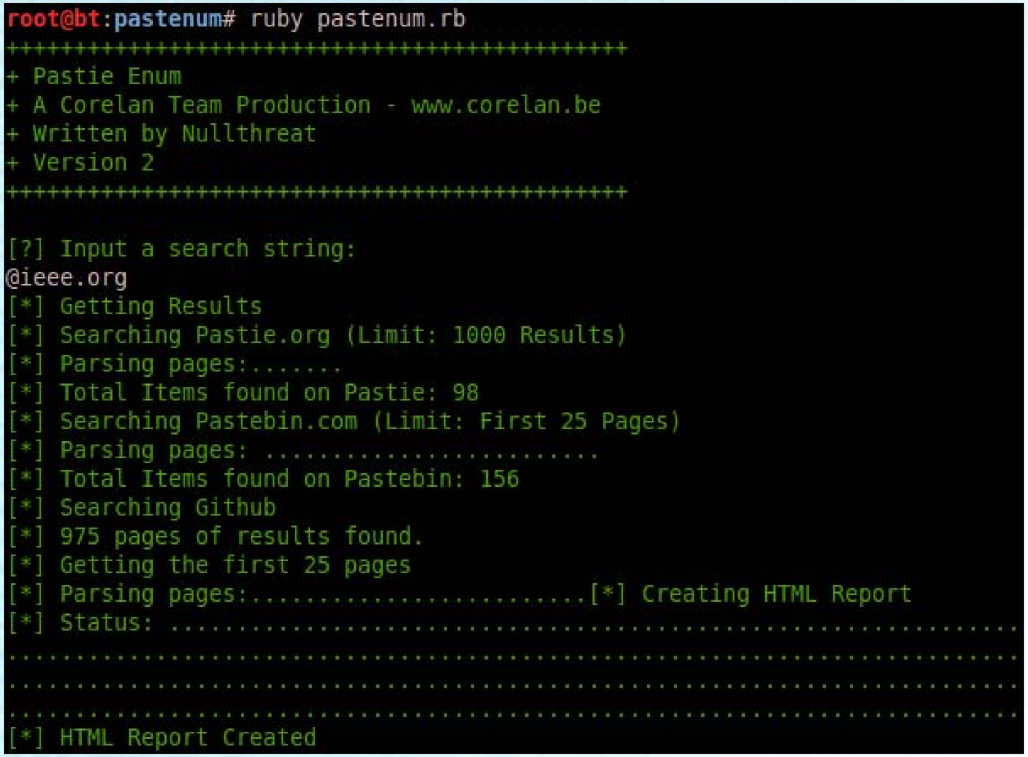
Id	Type	U
0	doc	htt
1	doc	htt
2	doc	htt
3	doc	htt
4	doc	htt
5	doc	htt

Metagoofil python script

FOCA Windows Tool

Discovery -> Footprinting -> Tools

Text dump sites (pastebin, pastie etc)



```
root@bt:pastenum# ruby pastenum.rb
++++++++++++++++++++++++++++++++++++++++++++++
+ Pastie Enum
+ A Corelan Team Production - www.corelan.be
+ Written by Nullthreat
+ Version 2
++++++++++++++++++++++++++++++++++++++++++++++

[?] Input a search string:
@ieee.org
[*] Getting Results
[*] Searching Pastie.org (Limit: 1000 Results)
[*] Parsing pages:.......
[*] Total Items found on Pastie: 98
[*] Searching Pastebin.com (Limit: First 25 Pages)
[*] Parsing pages: .........................
[*] Total Items found on Pastebin: 156
[*] Searching Github
[*] 975 pages of results found.
[*] Getting the first 25 pages
[*] Parsing pages:.........................[*] Creating HTML Report
[*] Status: ...............................................................
...........................................................................
...........................................................................
...........................................................................
[*] HTML Report Created
```

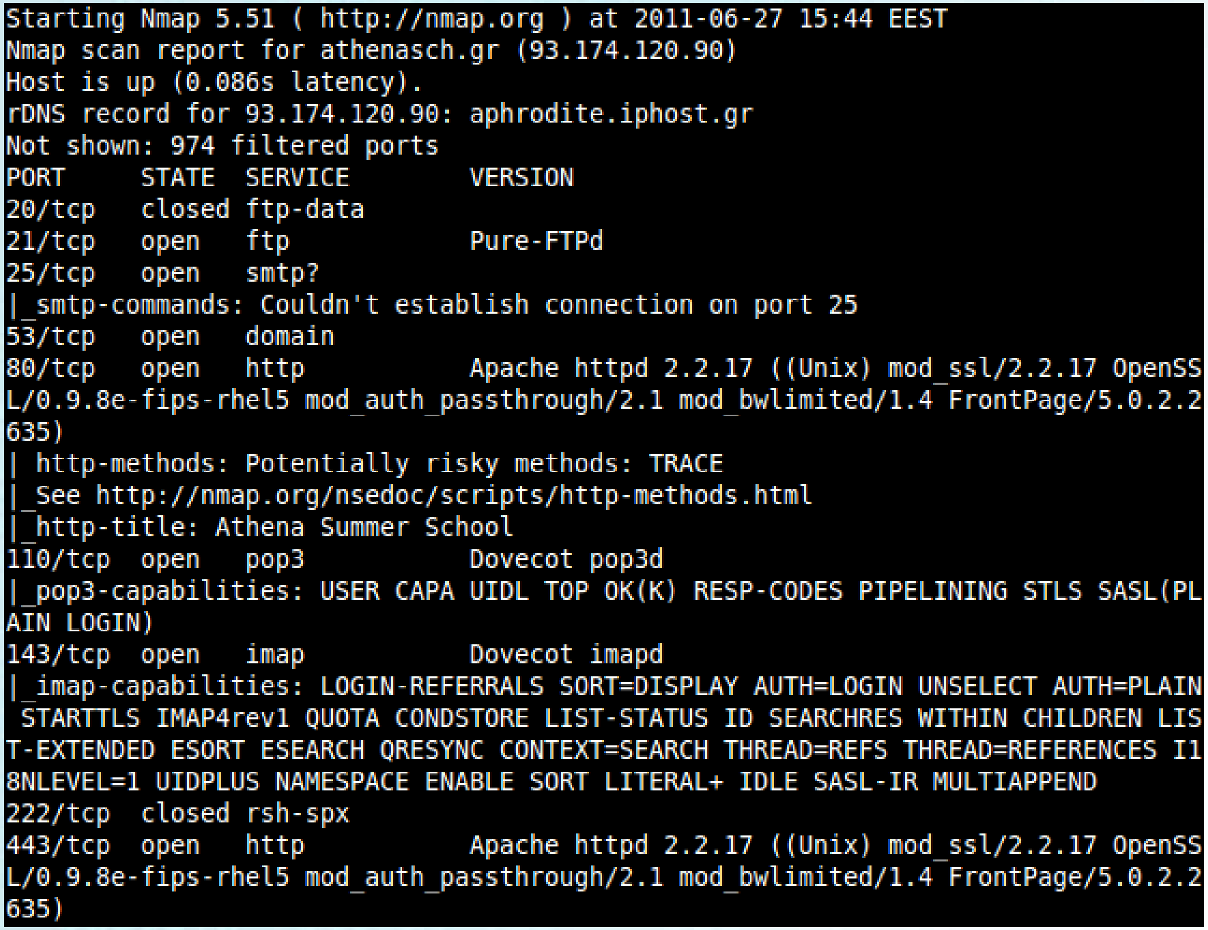
Pastenum ruby script

Discovery -> Scanning & Enumeration

- Active probing the target systems
  - Open/filtered ports
  - Running services
  - Mapping router/firewall rules
  - Identify OS details
  - Enumerate network devices
  - Mapping internal network architecture
  - …

Discovery -> Scanning & Enumeration -> Tools

NMAP : Open source network mapper

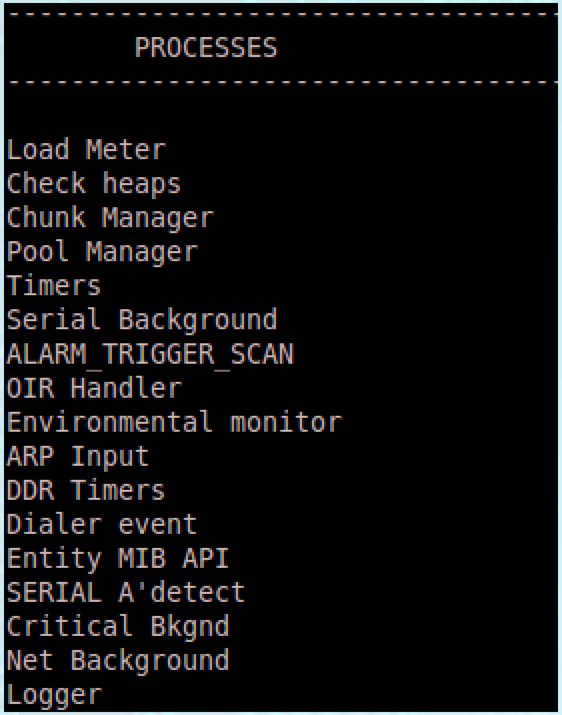


```
Starting Nmap 5.51 ( http://nmap.org ) at 2011-06-27 15:44 EEST
Nmap scan report for athenasch.gr (93.174.120.90)
Host is up (0.086s latency).
rDNS record for 93.174.120.90: aphrodite.iphost.gr
Not shown: 974 filtered ports
PORT     STATE  SERVICE        VERSION
20/tcp   closed ftp-data
21/tcp   open   ftp            Pure-FTPd
25/tcp   open   smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp   open   domain
80/tcp   open   http           Apache httpd 2.2.17 ((Unix) mod_ssl/2.2.17 OpenSS
L/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2
635)
| http-methods: Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-title: Athena Summer School
110/tcp  open   pop3           Dovecot pop3d
|_pop3-capabilities: USER CAPA UIDL TOP OK(K) RESP-CODES PIPELINING STLS SASL(PL
AIN LOGIN)
143/tcp  open   imap           Dovecot imapd
|_imap-capabilities: LOGIN-REFERRALS SORT=DISPLAY AUTH=LOGIN UNSELECT AUTH=PLAIN
 STARTTLS IMAP4rev1 QUOTA CONDSTORE LIST-STATUS ID SEARCHRES WITHIN CHILDREN LIS
T-EXTENDED ESORT ESEARCH QRESYNC CONTEXT=SEARCH THREAD=REFS THREAD=REFERENCES I1
8NLEVEL=1 UIDPLUS NAMESPACE ENABLE SORT LITERAL+ IDLE SASL-IR MULTIAPPEND
222/tcp  closed rsh-spx
443/tcp  open   http           Apache httpd 2.2.17 ((Unix) mod_ssl/2.2.17 OpenSS
L/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2
635)
```

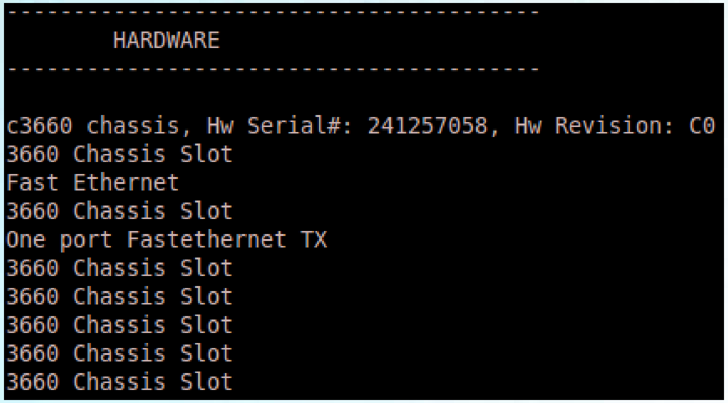
Discovery -> Scanning & Enumeration -> Tools

SNMP Enumeration

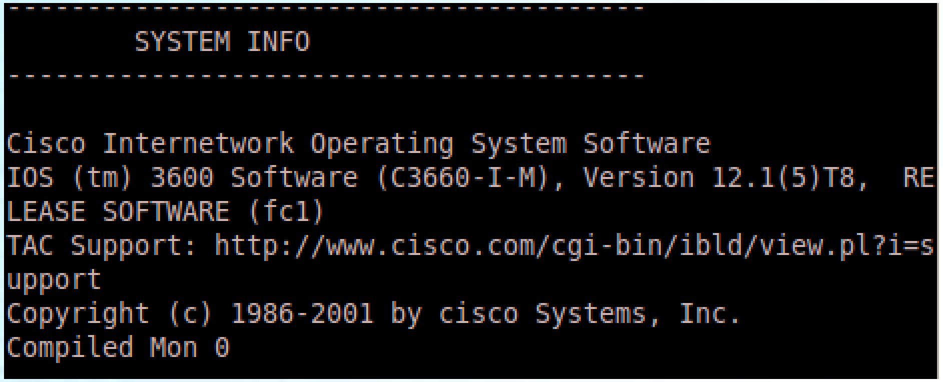
```
./snmpenum.pl 192.168.146.13 public cisco
```



```
----------------------------------------
        PROCESSES
----------------------------------------

Load Meter
Check heaps
Chunk Manager
Pool Manager
Timers
Serial Background
ALARM_TRIGGER_SCAN
OIR Handler
Environmental monitor
ARP Input
DDR Timers
Dialer event
Entity MIB API
SERIAL A'detect
Critical Bkgnd
Net Background
Logger
```



```
----------------------------------------
        HARDWARE
----------------------------------------

c3660 chassis, Hw Serial#: 241257058, Hw Revision: C0
3660 Chassis Slot
Fast Ethernet
3660 Chassis Slot
One port Fastethernet TX
3660 Chassis Slot
3660 Chassis Slot
3660 Chassis Slot
3660 Chassis Slot
3660 Chassis Slot
```



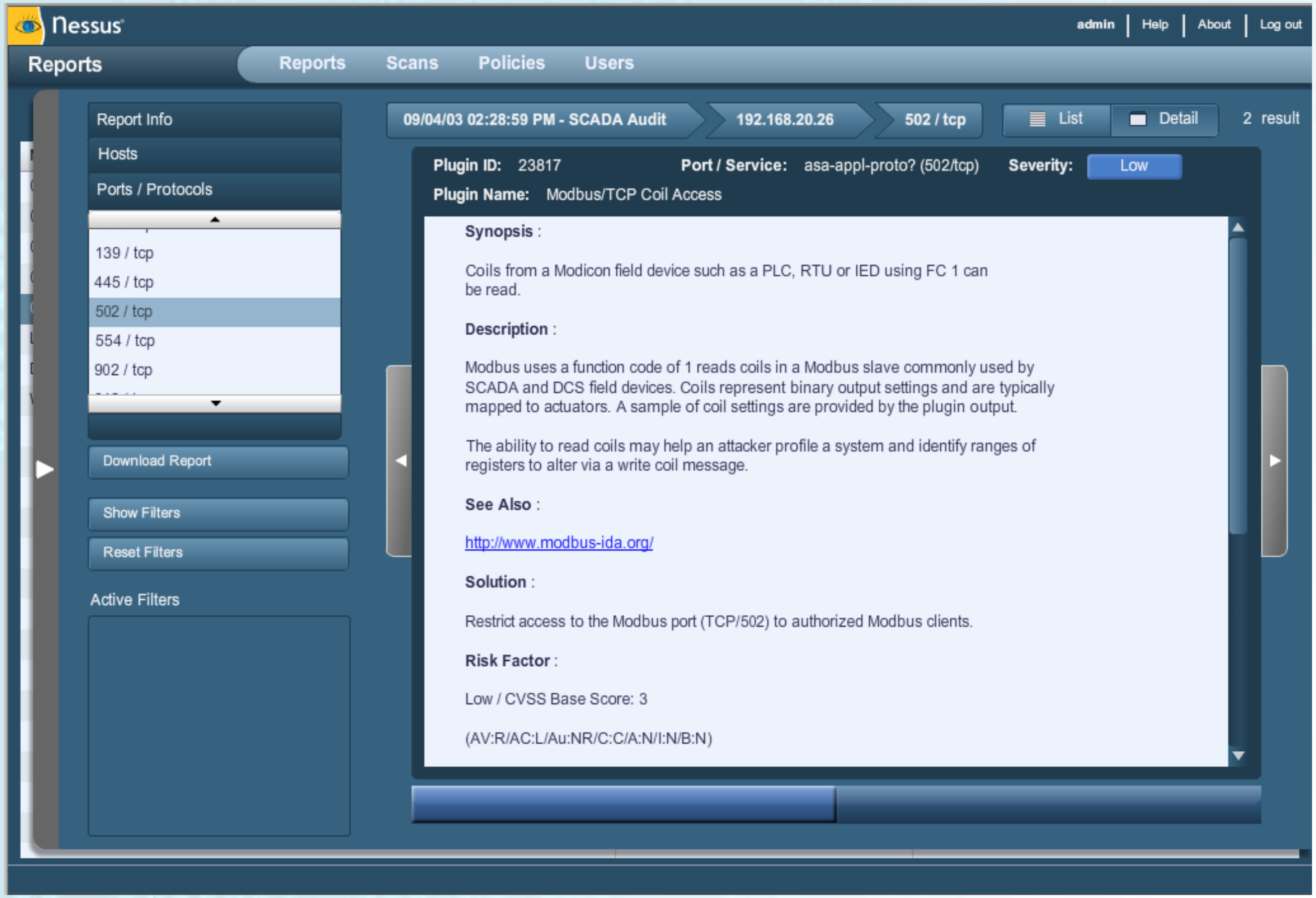
```
----------------------------------------
        SYSTEM INFO
----------------------------------------

Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3660-I-M), Version 12.1(5)T8,  RE
LEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/cgi-bin/ibld/view.pl?i=s
upport
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 0
```

Discovery -> Vulnerability Analysis

- Find possible vulnerabilities existing in target systems
  - Search in security databases: mailing lists, blogs, advisories etc.
  - Application scanners: buffer overflows, SQL injections, XSS, cookie manipulation etc.
  - Fuzzing (may discover unidentified vulnerabilities)
  - Web application assessment proxy
  - …

Discovery -> Vulnerability Analysis -> Tools

Nessus: Vulnerability Scanner



Plugin ID: 23817 **Port / Service:** asa-appl-proto? (502/tcp) **Severity:** Low

Plugin Name: Modbus/TCP Coil Access

Synopsis :

Coils from a Modicon field device such as a PLC, RTU or IED using FC 1 can be read.

Description :

Modbus uses a function code of 1 reads coils in a Modbus slave commonly used by SCADA and DCS field devices. Coils represent binary output settings and are typically mapped to actuators. A sample of coil settings are provided by the plugin output.

The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a write coil message.

See Also :

http://www.modbus-ida.org/

Solution :

Restrict access to the Modbus port (TCP/502) to authorized Modbus clients.

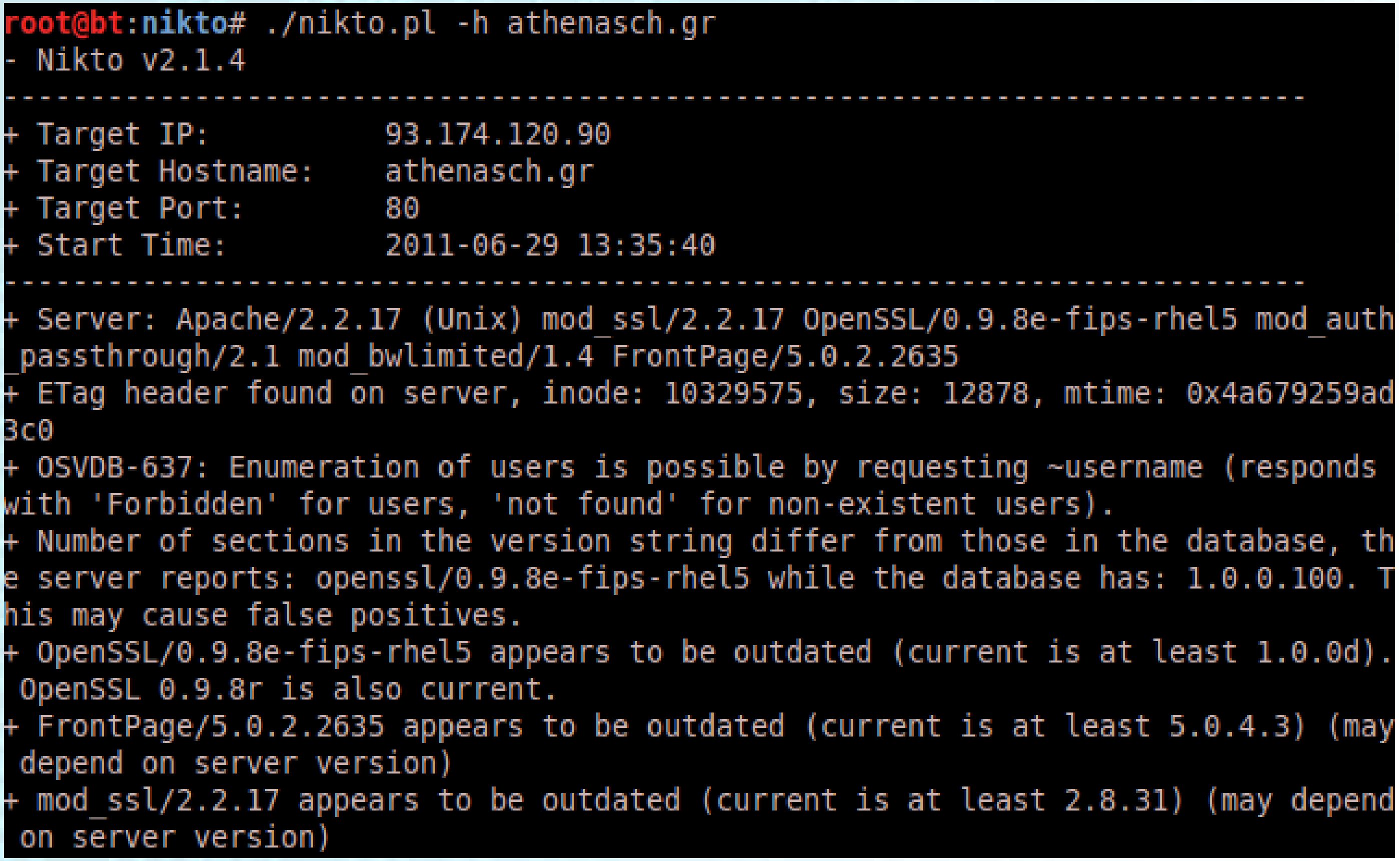
Risk Factor :

Low / CVSS Base Score: 3

(AV:R/AC:L/Au:NR/C:C/A:N/I:N/B:N)

Discovery -> Vulnerability Analysis -> Tools

Nikto: Web Server Vulnerability Assessment

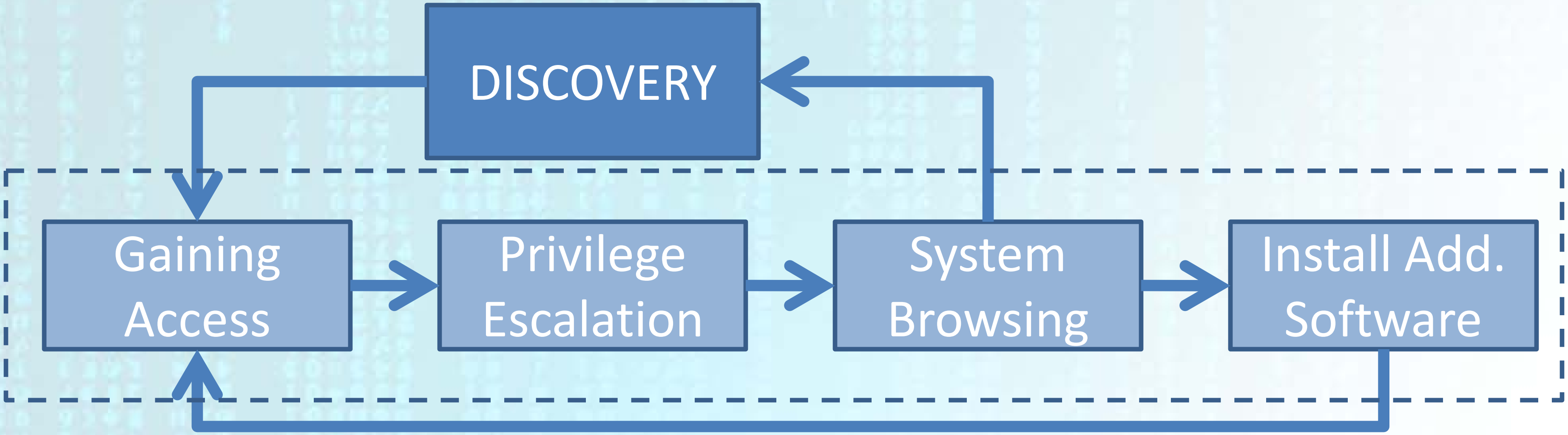


```
root@bt:nikto# ./nikto.pl -h athenasch.gr
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          93.174.120.90
+ Target Hostname:    athenasch.gr
+ Target Port:        80
+ Start Time:         2011-06-29 13:35:40
---------------------------------------------------------------------------
+ Server: Apache/2.2.17 (Unix) mod_ssl/2.2.17 OpenSSL/0.9.8e-fips-rhel5 mod_auth
_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635
+ ETag header found on server, inode: 10329575, size: 12878, mtime: 0x4a679259ad
3c0
+ OSVDB-637: Enumeration of users is possible by requesting ~username (responds
with 'Forbidden' for users, 'not found' for non-existent users).
+ Number of sections in the version string differ from those in the database, th
e server reports: openssl/0.9.8e-fips-rhel5 while the database has: 1.0.0.100. T
his may cause false positives.
+ OpenSSL/0.9.8e-fips-rhel5 appears to be outdated (current is at least 1.0.0d).
 OpenSSL 0.9.8r is also current.
+ FrontPage/5.0.2.2635 appears to be outdated (current is at least 5.0.4.3) (may
 depend on server version)
+ mod_ssl/2.2.17 appears to be outdated (current is at least 2.8.31) (may depend
 on server version)
```

Exploiting

- *“Let the party begin”*
- Use gathered information to attack target systems
- Case dependant: Targeting the actual system or launch attacks into a simulated lab
- Prior exploits testing and take all necessary precautions

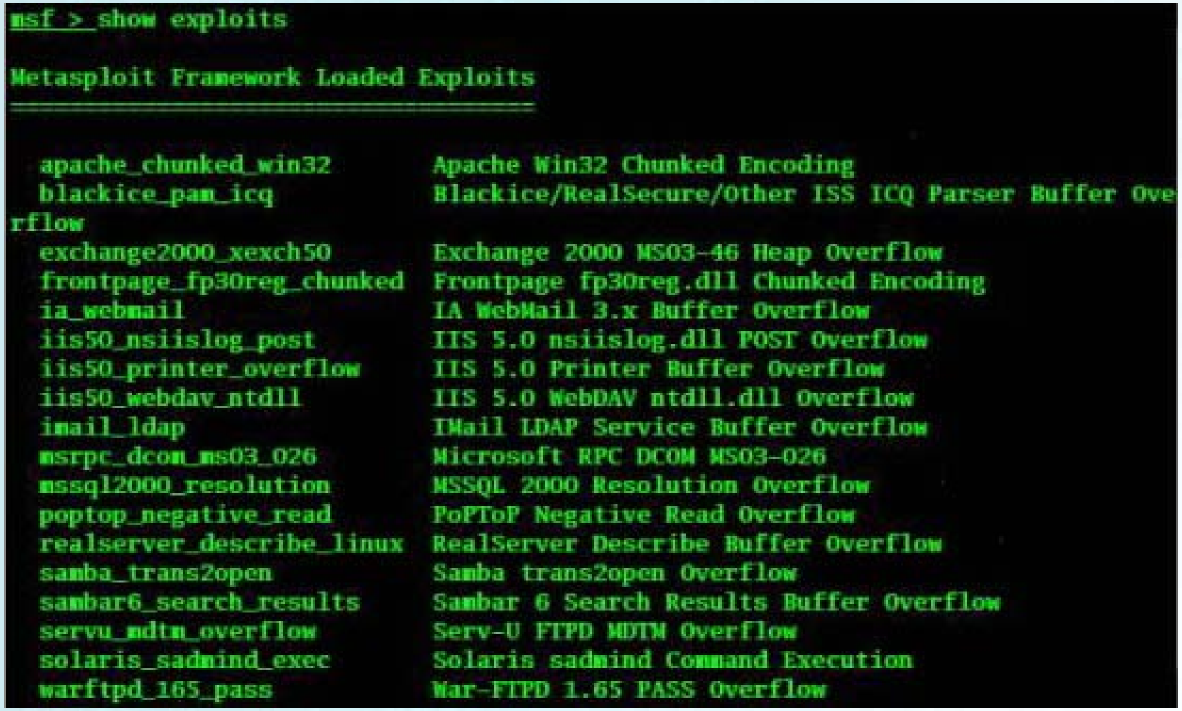
Exploiting



- Successful exploit might not lead to root access
- Pivoting through targeted systems

Exploiting -> Tools

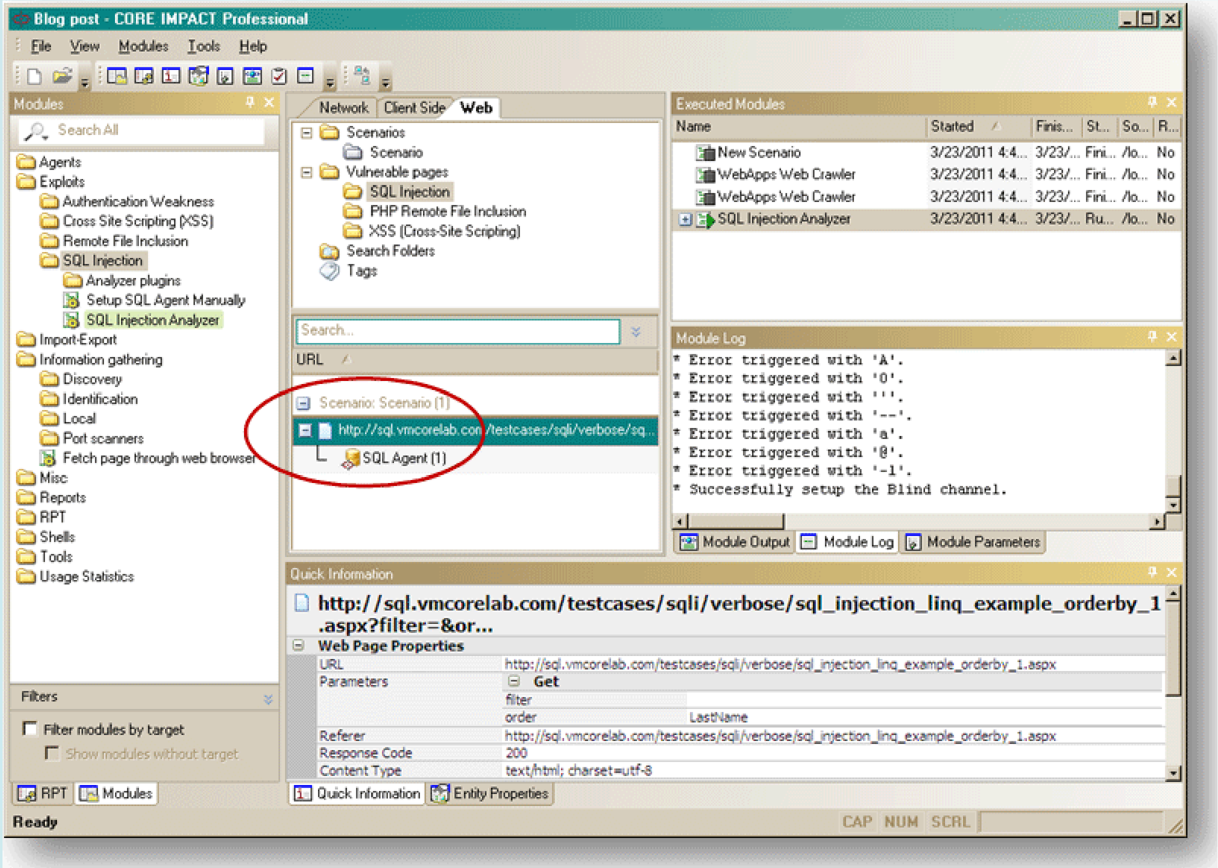
Metasploit: Exploitation Framework



```
msf > show exploits

Metasploit Framework Loaded Exploits
====================================

  apache_chunked_win32        Apache Win32 Chunked Encoding
  blackice_pam_icq            Blackice/RealSecure/Other ISS ICQ Parser Buffer Ove
rflow
  exchange2000_xexch50        Exchange 2000 MS03-46 Heap Overflow
  frontpage_fp30reg_chunked   Frontpage fp30reg.dll Chunked Encoding
  ia_webmail                  IA WebMail 3.x Buffer Overflow
  iis50_nsiislog_post         IIS 5.0 nsiislog.dll POST Overflow
  iis50_printer_overflow      IIS 5.0 Printer Buffer Overflow
  iis50_webdav_ntdll          IIS 5.0 WebDAV ntdll.dll Overflow
  imail_ldap                  IMail LDAP Service Buffer Overflow
  msrpc_dcom_ms03_026         Microsoft RPC DCOM MS03-026
  mssql2000_resolution        MSSQL 2000 Resolution Overflow
  poptop_negative_read        PoPToP Negative Read Overflow
  realserver_describe_linux   RealServer Describe Buffer Overflow
  samba_trans2open            Samba trans2open Overflow
  sambar6_search_results      Sambar 6 Search Results Buffer Overflow
  servu_mdtm_overflow         Serv-U FTPD MDTM Overflow
  solaris_sadmind_exec        Solaris sadmind Command Execution
  warftpd_165_pass            War-FTPD 1.65 PASS Overflow
```

Exploiting -> Tools

Core Impact: Full Pen-Testing Platform



- Agents
- Exploits
  - Authentication Weakness
  - Cross Site Scripting (XSS)
  - Remote File Inclusion
  - SQL Injection
    - Analyzer plugins
    - Setup SQL Agent Manually
    - SQL Injection Analyzer
- Import-Export
- Information gathering
  - Discovery
  - Identification
  - Local
  - Port scanners
  - Fetch page through web browser
- Misc
- Reports
- RPT
- Shells
- Tools
- Usage Statistics

Filters

☐ Filter modules by target

☐ Show modules without target

- Scenarios
  - Scenario
- Vulnerable pages
  - SQL Injection
  - PHP Remote File Inclusion
  - XSS (Cross-Site Scripting)
- Search Folders
- Tags

- Scenario: Scenario (1)
  - http://sql.vmcorelab.com/testcases/sqli/verbose/sq...
    - SQL Agent (1)

Executed Modules

Name	Started	Finis...	St...	So...	R...
New Scenario	3/23/2011 4:4...	3/23/...	Fini...	/lo...	No
WebApps Web Crawler	3/23/2011 4:4...	3/23/...	Fini...	/lo...	No
WebApps Web Crawler	3/23/2011 4:4...	3/23/...	Fini...	/lo...	No
SQL Injection Analyzer	3/23/2011 4:4...	3/23/...	Ru...	/lo...	No

Module Log

```
* Error triggered with 'A'.
* Error triggered with '0'.
* Error triggered with '''.
* Error triggered with '--'.
* Error triggered with 'a'.
* Error triggered with '@'.
* Error triggered with '-1'.
* Successfully setup the Blind channel.
```

Quick Information

http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&or...

Web Page Properties

URL	http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx	
Parameters	**Get**	
	filter	
	order	LastName
Referer	http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx	
Response Code	200	
Content Type	text/html; charset=utf-8	

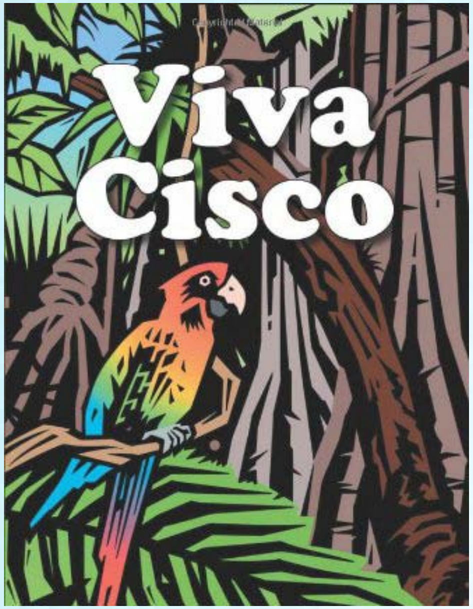
Reporting

- *“Paperwork headache”*
- Most important phase – They pay you for these final documents
- Keep in mind both Management & Technical aspects
- Clear and precise documentations are important for a successful penetration test

Demo

Enough with the theory.

Live Demo Time!

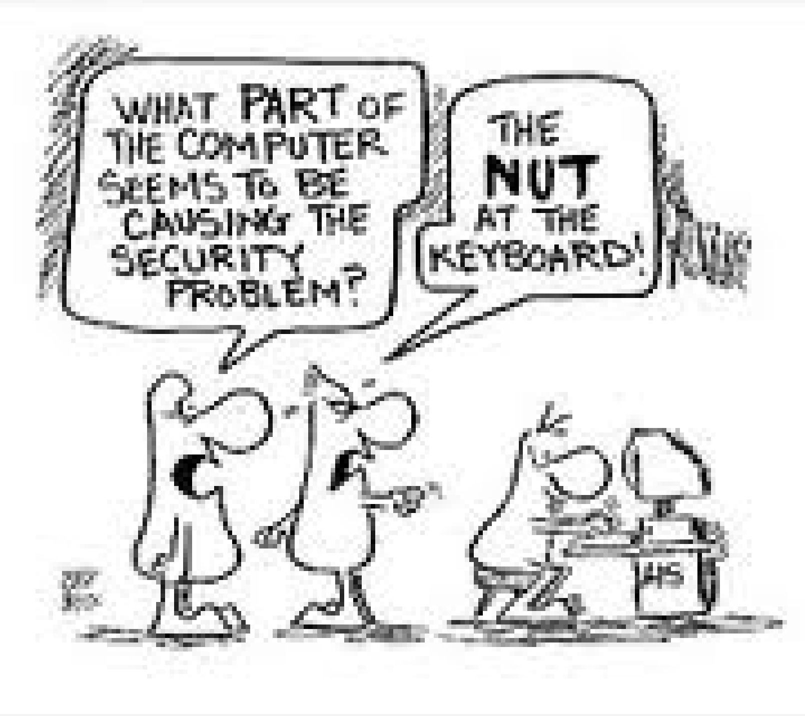


Conclusions

- Modern ICT infrastructures have large and more difficult than ever security demands
- Penetration Tests are a vital component of a comprehensive security policy
- Rapid changes in ICT security -> Regularity
- Learn to be proactive in order to prevent catastrophic hacking attacks & data leakage

Conclusions

And always remember…


WHAT PART OF THE COMPUTER SEEMS TO BE CAUSING THE SECURITY PROBLEM?
THE NUT AT THE KEYBOARD!
HS

Thank You!

Questions