

Managing Enterprise Cybersecurity

MIS 4596

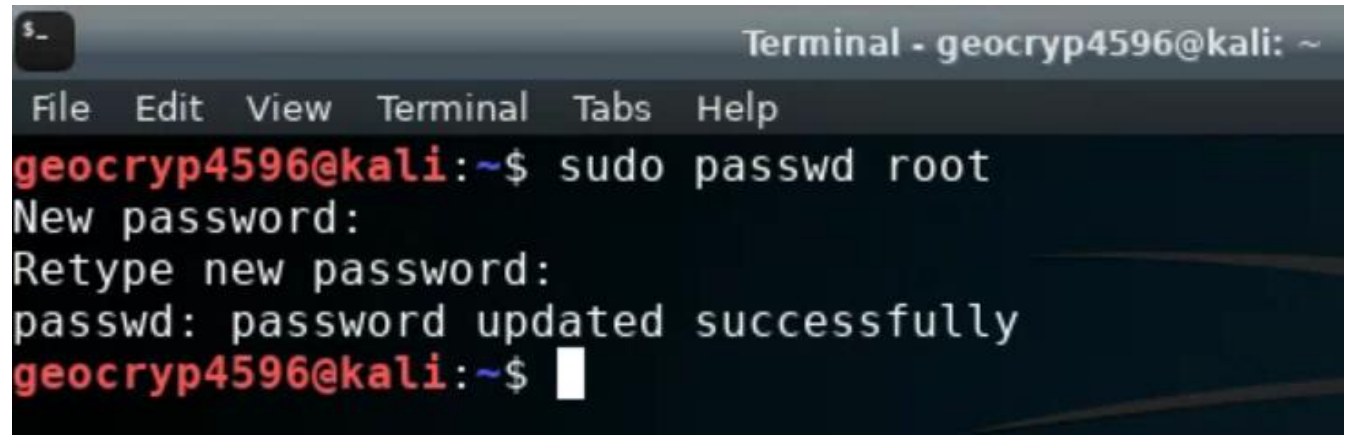
Unit #15

Agenda

- Change your Kali password!
- Application vulnerability and security testing
- Lab 6: Vulnerability Scanning – Part 2: Nessus
- Scan results
- Looking at a vulnerability
- ITACS Program

IMPORTANT: Change Kali's root Password Now!

- Kali's default root password is published and known to everyone
 - Login: root
 - Password: toor
- If you leave Kali running in the cloud (by mistake), someone may find it
- If they know enough to find it, they enough to login and access it
- If they use it, attack someone and create a problem – you are responsible!
- Change Kali's root password now!
- From the \$ prompt, type:
“sudo passwd root”



```
Terminal - geocryp4596@kali: ~
File Edit View Terminal Tabs Help
geocryp4596@kali:~$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
geocryp4596@kali:~$
```

Application Security

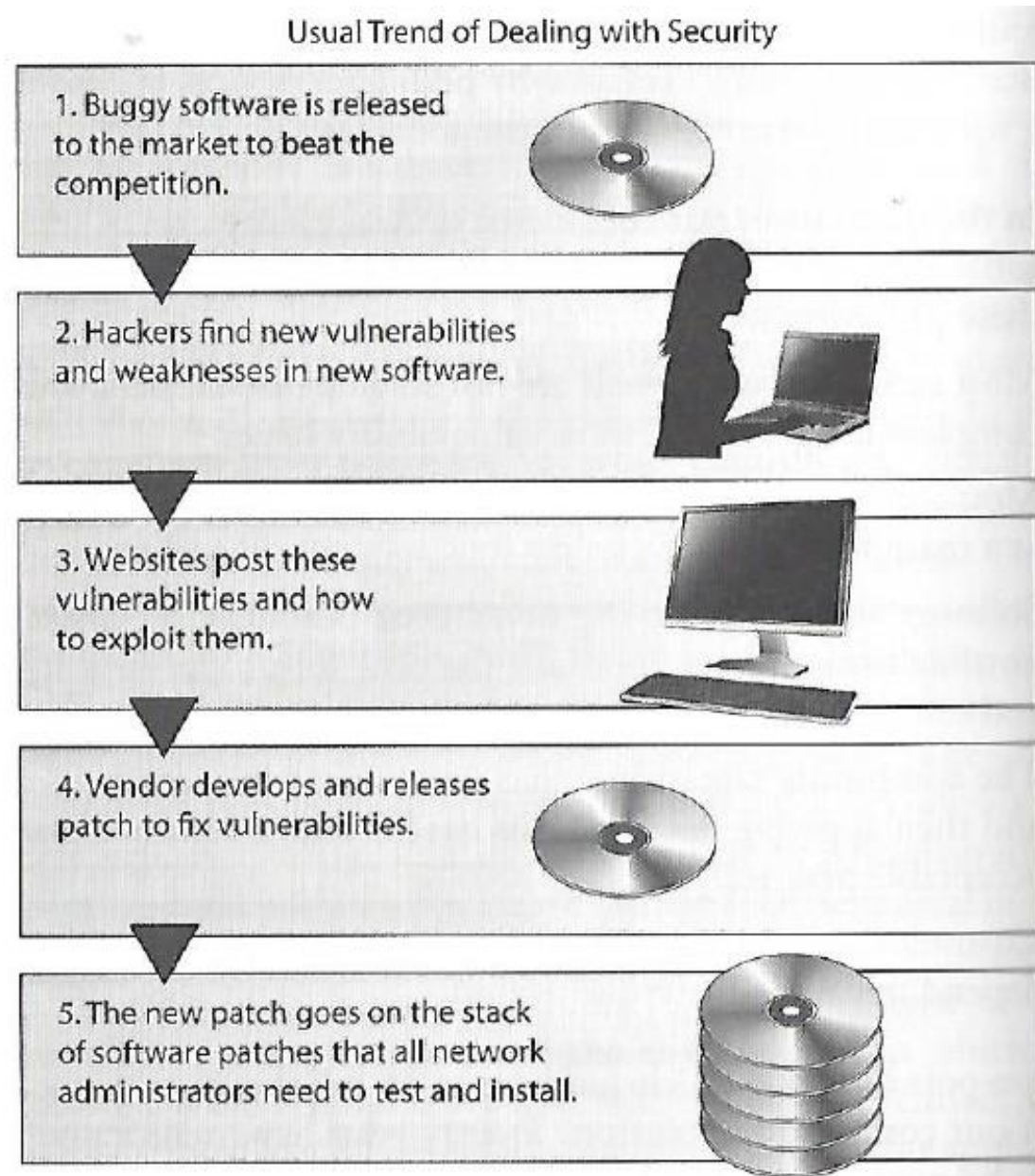
As applications become more accessible through the web, cloud and mobile devices,

organizations are being forced to abandon their reactive approach to security and, instead,

to take a proactive approach by minimizing risk directly in the software they buy, create and use to serve themselves and their customers



Usual trend

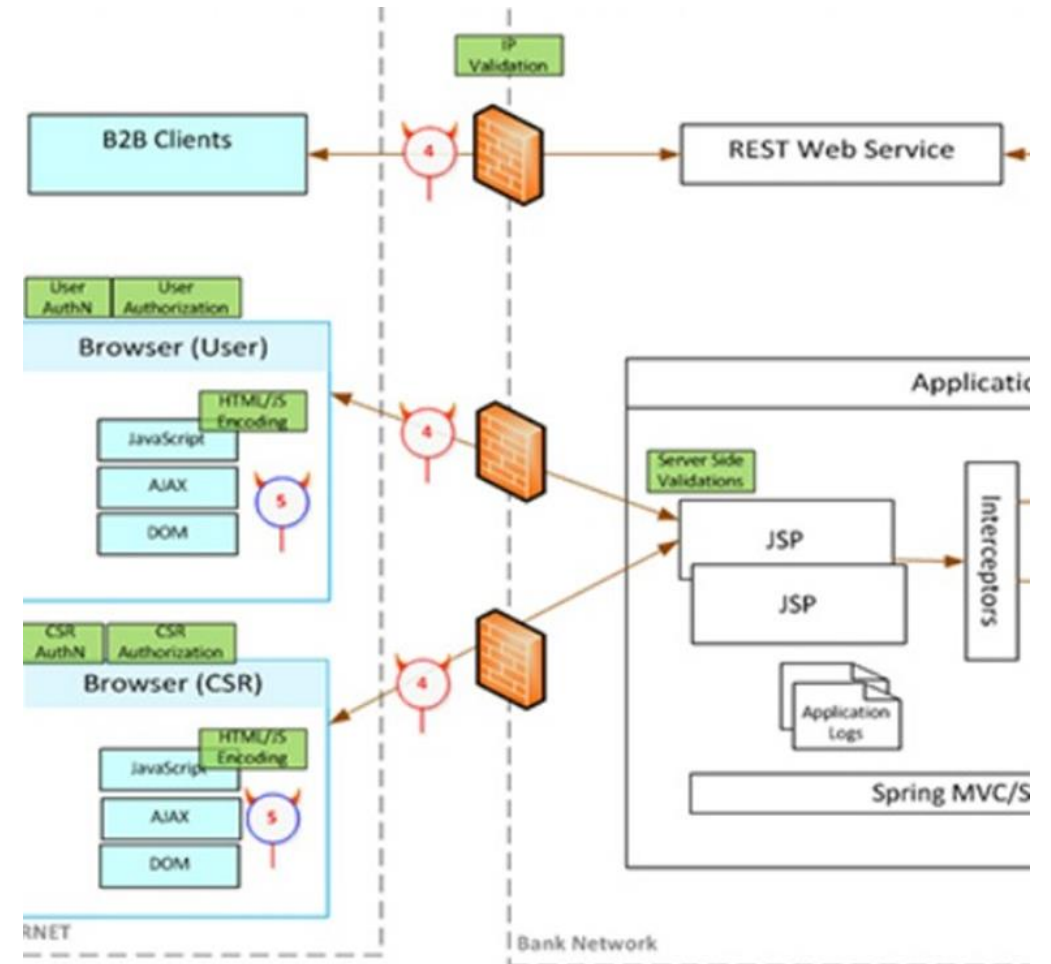


Software security, includes threat and attack surface analysis...

Attack surface is what is available to be used by an attacker against the application itself

Goal of attack surface analysis is to identify and reduce the amount of code and functionality accessible to untrusted users

Development team should reduce the attack surface as much as possible to remove “resources” that can be used as avenues for the attacker to use



Web Application Security Testing Methodology

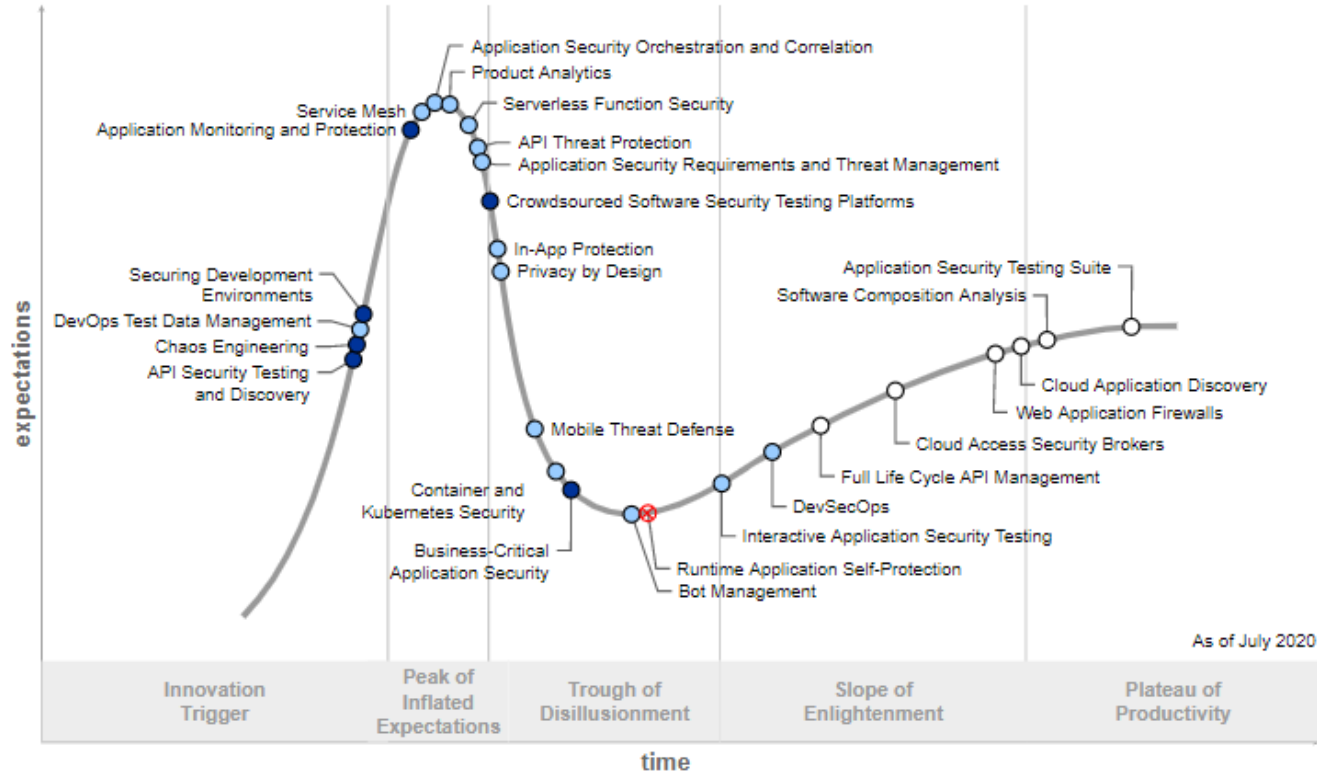


Application Security Testing (AST)

Fundamental Capabilities

- Static AST (SAST)
- Software Composition Analysis (SCA)
- Dynamic AST (DAST)
- API Testing

Interactive Hype Cycle



2020 Magic Quadrant



Estimated at \$1.33 billion, the AST market is projected to have a 10% compound annual growth rate through 2022



OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks



<https://owasp.org>

This work is licensed under a  **creative commons** [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)

T10- OWASP Top 10 Application Security Risks – 2017	6
A1:2017- Injection	7
A2:2017- Broken Authentication	8
A3:2017- Sensitive Data Exposure	9
A4:2017- XML External Entities (XXE)	10
A5:2017- Broken Access Control	11
A6:2017- Security Misconfiguration	12
A7:2017- Cross-Site Scripting (XSS)	13
A8:2017- Insecure Deserialization	14
A9:2017- Using Components with Known Vulnerabilities	15
A10:2017- Insufficient Logging & Monitoring	16

https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet

MITRE's Common Application Vulnerabilities

Secure | <https://cwe.mitre.org/data/definitions/699.html>

CWE Common Weakness Enumeration
A Community-Developed List of Software Weakness Types

CWE and SANS Institute
TOP 25 MOST DANGEROUS SOFTWARE ERRORS

Home > CWE List > CWE- Individual Dictionary Definition (3.0) ID Lookup: Go

Home | About | CWE List | Scoring | Community | News | Search

CWE VIEW: Development Concepts

View ID: 699 Status: Incomplete
Type: Graph

Objective

This view organizes weaknesses around concepts that are frequently used or encountered in software development. Accordingly, this view can align closely with the perspectives of developers, educators, and assessment vendors. It borrows heavily from the organizational structure used by Seven Pernicious Kingdoms, but it also provides a variety of other categories that are intended to simplify navigation, browsing, and mapping.

Audience

Stakeholder	Description
Assessment Vendors	
Software Developers	
Educators	

Relationships

Expand All

699 - Development Concepts

- Configuration - (16)
- Data Processing Errors - (19)
- Pathname Traversal and Equivalence Errors - (21)
- Numeric Errors - (189)
- 7PK - Security Features - (254)
- 7PK - Time and State - (361)
- Error Conditions, Return Values, Status Codes - (389)
- Resource Management Errors - (399)
- Channel and Path Errors - (417)
- Handler Errors - (429)
- Behavioral Problems - (438)
- Business Logic Errors - (840)
- Web Problems - (442)
- User Interface Security Issues - (355)
- Initialization and Cleanup Errors - (452)
- Pointer Issues - (465)
- Mobile Code Issues - (490)
- Often Misused: Arguments and Parameters - (559)
- Expression Issues - (569)
- Violation of Secure Design Principles - (657)
- Bad Coding Practices - (1006)

- Development Concepts

- Configuration - (16)
- Data Processing Errors - (19)
- Pathname Traversal and Equivalence Errors - (21)
- Numeric Errors - (189)
- 7PK - Security Features - (254)
- 7PK - Time and State - (361)
- Error Conditions, Return Values, Status Codes - (389)
- Resource Management Errors - (399)
- Channel and Path Errors - (417)
- Handler Errors - (429)
- Behavioral Problems - (438)
- Business Logic Errors - (840)
- Web Problems - (442)
- User Interface Security Issues - (355)
- Initialization and Cleanup Errors - (452)
- Pointer Issues - (465)
- Mobile Code Issues - (490)
- Often Misused: Arguments and Parameters - (559)
- Expression Issues - (569)
- Violation of Secure Design Principles - (657)
- Bad Coding Practices - (1006)

MITRE's Common Weakness Enumeration



[Login](#) | [Create Account](#)

[Find Training](#)

[Live Training](#)

[Online Training](#)

[Programs](#)

CWE/SANS TOP 25 Most Dangerous Software Errors

Insecure Interaction Between Components

These weaknesses are related to insecure ways in which data is sent and received between separate components, modules, programs, processes, threads, or systems.

CWE ID	Name
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')

Porous Defenses

The weaknesses in this category are related to defensive techniques that are often misused, abused, or just plain ignored.

CWE ID	Name
CWE-306	Missing Authentication for Critical Function
CWE-862	Missing Authorization
CWE-798	Use of Hard-coded Credentials
CWE-311	Missing Encryption of Sensitive Data
CWE-807	Reliance on Untrusted Inputs in a Security Decision
CWE-250	Execution with Unnecessary Privileges
CWE-863	Incorrect Authorization
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-307	Improper Restriction of Excessive Authentication Attempts
CWE-759	Use of a One-Way Hash without a Salt

Risky Resource Management

The weaknesses in this category are related to ways in which software does not properly manage the creation, usage, transfer, or destruction of important system resources.

CWE ID	Name
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-494	Download of Code Without Integrity Check
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-676	Use of Potentially Dangerous Function
CWE-131	Incorrect Calculation of Buffer Size
CWE-134	Uncontrolled Format String
CWE-190	Integer Overflow or Wraparound

Vulnerability Scanning

- Scanning methods:
 - Safe
 - Destructive
- Service recognition – Determines what service is running on which ports
- Reports
 - Indicates the threat level for vulnerabilities it detects
 - Critical
 - High
 - Medium
 - Low
 - Informational
 - Description of Vulnerability
 - Risk Factor
 - CVE Number

The screenshot displays the Metaspitable2 web interface. At the top, there are navigation buttons: 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below this, a summary bar shows 'Hosts 1', 'Vulnerabilities 96', 'Remediations 5', and 'History 2'. A search bar is present with the text 'Search Vulnerabilities' and a magnifying glass icon, followed by '96 Vulnerabilities'. The main content is a table of vulnerabilities with columns for 'Sev', 'Name', 'Family', and 'Count'. The table lists several critical vulnerabilities, including 'SSL (Multiple Iss...', 'Bind Shell Backdoor D...', 'NFS Exported Share In...', 'rexecd Service Detection', 'Unix Operating System...', and 'VNC Server 'password'...'. To the right of the table, there is a 'Scan Details' section with fields for Policy, Status, Scanner, Start, End, and Elapsed. Below that is a 'Vulnerabilities' section with a donut chart and a legend for severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Sev	Name	Family	Count
CRITICAL	SSL (Multiple Iss...	Gain a shell remotely	3
CRITICAL	Bind Shell Backdoor D...	Backdoors	1
CRITICAL	NFS Exported Share In...	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Unix Operating System...	General	1
CRITICAL	VNC Server 'password'...	Gain a shell remotely	1
MIXED	Phpmyadmin (Mul...	CGI abuses	4
MIXED	SSL (Multiple Iss...	Service detection	3
MIXED	PHP (Multiple Iss...	CGI abuses	3

Scan Details

Policy: Metaspitable2 Scan
Status: Completed
Scanner: Local Scanner
Start: February 19 at 9:56 PM
End: February 19 at 10:26 PM
Elapsed: 31 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Application Vulnerability Testing Reports

Burp Scanner Sample Report

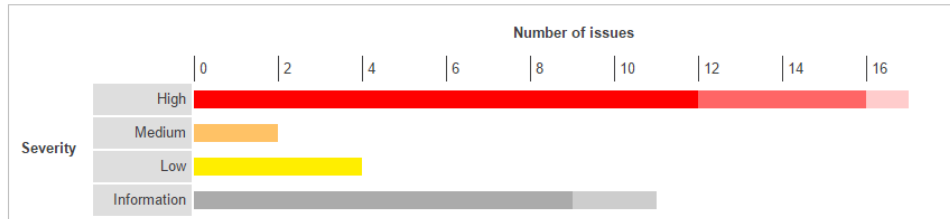


Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			Total
		Certain	Firm	Tentative	
Severity	High	12	4	1	17
	Medium	0	2	0	2
	Low	4	0	0	4
	Information	9	2	0	11

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. OS command injection

2. SQL injection

- 2.1. <http://mdsec.net/addressbook/32/Default.aspx> [Address parameter]
- 2.2. <http://mdsec.net/addressbook/32/Default.aspx> [Email parameter]
- 2.3. <https://mdsec.net/auth/319/Default.aspx> [password parameter]
- 2.4. <https://mdsec.net/auth/319/Default.aspx> [username parameter]

3. File path traversal

4. XML external entity injection

Executive Summary

Issue Types 32

TOC

Issue Type	Number of Issues
H Authentication Bypass Using SQL Injection	1
H Blind SQL Injection	1
H Cross-Site Scripting	11
H DOM Based Cross-Site Scripting	3
H Poison Null Byte Windows Files Retrieval	1
H Predictable Login Credentials	1
H SQL Injection	12
H Unencrypted Login Request	6
H XPath Injection	1
M Cross-Site Request Forgery	6
M Directory Listing	2
M HTTP Response Splitting	1
M Inadequate Account Lockout	1
M Link Injection (facilitates Cross-Site Request Forgery)	6
M Open Redirect	2
M Phishing Through Frames	6
M Session Identifier Not Updated	1
L Autocomplete HTML Attribute Not Disabled for Password Field	4
L Database Error Pattern Found	16
L Direct Access to Administration Pages	2
L Email Address Pattern Found in Parameter Value	2
L Hidden Directory Detected	3
L Microsoft ASP.NET Debugging Enabled	3
L Missing HttpOnly Attribute in Session Cookie	4
L Permanent Cookie Contains Sensitive Session Information	1
L Unencrypted __VIEWSTATE Parameter	4
L Unsigned __VIEWSTATE Parameter	4
I Application Error	15
I Application Test Script Detected	1
I Email Address Pattern Found	3
I HTML Comments Sensitive Information Disclosure	5
I Possible Server Path Disclosure Pattern Found	1

To run the Nessus portion of the vulnerability scanning lab...

You will need to complete the install and startup of Nessus

1. Startup Nessus Essentials scanner
2. Request and install your Nessus license key
3. Setup Nessus scan
4. Run Nessus scan...

Part 0. Ensure that your metasploitable2 instance is up-to-date

Part 1. Host Discovery and Scanning using NMAP

Part 2. Nessus
Start and register the Nessus Scanner
Run a Nessus Scan

Part 2. Nessus

Start and register the Nessus Scanner

1. Run the following to install nessus:

```
wget -O - https://gist.githubusercontent.com/deargle/d4dc4ea5a877ea13723d8e8ef9c11b08/raw/6ae94d25b0e1
```

If you get a sudo-related error, then log in as `root` and run it again, with just `bash` at the end instead of `sudo bash`.

What did I just run? The above script downloads a code snippet from [here](#), "writes" it to std out (that's the `-O` bit), and then pipes that code to be run by `bash` as root.

Any time you see this pattern, take heed -- you are about to run arbitrary code on your system. Do you trust it? You should carefully review any script you are about to run.
2. Start the nessus daemon

```
service nessusd start
```

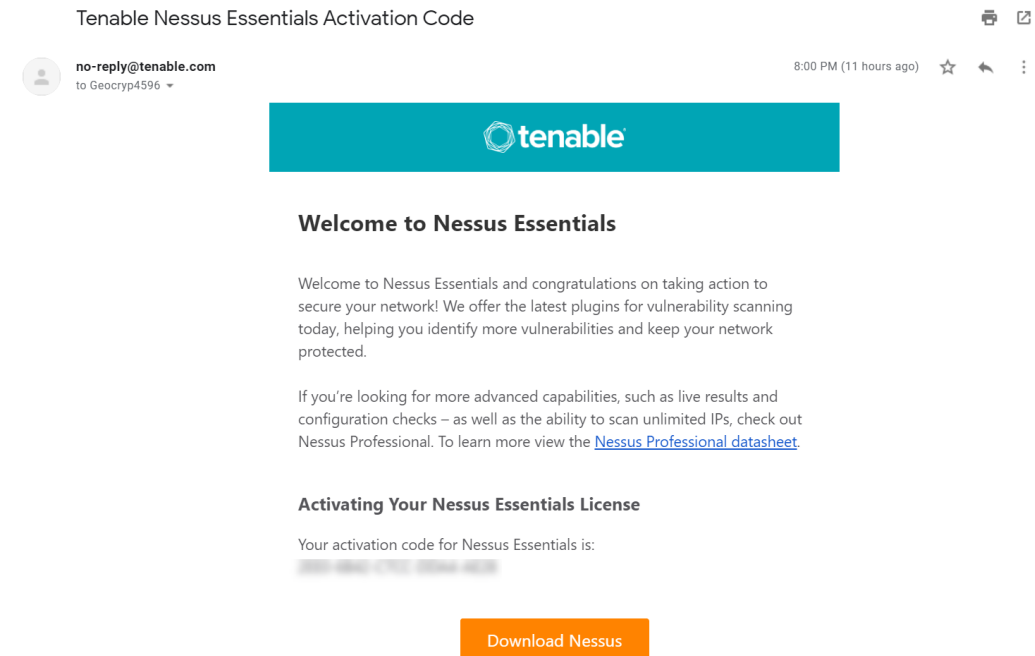
The `d` in `nessusd` stands for 'daemon'.
3. Open Firefox and browse to <https://kali:8834>. Click 'Advanced' > 'Add Security Exception' > 'Confirm Security Exception' to get past the SSL warning.
4. Select "Nessus Essentials"
5. Get a registration activation code by entering an email address.
6. Choose any `username:password` you prefer for use with nessus. For instance, you could use user `root` password `toor` when prompted by Nessus. Click "reload" if the page fails to load.

Run a Nessus Scan

1. Click the "Scans" tab and press the "New Scan" button.
2. Choose "Basic Network Scan"
3. In the "Name" field, enter "Metasploitable2" or something more cool-sounding. In the "Targets" field, enter the IP address of the Metasploitable2 VM.
4. Under the category "Discovery", change the "Scan Type" to "All ports"
5. Under "Assessment", change the dropdown to "Scan for known web vulnerabilities"
6. Under "Advanced", select Scan Type "Custom". Then select "General" on the left. Uncheck "Enable safe checks," and (Important!) set "Max number of concurrent TCP sessions per host" to 100.

Starting up Nessus Essentials

- In Kali, bring up Firefox browser
- Navigate to <https://kali:8834> (Nessus is installed and listening on port 8834)
- Request and provide your Nessus activation code, it will show up by email



To run the Nessus portion of the vulnerability scanning lab...

- You will need to complete the install and startup of Nessus
 1. Startup Nessus Essentials scanner
 2. Request and install your Nessus license key
 3. Start up Metaspolitable2
 4. Setup Nessus scan
 5. Run Nessus scan...

Applications Application Finder

Application Finder

virt

- All Applications
- Bookmarks
- Commands History
- 01 - Information ...
- 02 - Vulnerability ...
- 03 - Web Applicat...
- 04 - Database As...
- 05 - Password Att...
- 06 - Wireless Att...
- 07 - Reverse Engi...
- 08 - Exploitation ...
- 09 - Sniffing & Sp...
- 10 - Post Exploita...
- 11 - Forensics
- 12 - Reporting Tools

Preferences

Florence Virtual Keyboard
Florence Virtual Keyboard

Virtual Machine Manager
Manage virtual machines

Applications Virtual Machine Manager

Virtual Machine Manager

File Edit View Help

Open

Name CPU usage

Power on the virtual machine

Name	CPU usage
metasploitable2 Shutoff	
security-onion Shutoff	
Win7 Shutoff	

Virtual Machine Manager

File Edit View Help

Open

Name CPU us.

metasploitable2
Running

security-onion
Shutoff

Win7
Shutoff

metasploitable2 on QEMU/KVM

File Virtual Machine View Send Key

```
Login with username/password 'msfadmin/msfadmin' to get started

!!!Note that nothing will appear in the terminal when you type your password!!!!

metasploitable login:

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with username/password 'msfadmin/msfadmin' to get started

!!!Note that nothing will appear in the terminal when you type your password!!!!

metasploitable login:
```

Follow lab instructions to create a vulnerability scan of Metasploitable2

The screenshot displays the Nessus Professional interface for configuring a Metasploitable2 scan. The left sidebar shows navigation options like 'My Scans', 'All Scans', and 'Trash'. The main content area is titled 'Metasploitable2 scan / Configuration' and includes a 'Back to Scan Report' link. The 'Settings' tab is active, with sub-tabs for 'Settings', 'Credentials', and 'Plugins'. A vertical menu on the left lists categories: BASIC, DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The 'General' option under the 'ADVANCED' category is highlighted with a red circle. The 'General Settings' section contains several checkboxes: 'Enable safe checks', 'Stop scanning hosts that become unresponsive during the scan', 'Scan IP addresses in a random order', 'Automatically accept detected SSH disclaimer prompts', and 'Scan targets with multiple domain names in parallel'. The 'Performance Options' section includes a checkbox for 'Slow down the scan when network congestion is detected' and several input fields: 'Network timeout (in seconds)' set to 5, 'Max simultaneous checks per host' set to 4, 'Max simultaneous hosts per scan' set to 30, 'Max number of concurrent TCP sessions per host' set to 100 (circled in red), and 'Max number of concurrent TCP sessions per scan' which is empty.

Run the Nessus computer vulnerability scan...
(it may take ~30+ minutes)...

The screenshot shows the Nessus Essentials web interface in a browser. The browser's address bar displays the URL `https://kali:8834/#/scans/folders/my-scans`. The browser's bookmark bar includes links to Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, Exploit-DB, GHDB, and MSFU. The Nessus Essentials interface has a dark blue header with the logo and navigation tabs for 'Scans' and 'Settings'. The user's name 'geocryp4596' is visible in the top right. A left sidebar contains navigation options: 'My Scans', 'All Scans', 'Trash', 'RESOURCES', 'Policies', 'Plugin Rules', and 'Tenable News'. The main content area is titled 'My Scans' and features buttons for 'Import', 'New Folder', and 'New Scan'. A search bar labeled 'Search Scans' shows '1 Scan'. Below is a table with the following data:

<input type="checkbox"/>	Name	Schedule	Last Modified	Launch
<input type="checkbox"/>	Metaspitable2	On Demand	✓ February 19 at 10:26 PM	▶ ×

Review vulnerability scan results

The screenshot displays the Nessus Essentials web interface. The browser address bar shows the URL `https://kali:8834/#/scans/reports/5/hosts`. The page title is "Metaspolitable2". The interface includes a sidebar with navigation options like "My Scans", "All Scans", and "Trash". The main content area shows a summary of scan results: 1 Host, 96 Vulnerabilities, 5 Remediations, and 2 History items. A table lists the host `192.168.55.102` with a vulnerability score of 150, broken down into 8 Critical, 10 High, 38 Medium, and 9 Low vulnerabilities. A "Scan Details" panel on the right provides information about the scan policy, status, scanner, start/end times, and duration.

Nessus Essentials / Folde x +

https://kali:8834/#/scans/reports/5/hosts

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

nessus Essentials Scans Settings geocryp4596

Metaspolitable2

[Back to My Scans](#) Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 96 Remediations 5 History 2

Filter Search Hosts 1 Host

Host	Vulnerabilities
<input type="checkbox"/> 192.168.55.102	8 10 38 9 150

Scan Details

Policy: Metaspolitable2 Scan
Status: Completed
Scanner: Local Scanner
Start: February 19 at 9:56 PM
End: February 19 at 10:26 PM
Elapsed: 31 minutes

Review vulnerability scan results

Metaspitable2

[Back to My Scans](#)

Configure

Audit Trail

Launch

Report

Export

Hosts 1

Vulnerabilities 96

Remediations 5

History 2

Filter Search Vulnerabilities

96 Vulnerabilities

Sev	Name	Family	Count		
CRITICAL	SSL (Multiple Iss...	Gain a shell remotely	3		
CRITICAL	Bind Shell Backdoor D...	Backdoors	1		
CRITICAL	NFS Exported Share In...	RPC	1		
CRITICAL	rexecd Service Detection	Service detection	1		
CRITICAL	Unix Operating System...	General	1		
CRITICAL	VNC Server 'password'...	Gain a shell remotely	1		
MIXED	Phpmyadmin (Mul...	CGI abuses	4		
MIXED	SSL (Multiple Iss...	Service detection	3		
MIXED	PHP (Multiple Iss...	CGI abuses	3		

Scan Details

Policy: Metaspitable2 Scan
Status: Completed
Scanner: Local Scanner
Start: February 19 at 9:56 PM
End: February 19 at 10:26 PM
Elapsed: 31 minutes

Vulnerabilities



Metaspitable2

[Back to My Scans](#)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 96 Remediations 5 History 2

Filter Search Vulnerabilities 96 Vulnerabilities

Sev	Name	Family	Count		
CRITICAL	SSL (Multiple Iss...	Gain a shell remotely	3		
CRITICAL	Bind Shell Backdoor D...	Backdoors	1		
CRITICAL	NFS Exported Share In...	RPC	1		
CRITICAL	rexecd Service Detection	Service detection	1		
CRITICAL	Unix Operating System...	General	1		
CRITICAL	VNC Server 'password'...	Gain a shell remotely	1		
MIXED	Phpmyadmin (Mul...	CGI abuses	4		
MIXED	SSL (Multiple Iss...	Service detection	3		
MIXED	PHP (Multiple Iss...	CGI abuses	3		
MIXED	Twiki (Multiple Iss...	CGI abuses	2		
HIGH	CGI Generic Remote F...	CGI abuses	1		
HIGH	rlogin Service Detection	Service detection	1		
HIGH	rsh Service Detection	Service detection	1		
MIXED	SSL (Multiple Iss...	General	28		
MIXED	DNS (Multiple Iss...	DNS	4		
MIXED	HTTP (Multiple Is...	Web Servers	4		
MIXED	SSH (Multiple Iss...	Misc.	4		
MIXED	PHP (Multiple Iss...	Web Servers	3		
MEDIUM	CGI Generic XSS (quic...	CGI abuses : XSS	1		
MEDIUM	NFS Shares World Rea...	RPC	1		
MEDIUM	Samba Badlock Vulner...	General	1		
MEDIUM	SMB Signing not required	Misc.	1		
MEDIUM	Browsable Web Directo...	CGI abuses	1		
MEDIUM	CGI Generic Cookie Inj...	CGI abuses	1		
MEDIUM	CGI Generic HTML Inj...	CGI abuses : XSS	1		
MEDIUM	Web Application Poten...	Web Servers	1		
MIXED	Web Server (Multi...	Web Servers	4		
LOW	SSL/TLS Diffie-Hellma...	Misc.	1		
LOW	X Server Detection	Service detection	1		
INFO	Net-117-FYMaqpaaris...	Backdoors	9		
INFO	VNC (Multiple Iss...	Service detection	3		
INFO	Apache HTTP Se...	Web Servers	2		
INFO	HTTP (Multiple Is...	CGI abuses	2		
INFO	ISC Bind (Multiple...	DNS	2		
INFO	RPC (Multiple Iss...	RPC	2		
INFO	SSH (Multiple Iss...	General	2		

Scan Details

Policy: Metaspitable2 Scan
Status: Completed
Scanner: Local Scanner
Start: February 19 at 9:56 PM
End: February 19 at 10:26 PM
Elapsed: 31 minutes

Vulnerabilities



Results per page 50

Showing: 1 to 50 of 96

Computer vulnerability scan report...

192.168.55.102



Vulnerabilities Total: 148

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	51988	Bind Shell Backdoor Detection
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	61708	VNC Server 'password' Password
CRITICAL	10.0	10203	rexecd Service Detection

Vulnerabilities



[Hosts](#) 1[Vulnerabilities](#) 96[Remediations](#) 5[History](#) 2**CRITICAL**

Debian OpenSSH/OpenSSL Package Random Number Generator ...

Plugin Details

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Severity: Critical
ID: 32321
Version: 1.25
Type: remote
Family: Gain a shell remotely
Published: May 15, 2008
Modified: November 15, 2018

Metaspolitable2 / Plugin #32321

[Configure](#) [Audit Trail](#) [Launch ▾](#) [Report ▾](#) [Export ▾](#)[← Back to Vulnerability Group](#)[Hosts](#) 1 [Vulnerabilities](#) 96 [Remediations](#) 5 [History](#) 2**CRITICAL** Debian OpenSSH/OpenSSL Package Random Number Generator ...

Plugin Details

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

See Also<http://www.nessus.org/u/11079bdc><http://www.nessus.org/u/7146424>**Output**

No output recorded.	
Port	Hosts
5432/tcp/postgresql	192.168.55.102
35/tcp/ntp	192.168.55.102

Severity: Critical

ID: 32321

Version: 1.25

Type: remote

Family: Gain a shell remotely

Published: May 15, 2008

Modified: November 15, 2018

Risk Information

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Temporal Score: 8.3

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C

I:C/A:C

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Vulnerability Information

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: May 14, 2008

Vulnerability Pub Date: May 13, 2008

In the news: true

Exploitable With

Core Impact

Reference Information

CWE: 310

BID: 29179

CVE: CVE-2008-0166

Hosts 1

Vulnerabilities 96

Remediations 5

History 2

CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator ...

Plugin Details

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

See Also

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

Output

No output recorded.

Port *	Hosts
5432 / tcp / postgresql	192.168.55.102
25 / tcp / smtp	192.168.55.102

Severity: Critical
 ID: 32321
 Version: 1.25
 Type: remote
 Family: Gain a shell remotely
 Published: May 15, 2008
 Modified: November 15, 2018

Risk Information

Risk Factor: Critical
 CVSS Base Score: 10.0
 CVSS Temporal Score: 8.3
 CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C
 /I:C/A:C
 CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Vulnerability Information

Exploit Available: true
 Exploit Ease: Exploits are available
 Patch Pub Date: May 14, 2008
 Vulnerability Pub Date: May 13, 2008
 In the news: true

Exploitable With

Debian Security Advisory DSA-1571-1 security@debian.org
<http://www.debian.org/security/> Florian Weimer
 May 13, 2008 <http://www.debian.org/security/faq>

Package : openssl
 Vulnerability : predictable random number generator
 Problem type : remote
 Debian-specific: yes
 CVE Id(s) : CVE-2008-0166

Luciano Bello discovered that the random number generator in Debian's openssl package is predictable. This is caused by an incorrect Debian-specific change to the openssl package (CVE-2008-0166). As a result, cryptographic key material may be guessable.

This is a Debian-specific vulnerability which does not affect other operating systems which are not based on Debian. However, other systems can be indirectly affected if weak keys are imported into them.

It is strongly recommended that all cryptographic key material which has been generated by OpenSSL versions starting with 0.9.8c-1 on Debian systems is recreated from scratch. Furthermore, all DSA keys ever used on affected Debian systems for signing or authentication purposes should be considered compromised; the Digital Signature Algorithm relies on a secret random value used during signature generation.

The first vulnerable version, 0.9.8c-1, was upgraded to the unstable distribution on 2006-09-17, and has since propagated to the testing and current stable (etch) distributions. The old stable distribution (sarge) is not affected.

Affected keys include SSH keys, OpenVPN keys, DNSSEC keys, and key material for use in X.509 certificates and session keys used in SSL/TLS connections. Keys generated with GnuPG or GnuTLS are not affected, though.

A detector for known weak key material will be published at:

```
<http://security.debian.org/project/extra/dowkd/dowkd.pl.gz>
<http://security.debian.org/project/extra/dowkd/dowkd.pl.gz.asc>
(OpenPGP signature)
```

Instructions how to implement key rollover for various packages will be published at:

```
<http://www.debian.org/security/key-rollover/>
```

This web site will be continuously updated to reflect new and updated instructions on key rollovers for packages using SSL certificates. Popular packages not affected will also be listed.

In addition to this critical change, two other vulnerabilities have been fixed in the openssl package which were originally scheduled for release with the next etch point release: OpenSSL's DTLS (Datagram TLS, basically "SSL over UDP") implementation did not actually implement the DTLS specification, but a potentially much weaker protocol, and contained a vulnerability permitting arbitrary code execution (CVE-2007-4995). A side channel attack in the integer multiplication routines is also addressed (CVE-2007-3108).

For the stable distribution (etch), these problems have been fixed in version 0.9.8c-4etch3.

For the unstable distribution (sid) and the testing distribution (lenny), these problems have been fixed in version 0.9.8g-9.

We recommend that you upgrade your openssl package and subsequently regenerate any cryptographic material, as outlined above.

Upgrade instructions

```
wget url
will fetch the file for you
dpkg -i file.deb
will install the referenced file.
```

If you are using the apt-get package manager, use the line for sources.list as given below:

```
apt-get update
will update the internal database
apt-get upgrade
will install corrected packages
```

You may use an automated update by adding the resources from the footer to the proper configuration.

Debian GNU/Linux 4.0 alias etch

Source archives:

```
http://security.debian.org/pool/updates/main/o/openssl/openssl_0.9.8c-4etch3
Size/MD5 checksum: 1099 5e60a893c9c3258669845b0a56d9d9d6
```

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

See Also

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>


```

Package      : openssl
Vulnerability : predictable random number generator
Problem type  : remote
Debian-specific: yes
CVE Id(s)    : CVE-2008-0166

```

Luciano Bello discovered that the random number generator in Debian's openssl package is predictable. This is caused by an incorrect Debian-specific change to the openssl package (CVE-2008-0166). As a result, cryptographic key material may be guessable.

This is a Debian-specific vulnerability which does not affect other operating systems which are not based on Debian. However, other systems can be indirectly affected if weak keys are imported into them.

It is strongly recommended that all cryptographic key material which has been generated by OpenSSL versions starting with 0.9.8c-1 on Debian systems is recreated from scratch. Furthermore, all DSA keys ever used on affected Debian systems for signing or authentication purposes should be considered compromised; the Digital Signature Algorithm relies on a secret random value used during signature generation.

The first vulnerable version, 0.9.8c-1, was uploaded to the unstable distribution on 2006-09-17, and has since propagated to the testing and current stable (etch) distributions. The old stable distribution (sarge) is not affected.

Affected keys include SSH keys, OpenVPN keys, DNSSEC keys, and key material for use in X.509 certificates and session keys used in SSL/TLS connections. Keys generated with GnuPG or GNUTLS are not affected, though.

```

Package      : openssl
Vulnerability : predictable random number generator
Problem type  : remote
Debian-specific: yes
CVE Id(s)    : CVE-2008-0166

```

Luciano Bello discovered that the random number generator in Debian's openssl package is predictable. This is caused by an incorrect Debian-specific change to the openssl package (CVE-2008-0166). As a result, cryptographic key material may be guessable.

This is a Debian-specific vulnerability which does not affect other operating systems which are not based on Debian. However, other systems can be indirectly affected if weak keys are imported into them.

It is strongly recommended that all cryptographic key material which has been generated by OpenSSL versions starting with 0.9.8c-1 on Debian systems is recreated from scratch. Furthermore, all DSA keys ever used on affected Debian systems for signing or authentication purposes should be considered compromised; the Digital Signature Algorithm relies on a secret random value used during signature generation.

The first vulnerable version, 0.9.8c-1, was uploaded to the unstable distribution on 2006-09-17, and has since propagated to the testing and current stable (etch) distributions. The old stable distribution (sarge) is not affected.

Affected keys include SSH keys, OpenVPN keys, DNSSEC keys, and key material for use in X.509 certificates and session keys used in SSL/TLS connections. Keys generated with GnuPG or GNUTLS are not affected, though.

A detector for known weak key material will be published at:

<<http://security.debian.org/project/extra/dowkd/dowkd.pl.gz>>
 <<http://security.debian.org/project/extra/dowkd/dowkd.pl.gz.asc>>
 (OpenPGP signature)

Instructions how to implement key rollover for various packages will be published at:

<<http://www.debian.org/security/key-rollover/>>

This web site will be continuously updated to reflect new and updated instructions on key rollovers for packages using SSL certificates. Popular packages not affected will also be listed.

In addition to this critical change, two other vulnerabilities have been fixed in the openssl package which were originally scheduled for release with the next etch point release: OpenSSL's DTLS (Datagram TLS, basically "SSL over UDP") implementation did not actually implement the DTLS specification, but a potentially much weaker protocol, and contained a vulnerability permitting arbitrary code execution (CVE-2007-4995). A side channel attack in the integer multiplication routines is also addressed (CVE-2007-3108).

For the stable distribution (etch), these problems have been fixed in version 0.9.8c-4etch3.

For the unstable distribution (sid) and the testing distribution (lenny), these problems have been fixed in version 0.9.8g-9.

We recommend that you upgrade your openssl package and subsequently regenerate any cryptographic material, as outlined above.

Upgrade instructions

```

wget url
will fetch the file for you
dpkg -i file.deb
will install the referenced file.

```

If you are using the apt-get package manager, use the line for sources.list as given below:

```

apt-get update
will update the internal database
apt-get upgrade
will install corrected packages

```

You may use an automated update by adding the resources from the footer to the proper configuration.

Debian GNU/Linux 4.0 alias etch

Source archives:

http://security.debian.org/pool/updates/main/o/openssl/openssl_0.9.8c-4etch3
 Size/MD5 checksum: 1099 5e60a893c9c3258669845b0a56d9d9d6

Upgrade instructions

```
wget url
    will fetch the file for you
dpkg -i file.deb
    will install the referenced file.
```

If you are using the apt-get package manager, use the line for sources.list as given below:

```
apt-get update
    will update the internal database
apt-get upgrade
    will install corrected packages
```

Package : openssl
Vulnerability : predictable random number generator
Problem type : remote
Debian-specific: yes
CVE Id(s) : CVE-2008-0166

Luciano Bello discovered that the random number generator in Debian's openssl package is predictable. This is caused by an incorrect Debian-specific change to the openssl package (CVE-2008-0166). As a result, cryptographic key material may be guessable.

This is a Debian-specific vulnerability which does not affect other operating systems which are not based on Debian. However, other systems can be indirectly affected if weak keys are imported into them.

It is strongly recommended that all cryptographic key material which has been generated by OpenSSL versions starting with 0.9.8c-1 on Debian systems is recreated from scratch. Furthermore, all DSA keys ever used on affected Debian systems for signing or authentication purposes should be considered compromised; the Digital Signature Algorithm relies on a secret random value used during signature generation.

The first vulnerable version, 0.9.8c-1, was uploaded to the unstable distribution on 2006-09-17, and has since propagated to the testing and current stable (etch) distributions. The old stable distribution (sarge) is not affected.

Affected keys include SSH keys, OpenVPN keys, DNSSEC keys, and key material for use in X.509 certificates and session keys used in SSL/TLS connections. Keys generated with GnuPG or GnuTLS are not affected, though.

A detector for known weak key material will be published at:

<<http://security.debian.org/project/extra/dowkd/dowkd.pl.gz>>
<<http://security.debian.org/project/extra/dowkd/dowkd.pl.gz.asc>>
(OpenPGP signature)

Instructions how to implement key rollover for various packages will be published at:

<<http://www.debian.org/security/key-rollover/>>

This web site will be continuously updated to reflect new and updated instructions on key rollovers for packages using SSL certificates. Popular packages not affected will also be listed.

In addition to this critical change, two other vulnerabilities have been fixed in the openssl package which were originally scheduled for release with the next etch point release: OpenSSL's DTLS (Datagram TLS, basically "SSL over UDP") implementation did not actually implement the DTLS specification, but a potentially much weaker protocol, and contained a vulnerability permitting arbitrary code execution (CVE-2007-4995). A side channel attack in the integer multiplication routines is also addressed (CVE-2007-3108).

For the stable distribution (etch), these problems have been fixed in version 0.9.8c-4etch3.

For the unstable distribution (sid) and the testing distribution (lenny), these problems have been fixed in version 0.9.8g-9.

We recommend that you upgrade your openssl package and subsequently regenerate any cryptographic material, as outlined above.

Upgrade instructions

```
wget url
    will fetch the file for you
dpkg -i file.deb
    will install the referenced file.
```

If you are using the apt-get package manager, use the line for sources.list as given below:

```
apt-get update
    will update the internal database
apt-get upgrade
    will install corrected packages
```

You may use an automated update by adding the resources from the footer to the proper configuration.

Debian GNU/Linux 4.0 alias etch

Source archives:

http://security.debian.org/pool/updates/main/o/openssl/openssl_0.9.8c-4etch3
Size/MD5 checksum: 1099 5e60a893c9c3258669845b0a56d9d9d6

Hosts 1

Vulnerabilities 96

Remediations 5

History 2

CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator ... >**Description**

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

See Also

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

Output

No output recorded.

Port ▲	Hosts
5432 / tcp / postgresql	192.168.55.102
25 / tcp / smtp	192.168.55.102

Plugin Details

Severity: Critical
 ID: 32321
 Version: 1.25
 Type: remote
 Family: Gain a shell remotely
 Published: May 15, 2008
 Modified: November 15, 2018

Risk Information

Risk Factor: Critical
 CVSS Base Score: 10.0
 CVSS Temporal Score: 8.3
 CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C
 /I:C/A:C
 CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Vulnerability Information

Exploit Available: true
 Exploit Ease: Exploits are available
 Patch Pub Date: May 14, 2008
 Vulnerability Pub Date: May 13, 2008
 In the news: true

Exploitable With

Core Impact

Reference Information

CWE: [310](#)
 BID: [29179](#)
 CVE: [CVE-2008-0166](#)

Vulnerability Information

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: May 14, 2008

Vulnerability Pub Date: May 13, 2008

In the news: true

Exploitable With

Core Impact

Reference Information

CWE: [310](#)
 BID: [29179](#)
 CVE: [CVE-2008-0166](#)

Common Vulnerabilities and Exposures

- CVE created by <https://cve.mitre.org/>
- CVE search engine at: <https://nvd.nist.gov/search>

Search for the issue (CVE-2008-0166) we are looking at from the Nessus report...

- [NIST National Vulnerability Database](#)
- [CVE.MITRE.ORG](#)

Hosts 1

Vulnerabilities 96

Remediations 5

History 2

Search Actions



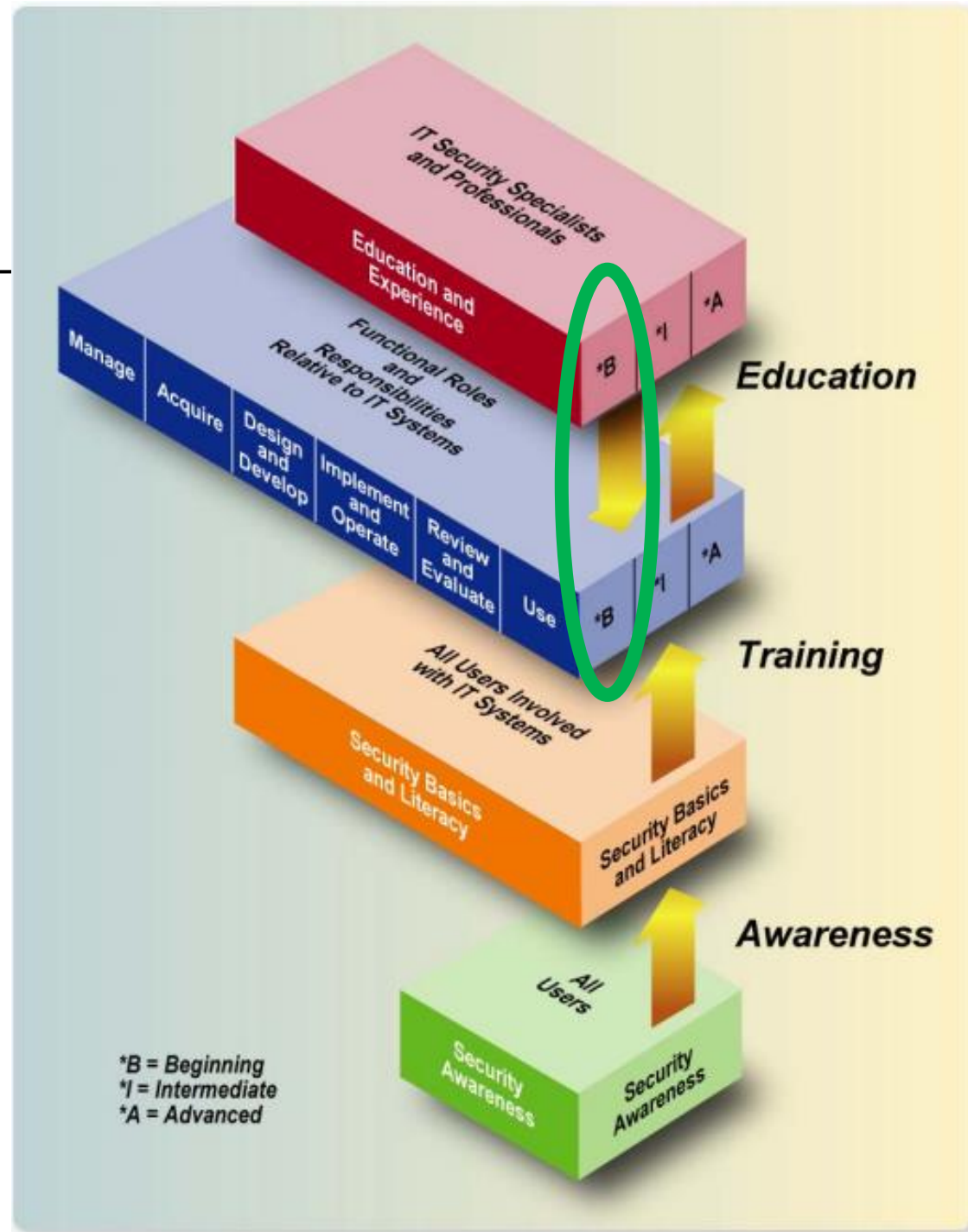
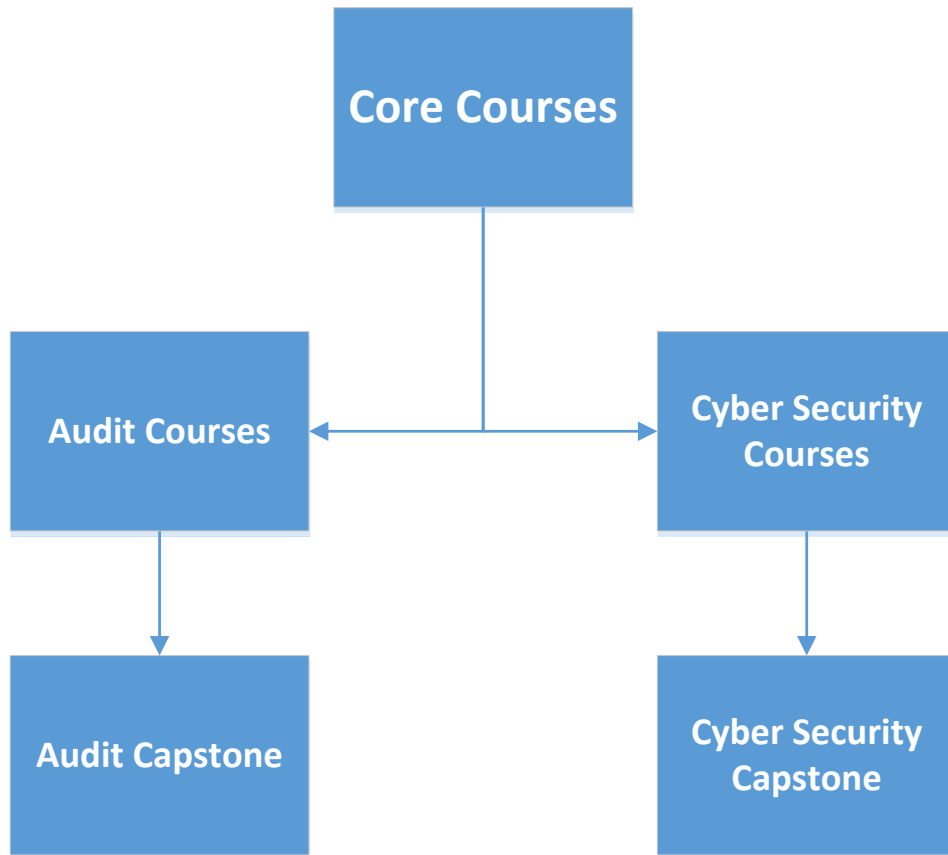
5 Actions

Action	Vulns ▾	Hosts
phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3): Upgrade to phpMyAdmin version 4.8.6 or later. Alternatively, apply the patches referenced in the vendor advisories.	5	1
Apache PHP-CGI Remote Code Execution: Upgrade to PHP 5.3.13 / 5.4.3 or later.	4	1
PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution: If using Lotus Foundations, upgrade the Lotus Foundations operating system to version 1.2.2b or later. Otherwise, upgrade to PHP 5.3.13 / 5.4.3 or later.	2	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
TWiki 'rev' Parameter Arbitrary Command Execution: Apply the appropriate hotfix referenced in the vendor advisory.	0	1

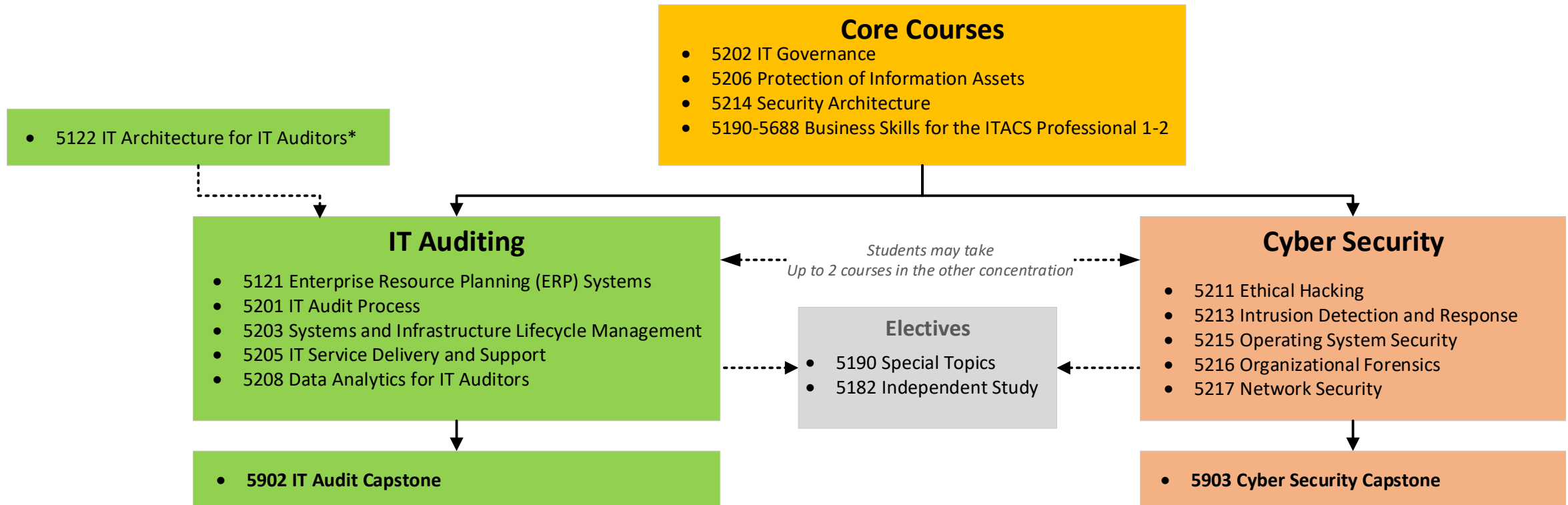
Scan Details

Policy: Metaspolitable2 Scan
Status: Completed
Scanner: Local Scanner
Start: February 19 at 9:56 PM
End: February 19 at 10:26 PM
Elapsed: 31 minutes

ITACS program



ITACS Curriculum



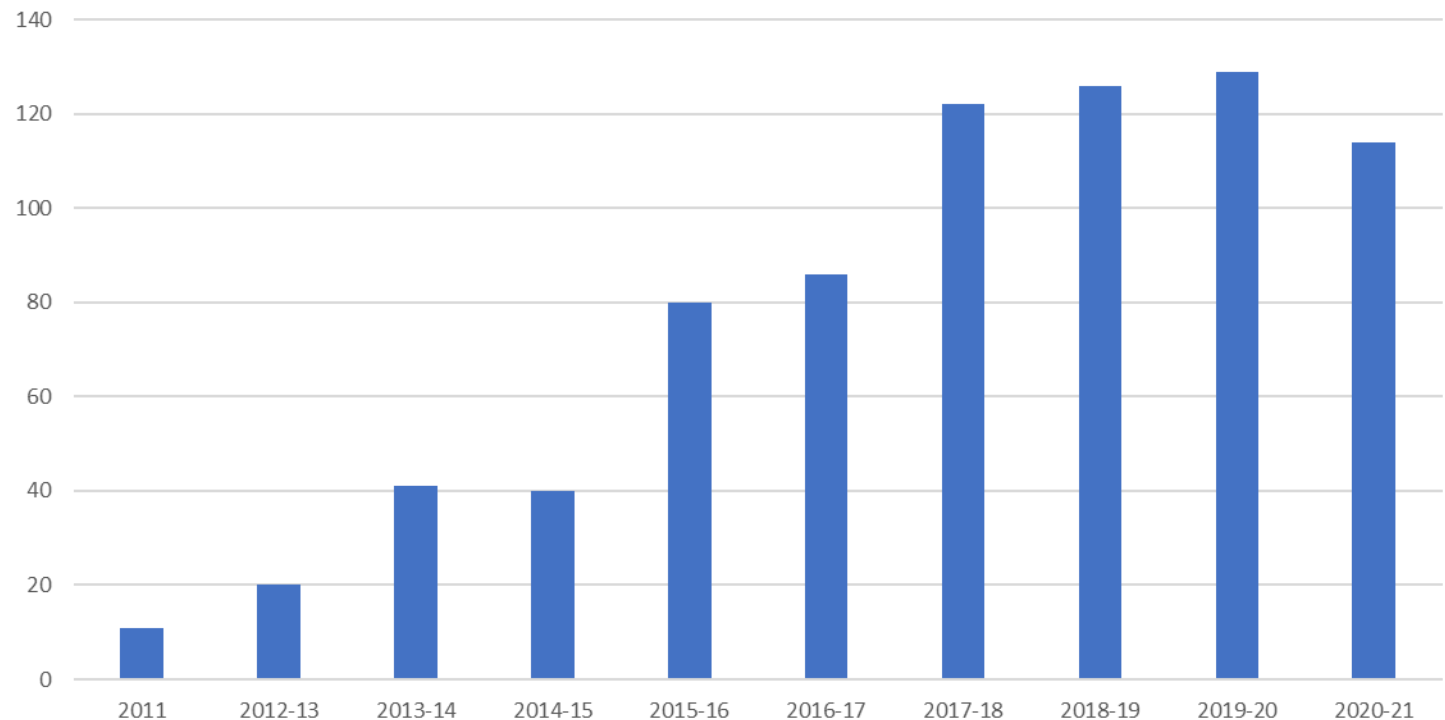
ITACS Faculty

Caswell Anderson	Risk Technical Manager	The Vanguard Group
Bill Bailey	Cyber Security Specialist	Science Applications International Corporation
James Baranello	Consultant	Technology & Risk Management Services
Lonnie Barone	President	Barone Associates
Larry Brandolph	Chief Information Security Officer	Temple University
Ryan Calef	VP Audit Services Regulatory Relations	Wells Fargo & Co.
Allen Chou	VP IT Audit	WSFS Bank
Ed Ferrara	Chief Information Security Officer	CSL Behring
Richard Flanagan	ITACS Program Founder	Temple University
Jose Gomez	VP Enterprise Technology Infrastructure	Wells Fargo & Co.
Brian Green	Segment Specialist	GE Healthcare Digital
David Lanter	ITACS Program Director	Temple University
Wade Mackey	Risk Technical Manager	The Vanguard Group
Thu Nguyen	Audit Manager	Wells Fargo Audit Services
Deval Shah	IT Security	U.S. Department of Homeland Security
Paul Smith	Senior Information Security Architect	CSL Behring
Andrew Sjaikai	Security Architect	The Vanguard Group
Christie Vazquez	Supervising IT Examiner	Federal Reserve Bank of Philadelphia
Paul Warner	Cybersecurity Dept. Chair	Rowan College at Burlington County
Patrick Wasson	Assistant Director Applications Dev.	Temple University Lewis Katz School of Medicine
Liang Yao	National Bank Examiner /Large Bank Supervisor	U.S. Department of the Treasury

ITACS Delivers Success!

- *Preparation for CISA and CISSP certification exams*
- *Students leveraging their ITACS skills and knowledge in their jobs*
- *ITACS students placed 1st, 2nd, and 3rd place in ISACA Philadelphia Chapter's 2018 Scholarship Competition*
- *ITACS students placed 1st & 2nd place in ISACA Philadelphia Chapter's 2017 Scholarship Competition*

ITACS Students
Enrollment 2020-21: 114



Certifications



Globally recognized certification in fields of IT security, IT audit, IT risk management and governance. Exam is known to be difficult and associated with a high failure rates.

Average U.S. entry level salaries ranging \$52,459 - \$122,326



Offered by Internationally Information System Security Certification Consortium, described as "world's largest IT security organization" -Wikipedia.org

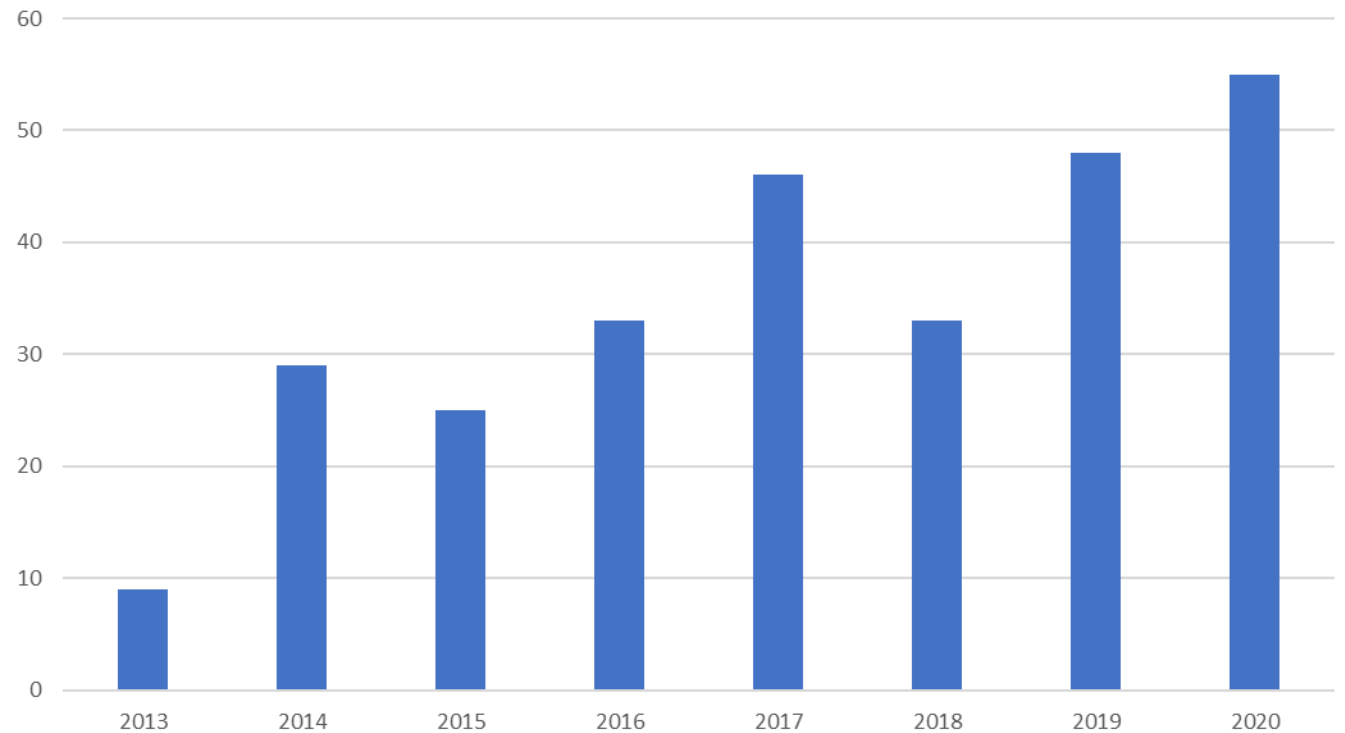
Average U.S. entry level salaries ranging \$73,627 - \$119,184

Salaries courtesy of infosecinstitute.com

ITACS delivers: Job placements and Career Growth!



ITACS Graduates



...

JPMORGAN CHASE & Co.

Agenda

- ✓ Change your Kali password!
- ✓ Application vulnerability and security testing
- ✓ Lab 6: Vulnerability Scanning – Part 2: Nessus
- ✓ Scan results
- ✓ Looking at a vulnerability
- ✓ ITACS Program