ECSA/LPT v8

Product Marketing Slides

Designed by Security Auditors. Presented by Professionals.

ECSA™

EC-Council Certified Security Analyst

Presentation Flow

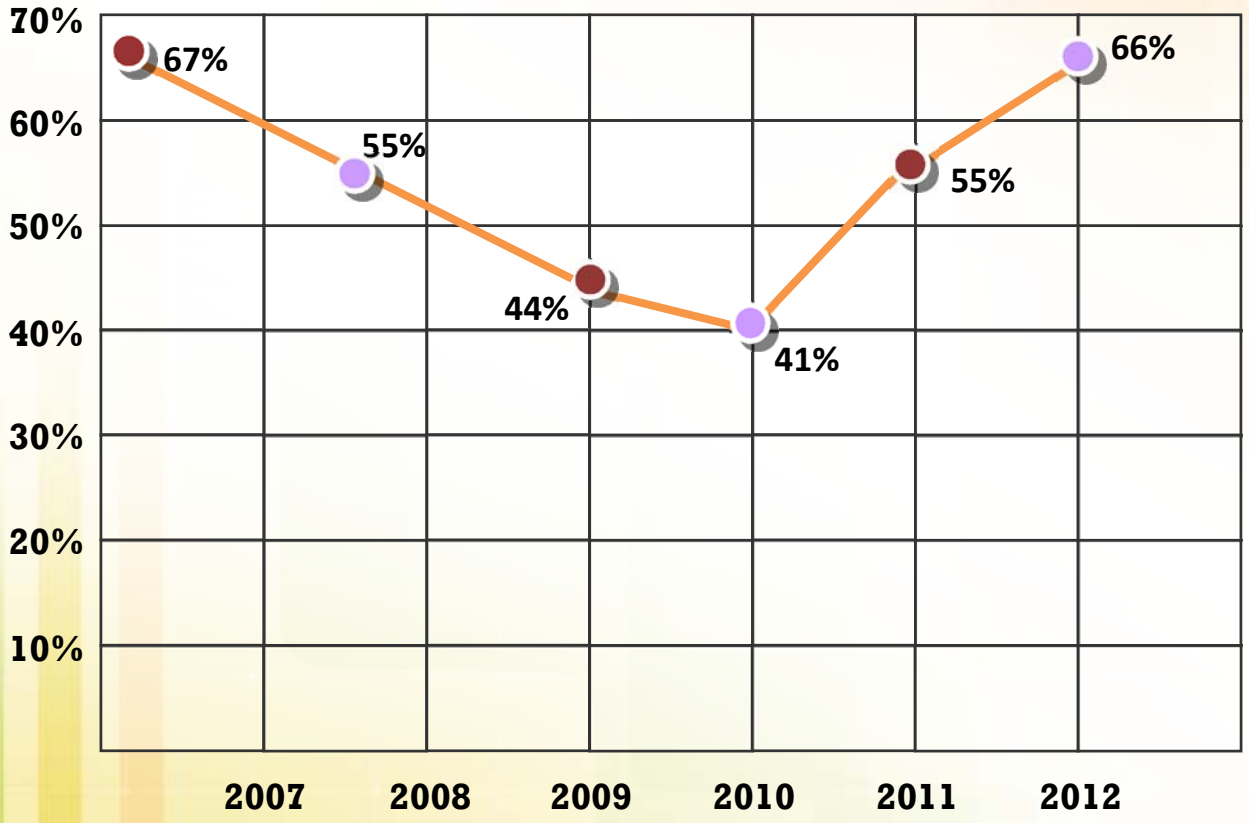
Threat Landscape

Cost of Information Security Breaches

Demand for Pen Testers

What is ECSA/LPT Program

Percent of Breaches that Remains Undiscovered for Months or More - 2013



Are we giving attackers more than enough time to cause havoc and retract?

http://www.verizonenterprise.com

How Target Detected Hack But Failed to Act

Despite alerts received through a **$1.6 million malware detection system**, Target failed to stop hackers from stealing credit card numbers and personal information of millions of customers, Bloomberg reports.

http://www.cnet.com

According to McAfee Q4 2013 report, 2.4 million new mobile malware samples were added in 2013, up 197% from 2012

http://www.mcafee.com

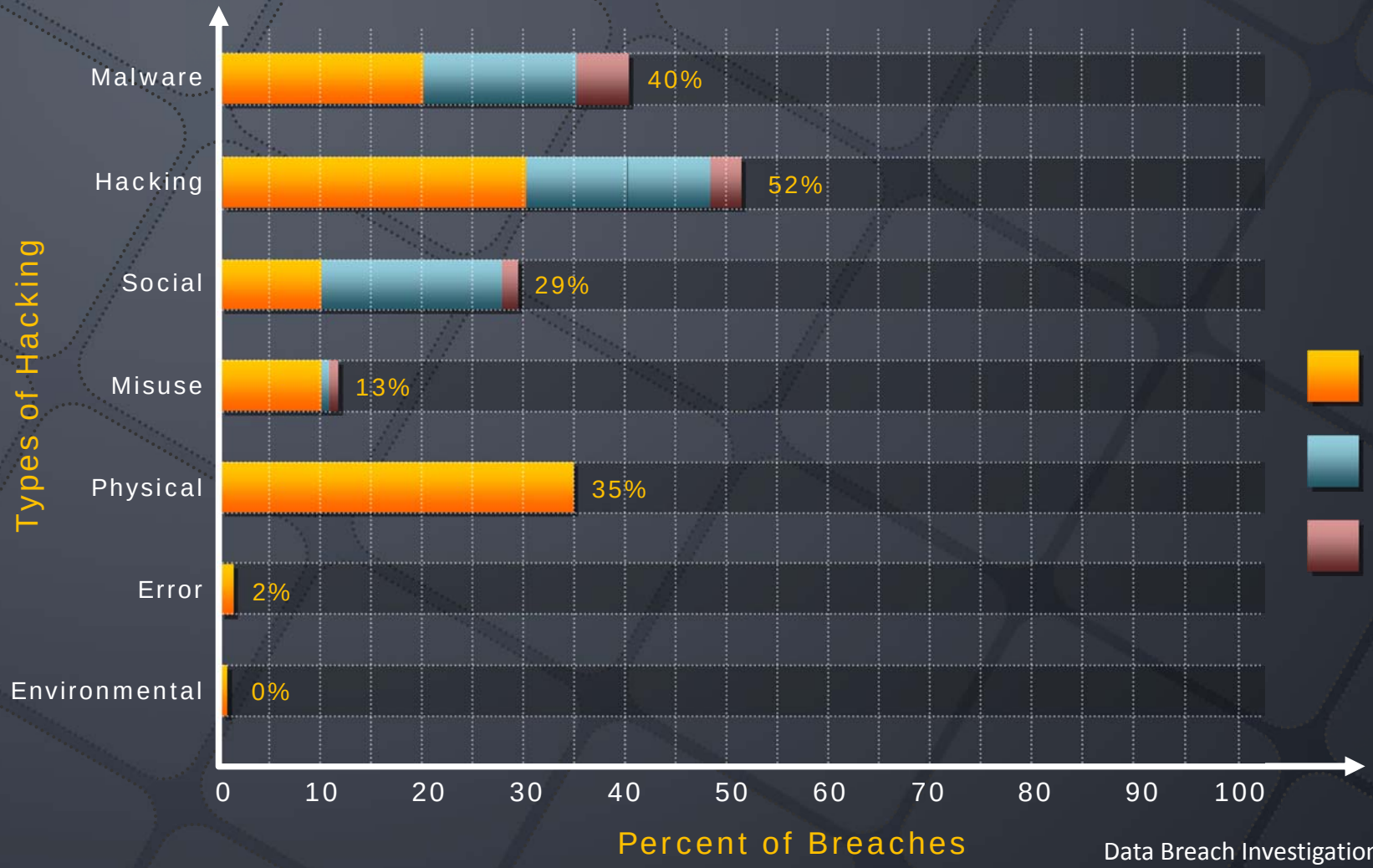
According to McAfee Q4 2013 report, one of the biggest breaches this quarter affected multiple retail chains across the United States by a series of point-of-sale (POS) attacks

Millions of credit card numbers stolen and this attack has been ranked among the largest data-loss incidents of all time

McAfee
Proven Security

http://www.mcafee.com

Data Breach Investigations Report - 2013



Data Breach Investigations Report 2013,
Source: *http://www.verizonbusiness.com*

2013-14 Hacking Trends

1

Researchers have observed sophisticated hacking groups conducting automated scans of the internet in search of web servers vulnerable to the theft of data, including passwords, confidential communications and credit card numbers, due to the Heartbleed bug

http://www.cbc.ca

Millions of passwords, credit card numbers and other personal information may be at risk as a result of a major breakdown in internet security revealed, due to the Heartbleed bug

http://timesofindia.indiatimes.com

2

Famous South Korean search portal NAVER hacked, 25 million accounts hacked using stolen data

http://hackread.com

2013-14 Hacking Trends

3

Largest single personal data hack ever?

A cyber security firm has reported a "mind boggling" cache of stolen credentials which has been put up for **sale on online black markets**

A total of **360 million** accounts were affected in a series of hacks, one of which seems to be the biggest in history

http://rt.com

4

More than **4.5 million** Snapchat usernames and phone numbers have leaked after hackers exploited a security flaw exposed by Australian white-hat hackers and **posted the information online**

http://www.smh.com.au

2013-14 Hacking Trends

5

AVG in trouble

The internet security software company AVG is in trouble, this time around the company, has been attacked by hackers from Indonesia and Pakistan

Already, **19 official domains of the company have been hacked and defaced**

http://hackread.com

6

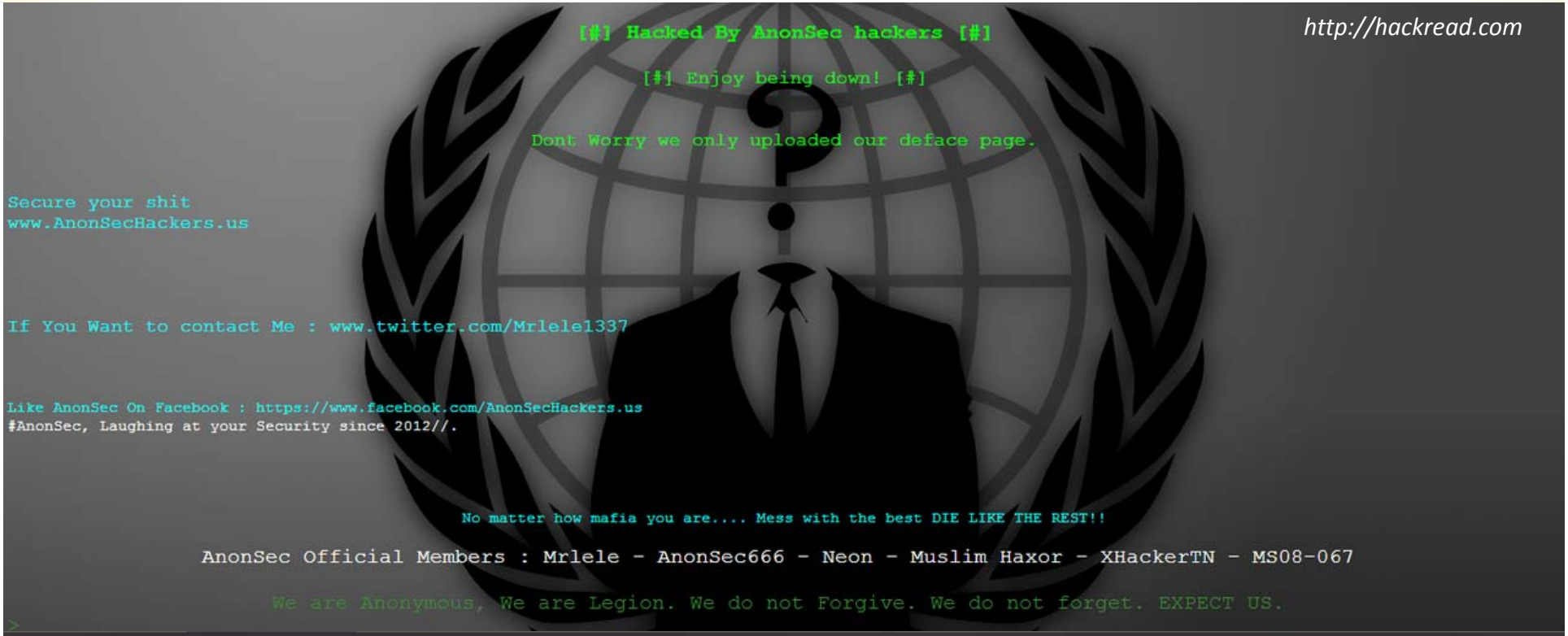
The world's second largest email service provider **Yahoo Inc.** has around **273 million** email accounts all over the world

Yahoo has been hacked again. Yahoo announced that **usernames and passwords** of its email users have been stolen by unknown hackers

http://hackread.com

2013-14 Hacking Trends

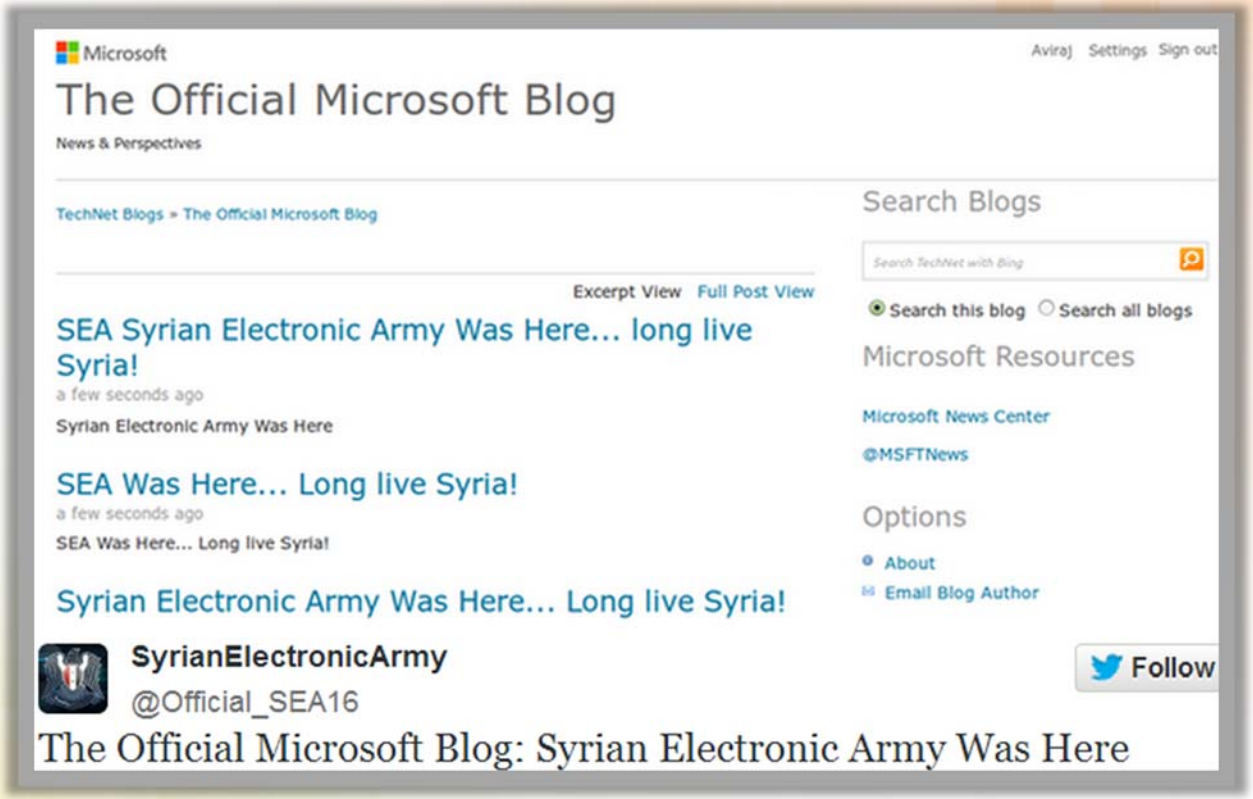
A group of hackers going with the handle of AnonSec has **hacked and defaced 720 random websites from all over the world**



http://hackread.com

2013-14 Hacking Trends

On New Year's Day, the Syrian Electronic Army hacked **Skype's Twitter account** and its **official Microsoft blog**, allegedly in order to warn people away from Microsoft's email services



http://www.theverge.com

Snapchat Update to Close Loophole after Mass Hack

Snapchat is updating its app to close a **loophole** that saw millions of Snapchatters' details leaked by hackers.

Usernames and phone numbers of 4.6 million accounts were posted online on New Year's Eve by hackers, who left off only the last two digits of each number when posting them publicly. The hackers say they leaked the data to "put public pressure on Snapchat to get this exploit fixed".

Can we detect these loopholes before attackers do?

http://www.cnet.com

200M Consumer Records Exposed in Experian Security Lapse

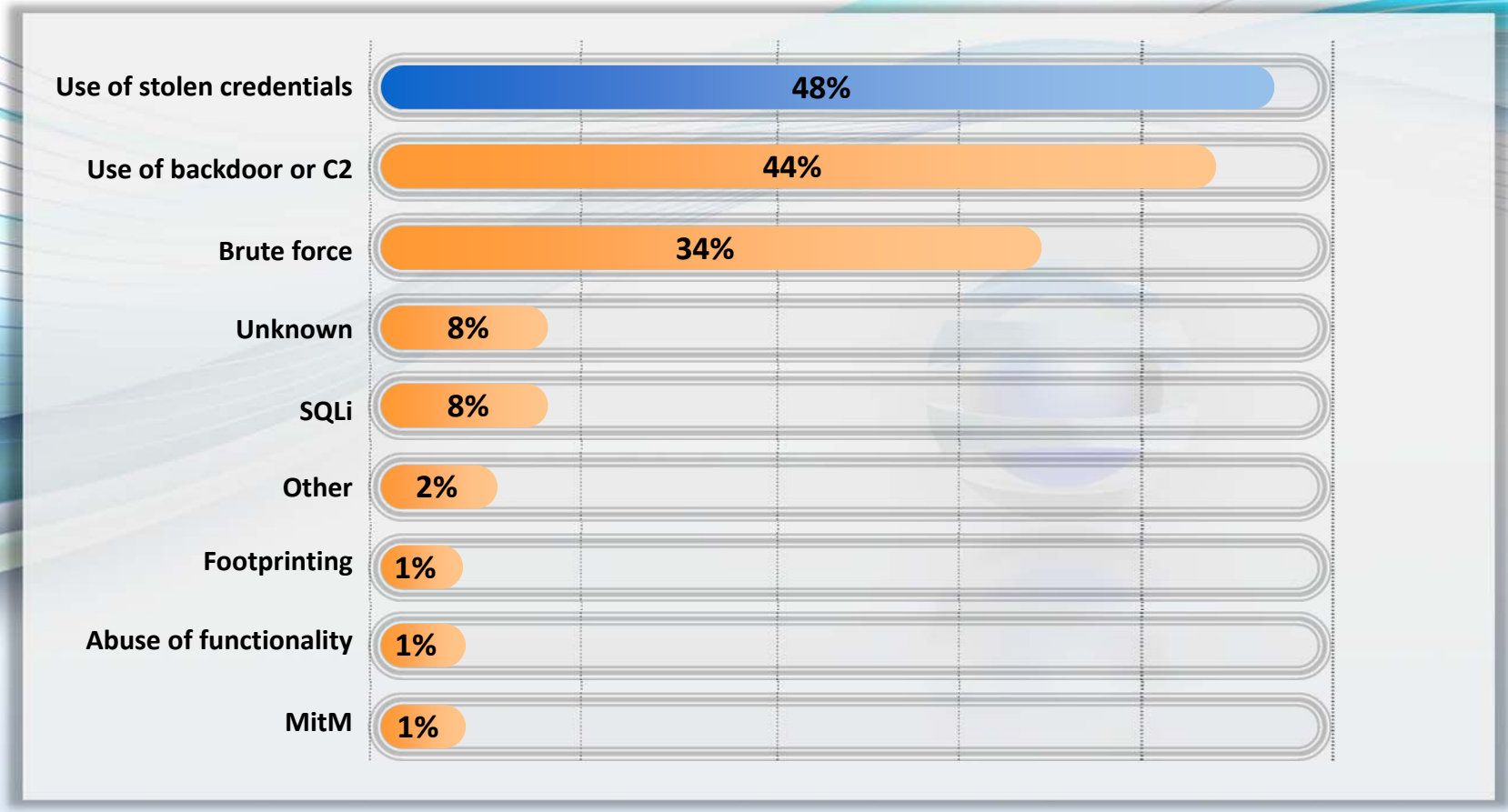
The US government alleges that the data was used for **fraudulent purposes**, including fraudulent tax returns, opening lines of credit and racking up bills in the names of victims.

Experian's senior vice president of government affairs, said at the hearing Experian **failed to perform due diligence** and stop Ngo's activities

How to ensure that the data security controls are enough or serving the purpose?

http://www.cnet.com

Hacking Methods by Percent of Breaches Within Hacking – 2013



http://www.verizonbusiness.com

Presentation Flow

The average annualized cost of cybercrime incurred per organization in 2013 was $11.56 million, with a range of $1.3 million to $58 million. This is an increase of 26 percent, or $2.6 million, over the average cost reported in 2012.

Ponemon Institute Research Report

Security News

July 22, 2013

Report: Cyber Crime Costs Global Economy Up to $500B a Year

Cyber evil doers are inflicting serious damage to the world's already-sluggish economy.

According to a newly-released report sponsored by McAfee, global cyber activity is costing up to **$500 billion each year**, which is almost as much as the estimated cost of drug trafficking.

In the U.S. alone, the report estimates that cyber crime is the catalyst behind the loss of as many as **500,000 jobs** as companies grapple with the loss of coveted intellectual property, confidential strategies that are snooped on, and suffer reputational harm.

"**Extracting value from the computers of unsuspecting companies and government agencies is a big business**," the 20-page report from McAfee and the Center for Strategic and International Studies says.

"These losses could just be the cost of doing business or they could be a major new risk for companies and nations as these illicit acquisitions damage global economic competitiveness and undermine technological advantage," the report said.

McAfee, which is a unit of Intel (INTC), and CSIS said their work is the first research to use actual economic modeling to forecast the financial costs of cyber crime.

http://www.foxbusiness.com

Security News

May 15, 2013

Internet Crime Cost Consumers More Than A Half-Billion Dollars Last Year

Number of cases reported by consumers to FBI-partnered Internet Crime Complaint Center increased by nearly **10 percent** last year, with scams in auto fraud, FBI impersonation via email, extortion at the top of the list

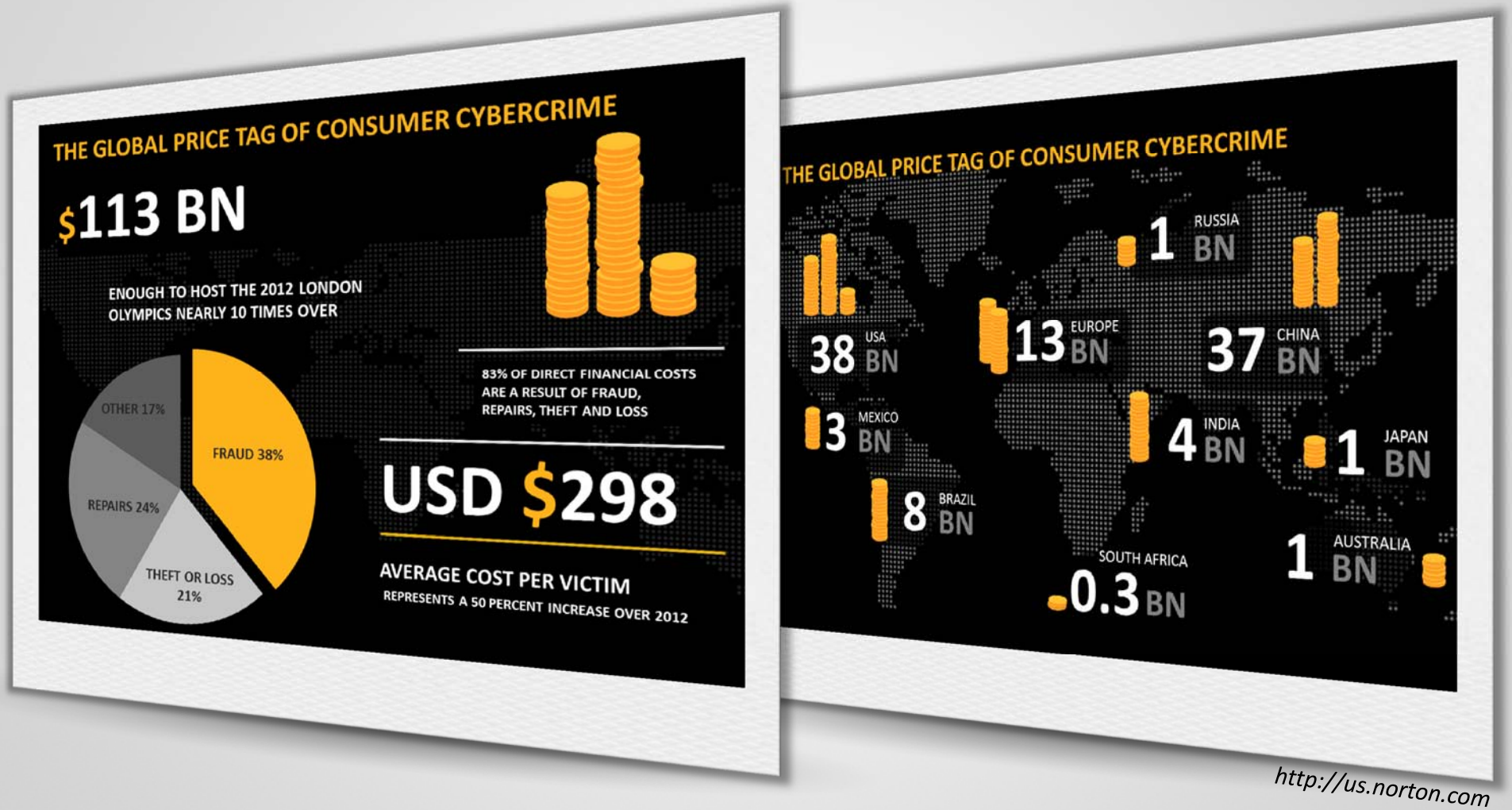
Consumers lost an average of **$1,800** last year in Internet crimes and a total of $535 million overall, according to the Internet Crime Complaint Center's (IC3) annual report on consumer complaints it received in 2012.

IC3, a partnership between the FBI, the National White Collar Crime Center, and the Bureau of Justice Assistance, **received 289,874 consumer complaints, 40% of which reported financial losses**. That was an 8.3 increase in the total number of complaints from 2011. The median dollar loss for consumers who reported financial loss to the IC3 was $600, and the average dollar loss for those who reported financial loss was $4,573.

The states where consumers reported crime most were California (13.41 percent), Florida (7.9 percent), Texas (7.22 percent), and New York (5.7 percent).

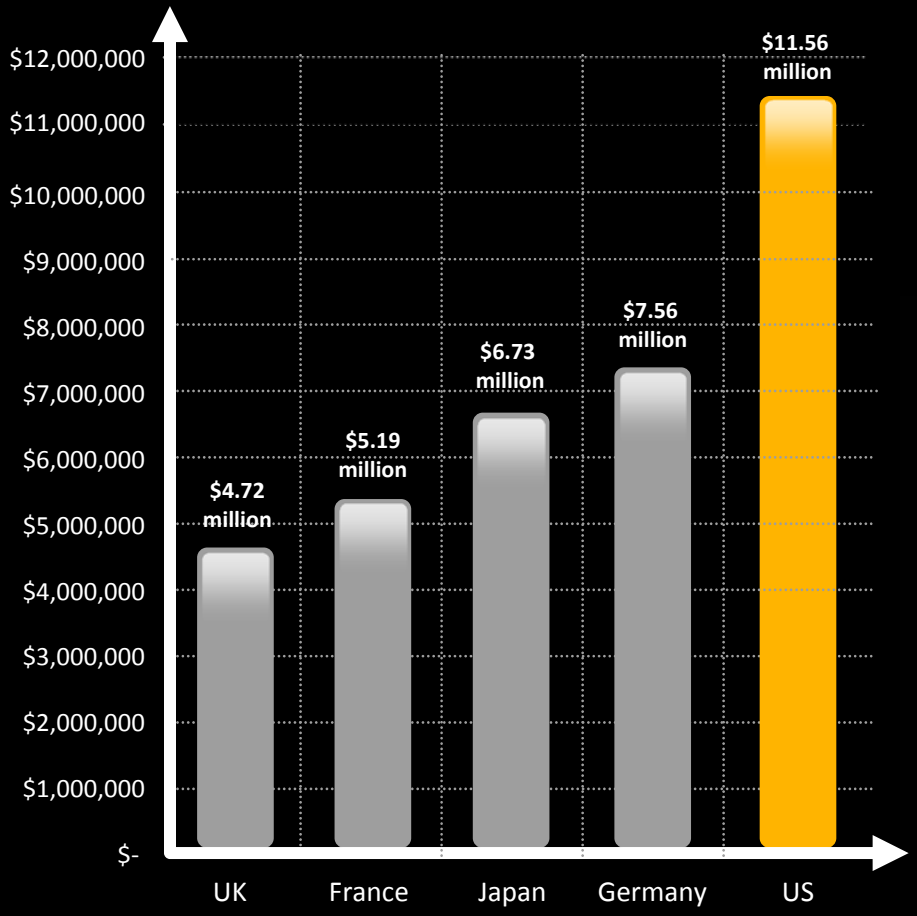
http://www.darkreading.com

2013 Norton Cybercrime Report



http://us.norton.com

Total Cost of Cyber Crime in Five Countries - 2013

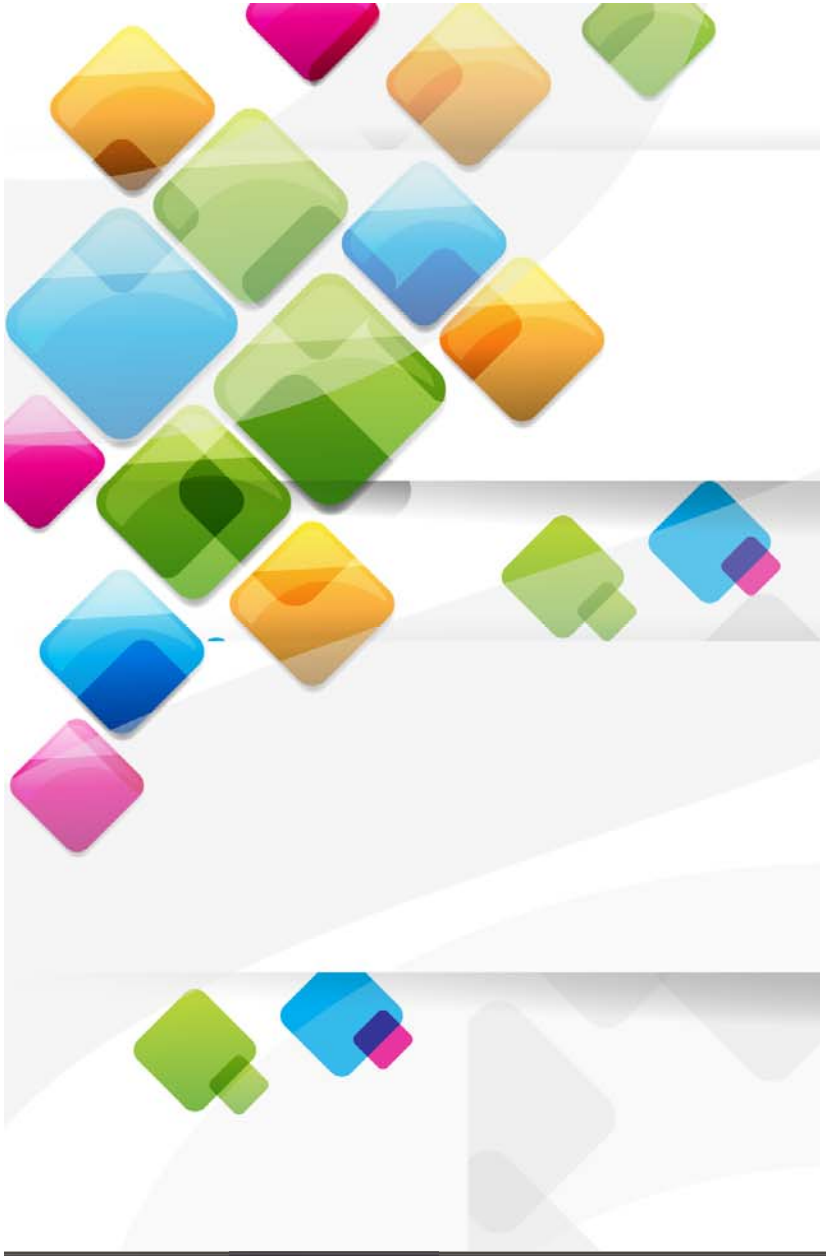


Cost expressed in US dollars, n = 234 separate companies

According to Ponemon Institute Research Report on the estimated average cost of cyber crime, the US sample reports the highest total average cost at

$11.56 million

Ponemon Institute Research Report



The **Chameleon botnets have targeted at least 202 Web sites**, hitting them with as little as **9 billion** ad impressions. The sites themselves are receiving 14 billion ad impressions, meaning the majority are coming from the botnet

But here's the crux of the issue: advertisers are paying the sites 69 cents per thousand ad impressions, believing that they're **legitimate**. The Chameleon botnet, therefore, is able to siphon **$6 million per month** in cash from the advertisers

http://news.cnet.com

Presentation Flow

The Pentagon plans to **triple its cyber security personal** over the next several years to bolster US national security, said Defense Secretary Chuck Hagel.

Speaking at what has been considered the *"first-ever live broadcast"* from the National Security Agency's headquarters at Ft. Meade, Maryland, Hagel said that an ongoing campaign to both recruit civilians as well as encourage military personal to retrain for the positions will see the number of *"cyber professionals"* reach 1,800 by year's end. By 2016, the Pentagon should have **6,000 cyber professionals**.

http://rt.com

Demand for Security and Big Data Experts Grows

A new survey by TEKsystems compares current market conditions to the state of spending, skills needs, and impact areas. The survey represents the views of 244 IT leaders including CIOs, CTOs and IT vice presidents, as well as IT directors and managers.

Heading into 2014, **62 percent** of IT leaders expected their IT budgets to increase, yet just **47 percent** now see this to be the case. The number of leaders whose budgets stayed the same increased from 26 to 38 percent. Those expecting decreases remained virtually unchanged, shifting less than 3 percent, from 12 to 15 percent.

Despite the reality of more IT leaders seeing flat budgets, the number of IT leaders who are confident in their IT department's ability to satisfy business demands has increased from **66 percent** at the end of 2013 to **72 percent** at the end of the first quarter of 2014. IT leaders expressing a neutral position decreased from 21 to 15 percent. Those that lack confidence in the ability to satisfy business demands have increased from 6 to 12 percent.

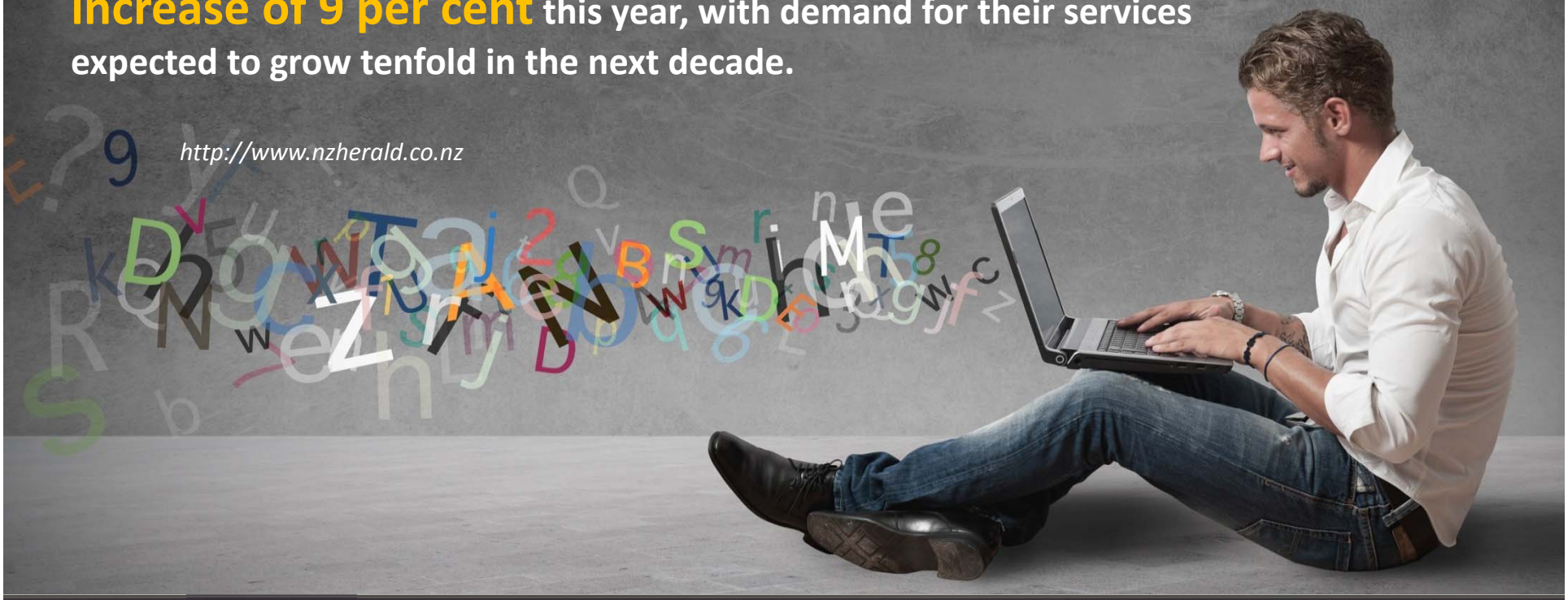
http://www.net-security.org

Huge Demand for IT Security Staff

Fears sparked by the likes of **WikiLeaks** and **Edward Snowden** mean information security staff are now among the most sought after professionals.

According to the **2014 Global Salary Survey**, released today, IT security staff who can "thoroughly review company security systems'' should expect a pay **increase of 9 per cent** this year, with demand for their services expected to grow tenfold in the next decade.

http://www.nzherald.co.nz



Penetration Test Skills in Demand

Hackers will try anything once to compromise a web site, server, network or application. The only way to stop this activity, which is usually organized crime, is to get in there first.

Think and act like a hacker and see what vulnerabilities you can find, before they do. This is **penetration testing**, and today it is required by many customers that have something to protect, whether it be customer data, financial information, intellectual property, or reputation.

Regulations such as the Sarbanes-Oxley Act, the Payment Card Industry Data Security Standard (PCI DSS), and the government's Code of Connection require networks, firewalls, databases, servers, applications, mobile devices and more to be checked thoroughly for vulnerabilities.

Penetration testers are in greater demand than ever.

Historically, testing was retrospective. You would build an application, device, network or web site and then let an ethical hacker throw everything he or she could at it, documenting any failures, ideally before anything was put live.

Today, many such specialists charge upwards of **£1000 per day**.

http://www.channelweb.co.uk

Security News

Skills in demand: Penetration testers

Skills in demand

Significant expansions of IT infrastructures have increased demand for experienced penetration testers to find security vulnerabilities in targeted apps, networks, and systems.

Skills in demand: Automation systems professionals

What it takes

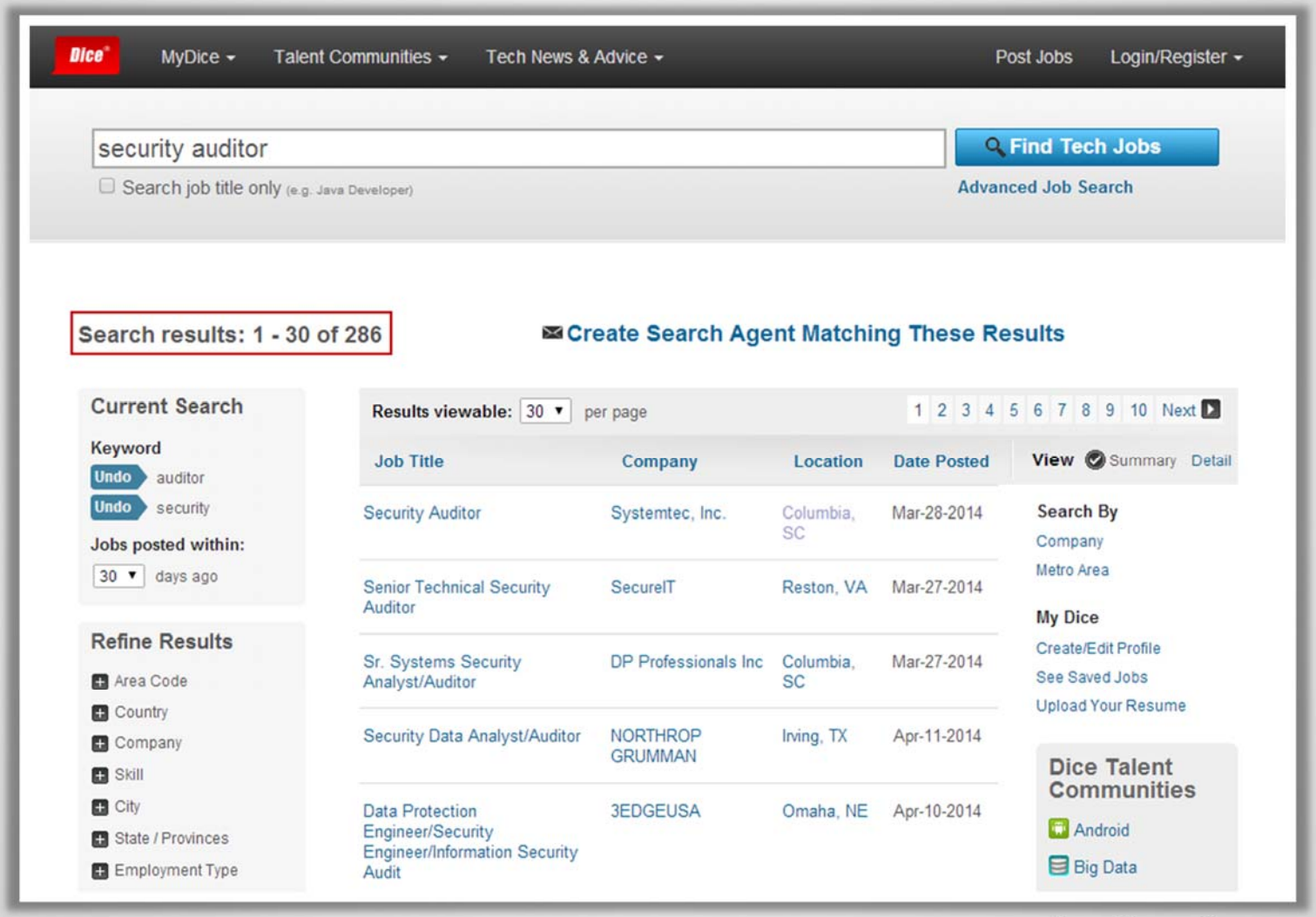
Hands-on experience with reverse engineering and scripting languages is helpful. Expertise in identifying flaws is critical. Designing creative solutions to complex problems, paired with stellar documentation and communication skills, are most valuable.

Compensation

Specialist-level roles start around $100K, with senior and lead often earning $110K to $130K.

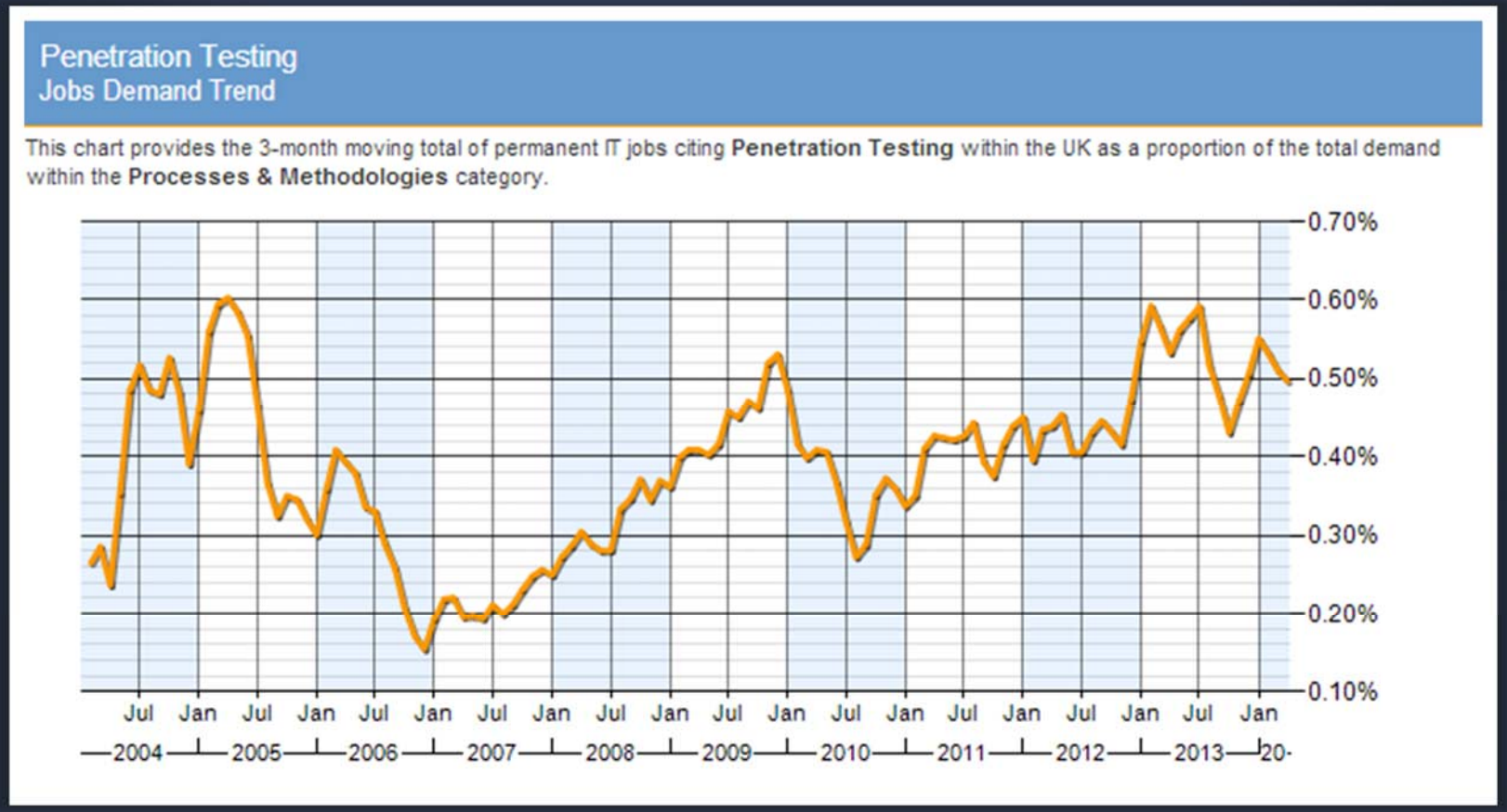
http://www.scmagazine.com

Industry Job Requirements for Security Analyst



http://www.dice.com

Penetration Testing Job Trends



http://www.itjobswatch.co.uk

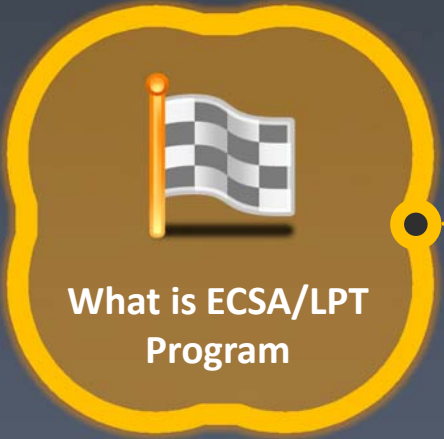
Penetration Tester Salary Trends

http://www.payscale.com

Location UK	3 months to 11 Apr 2014	Same period 2013	Same period 2012
Penetration Testing			
Rank	503	457	522
Rank change year-on-year	▼ -46	▲ +65	
Permanent jobs citing Penetration Testing	493	495	425
As % of all permanent IT jobs located in the UK	0.41%	0.44%	0.33%
As % of the Processes & Methodologies category	0.51%	0.56%	0.44%
Number of salaries quoted	392	328	325
Average salary	**£55,000**	£47,500	£44,000
Average salary % change year-on-year	+15.78%	+7.95%	
90% offered a salary of more than	£38,450	£35,000	£34,000
10% offered a salary of more than	£75,000	£66,500	£72,500
UK excluding London average salary	£50,500	£45,000	£40,000
% change year-on-year	+12.22%	+12.50%	
Processes & Methodologies Category UK			
Permanent IT job ads with a match in the **Processes & Methodologies** category	97525	88109	97313
As % of all permanent IT jobs located in the UK	80.44%	78.80%	76.54%
Number of salaries quoted	78221	72335	82780
Average salary	£47,500	£45,000	£47,500
Average salary % change year-on-year	+5.55%	-5.26%	
90% offered a salary of more than	£30,000	£30,000	£30,000
10% offered a salary of more than	£72,500	£75,000	£70,000
UK excluding London average salary	£42,500	£40,000	£40,000
% change year-on-year	+6.25%	-	

http://www.itjobswatch.co.uk

Presentation Flow



EC-Council Information Security
Certification Path

Ethical Hacking

CEH

Threat Agents

Discover and Exploit Vulnerabilities

Security Analysis

ECSA

Application of Methodology

Penetration Testing Framework

Penetration Testing

LPT

"So You Can Do It? .....Prove It"

Report Writing and Ethics

What is ECSA/LPT Program?

You know how to successfully attack fully patched and hardened systems and circumvent common security controls.

Do you lack the knowledge to correctly apply ethical hacking tools while effectively conducting a security analysis of your organization's network infrastructure?

You may be asking yourself, "Is that enough? **What's next?**"

The answer is **EC-Council Certified Security Analyst – Licensed Penetration Tester**

What is ECSA/LPT Program?

ECSA/LPT program is a **comprehensive**, standards-based, **methodological approach** to train and validate **IT security professional's Penetration Testing** and **Information System Security Auditing** capabilities

ECSA/LPT Program consists of two components:

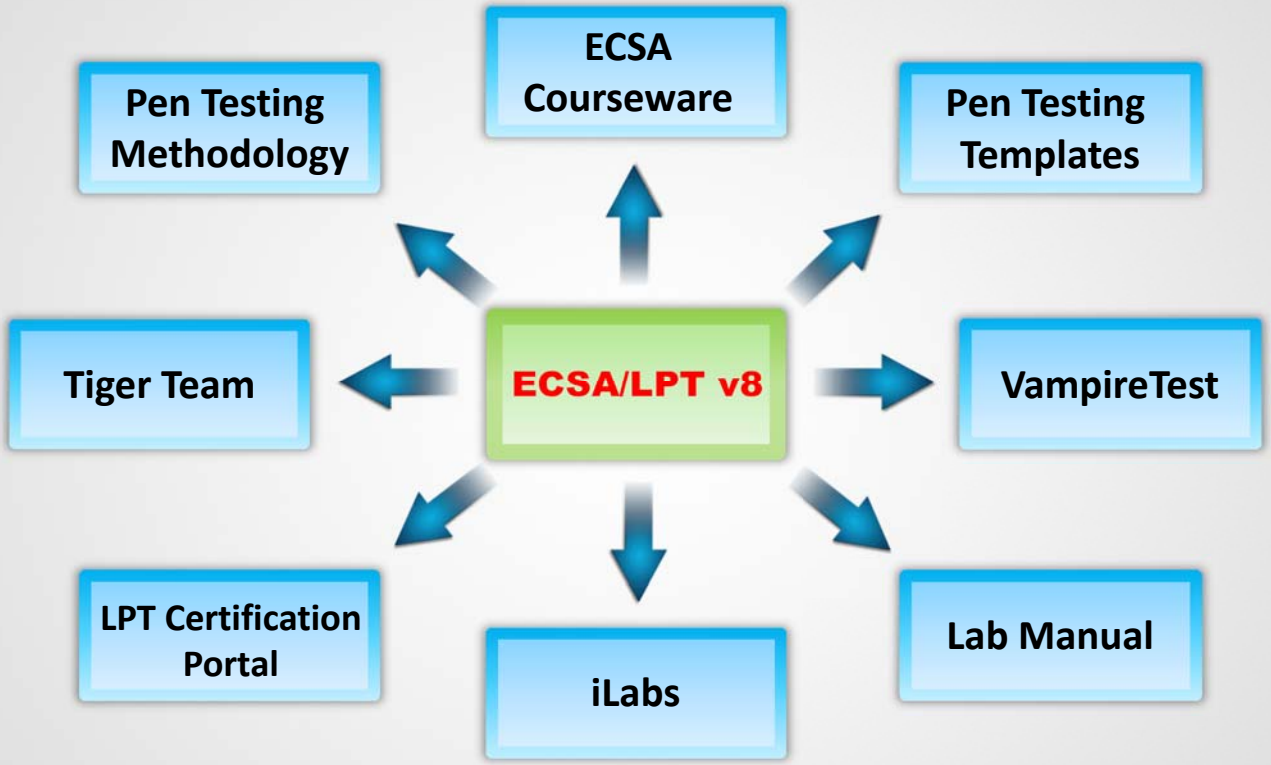
ECSA Training

- ECSA is a **5-day** complete hands-on training program
- It uses **simulated real-time scenarios** to train students in standard penetration testing methodologies

LPT Practical Exam

- LPT is a **online practical exam** designed to evaluate and validate students' pen testing skills

What is ECSA/LPT Program?

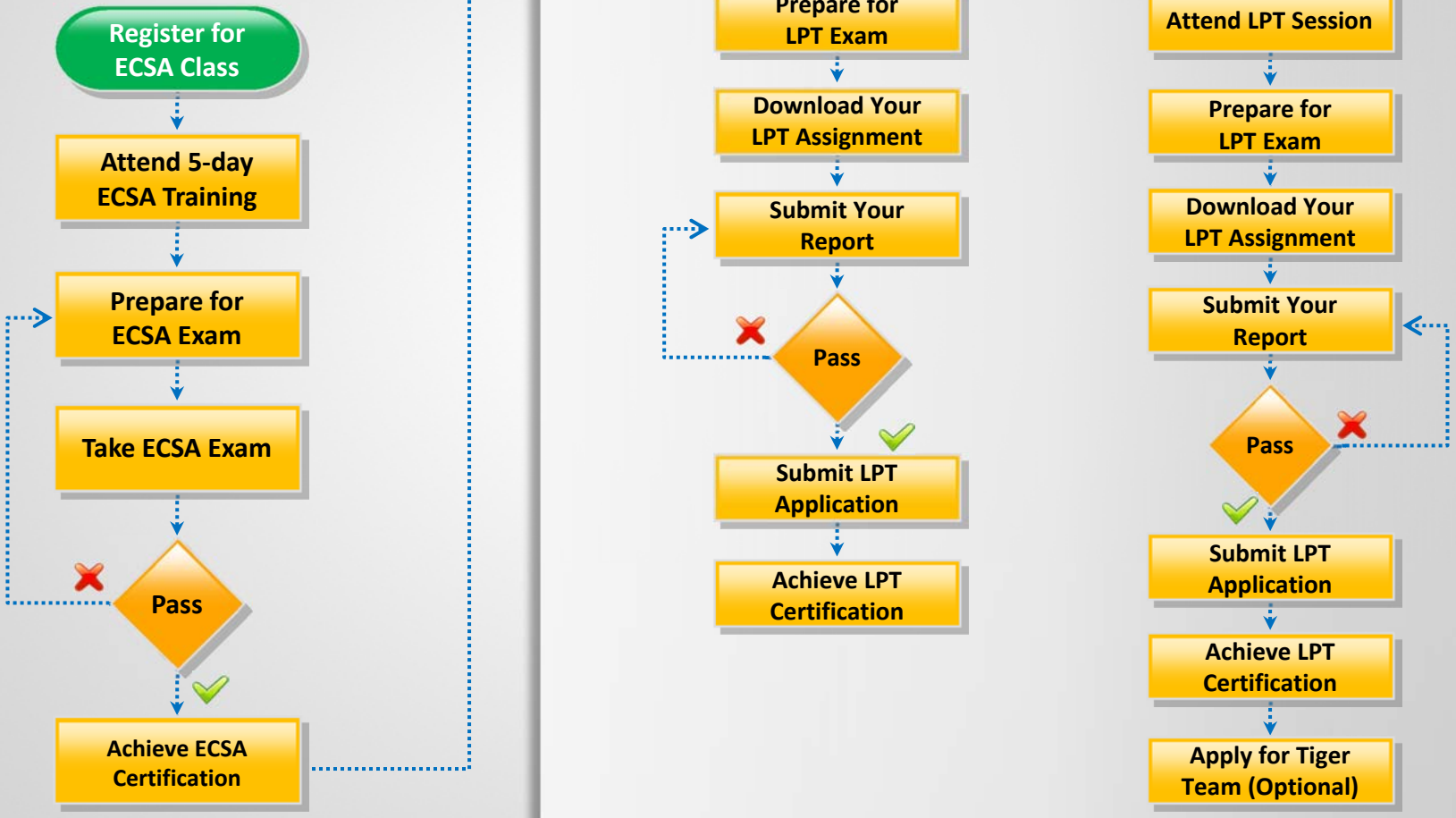


ECSA/LPT ecosystem contains a set of **pen testing standards**, **methodologies**, real-time simulated pen testing challenges, pen testing licence accreditation, **automated report writing suite**, and **reporting templates**

How Many Certificates will I Get

- ECSA/LPT program awards **two certificates** to successful candidates
- The ECSA certificate is provided on successfully passing the **online ECSA exam** and LPT credentials are provided upon meeting the requirements stated in **LPT application form**

ECSA/LPT Certification Track



Do I have to be CEH to Join ECSA/LPT

No. While the Certified Ethical Hacker (CEH) certification is not a prerequisite for the ECSA course, we strongly advise candidates to attain the CEH prior to the commencement of the ECSA course.

Can I Take the ECSA Training Only and Skip the LPT License

Yes. However, we strongly recommend candidates to pursue the Licensed Penetration Tester certification as it can be a major milestone in your career and establish you as a penetration tester and Information Security Auditor.

What is New in ECSA/LPTv8?

- Updated information for all penetration testing and security concepts
- Well organized content for a better understanding
- Classroom and instructor friendly
- Diagrammatic representation of concepts and pen testing process
- New penetration testing techniques and security tools
- Well tested lab to evaluate the presented concepts
- Detailed recommendation after each penetration testing steps

EC-Council Certified Security Analyst (ECSA)

What is ECSA

ECSA program is a comprehensive, standards-based, **methodology** intensive training program which teaches information security professionals to conduct real life **penetration tests** by utilizing EC-Council's published penetration testing methodology

The ECSA Program is a 5-day **complete hands-on training** program. This Penetration Testing training course uses real-time scenarios to train students in penetration testing methodologies

ECSA course will help you **master a documented penetration testing methodology** that is repeatable and that can be used in a penetration testing engagement, globally

Why ECSA is Best

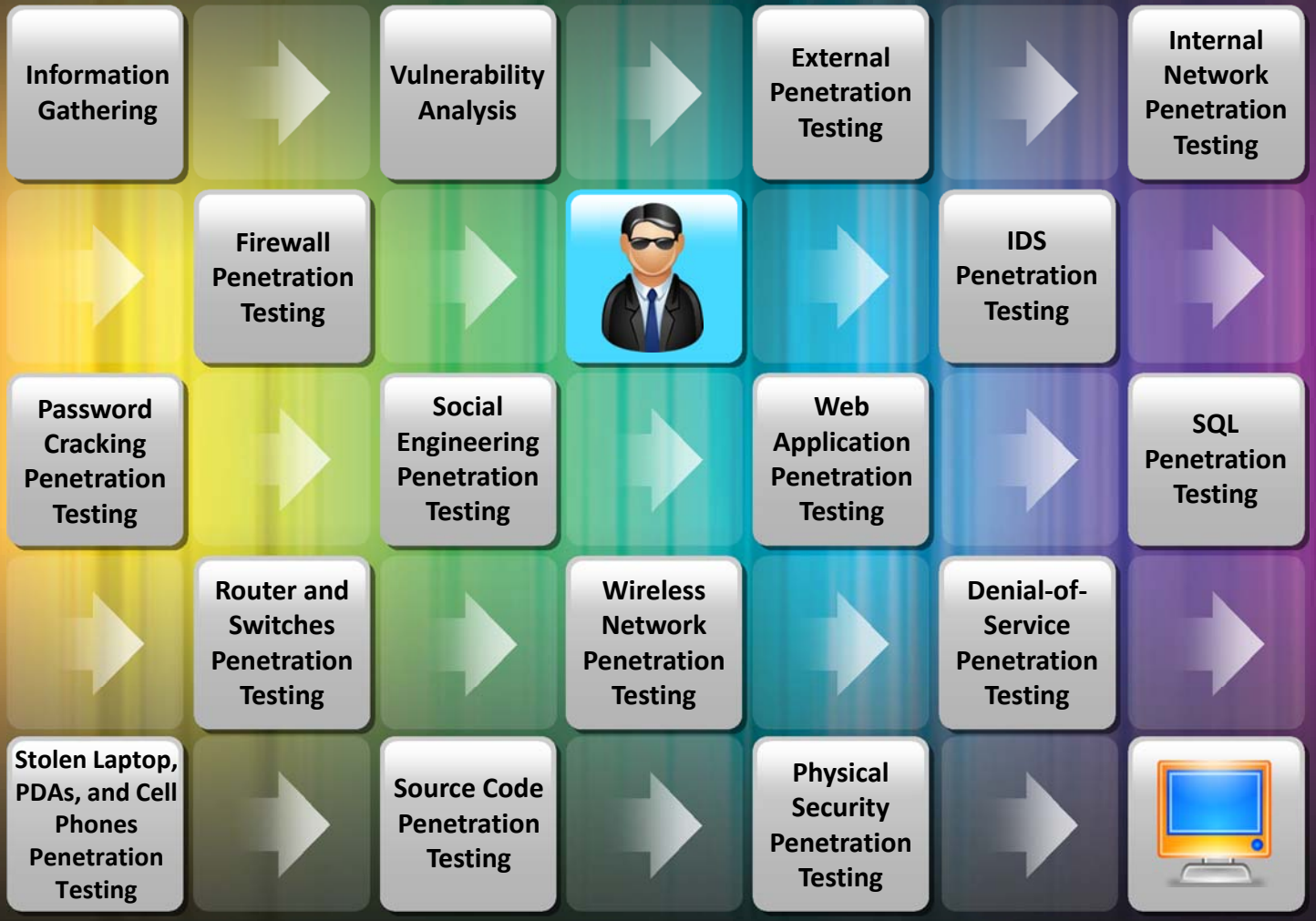
Presents industry accepted comprehensive pen testing (LPT) framework on **44 Domains**

Covers **advanced topics** such as mobile, cloud, and virtual machine pen testing

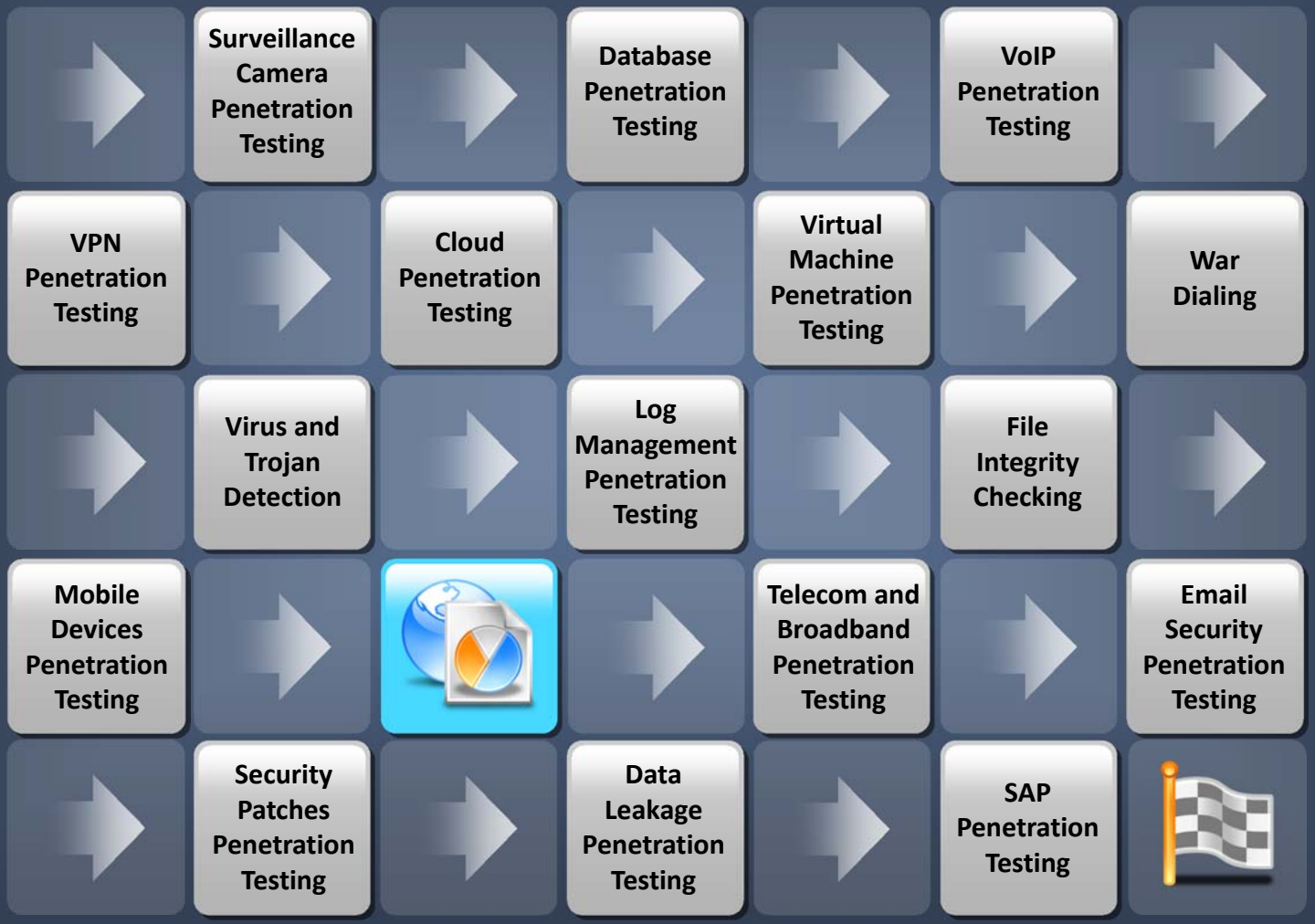
Covers all the requirements of National Information Assurance Training Standard For Information Systems Security Officers (**CNSS - 4014**) and National Training Standard for System Certifiers (**NSTISSI - 4015**)

Completely **maps to NICE's** Protect and Defend, Operate and Collect, and Analyze Specialty Area Category

What is LPT Framework



What is LPT Framework



Why LPT Framework

(What is not there in the Existing Frameworks)

Comprehensive

Open to all

Includes best of the open source pen testing frameworks such as OSSTMM and OWASP

References to proprietary frameworks

Target Audience

I. Network Server Administrators

II. Firewall Administrators

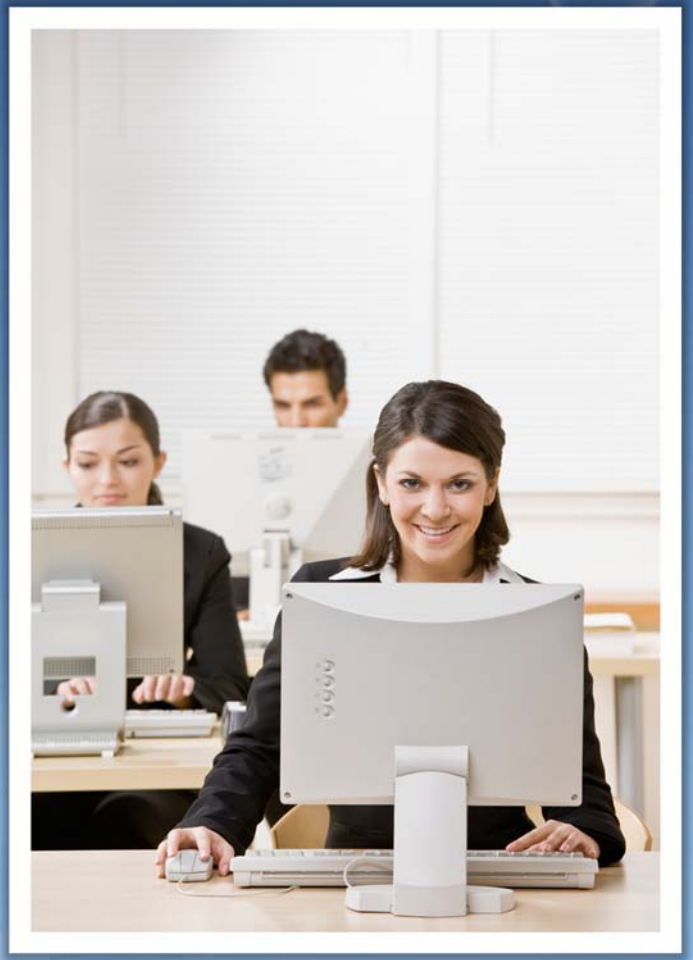
III. Information Security Testers

IV. System Administrators

V. Risk Assessment Professionals

Benefits of Becoming ECSA

- ECSA is for **experienced hands in the industry** and is backed by a curriculum designed by the best in the field
- Greater industry acceptance as **seasoned security professional**
- Learn to analyze the outcomes from using **security tools** and **security testing techniques**
- Requirement for the **LPT certification**



What is the Outline of ECSA

1. Need for Security Analysis
2. TCP IP Packet Analysis
3. Penetration Testing Methodologies
4. Customers and Legal Agreements
5. Rules of Engagement
6. Penetration Testing Planning and Scheduling
7. Pre-penetration Testing Steps
8. Information Gathering
9. Vulnerability Analysis
10. External Penetration Testing
11. Internal Network Penetration Testing
12. Firewall Penetration Testing
13. IDS Penetration Testing
14. Password Cracking Penetration Testing
15. Social Engineering Penetration Testing
16. Web Application Penetration Testing
17. SQL Penetration Testing
18. Penetration Testing Reports and Post Testing Actions

What is the Outline of ECSA - Self Study Modules

1. Router and Switches Penetration Testing
2. Wireless Network Penetration Testing
3. Denial-of-Service Penetration Testing
4. Stolen Laptop, PDAs and Cell Phones Penetration Testing
5. Source Code Penetration Testing
6. Physical Security Penetration Testing
7. Surveillance Camera Penetration Testing
8. Database Penetration Testing
9. VoIP Penetration Testing
10. VPN Penetration Testing
11. Cloud Penetration Testing
12. Virtual Machine Penetration Testing
13. War Dialing
14. Virus and Trojan Detection
15. Log Management Penetration Testing
16. File Integrity Checking
17. Mobile Devices Penetration Testing
18. Telecommunication and Broadband Communication Penetration Testing
19. Email Security Penetration Testing
20. Security Patches Penetration Testing
21. Data Leakage Penetration Testing
22. SAP Penetration Testing
23. Standards and Compliance
24. Information System Security Principles
25. Information System Incident Handling and Response
26. Information System Auditing and Certification

Note: Self study modules are available on ASPEN portal

Note: Check *www.eccouncil.org* for any changes

What Will You Learn?

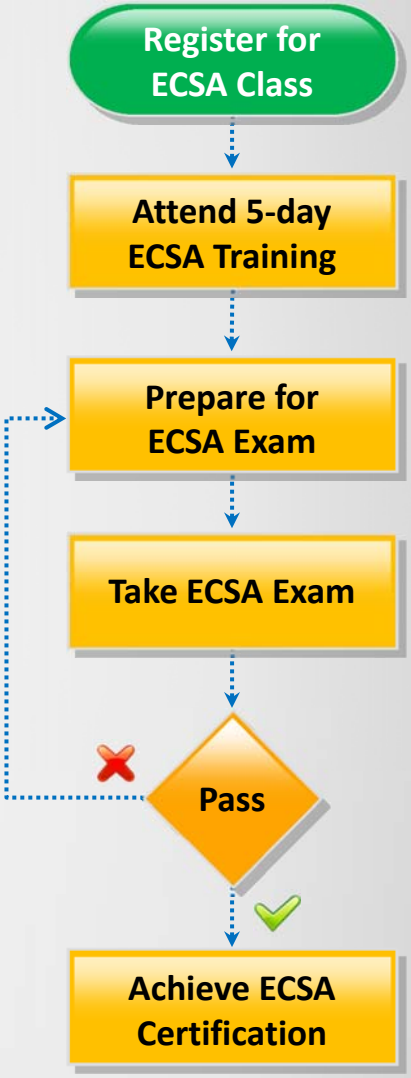
After successfully completing this course, the student will be able to:

- Understand the various elements of security concerns due to intrusions and also information **security standards and laws** to protect the data
- Develop the **penetration test plan** to perform external and internal network penetration testing in the organization
- Understand the various **components of the TCP/IP model** and its security
- Gather information about the target company, perform **vulnerability analysis** and list the areas that need testing and penetration
- Identify **what should be tested** and **which type of penetration testing** needs to perform
- Perform **Firewall**, **IDS**, **password cracking**, **social engineering**, **web application**, **SQL**, etc. penetration testing in the organization
- Prepare '**Rules of Behavior**' agreement that outlines the framework for external and internal penetration testing and **Rules of Engagement (ROE)** to overcome legal, federal, and policy-related restrictions
- Create a final **penetration testing report**

ECSA Exam Information

- Credit Towards Certification: ECSA
- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 hours
- Test Format: Multiple Choice
- Test Delivery: Prometric Prime / VUE / ECCEXAM

How to Become ECSA



Where can I Attend Training

We provide various training options for students such as:

- Ground Classes (Authorized Training Centers - ATC)
- Instructor-led Online Training (iClass)
- Self-paced Online Training (iLearn)

For more information, visit the webpage http://www.eccouncil.org/Training

Job Roles for ECSA

- Perform network and application **penetration testing** using both automated and manual techniques
- Design/perform audits of computer systems to ensure they are operating securely and that data is **protected from both internal and external attacks**
- Assess assigned system to determine **system security status**
- Design and recommend **security policies** and procedures
- Ensure **compliance** to policies and procedures

- Evaluate highly complex security systems according to industry best practices to **safeguard internal information systems and databases**
- Lead investigations of **security violations and breaches** and recommend solutions; prepare reports on intrusions as necessary and provide an analysis summary for management
- **Respond to more complex queries** and request for computer security information and report from both internal and external customers

ECSAv4 and ECSAv8
Version Comparison

Module Comparison of ECSAv4 with ECSAv8

- IT security is often allocated a small portion of **overall IT budgets** (on average, less than 3%)

The topics highlighted in red under **ECSAv8 Module 01: Need for Security Analysis** are the new additions

ECSAv4 Module 01: Need for Security Analysis

- Computer Security Concerns
- Greatest Challenges of Security
- Assessment Questions
- Information Security Awareness
- Types of Security Policies
- Sample Policies
- Fair and Accurate Credit Transactions Act of 2003 (FACTA)
- Information Security Standards
- Information Security Acts and Laws
- Health Insurance Portability and Accountability Act (HIPAA)
- Interception of Communications

ECSAv8 Module 01: Need for Security Analysis

- Computer Security Concerns
- Greatest Challenges of Security
- Data Security Measures
- Assessment Questions
- Security Limit
- Hardening Security
- Information Security Awareness
- Types of Security Policies
- Sample Policies (7 More Added)
- Fair and Accurate Credit Transactions Act of 2003 (FACTA)
- Information Security Standards (2 More Added)
- Information Security Acts and Laws
- Health Insurance Portability and Accountability Act (HIPAA)
- Interception of Communications

Module Comparison of ECSAv4 with ECSAv8

- TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that define the **communication in an IP-based network**

The topics highlighted in red under **ECSAv8 Module 02: TCP IP Packet Analysis** are the new additions

ECSAv4 Module 03: TCP IP Packet Analysis

- TCP/IP Model
- Comparing OSI and TCP/IP
- TCP/IP Connection
- Three-Way Handshake
- Flow Control
- Windowing
- Introduction to IPv6
- IPv4/IPv6 Transition Mechanisms
- TCP/IP Security
- IPsec
- ICMP and ICMP Control Messages

ECSAv8 Module 02: TCP IP Packet Analysis

- TCP/IP Model
- Comparing OSI and TCP/IP
- TCP/IP Connection
- Three-Way Handshake
- Flow Control
- Windowing
- TCP Services
- Introduction to IPv6
- IPv4/IPv6 Transition Mechanisms
- IPv6 Address Notation
- IPv4 vs. IPv6
- TCP/IP Security
- IPsec
- DNSSec
- ICMP and ICMP Control Messages
- TCP/IP in Mobile Communications

Module Comparison of ECSAv4 with ECSAv8

- Penetration testing is a method of **actively evaluating the security of an information system or network** by simulating an attack from a malicious source

The topics highlighted in red under **ECSAv8 Module 03: Penetration Testing Methodologies** are the new additions

LPTv4 Module 11: Penetration Testing Methodologies

- What Is Penetration Testing?
- Why Penetration Testing?
- Common Penetration Testing Techniques
- Types of Penetration Testing
- Penetration Testing Process
- Phases of Penetration Testing
- Penetration Testing Methodology
- Penetration Testing Strategies
- Operational Strategies for Security Testing
- ROI on Penetration Testing
- Guidelines for Security Checking
- Required Skill Sets of a Penetration Tester
- Responsibilities of a Penetration Tester

ECSAv8 Module 03: Penetration Testing Methodologies

- What Is Penetration Testing?
- Why Penetration Testing?
- Constraints of Penetration Testing
- Common Penetration Testing Techniques
- Types of Penetration Testing
- Penetration Testing Process
- Phases of Penetration Testing
- Penetration Testing Methodology
- Penetration Testing Strategies
- Operational Strategies for Security Testing
- ROI on Penetration Testing
- Guidelines for Security Checking
- Required Skill Sets of a Penetration Tester
- Responsibilities of a Penetration Tester
- Penetration Tester Salary Trend
- Ethics of a Licensed Penetration Tester
- Communication Skills of a Penetration Tester

Module Comparison of ECSAv4 with ECSAv8

- Penetration 'Rules of Behavior' is a **penetration testing agreement** that outlines the framework for external and internal penetration testing

The topics highlighted in red under **ECSAv8 Module 04: Customers and Legal Agreements** are the new additions

LPTv4 Module 12: Customers and Legal Agreements

- Why Do Organizations Need Pen Testing?
- Initial Stages in Penetration Testing
- Penetration Testing 'Rules of Behavior'
- Penetration Testing Risks
- Penetration Testing by Third Parties
- Legal Issues in Penetration Testing
- Get Out of Jail Free Card
- Confidentiality and NDA Agreements
- Pen Testing Contract
- Drafting Contracts
- Sample Penetration Testing Contract
- Liability Issues
- Negligence Claim
- How Much to Charge?

ECSAv8 Module 04: Customers and Legal Agreements

- Why Do Organizations Need Pen Testing?
- Initial Stages in Penetration Testing
- Penetration Testing 'Rules of Behavior'
- Penetration Testing Risks
- Penetration Testing by Third Parties
- Legal Issues in Penetration Testing
- Get Out of Jail Free Card
- Confidentiality and NDA Agreements
- Pen Testing Contract
- Drafting Contracts
- Sample Penetration Testing Contract
- Liability Issues
- Negligence Claim
- Limitations of the Contract
- How Much to Charge?
- How to Reduce the Cost of Penetration Testing

Module Comparison of ECSAv4 with ECSAv8

- Rules of engagement (ROE) is the **formal permission** to conduct penetration testing. It helps testers to **overcome legal, federal, and policy-related restrictions** to use different penetration testing tools and techniques

The topics highlighted in red under **ECSAv8 Module 05: Rules of Engagement** are the new additions

LPTv4 Module 13: Rules Of Engagement

- Rules of Engagement (ROE) between an Organization and Penetration Testers
- Scope of ROE
- Steps for Framing ROE
- Clauses in ROE

ECSAv8 Module 05: Rules of Engagement

- Rules of Engagement (ROE) between an Organization and Penetration Testers
- Statement of Work (SOW)
- Scope of ROE
- Points of Contact Template
- Steps for Framing ROE
- Review Engagement Letter
- Clauses in ROE
- Rules of Engagement Template (Sample)

Module Comparison of ECSAv4 with ECSAv8

- A penetration test plan will establish the **ground rules, limits, and scope of testing**. It enhances the probability of **achieving good results** while conducting a penetration test

The topics highlighted in red under **ECSAv8 Module 06: Penetration Testing Planning and Scheduling** are the new additions

LPTv4 Module 14: Penetration Testing Planning and Scheduling

- Test Plan and Its Purpose
- Building a Penetration Test Plan
- Test Plan Identifier and Test Deliverables
- Penetration Testing Planning Phase
- Define the Pen Testing Scope and Project Scope
- Penetration Testing Teams
- Tiger Team
- Kickoff Meeting
- Penetration Testing Project Plan
- Project Plan Overview
- Work Breakdown Structure
- Project Scheduling Tools

ECSAv8 Module 06: Penetration Testing Planning and Scheduling

- Test Plan and Its Purpose
- Content of a Test Plan
- Building a Penetration Test Plan
- Test Plan Identifier and Test Deliverables
- Penetration Testing Planning Phase
- Define the Pen Testing Scope and Project Scope
- Penetration Testing Teams
- Tiger Team
- Kickoff Meeting
- Penetration Testing Project Plan
- Project Plan Overview
- Work Breakdown Structure
- Project Scheduling Tools
- Penetration Testing Hardware/Software Requirements

Module Comparison of ECSAv4 with ECSAv8

The topics highlighted in red under **ECSAv8 Module 07: Pre-penetration Testing Steps** are the new additions

LPTv4 Module 15: Pre Penetration Testing Checklist

- Examine the Client Organization's Penetration Testing Requirements
- Analyze Detailed Proposal of Test and Services
- Identify the Type of Testing: Black Box or White Box
- Examine the Servers, Workstations, Desktops, and Network Devices
- Obtain Liability Insurance from a Local Insurance Firm
- Gather Information about the Client's Organization
- Hardware and Software Requirements for the Penetration Testing Project
- Identify How the Final Penetration Testing Report Will Be Delivered

ECSAv8 Module 07: Pre-penetration Testing Steps

- Examine the Client Organization's Penetration Testing Requirements
- Analyze Detailed Proposal of Test and Services
- Identify the Type of Testing: Black Box or White Box
- Examine the Servers, Workstations, Desktops, and Network Devices
- Obtain Liability Insurance from a Local Insurance Firm
- Introduction to Tiger Team
- Gather Information about the Client's Organization
- Hardware and Software Requirements for the Penetration Testing Project
- List the Known Waivers/Exemptions
- Identify How the Final Penetration Testing Report Will Be Delivered

Module Comparison of ECSAv4 with ECSAv8

- Information gathering refers to **uncovering and collecting as much information** as possible about a target company. Competitive intelligence helps a company in identifying how much information can be extracted by hackers using the Internet

The topics highlighted in red under **ECSAv8 Module 08: Information Gathering** are the new additions

LPTv4 Module 16: Information Gathering

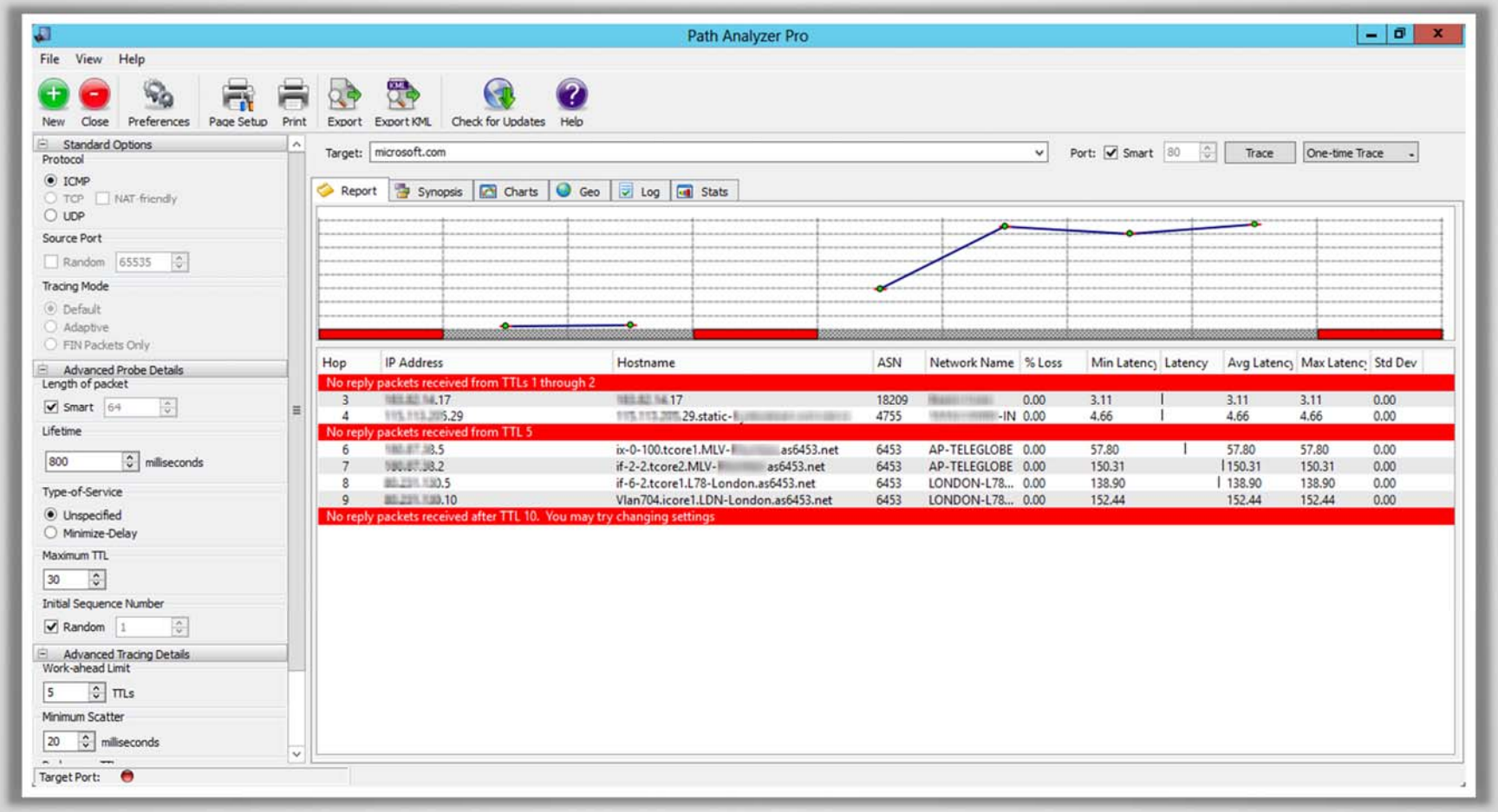
- What Is Information Gathering?
- List Employees of the Company
- Search for Link Popularity of the Company's Website
- List the Company's Partners and Distributors
- Visit the Company as Inquirer and Extract Privileged Information
- Look Up Registered Information in Whois Database

ECSAv8 Module 08: Information Gathering

- What Is Information Gathering?
- Information Gathering Terminologies
- Find the Company's URL
- Search for Company's Information
- List Employees of the Company
- Use People Search Online Services to Collect the Information
- Search for Link Popularity of the Company's Website
- Gather Competitive Intelligence
- List the Company's Partners and Distributors
- Visit the Company as Inquirer and Extract Privileged Information
- Look Up Registered Information in Whois Database
- Extract DNS Information Using Domain Research Tools
- Locate the Network Range
- Track Email Communications

Major Tools Covered: Path Analyzer Pro

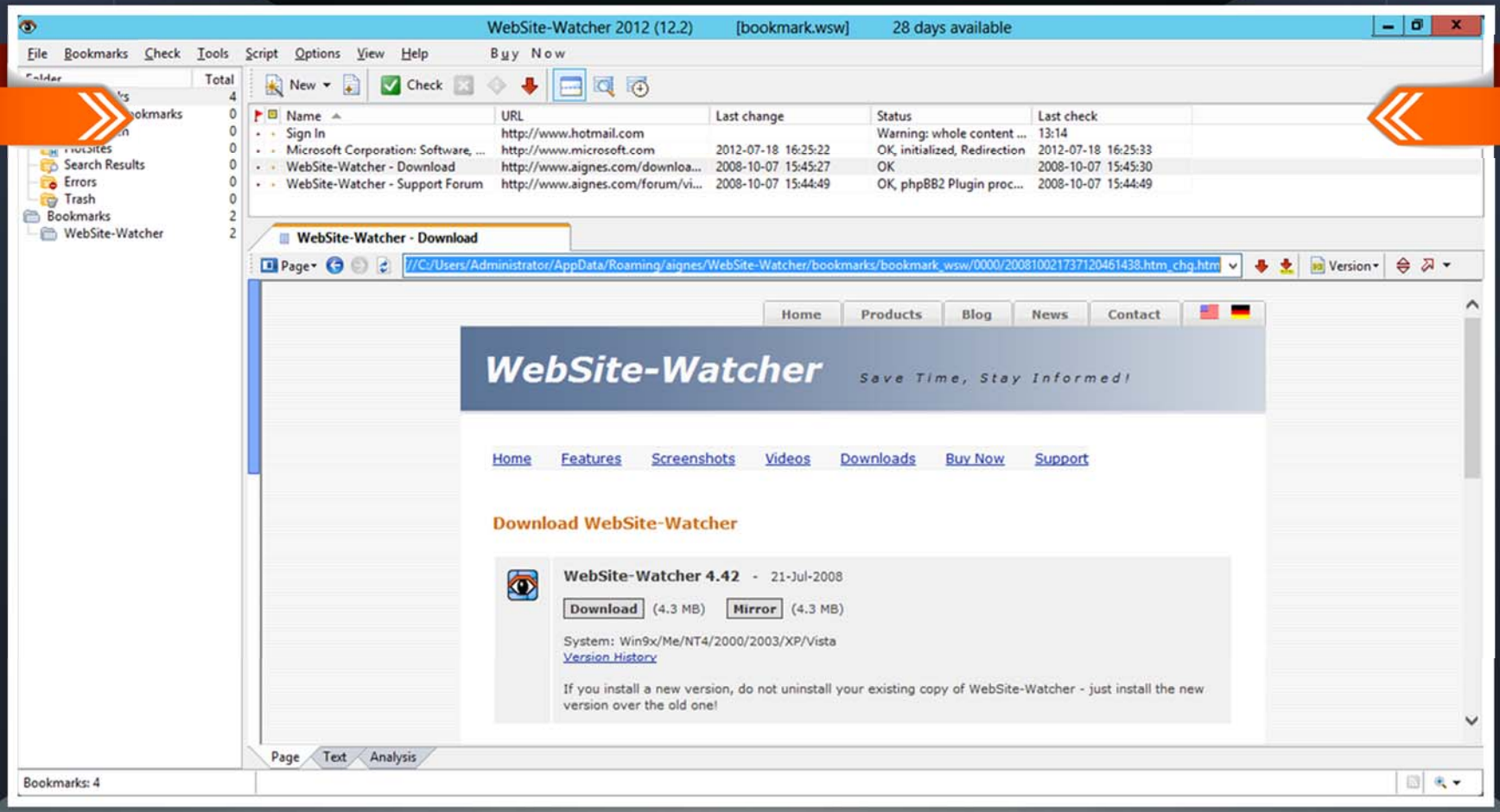
- Use Path Analyzer Pro to get the DNS, Whois, and **network resolution** information



http://www.pathanalyzer.com

Major Tools Covered: Website Watcher

- Website Watcher automatically checks web pages for updates and changes
- It allows you to monitor new pages, postings, RSS feeds, and newsgroups



http://aignes.com

Module Comparison of ECSAv4 with ECSAv8

- Vulnerability assessment is an **examination of the ability of a system or application**, including current security procedures and controls, to withstand assault

The topics highlighted in red under **ECSAv8 Module 09: Vulnerability Analysis** are the new additions

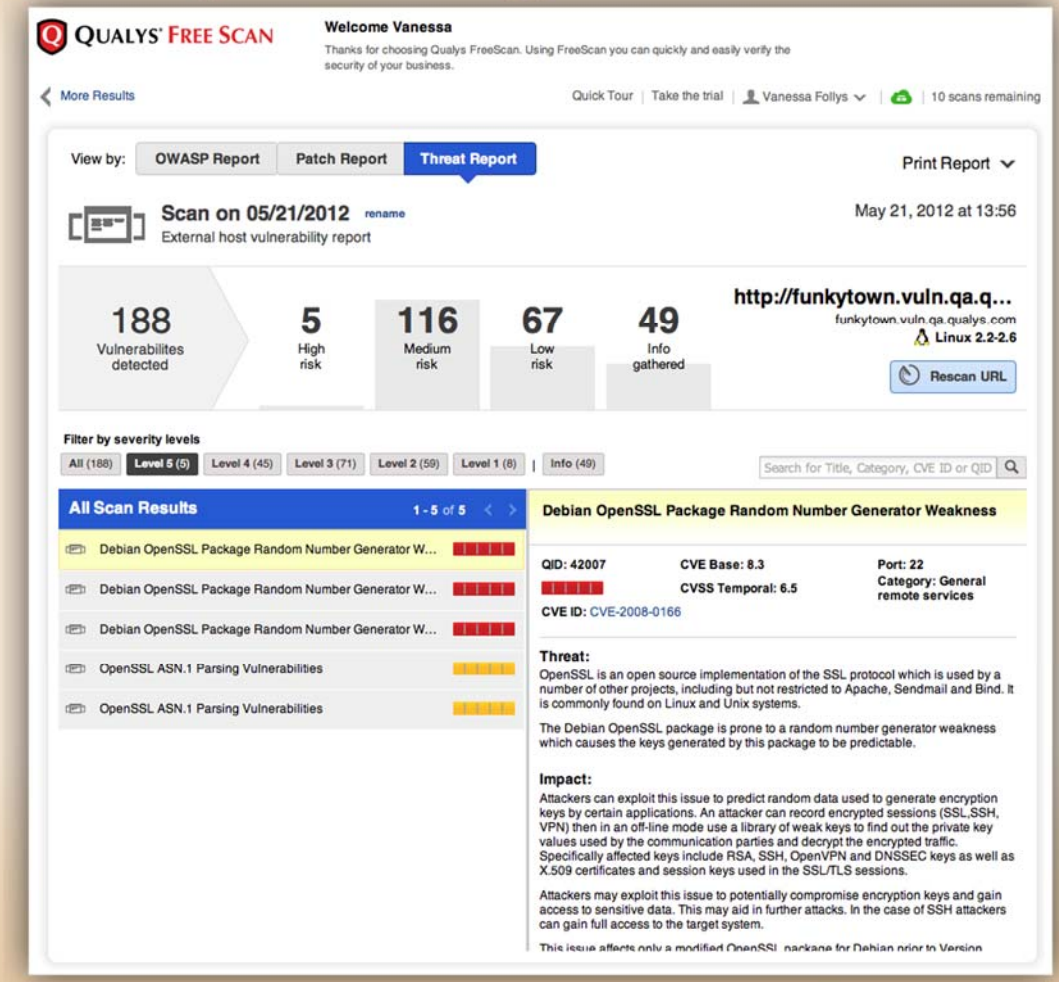
LPTv4 Module 17: Vulnerability Analysis

- What Is Vulnerability Assessment?
- Why Assessment
- How to Conduct a Vulnerability Assessment?
- Types of Vulnerability Assessment
- Vulnerability Assessment Phases
- Vulnerability Analysis Stages
- Vulnerability Assessment Considerations
- Types of Vulnerability Assessment Tools
- Criteria for Choosing a Vulnerability Assessment Tool
- Report

ECSAv8 Module 09: Vulnerability Analysis

- What Is Vulnerability Assessment?
- Why Assessment
- How to Conduct a Vulnerability Assessment?
- Types of Vulnerability Assessment
- Vulnerability Assessment Phases
- Vulnerability Analysis Stages
- Vulnerability Assessment Considerations
- Sample Vulnerability Assessment Report
- Types of Vulnerability Assessment Tools
- Criteria for Choosing a Vulnerability Assessment Tool
- Report
- AVDS - Automated Vulnerability Detection System
- Vulnerability Analysis Chart

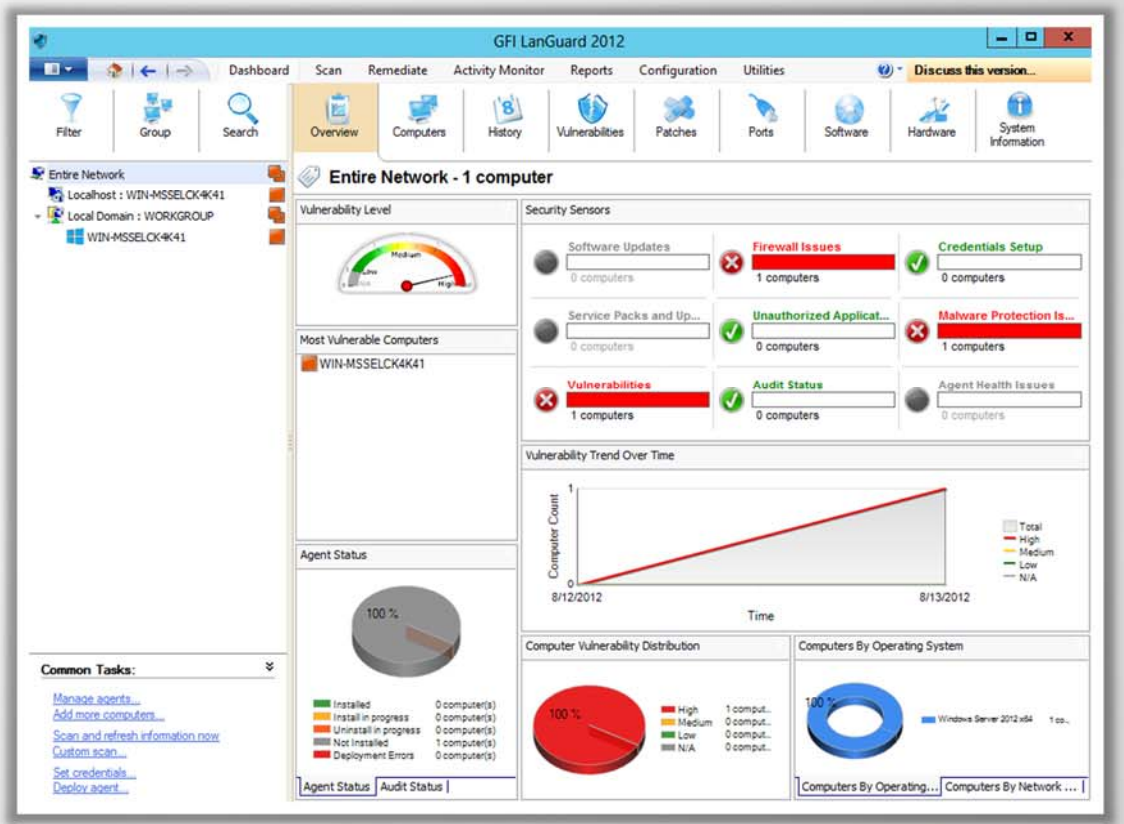
Major Tools Covered: QualysGuard Vulnerability Management



http://www.qualys.com

Major Tools Covered: GFI LANGuard

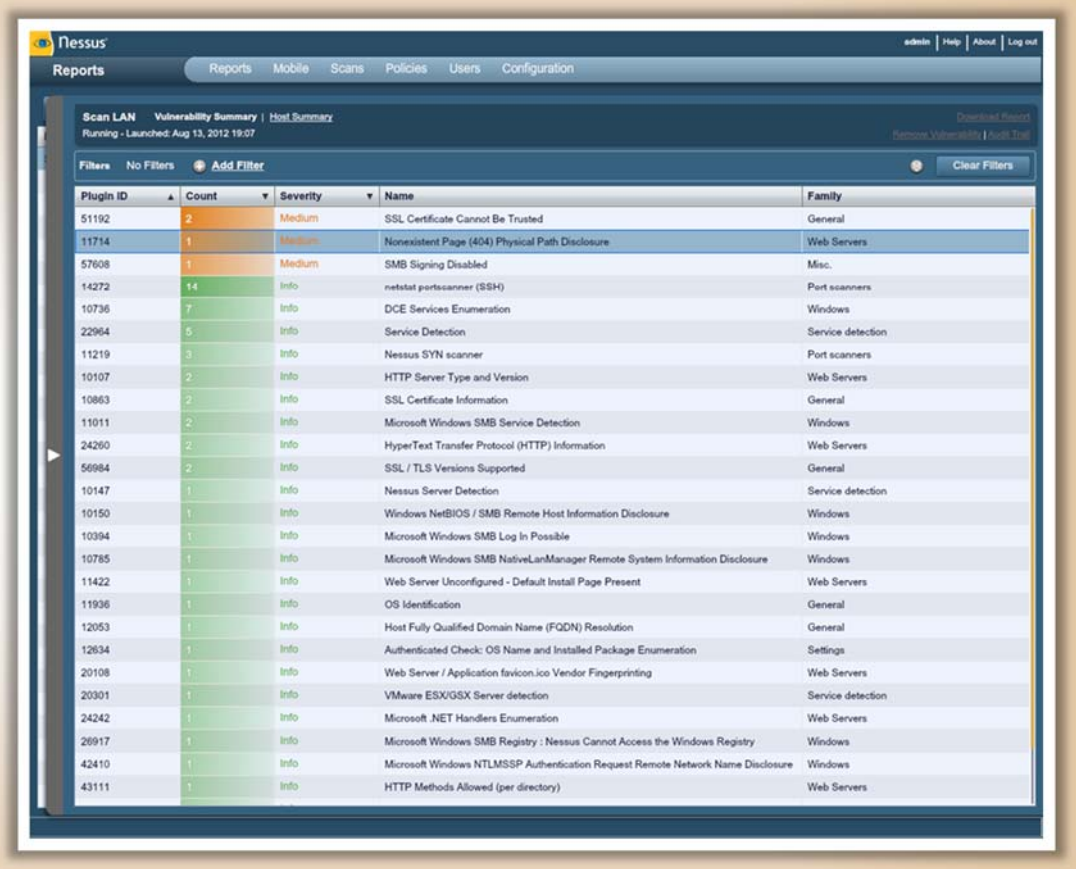
- GFI LANGuard scans the **network** and **ports** to detect, assess, and correct security vulnerabilities with minimal administrative effort
- It assists you in patch management, vulnerability assessment, network and software auditing, asset inventory, change management, risk analysis, and compliance



http://www.gfi.com

Major Tools Covered: Nessus

- Nessus allows you to **remotely audit a given network** and determine if it has been broken into or misused in some way
- It also provides the **ability to locally audit a specific machine** for vulnerabilities, compliance specifications, content policy violations, and more
- **Features:**
  - Agentless auditing
  - Compliance checks
  - Content audits
  - High-speed vulnerability discovery
  - In-depth assessments
  - Scan scheduling & enhanced reporting



http://www.tenable.com

Module Comparison of ECSAv4 with ECSAv8

- An external intrusion test and analysis identifies security **weaknesses and strengths of the client's systems and networks** as they appear from outside the client's security perimeter, usually from the Internet

The topics highlighted in red under **ECSAv8 Module 10: External Penetration Testing** are the new additions

LPTv4 Module 18: External Penetration Testing

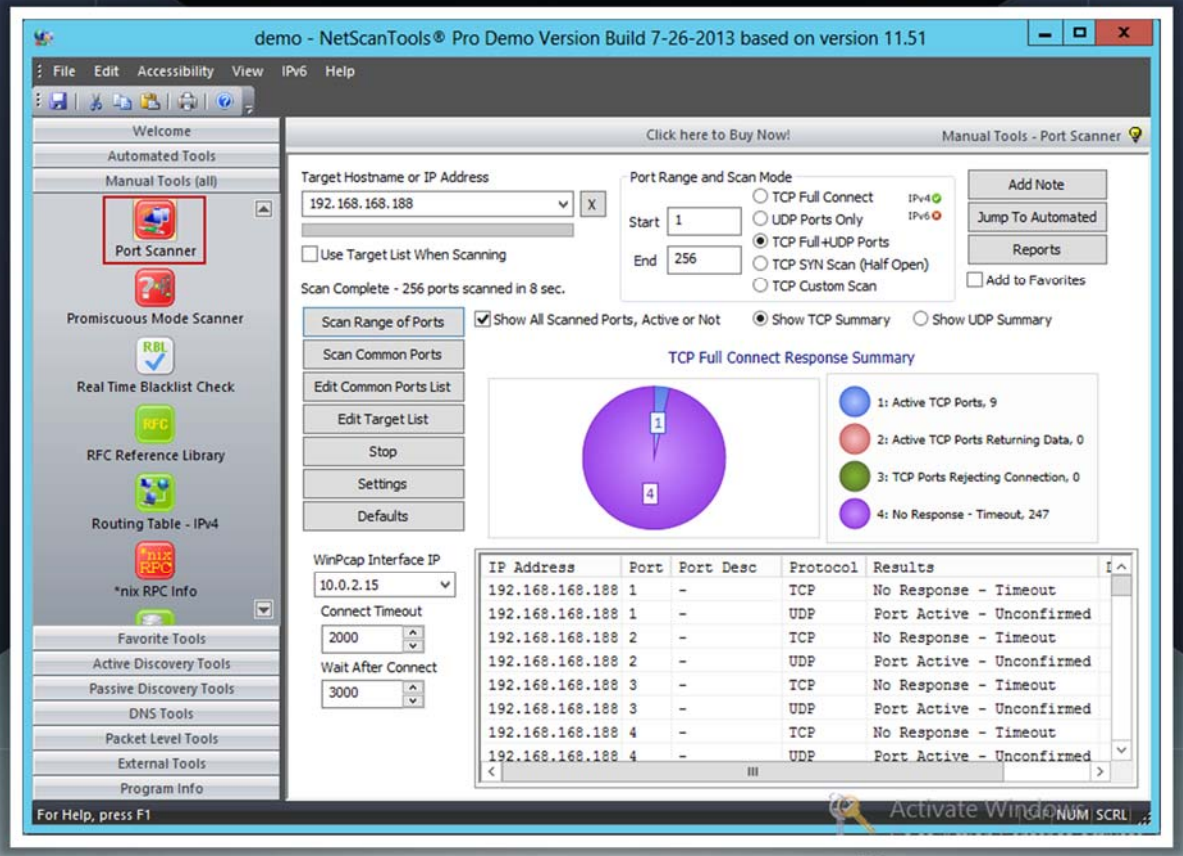
- External Intrusion Test and Analysis
- External Penetration Testing
- Steps for Conducting External Penetration Testing
- Create Topological Map of the Network
- Port Scan Every Port (65,536) on the Target's Network
- Perform Scanning on the Target and See the Response
- Attempt URL Encodings on the Web Pages
- Try Various SQL Injection Techniques
- Grab the Banner of Various Servers
- OS Fingerprint Target Servers
- Test for Various Ports

ECSAv8 Module 10: External Penetration Testing

- External Intrusion Test and Analysis
- External Penetration Testing
- Steps for Conducting External Penetration Testing
- Create Topological Map of the Network
- Look Up Domain Registry for IP Information
- Port Scan Every Port (65,536) on the Target's Network
- Perform Scanning on the Target and See the Response
- Attempt URL Encodings on the Web Pages
- Try Various SQL Injection Techniques
- Grab the Banner of Various Servers
- OS Fingerprint Target Servers
- Test for Various Ports
- Recommendations to Protect Your System from External Threats

Major Tools Covered: NetScan Tools Pro

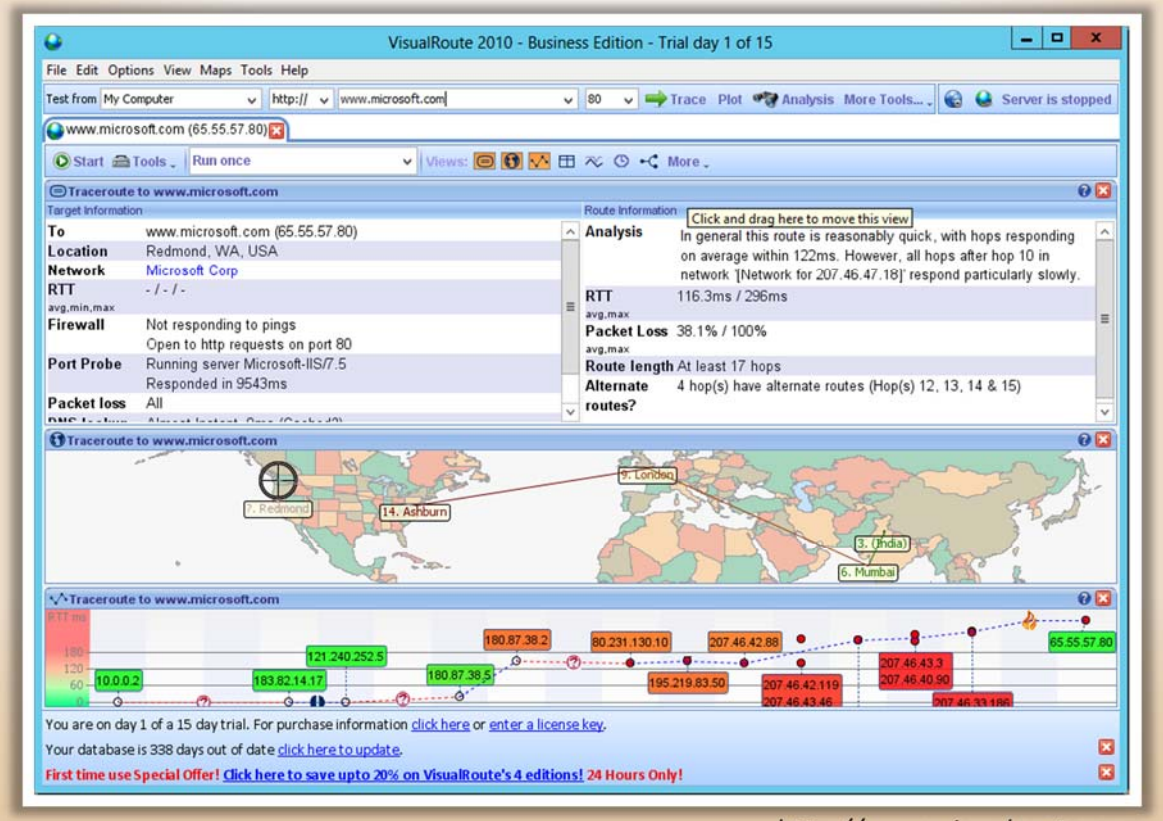
- NetScan Tools Pro's Port Scanner is a security tool for finding **open ports** corresponding to the **TCP** or **UDP** services/daemons running on a **target device**



http://www.netscantools.com

Major Tools Covered: VisualRoute

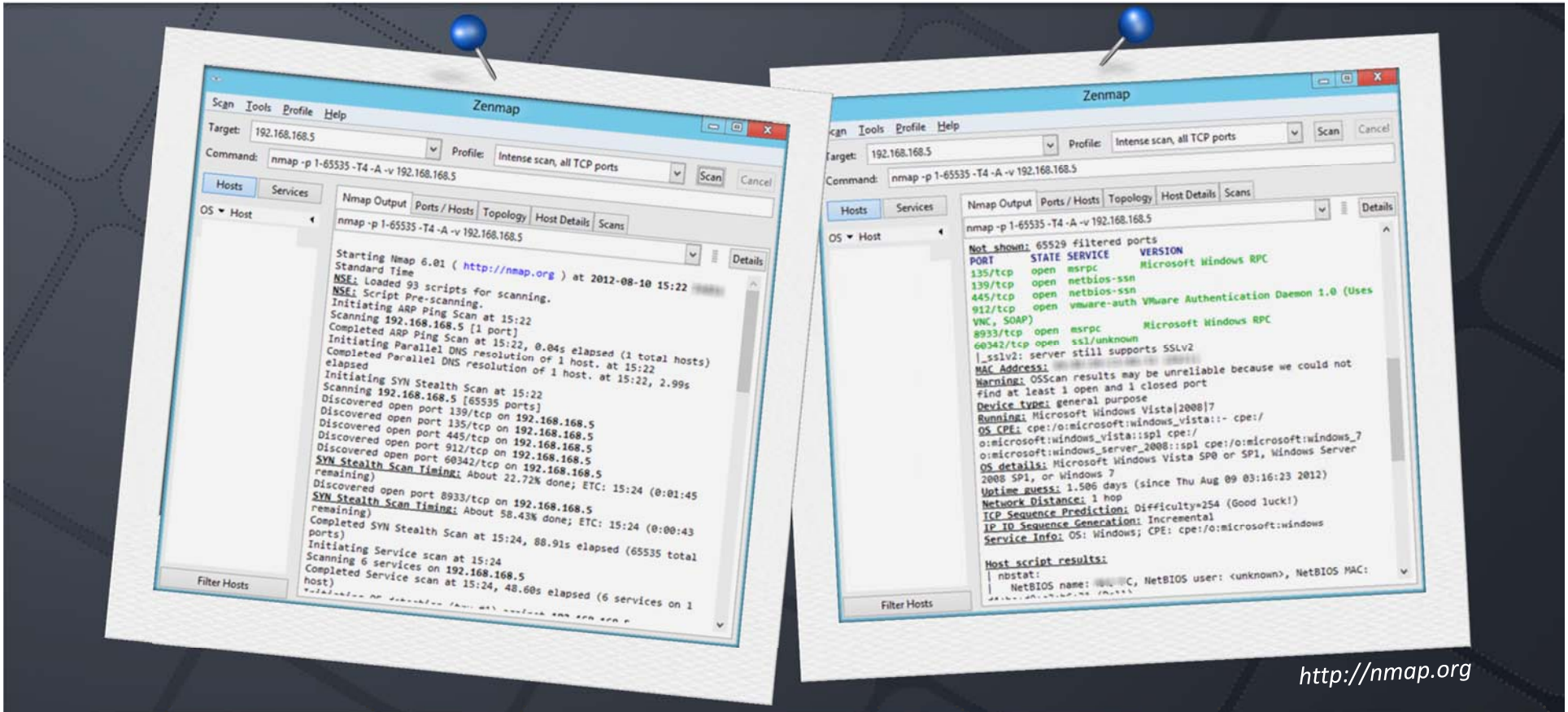
- Use the VisualRoute tool to identify the **physical location** of the target servers



http://www.visualroute.com

Major Tools Covered: Nmap

- Network administrators can use Nmap for **network inventory**, managing service upgrade schedules, and **monitoring host or service uptime**
- Attacker uses Nmap to extract information such as **live hosts on the network**, **services** (application name and version), type of **packet filters/firewalls**, **operating systems and OS versions**



Module Comparison of ECSAv4 with ECSAv8

- Internal testing involves testing **computers and devices within the company**. It is more like white-box testing

The topics highlighted in red under **ECSAv8 Module 11: Internal Network Penetration Testing** are the new additions

LPTv4 Module 19: Internal Network Penetration Testing

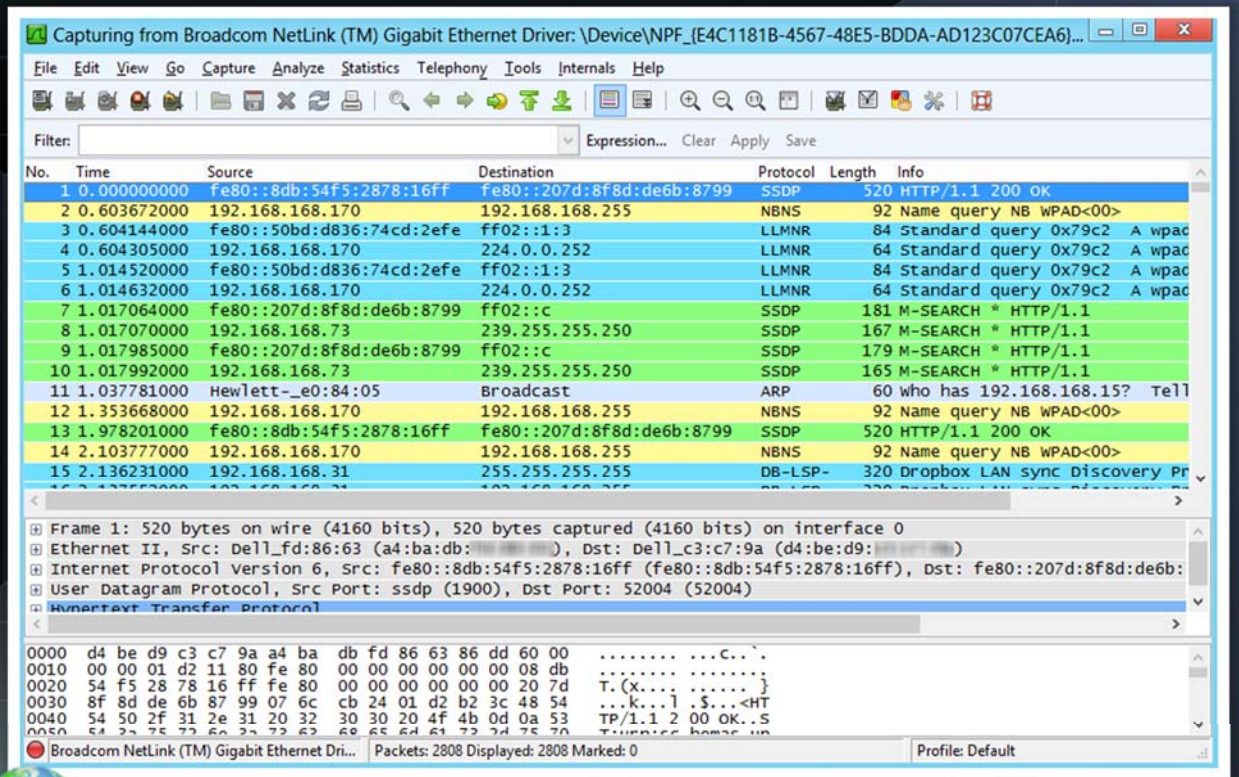
- Introduction to Internal Network Penetration Testing
- Steps for Conducting Internal Network Penetration Testing
- Try to Gain Access Using Known Vulnerabilities
- Sniff POP3/FTP/Telnet Passwords
- Boot the PC Using Alternate OS and Steal the SAM File
- Attempt to Plant a Software Keylogger to Steal Passwords
- Attempt to Create a Backdoor Account on the Target Machine
- Escalate User Privileges
- Capture the Communications between FTP Client and FTP Server
- Attempt Session Hijacking on Telnet Traffic

ECSAv8 Module 11: Internal Network Penetration Testing

- Introduction to Internal Network Penetration Testing
- Steps for Conducting Internal Network Penetration Testing
- Try to Gain Access Using Known Vulnerabilities
- Sniff POP3/FTP/Telnet Passwords
- Boot the PC Using Alternate OS and Steal the SAM File
- Attempt to Plant a Software Keylogger to Steal Passwords
- Attempt to Create a Backdoor Account on the Target Machine
- Escalate User Privileges
- Capture the Communications between FTP Client and FTP Server
- Attempt Session Hijacking on Telnet Traffic
- Recommendations for Internal Network Penetration Testing

Major Tools Covered: Wireshark

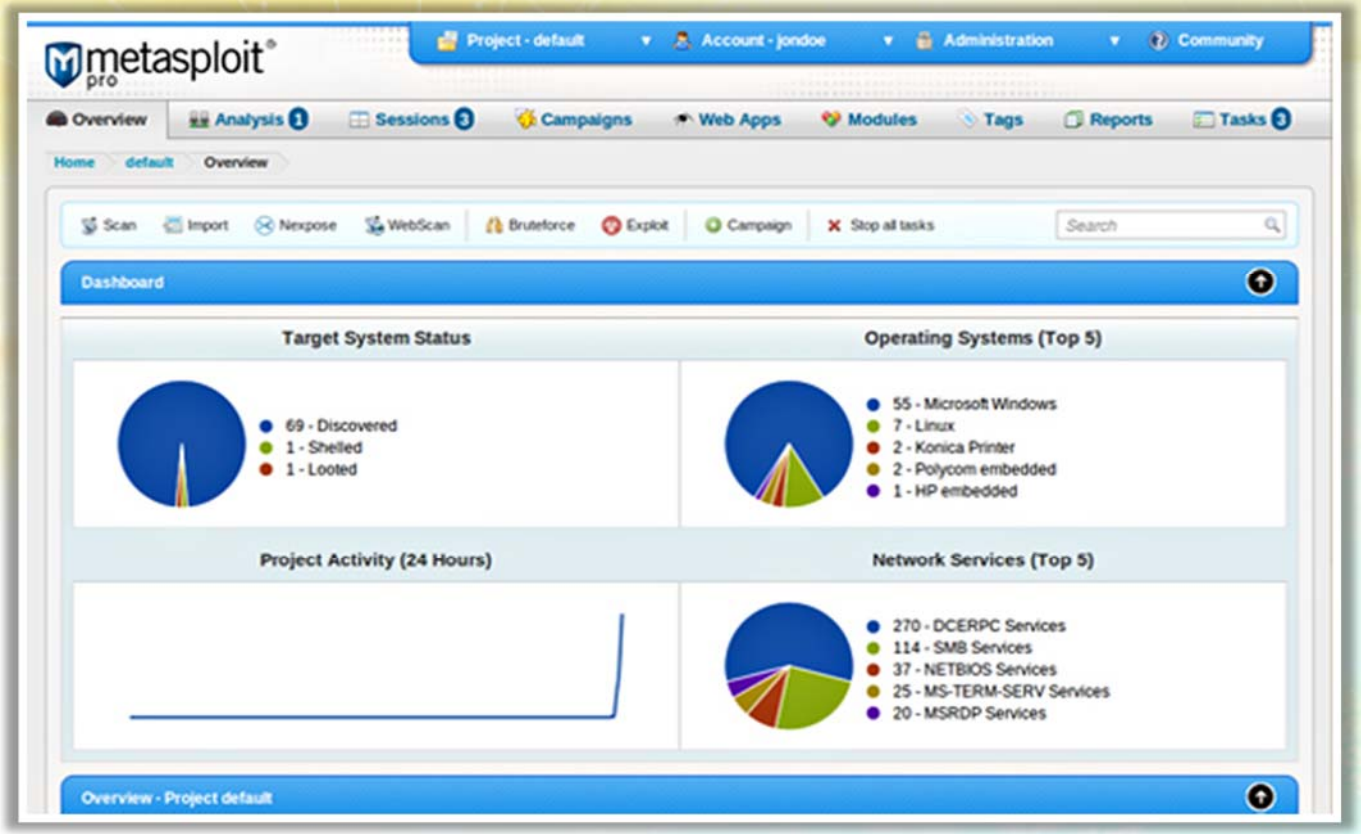
- Use **Wireshark** to capture raw packets
- If a **hub** is used, then sniffing is straightforward
- The following tools are used for sniffing the network:
  - Wireshark
  - Tcpdump
  - Kismet



http://www.wireshark.org

Major Tools Covered: Metasploit

Metasploit is another collection of hacking tools which comes with its own framework



http://www.metasploit.com

Module Comparison of ECSAv4 with ECSAv8

- A firewall is a **set of related programs**, located at a network gateway server, that protects the resources of a private network from users from other networks

The topics highlighted in red under **ECSAv8 Module 12: Firewall Penetration Testing** are the new additions

LPTv4 Module 21: Firewall Penetration Testing

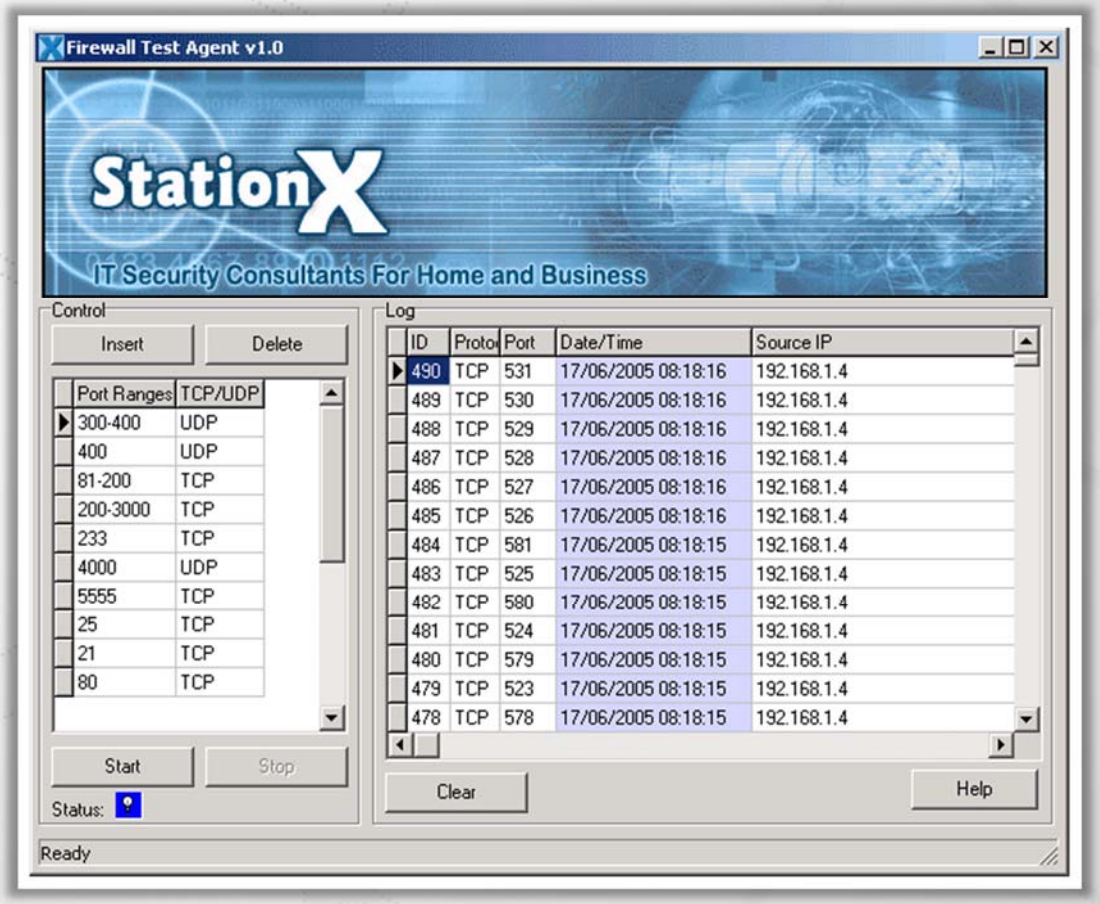
- What Is a Firewall?
- What Does a Firewall Do?
- Explain Packet Filtering
- How Does a Firewall Work?
- Assess Firewall Policy
- Build a Firewall Ruleset
- Maintenance and Management of Firewall
- Explain Hardware and Software Firewalls
- Explain Firewall Types
- Steps for Conducting Firewall Penetration Testing

ECSAv8 Module 12: Firewall Penetration Testing

- What Is a Firewall?
- What Does a Firewall Do?
- Explain Packet Filtering
- How Does a Firewall Work?
- Assess Firewall Policy
- Build a Firewall Ruleset
- Maintenance and Management of Firewall
- Explain Hardware and Software Firewalls
- Explain Firewall Types
- Assess Firewall Penetration Testing Tools
- Firewall Ruleset Mapping
- Best Practices for Firewall configuration
- Steps for Conducting Firewall Penetration Testing
- Bypass Firewall using various Attacks
- Test Firewall-Specific Vulnerabilities

Major Tools Covered: Firewall Test Agent

- Firewall Test Agent is used to test and log the **rules on a firewall**
- The Firewall Test Agent is able to open up any number of **TCP and UDP ports on a windows machine** and log any connection attempts



http://www.stationx.net

Module Comparison of ECSAv4 with ECSAv8

- An IDS is software/hardware that **detects and logs inappropriate, incorrect, or anomalous activity**

The topics highlighted in red under **ECSAv8 Module 13: IDS Penetration Testing** are the new additions

LPTv4 Module 22: IDS Penetration Testing

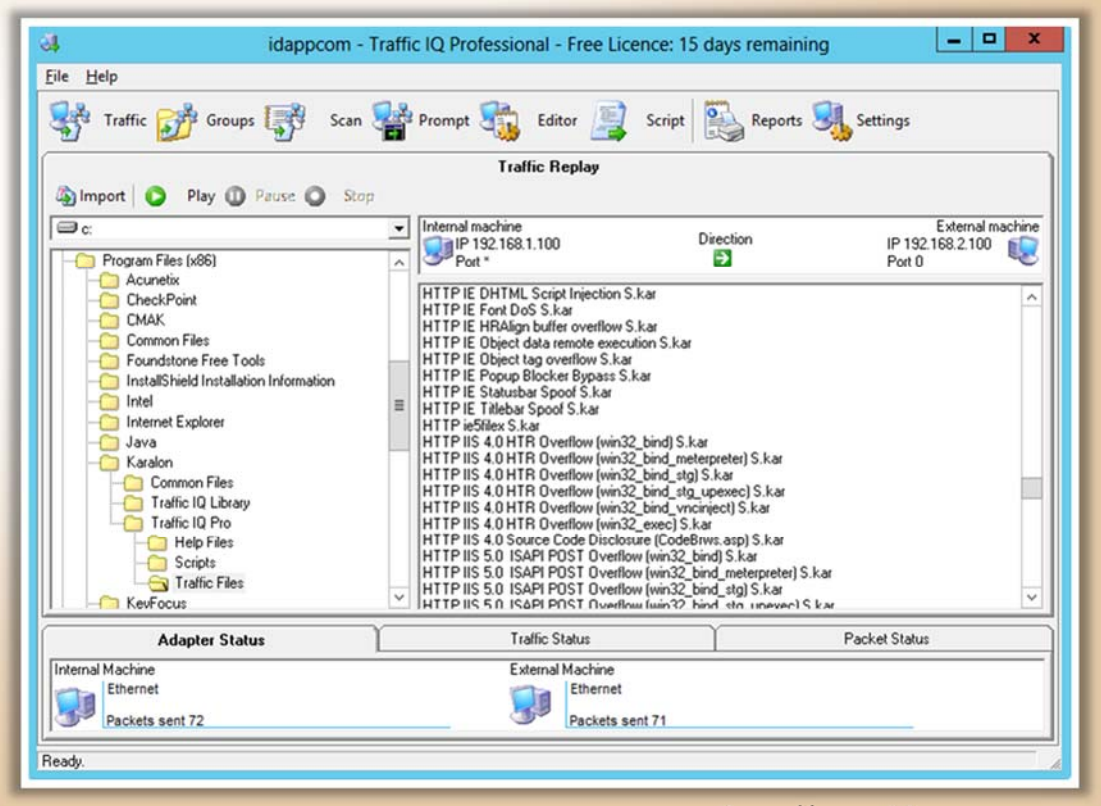
- Introduction to IDS
- Wireless Intrusion Detection Systems (WIDSs)
- IDS Penetration Testing Steps
- Test IP Packet Fragmentation
- Understanding TCP Flags
- Test for Backscatter
- Test the IDS Using Covert Channels
- Test the IDS Using Method Matching
- Test for Self-Referencing Directories
- Test for HTTP Misformatting
- Test for Null Method Processing

ECSAv8 Module 13: IDS Penetration Testing

- Introduction to IDS
- Wireless Intrusion Detection Systems (WIDSs)
- IDS Penetration Testing Steps
- Examine the Insertion on IDS
- Test IP Packet Fragmentation
- Understanding TCP Flags
- Test for Backscatter
- Check for False Positive Generation
- Test the IDS Using Covert Channels
- Test the IDS Using Method Matching
- Test for Self-Referencing Directories
- Test for HTTP Misformatting
- Test for Null Method Processing
- Try to Bypass Invalid RST Packets through IDS
- Intrusion Detection Tools
- Recommendations for IDS Penetration Testing

Major Tools Covered: Traffic IQ Professional

- Traffic IQ Professional enables security professionals to **quickly** and **easily audit** and validate the behavior of security devices by generating **standard application** traffic or attack traffic between two **virtual machines**
- It can be used to **assess**, **audit**, and test the behavioral characteristics of any **non-proxy** packet-filtering device, including:
  - Application layer firewalls
  - Intrusion detection systems
  - Intrusion prevention systems
  - Routers and switches



http://www.idappcom.com

Major Tools Covered: Snort

1. Snort is an open source network intrusion detection system, capable of performing real-time **traffic analysis and packet logging on IP networks**

2. It can perform **protocol analysis** and **content searching/matching**, and is used to detect a variety of **attacks and probes**, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts

3. It uses a flexible **rules language** to describe traffic that it should collect or pass, as well as a **detection engine** that utilizes a modular plug-in architecture

4. **Uses of Snort**:
   - Straight packet sniffer like tcpdump
   - Packet logger (useful for network traffic debugging, etc.)
   - Network intrusion prevention system

Command Prompt

```
Snort Commands
c:\Snort\bin>snort -c c:\Snort\etc\snort.conf -l c:\Snort\log -i 2
        --== Initialization Complete ==--
   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.0.2-ODBC-MySQL-FlexRESP-WIN32 GRE (Build 92)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
           Copyright (C) 1998-2010 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3
           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 1.12  <Build 18>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
Commencing packet processing (pid=5896)
S5: Session exceeded configured max bytes to queue 1048576 using 1048979 bytes (
client queue). 192.168.168.7 11616 --> 92.46.53.163 80 (0) : LWstate 0x1 LWFlags
 0x2003
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 5985.944000 seconds
Snort processed 11774 packets.
Snort ran for 0 days 1 hours 39 minutes 45 seconds
    Pkts/hr:        11774
   Pkts/min:          118
   Pkts/sec:            1
S5: Pruned session from cache that was using 1098947 bytes (purge whole cache).
192.168.168.7 11616 --> 92.46.53.163 80 (0) : LWstate 0x1 LWFlags 0x222003
===============================================================================
Packet I/O Totals:
   Received:       147490
   Analyzed:        11774 (  7.983%)
    Dropped:       135707 ( 92.011%)
   Filtered:            0 (  0.000%)
Outstanding:       135716 ( 92.017%)
   Injected:            0
===============================================================================
```

http://www.snort.org

Module Comparison of ECSAv4 with ECSAv8

- A password is a secret series of characters that **enables a user to access a file, computer, or a program**

The topics highlighted in red under **ECSAv8 Module 14: Password Cracking Penetration Testing** are the new additions

LPTv4 Module 25: Password Cracking Penetration Testing

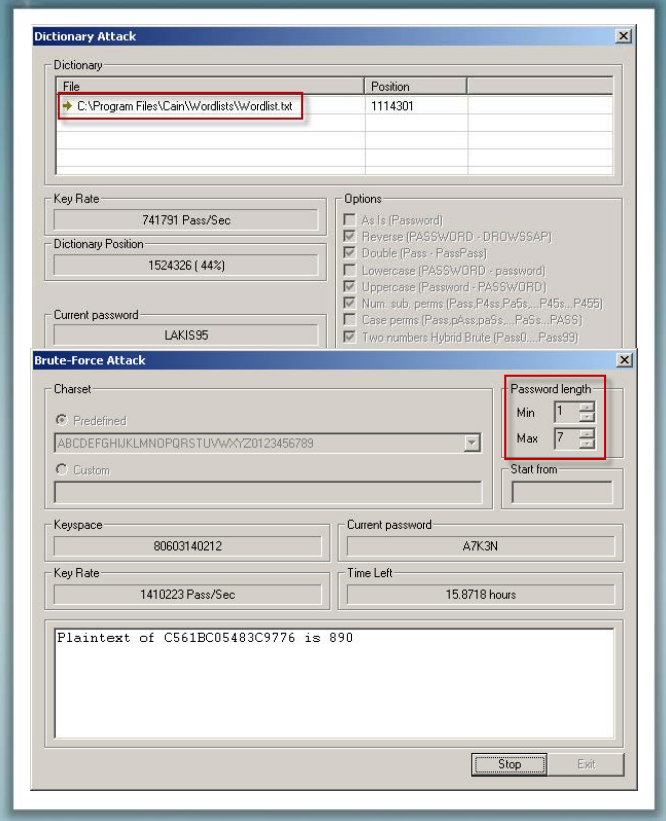
- Common Password Vulnerabilities
- Password Cracking Techniques
- Types of Password Attacks
- How Are Passwords Stored in Windows?
- How Are Passwords Stored in Linux?
- Steps for Password Cracking Penetration Testing
- Perform Brute Force and Dictionary Attacks
- Password Cracking Using Distributed Network Attack

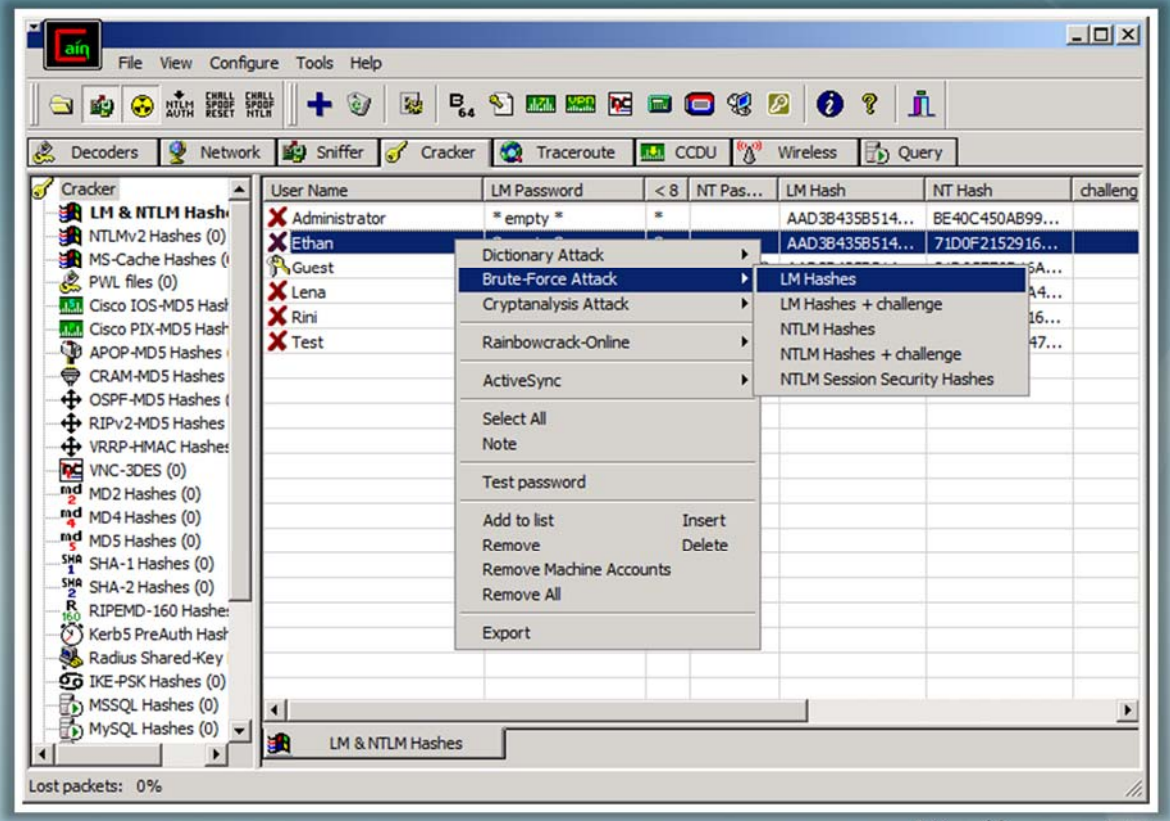
ECSAv8 Module 14: Password Cracking Penetration Testing

- Password - Terminology
- Importance of Passwords
- Password Types
- Common Password Vulnerabilities
- Password Cracking Techniques
- Types of Password Attacks
- How Are Passwords Stored in Windows?
- LM, NTLM, and Kerberos Authentication
- How Are Passwords Stored in Linux?
- Steps for Password Cracking Penetration Testing
- Perform Non-Electronic Attacks
- Perform Brute Force and Dictionary Attacks
- Perform Man-in-the-Middle Attack to Collect Passwords
- Perform Hash Injection and Rainbow Attack
- Password Cracking Using Distributed Network Attack
- Use Trojan/Spyware/Keyloggers to Capture Passwords
- Spyware Tools and Keyloggers
- Recommendations for Password Cracking Penetration Testing

Major Tools Covered: Cain & Abel

- Cain & Abel allows **recovery of various kind of passwords** by sniffing the network; cracking encrypted passwords using dictionary, brute-force and cryptanalysis attacks; decoding scrambled passwords; recovering wireless network keys; revealing password boxes; and uncovering cached passwords





http://www.oxid.it

Major Tools Covered: Tcpdump/WinDump

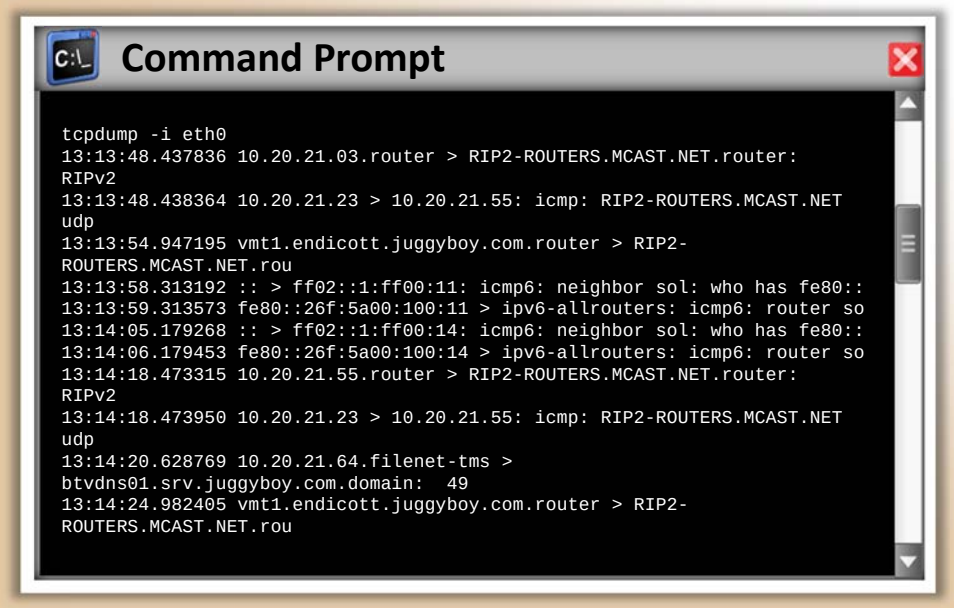
- Tcpdump is a **command line interface packet sniffer** which runs on Linux and UNIX

Tcpdump

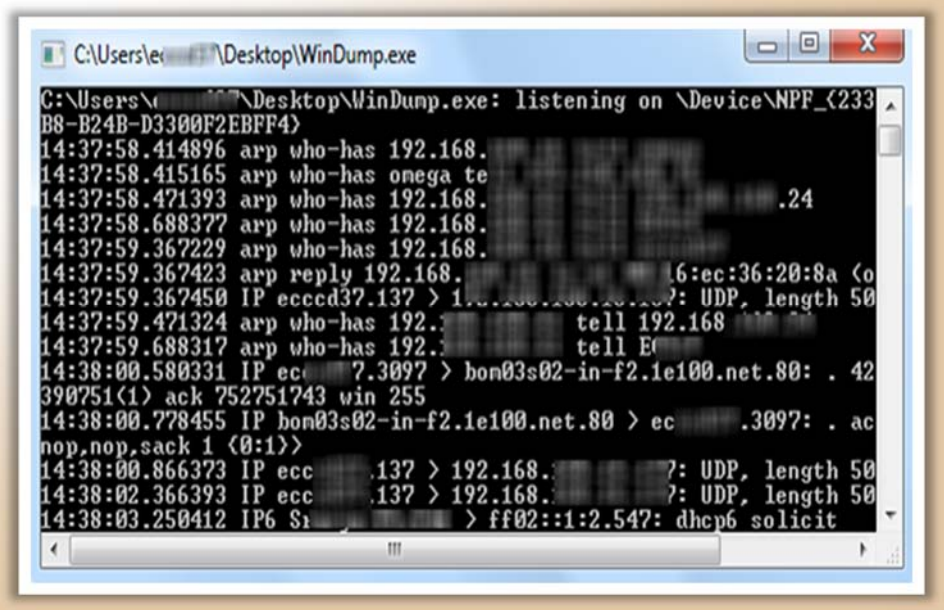
Runs on Linux and UNIX systems

WinDump

Runs on Windows systems

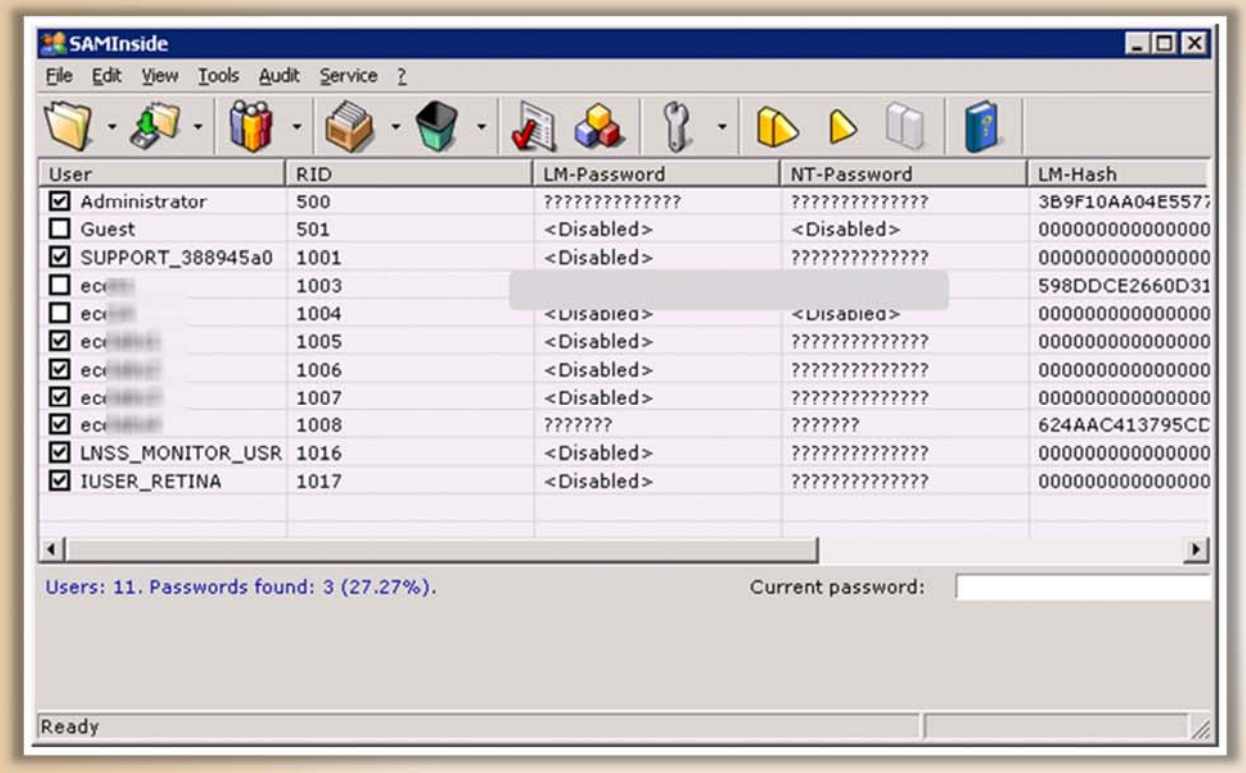


http://www.tcpdump.org



http://www.winpcap.org

Major Tools Covered: SAMInside



http://insidepro.com

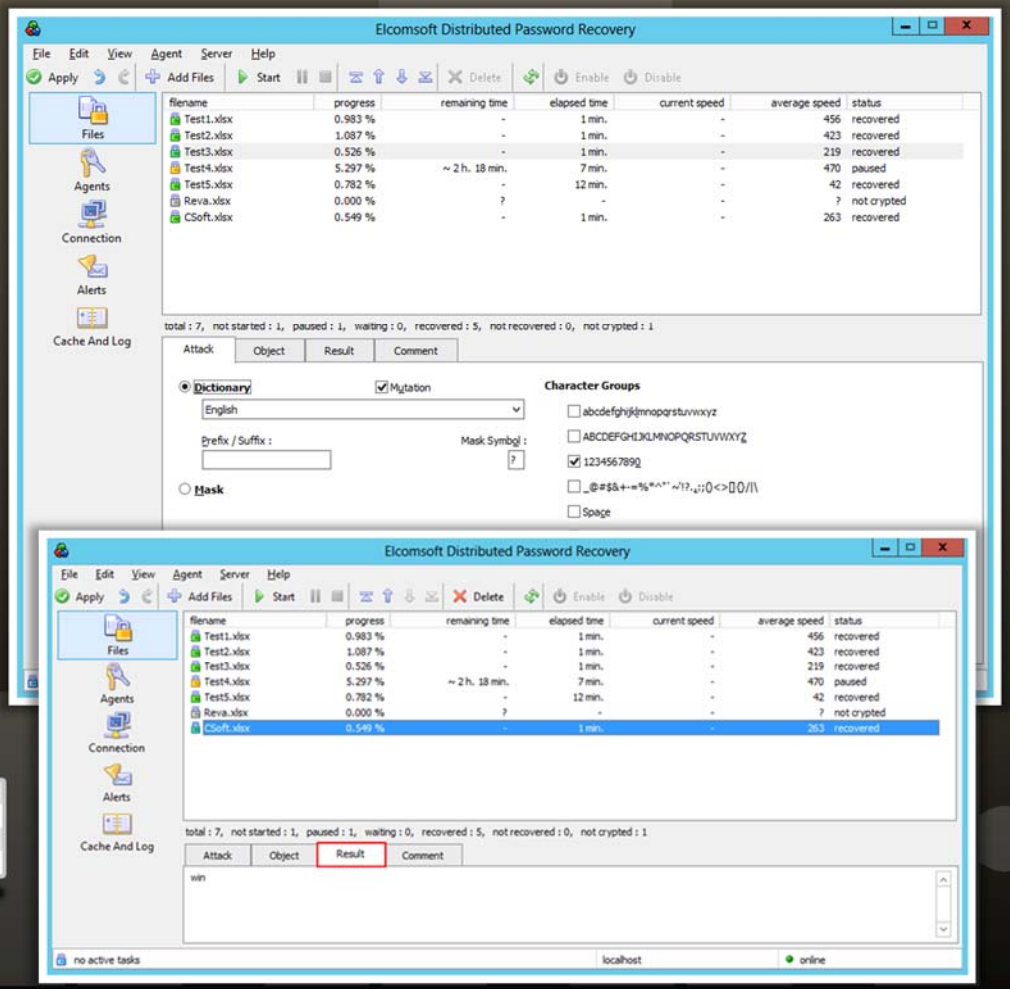
- SAMInside is designated for the **recovery** of Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista, and Windows 7 **user passwords**
- It has a **small footprint** and can be run from a diskette, CD/DVD disc or USB drive
- It includes over **10 types of data import** and **6 types of password attack** to recover the password

Major Tools Covered: Elcomsoft Distributed Password Recovery

- Elcomsoft Distributed Password Recovery **breaks complex passwords**, **recovers strong encryption keys**, and **unlocks documents** in a production environment

Features

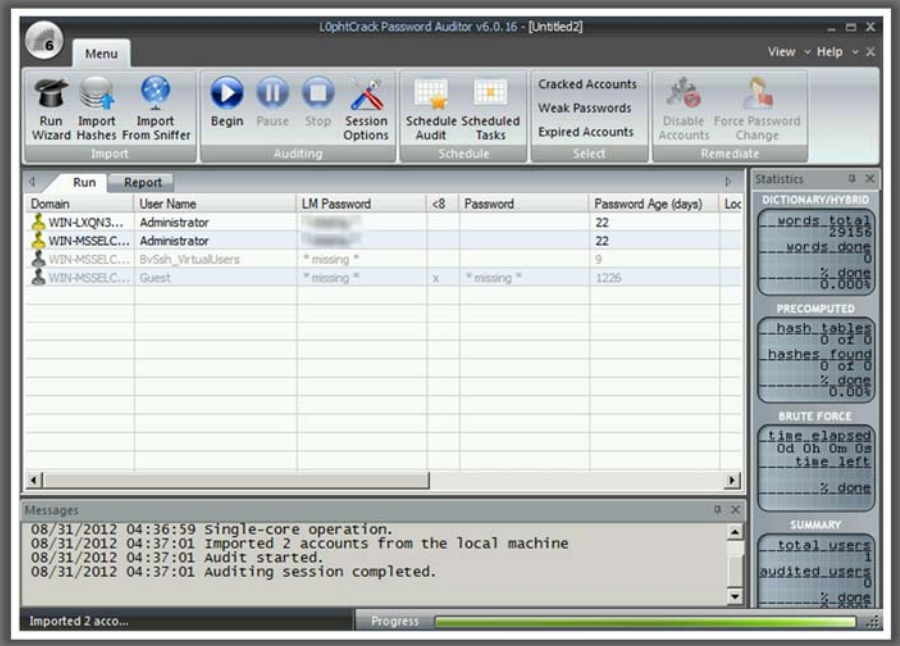
- Brute-force and dictionary attacks
- Distributed password recovery over LAN, Internet, or both
- Install and remove password recovery clients remotely



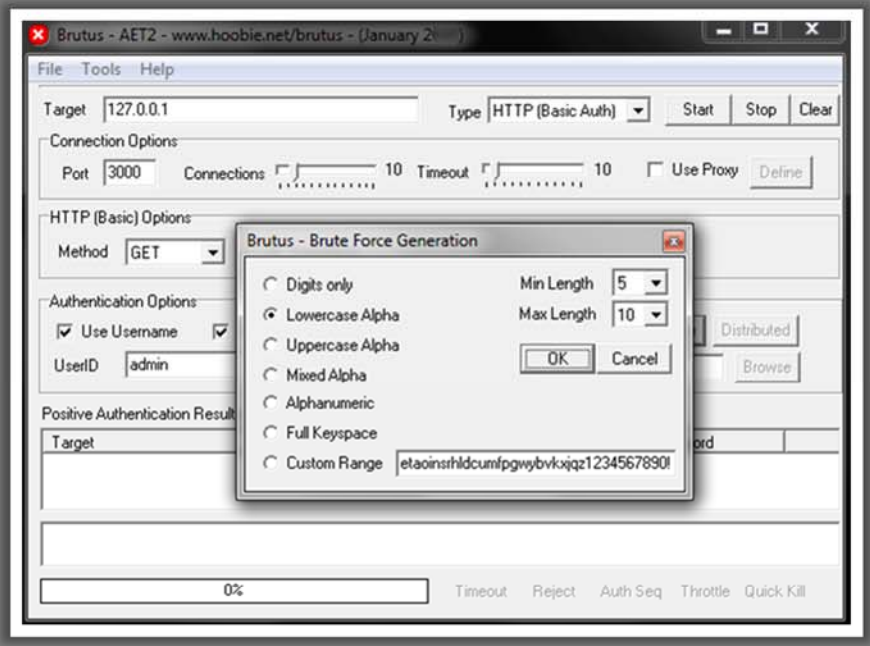
http://www.elcomsoft.com

Major Tools Covered: L0phtCrack and Brutus

- Use password cracking tools such as Brutus and L0phtCrack to break password-protected files
- L0phtCrack recovers lost Microsoft Windows passwords by using dictionary and hybrid attacks, rainbow tables, and brute force; it also checks password strength



http://www.l0phtcrack.com



http://www.hoobie.net

Module Comparison of ECSAv4 with ECSAv8

- The objective of social engineering pen testing is to **test the strength of human factors in a security chain within the organization**

The topics highlighted in red under **ECSAv8 Module 15: Social Engineering Penetration Testing** are the new additions

LPTv4 Module 26: Social Engineering Penetration Testing

- What Is Social Engineering?
- Steps in Conducting Social Engineering Penetration Test
- Attempt Social Engineering Using Phone
- Attempt Social Engineering Using Email
- Attempt Social Engineering by Dumpster Diving
- Attempt Social Engineering by Shoulder Surfing
- Attempt Social Engineering Using Phishing Attacks
- Try to Obtain the Details of an Employee from Social Networking Sites
- Document Everything

ECSAv8 Module 15: Social Engineering Penetration Testing

- What Is Social Engineering?
- Social Engineering Pen Testing
- Impact of Social Engineering on the Organization
- Common Targets of Social Engineering
- Steps in Conducting Social Engineering Penetration Test
- Attempt Social Engineering Using Phone
- Attempt Social Engineering Using Email
- Attempt Social Engineering by Dumpster Diving
- Attempt Social Engineering by Shoulder Surfing
- Attempt Social Engineering Using Phishing Attacks
- Attempt Identity Theft
- Try to Obtain the Details of an Employee from Social Networking Sites
- Document Everything

Module Comparison of ECSAv4 with ECSAv8

- Web applications provide an **interface between end users and web servers** through a set of web pages that are generated at the server end or contain script code to be executed dynamically within the client web browser

The topics highlighted in red under **ECSAv8 Module 16: Web Application Penetration Testing** are the new additions

LPTv4 Module 28: Application Penetration Testing

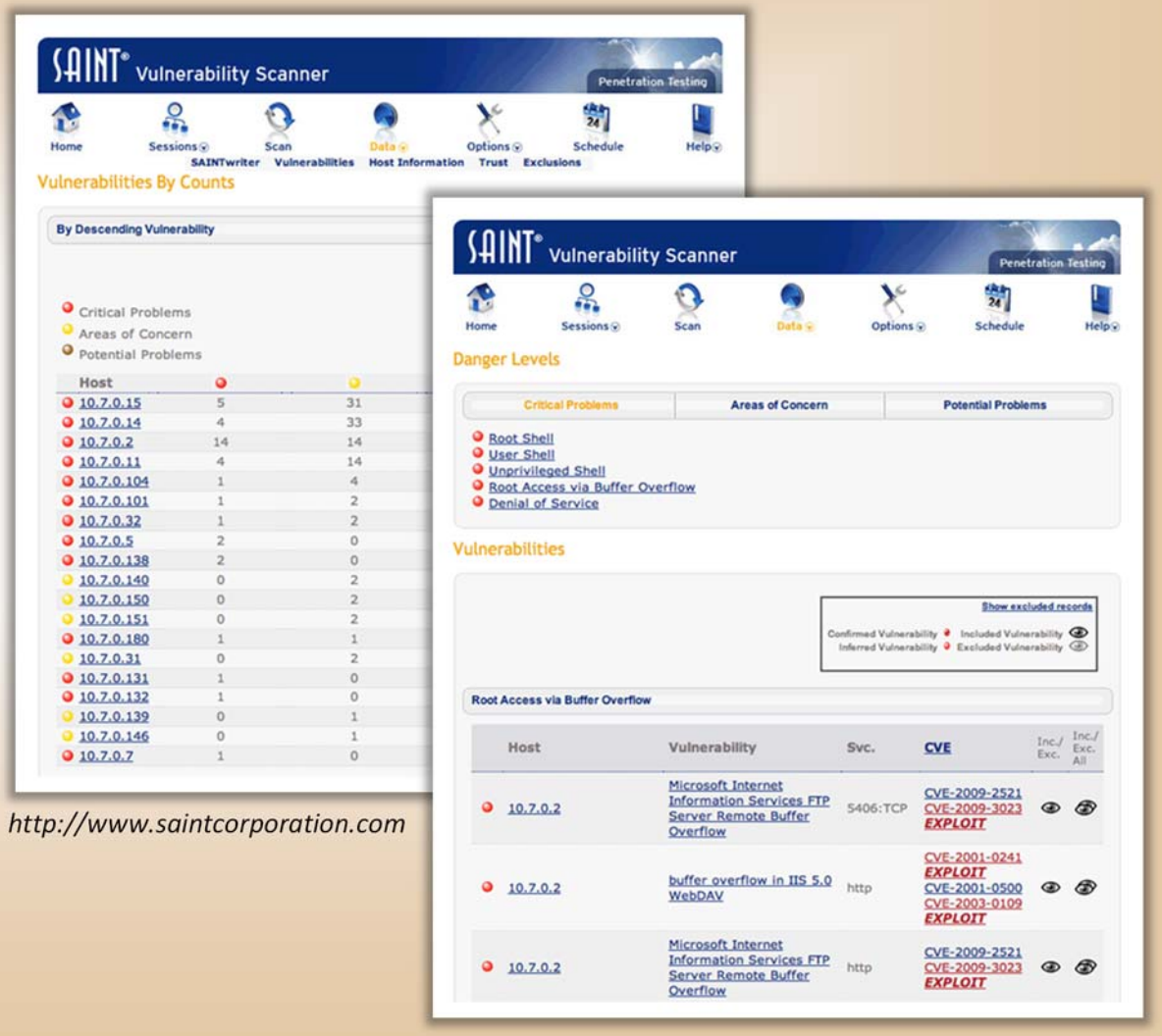
- Introduction to Web Applications
- Web App Pen Testing Phases
- Test for the Recognized File Types/Extensions/Directories
- Examine Source of the Available Pages
- Test the Database Connectivity
- Test for Known Vulnerabilities
- Identify Client-side Scripting

ECSAv8 Module 16: Web Application Penetration Testing

- Introduction to Web Applications
- Web App Pen Testing Phases
- Perform Web Spidering
- Perform Server Discovery
- Test for the Recognized File Types/Extensions/Directories
- Examine Source of the Available Pages
- Test for Proxy Functionality
- Test the Database Connectivity
- Test for Improper Error Handling
- Identify Entry Points for User Input
- Test for Known Vulnerabilities
- Check for Insecure Cryptographic Storage
- Identify Client-side Scripting
- Test for Username Enumeration
- Testing for Logic Flaws

Major Tools Covered: SAINT

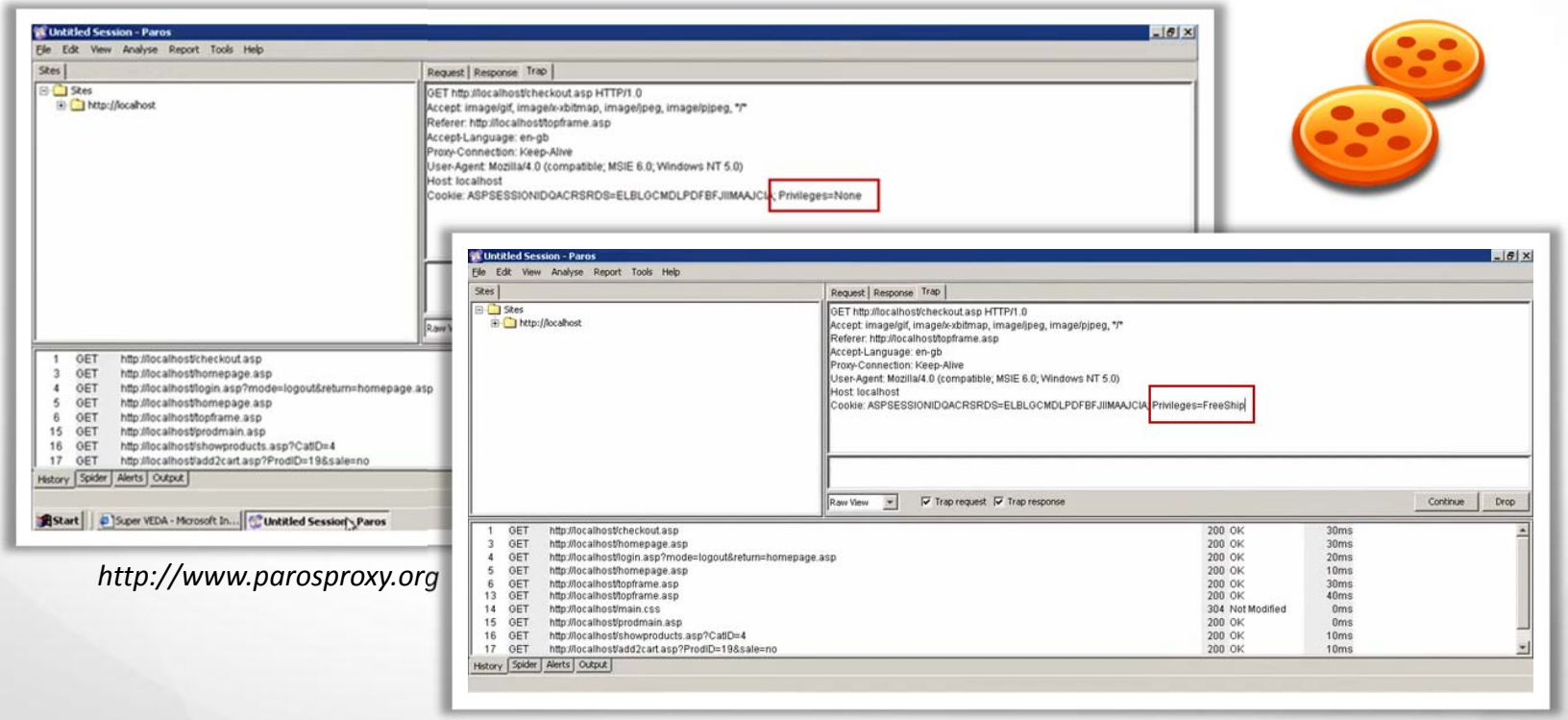
Use **web vulnerability scanning tools** such as Nessus, Netsparker, SAINT, etc., to find any vulnerabilities in the host web server



http://www.saintcorporation.com

Major Tools Covered: Paros Proxy

- In the first step, the attacker collects some cookies set by the web application and analyzes them to determine the **cookie generation mechanism**
- The attacker then traps cookies set by the web application, tampers with the parameters using tools such **Paros Proxy**, and replays to the application



http://www.parosproxy.org

Module Comparison of ECSAv4 with ECSAv8

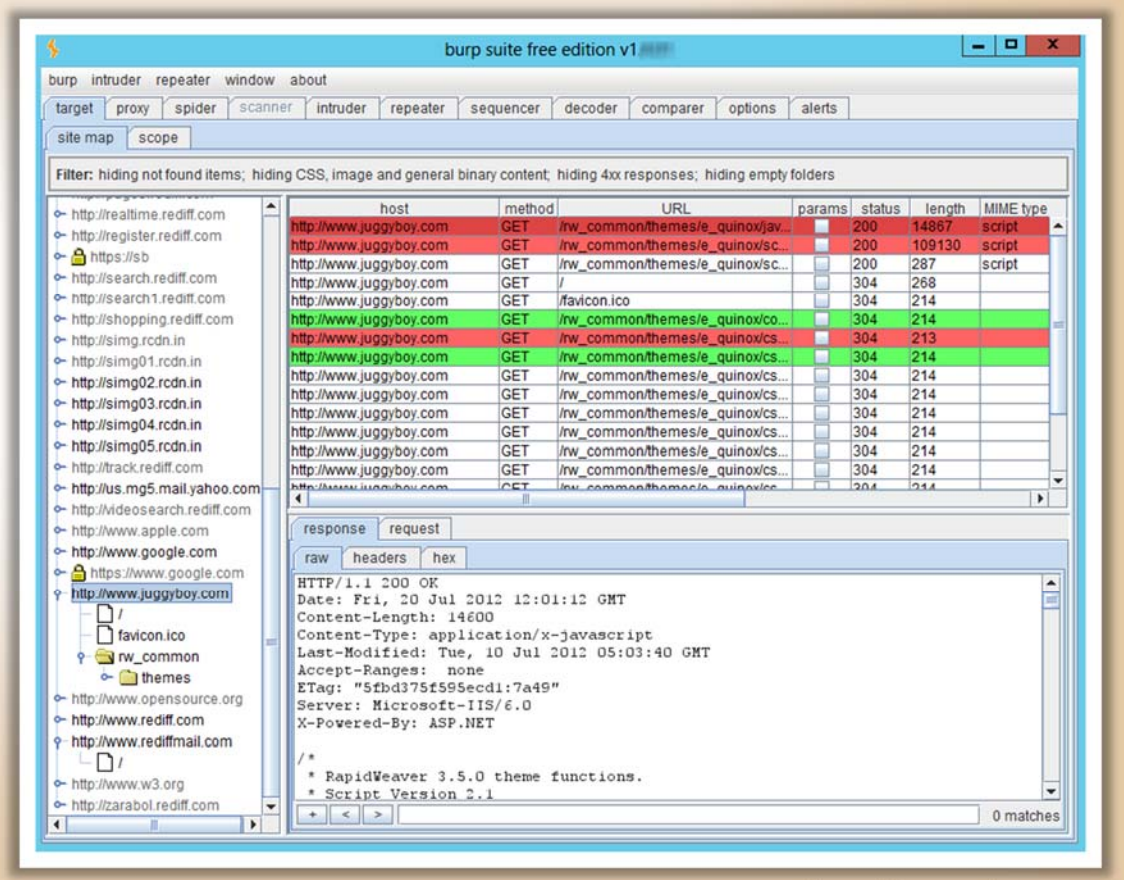
- SQL injection is a technique used to take advantage of **non-validated input vulnerabilities** to pass SQL commands through a web application for execution by a back-end database
- SQL injection is the **most common web vulnerability** on the Internet

ECSAv8 Module 17 SQL Penetration Testing is a new module which covers the following topics:

- Introduction to SQL Injection
- How Do Web Applications Work?
- How Does SQL Injection Work?
- SQL Injection Attack Paths
- Impact of SQL Injection Attacks
- Types of SQL Injection Attacks
- SQL Injection Attack Characters
- SQL Injection Penetration Testing Steps
- SQL Injection Detection Tools
- SQL Injection Penetration Testing Tools
- Best Practices to Prevent SQL Injection

Major Tools Covered: Burp Suite Tool

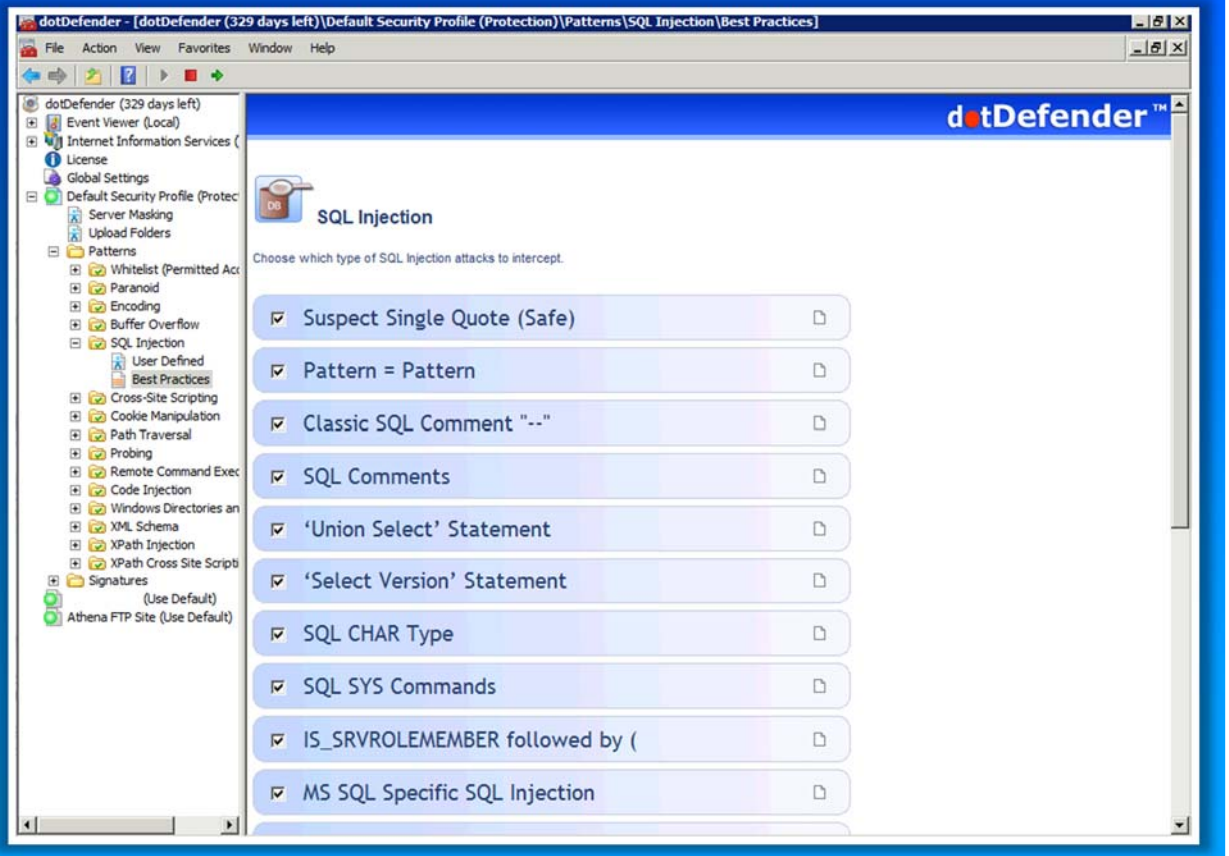
- Burp Suite is an intercepting proxy, which lets you **inspect and modify traffic** between your browser and the target application
- It contains an advanced web application scanner, for automating the detection of **numerous types of vulnerabilities**



http://portswigger.net

Major Tools Covered: dotDefender

- SQL injection is a major **web application vulnerability** and most of the web application vulnerability scanners can detect SQL injection vulnerability and identify the vulnerable **source code**
- Use SQL detection tools such as **dotDefender** to detect SQL injection vulnerabilities

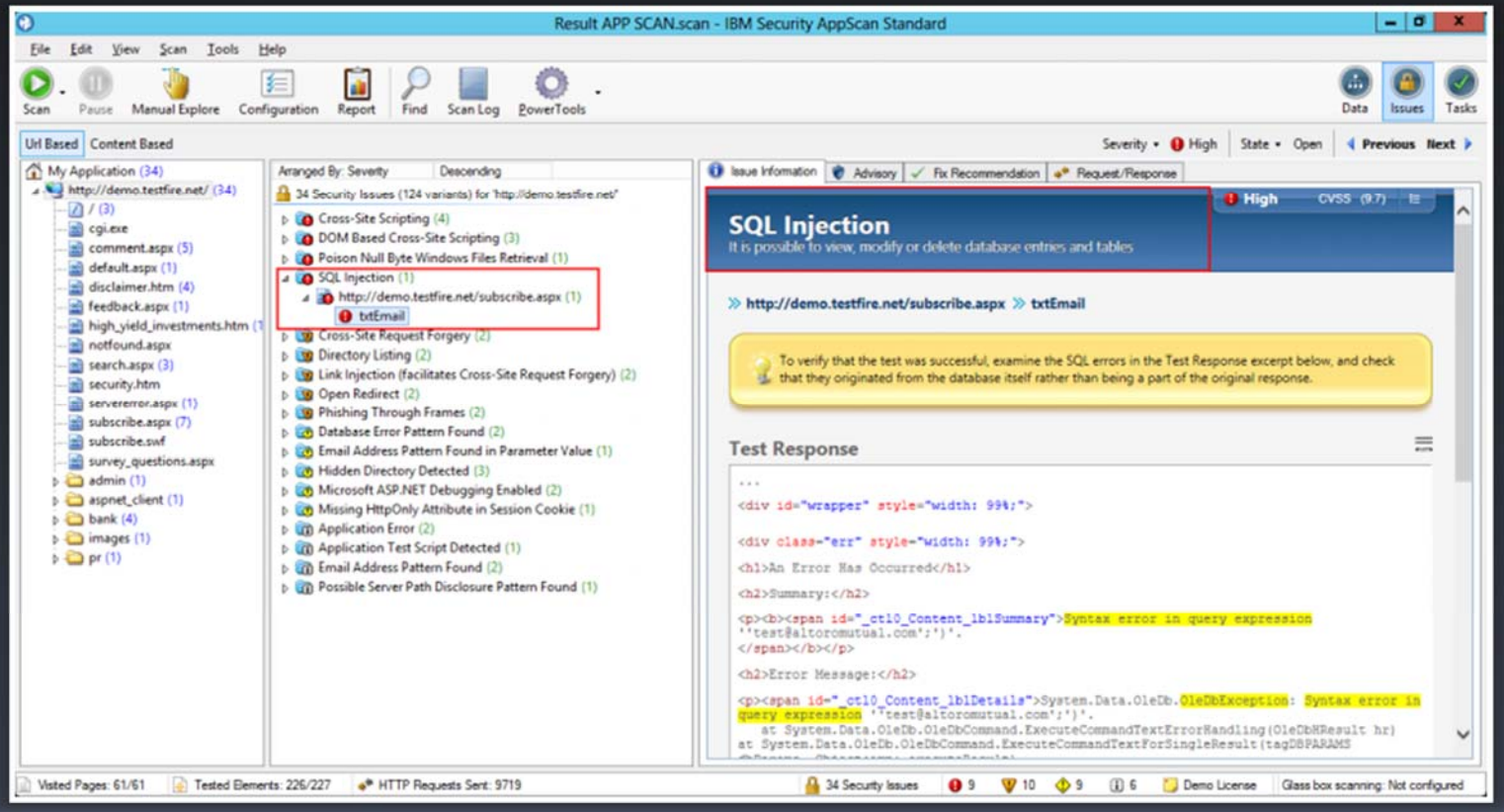


http://www.applicure.com

Major Tools Covered: IBM Security AppScan

- IBM Security AppScan is a web application security testing tool that automates **vulnerability assessments**

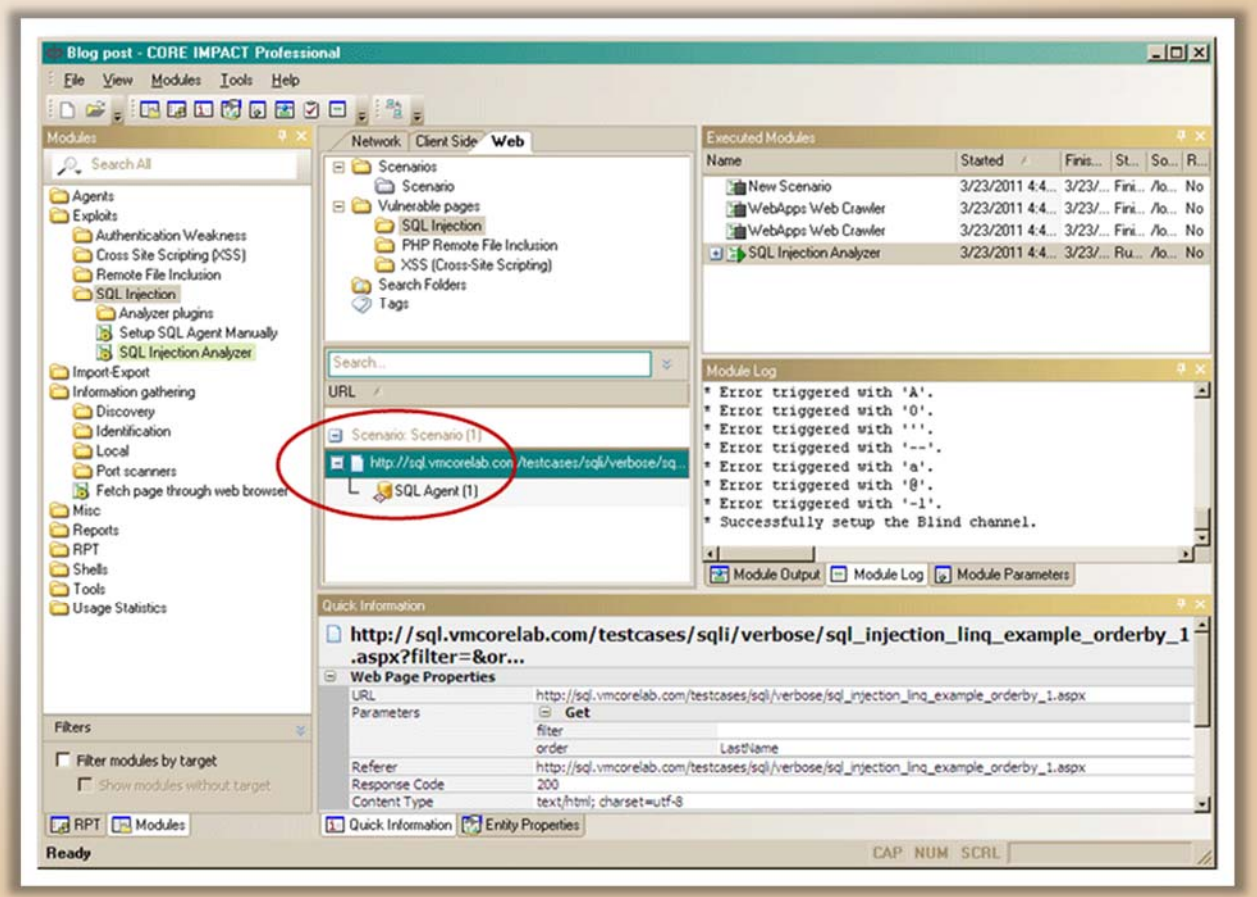
- Prevents SQL injection attacks on **websites**
- Scans websites for embedded **malware**
- Regulatory compliance and reporting



http://www.ibm.com

Major Tools Covered: CORE IMPACT Pro

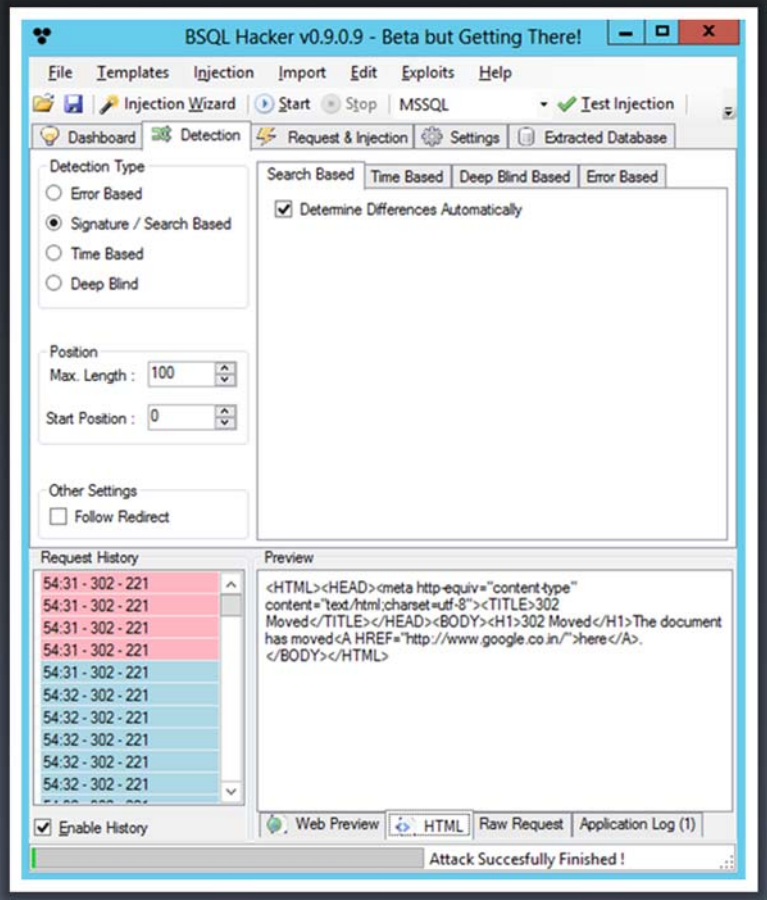
- CORE IMPACT Pro can pinpoint exploitable SQL injection and other vulnerabilities in web applications, not only **providing visibility** into where application weaknesses exist, but also determining how they can open the door to subsequent network-based attacks

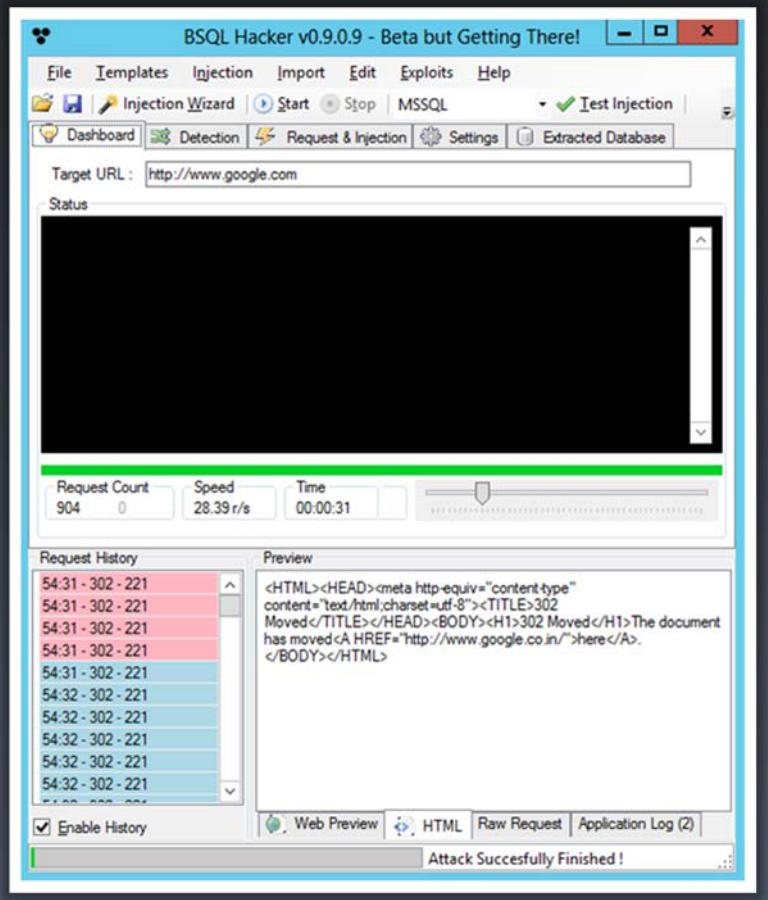


http://coresecurity.com

Major Tools Covered: BSQL Hacker

- BSQL Hacker is an automated SQL injection tool which supports **blind SQL injection**, time-based blind SQL injection, deep blind (based on advanced time delays) SQL injection, and error-based SQL injection





http://labs.portcullis.co.uk

Module Comparison of ECSAv4 with ECSAv8

- The pen testing report helps executive management to **take decisions on implementing security controls in the organization**

The topics highlighted in red under **ECSAv8 Module 18: Penetration Testing Reports and Post Testing Actions** are the new additions

LPTv4 Module 42 Penetration Testing Deliverables and Conclusion
LPTv4 Module 43 Penetration Testing Report and Documentation Writing
LPTv4 Module 44 Penetration Testing Report Analysis
LPTv4 Module 45 Post Testing Actions

- Analyze Report Development Process
- Review and Finalization of the Report
- Sample Pen Testing Report Format
- Comprehensive Technical Report
- Examine Penetration Testing Report Analysis
- Develop and Implement Data Backup Plan
- Create Security Policies for Testing Reports
- Examine Report Retention

ECSAv8 Module 18: Penetration Testing Reports and Post Testing Actions (Combined Module)

- Goal of the Penetration Testing Report
- Examine Types of Pen Testing Reports
- Characteristics of a Good Pen Testing Report
- Writing Pen Testing Report
- Analyze Report Development Process
- Review and Finalization of the Report
- Sample Pen Testing Report Format
- Comprehensive Technical Report
- Examine Penetration Testing Report Analysis
- Develop and Implement Data Backup Plan
- Create Security Policies for Testing Reports
- Examine Report Retention

EC-Council's Licensed Penetration Testing (LPT) Certification

What is LPT

- LPT is a **online practical exam** designed to evaluate and validate students' pen testing skills
- The LPT standardizes the knowledge base for penetration testing professionals by incorporating **best practices** followed by experienced experts in the field

1

- It ensures that each professional licensed by EC-Council **follows a strict code of ethics**, is exposed to the best practices in the domain of penetration testing course and aware of all the **compliance requirements** required by the industry

2

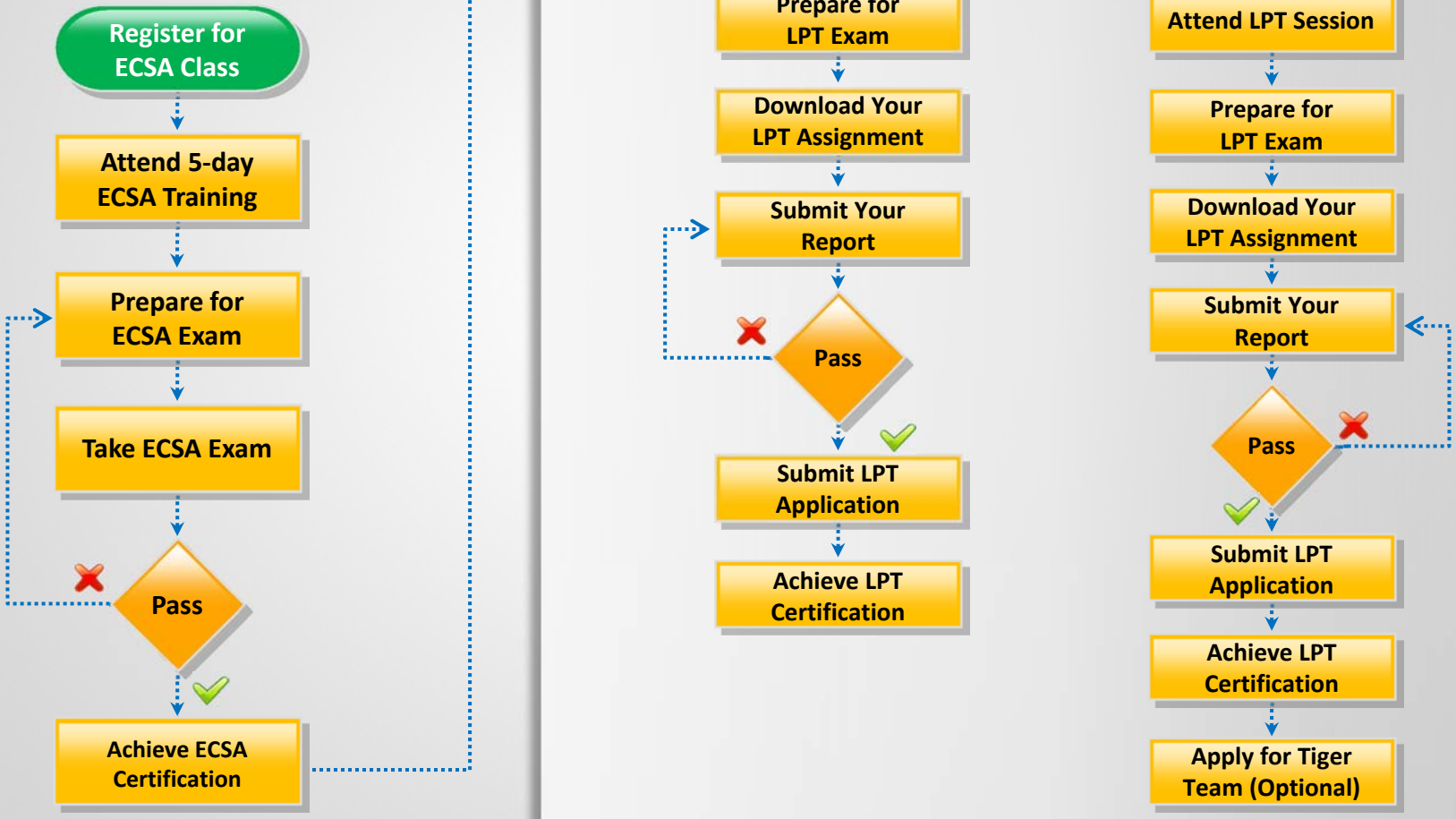
- Unlike a normal security certification, the LPT is a program which trains security professionals to **analyze the security posture** of a network exhaustively and recommend corrective measures authoritatively
- EC-Council's license vouches for their **professionalism and expertise** thereby making these professionals more sought after by organizations and consulting firms globally

3

How Does the LPT License Help Me in Conducting Pen Tests

- LPT licence provides an assurance to your employer or prospective clients that you posses a set of skills to **perform a methodological security assessment**
- It also helps you join the **EC-Council's elite Tiger Team** which provide you a platform to showcase your skills and get pen testing engagements

How to Become an LPT

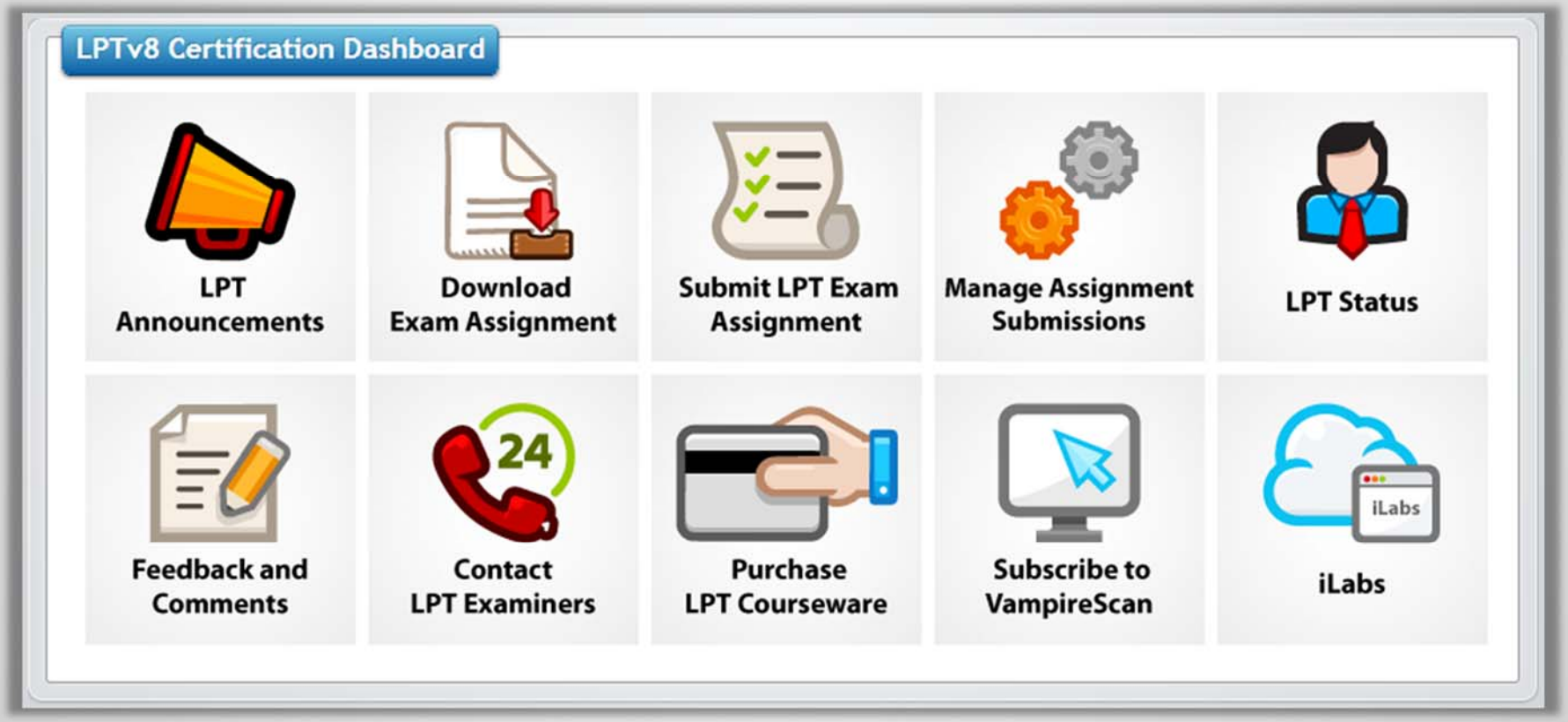


What is New in LPTv8

- Performance based evaluation on **iLabs**
- **ASPEN dashboard** to take LPT exam and to check your license status
- New **pen testing templates**
- Option to join **Tiger Team**

LPT Certification Portal

LPT certification is specifically designed for LPT candidates where they can **download** and **submit** their LPT **practical exam assignments** and check their LPT status



What is Tiger Team

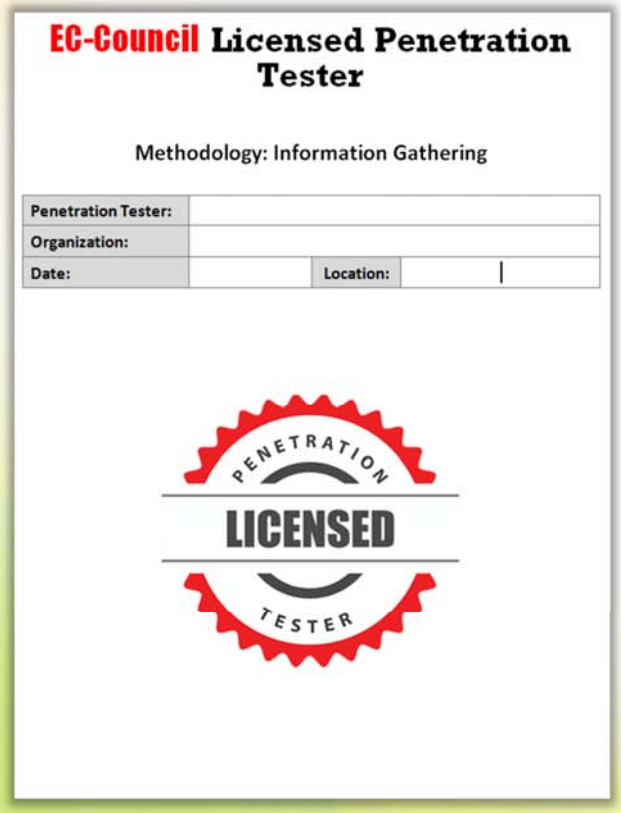
- Tiger Team is an **elite set of professionals** who hold LPT credential that engage in Penetration Testing projects worldwide
- Members of Tiger Team have high chances of participating in **Penetration Testing assignments worldwide**
- The list will be displayed on our website and will act as an **endorsement of the professionals' skills and ethics**

How to Join the Tiger Team

- Selected Certified Licensed Penetration Tester professionals will be invited in EC-Council's elite Tiger Team
- Police clearance / verification / background check / legal agreements will be involved before joining the team

Pen Testing Templates

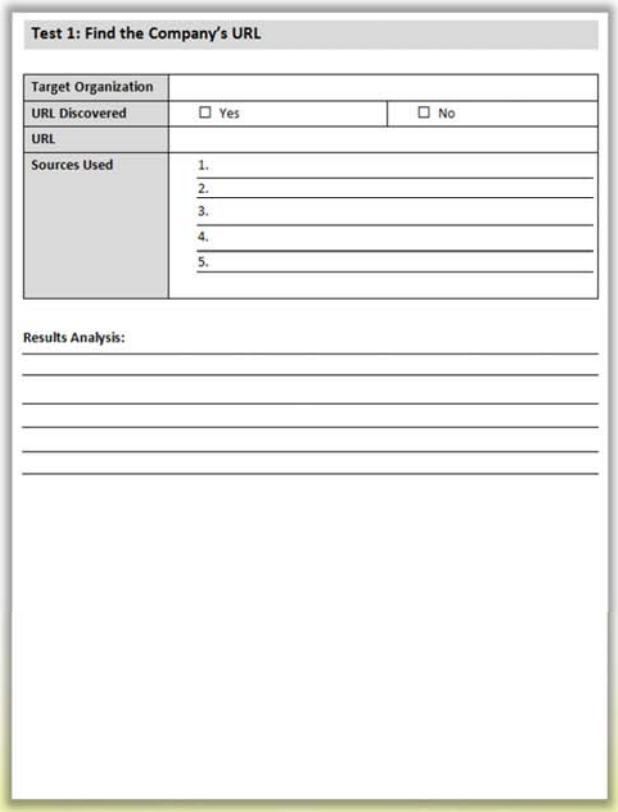
- ECSA/LPT program comes with a **huge repository of professional pen testing report** that will help you to create pen testing report
- You can download it from ASPEN portal



EC-Council Licensed Penetration Tester

Methodology: Information Gathering

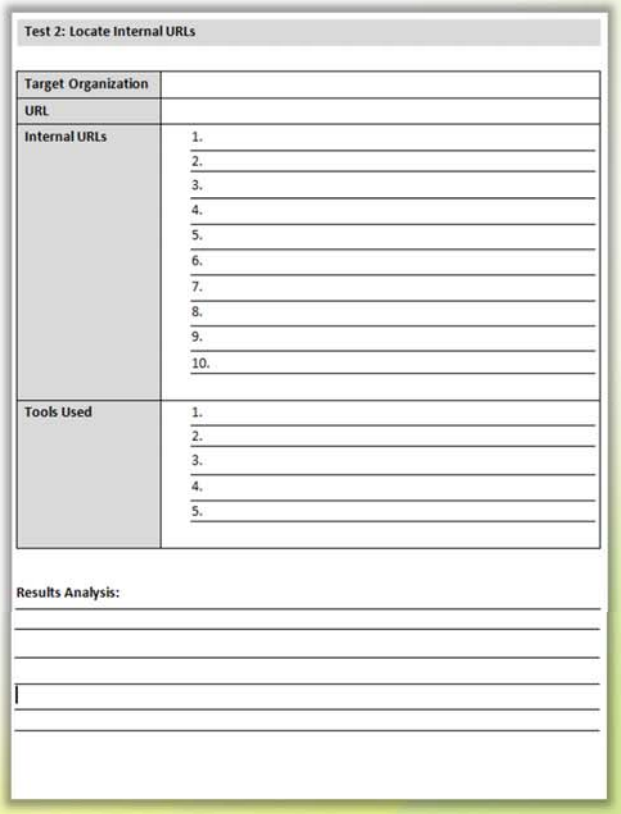
Penetration Tester:			
Organization:			
Date:		Location:	



Test 1: Find the Company's URL

Target Organization		
URL Discovered	☐ Yes	☐ No
URL		
Sources Used	1. 2. 3. 4. 5.	

Results Analysis:



Test 2: Locate Internal URLs

Target Organization	
URL	
Internal URLs	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Tools Used	1. 2. 3. 4. 5.

Results Analysis:

What is VampireTest

- VampireTest is designed to be used by penetration testers to **input penetration test data results**
- The program accepts various inputs and **delivers final report of the data content**

How to Buy LPT Framework

You can access and use LPT framework after registering for ECSA/LPT program

Thank You