

Managing Enterprise Cybersecurity

MIS 4596

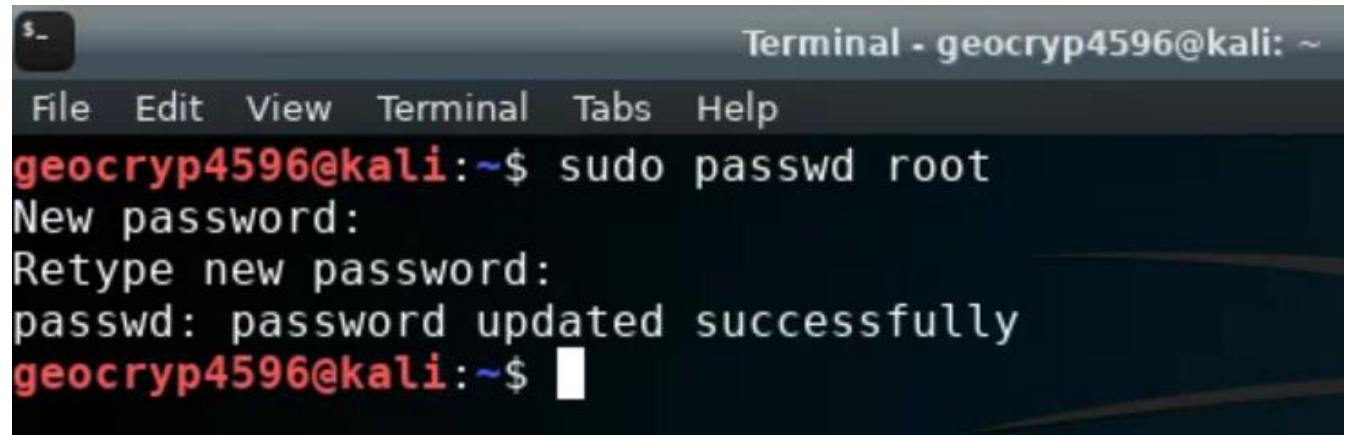
Unit #14

Agenda

- Change your Kali password!
- Application vulnerability and security testing
- Lab 8: Vulnerability Scanning –
 - Startup and access virtual machines
 - Part 1: Nmap
 - Part 2: Nessus
- Scan results
 - Looking at a vulnerability
- ITACS Program

Reminder: Change Kali's root Password Now (if you have not already done so)!

- 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

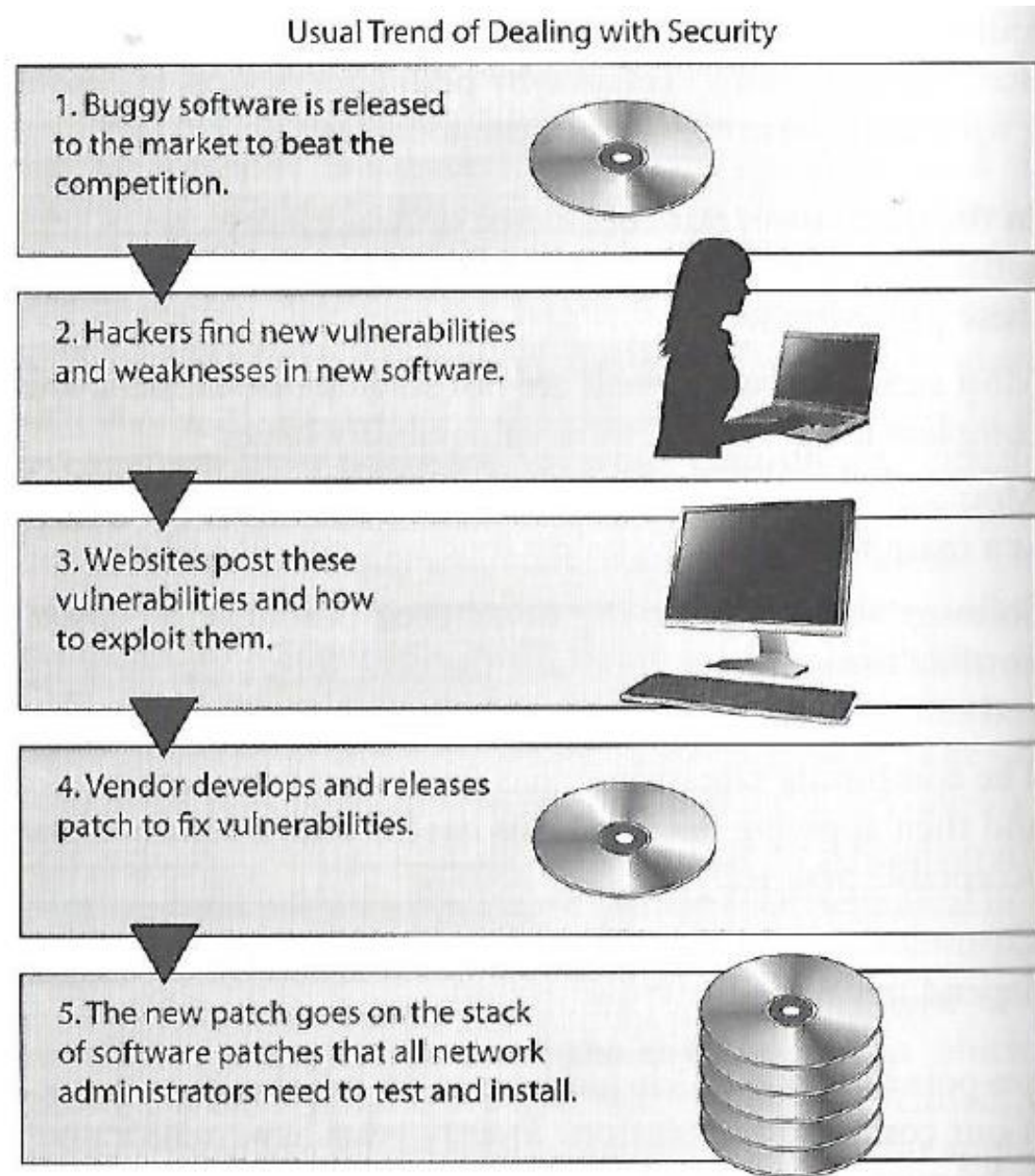
As applications become more accessible through the web, cloud and mobile devices,

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

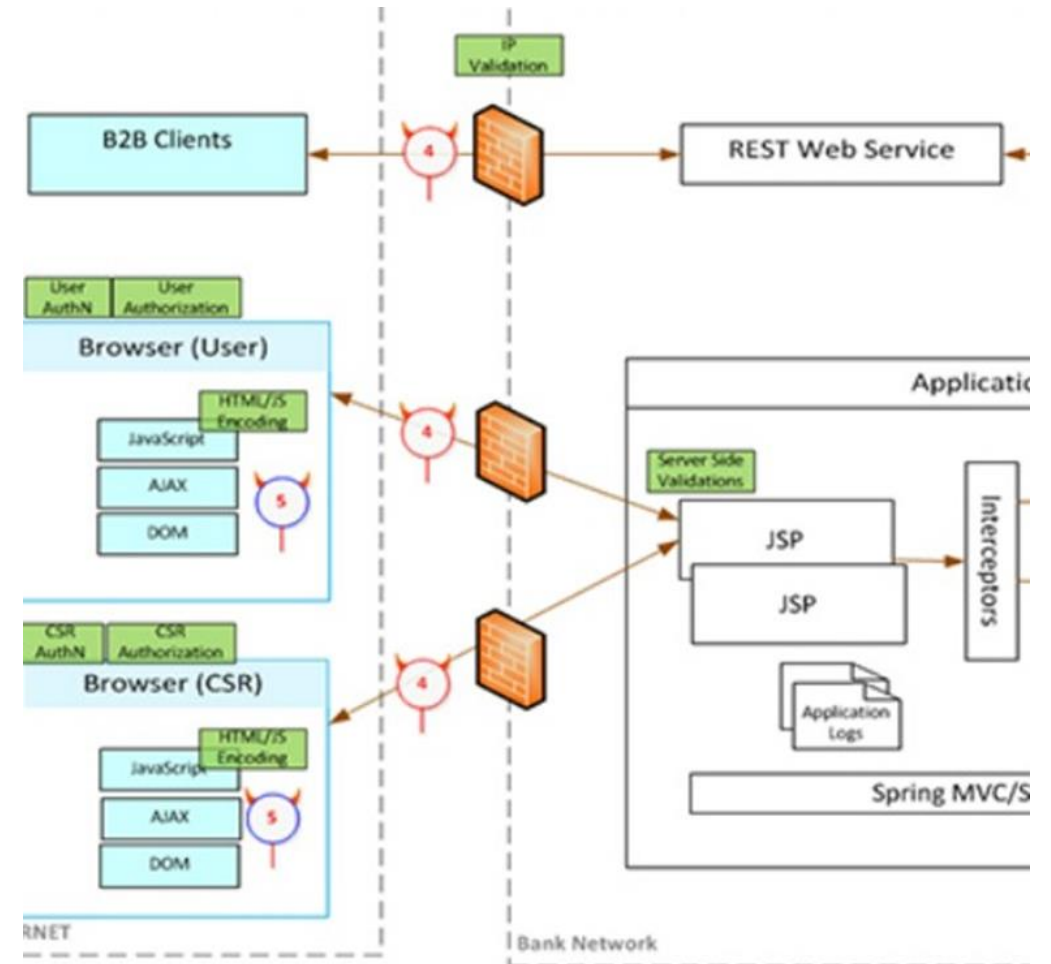


Software security, includes threat and attack surface analysis...

***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





Application Security Verification Levels

The Application Security Verification Standard defines three security verification levels, with each level increasing in depth.

- ASVS Level 1 is for low assurance levels, and is completely penetration testable
- ASVS Level 2 is for applications that contain sensitive data, which requires protection and is the recommended level for most apps
- ASVS Level 3 is for the most critical applications - applications that perform high value transactions, contain sensitive medical data, or any application that requires the highest level of trust.

Each ASVS level contains a list of security requirements. Each of these requirements can also be mapped to security-specific features and capabilities that must be built into software by developers.

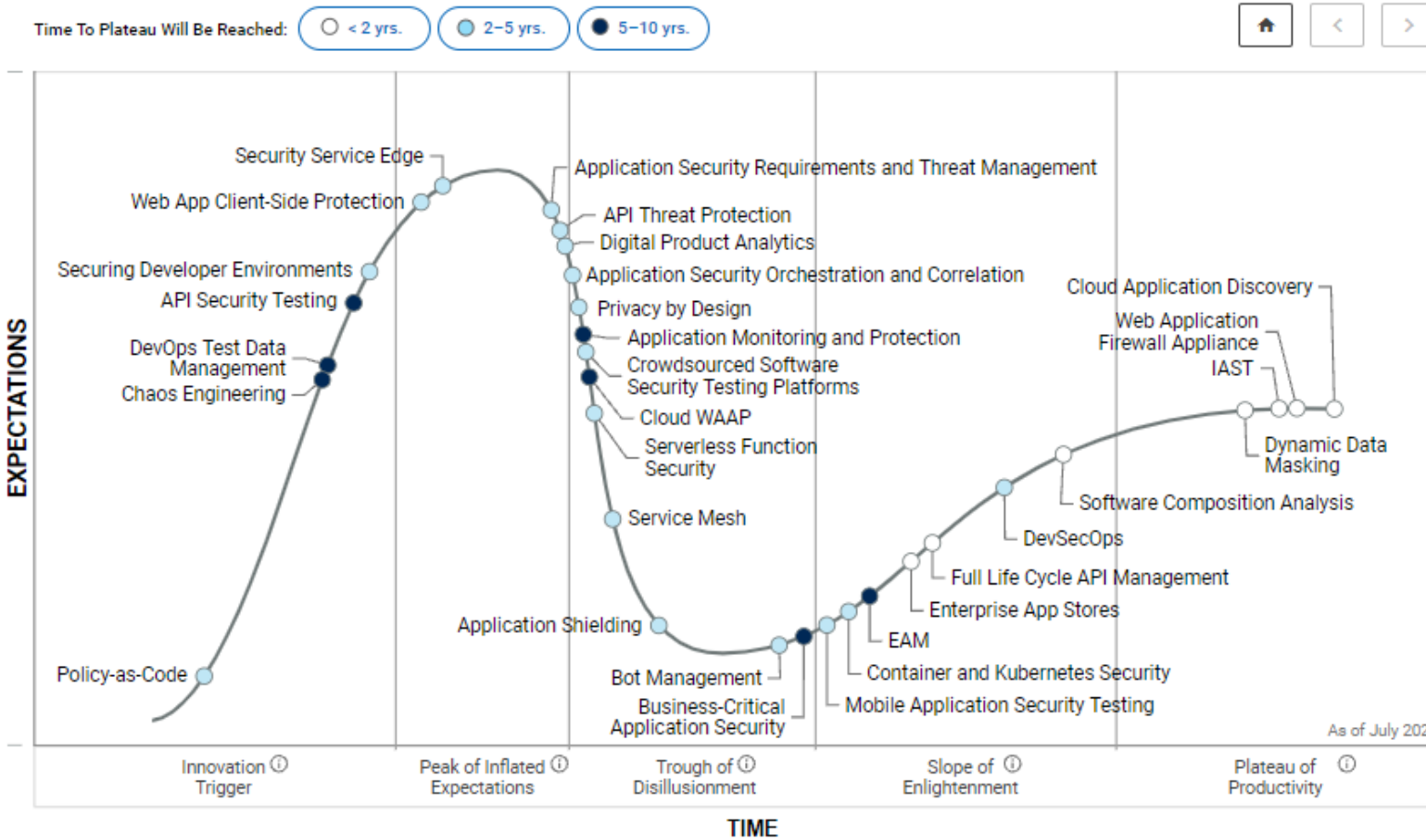
	Applicability	Building			Building, Configuration, Deployment Assurance and Verification			Assurance and Verification	
Level 1	All apps		Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Penetration Testing	DAST
Level 2	All apps	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
Level 3	High Assurance	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
Legend		Acceptable	Suitable						

Figure 1 - OWASP Application Security Verification Standard 4.0 Levels

Application Security Testing (AST)

Fundamental Capabilities

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



2021 Magic Quadrant



Estimated at \$2.6 billion, the AST market is projected to have a 18% compound annual growth rate through 2021

Welcome to the OWASP Top 10 - 2021



TOP 10

Welcome to the latest installment of the OWASP Top 10! The OWASP Top 10 2021 is all-new, with a new graphic design and an available one-page infographic you can print or obtain from our home page.

A huge thank you to everyone that contributed their time and data for this iteration. Without you, this installment would not happen. **THANK YOU!**

Top 10:2021 List

A01 Broken Access Control

A02 Cryptographic Failures

A03 Injection

A04 Insecure Design

A05 Security Misconfiguration

A06 Vulnerable and Outdated Components

A07 Identification and Authentication Failures

A08 Software and Data Integrity Failures

A09 Security Logging and Monitoring Failures

A10 Server Side Request Forgery (SSRF)

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

MITRE's Common Application Vulnerabilities



Home > CWE List > CWE- Individual Dictionary Definition (4.5)

CWE VIEW: Software Development

View ID: 699
Type: Graph

Objective
This view organizes weaknesses around concepts that are frequently used or encountered in software development. The vendors. It provides a variety of categories that are intended to simplify navigation, browsing, and mapping.

Audience

Stakeholder	Description
Software Developers	Software developers (including architects, designers, coders, and testers) use this view to better introduction can enable focus on a specific phase of the development lifecycle.
Educators	Educators use this view to teach future developers about the types of mistakes that are common

Relationships
The following graph shows the tree-like relationships between weaknesses that exist at different levels of abstraction. A weaknesses that are described in the most abstract fashion. Below these top-level entries are weaknesses are varying I that is described at a very low level of detail, typically limited to a specific language or technology. A chain is a set of w vulnerability.

699 - Software Development

- API / Function Errors - (1228)
- Audit / Logging Errors - (1210)
- Authentication Errors - (1211)
- Authorization Errors - (1212)
- Bad Coding Practices - (1006)
- Behavioral Problems - (438)
- Business Logic Errors - (840)
- Communication Channel Errors - (417)
- Complexity Issues - (1226)
- Concurrency Issues - (557)
- Credentials Management Errors - (255)
- Cryptographic Issues - (310)
- Key Management Errors - (320)
- Data Integrity Issues - (1214)
- Data Processing Errors - (19)
- Data Neutralization Issues - (137)
- Documentation Issues - (1225)
- File Handling Issues - (1219)
- Encapsulation Issues - (1227)
- Error Conditions, Return Values, Status Codes - (389)
- Expression Issues - (569)
- Handler Errors - (429)
- Information Management Errors - (199)
- Initialization and Cleanup Errors - (452)
- Data Validation Issues - (1215)
- Lockout Mechanism Errors - (1216)
- Memory Buffer Errors - (1218)
- Numeric Errors - (189)
- Permission Issues - (275)
- Pointer Issues - (465)
- Privilege Issues - (265)
- Random Number Issues - (1213)
- Resource Locking Problems - (411)
- Resource Management Errors - (399)
- Signal Errors - (387)
- State Issues - (371)
- String Errors - (133)
- Type Errors - (136)
- User Interface Security Issues - (355)
- User Session Errors - (1217)

- ## 699 - Software Development
- API / Function Errors - (1228)
 - Use of Inherently Dangerous Function - (242)
 - Use of Function with Inconsistent Implementations - (474)
 - Undefined Behavior for Input to API - (475)
 - Use of Obsolete Function - (477)
 - Use of Potentially Dangerous Function - (676)
 - Use of Low-Level Functionality - (695)
 - Exposed Dangerous Method or Function - (749)
 - Audit / Logging Errors - (1210)
 - Authentication Errors - (1211)
 - Authentication Bypass Using an Alternate Path or Channel - (288)
 - Authentication Bypass by Spoofing - (290)
 - Authentication Bypass by Capture-replay - (294)
 - Improper Certificate Validation - (295)
 - Improper Following of a Certificate's Chain of Trust - (296)
 - Improper Check for Certificate Revocation - (299)
 - Incorrect Implementation of Authentication Algorithm - (303)
 - Missing Critical Step in Authentication - (304)
 - Authentication Bypass by Primary Weakness - (305)
 - Missing Authentication for Critical Function - (306)
 - Improper Restriction of Excessive Authentication Attempts - (307)
 - Use of Single-factor Authentication - (308)
 - Use of Password System for Primary Authentication - (309)
 - Key Exchange without Entity Authentication - (322)
 - Use of Client-Side Authentication - (603)
 - Overly Restrictive Account Lockout Mechanism - (645)
 - Guessable CAPTCHA - (804)
 - Use of Password Hash Instead of Password for Authentication - (836)
 - Authorization Errors - (1212)
 - Bad Coding Practices - (1006)
 - Behavioral Problems - (438)
 - Business Logic Errors - (840)
 - Communication Channel Errors - (417)
 - Complexity Issues - (1226)
 - Concurrency Issues - (557)

MITRE's Common Weakness Enumeration



[Train and Certify](#) [Manage Your Team](#) [Resources](#) [Focus Areas](#) [Get Involved](#)

CWE/SANS TOP 25 Most Dangerous Software Errors

Rank	ID	Name
1	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
3	CWE-20	Improper Input Validation
4	CWE-200	Information Exposure
5	CWE-125	Out-of-bounds Read
6	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
7	CWE-416	Use After Free
8	CWE-190	Integer Overflow or Wraparound
9	CWE-352	Cross-Site Request Forgery (CSRF)
10	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
11	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
12	CWE-787	Out-of-bounds Write
13	CWE-287	Improper Authentication
14	CWE-476	NULL Pointer Dereference
15	CWE-732	Incorrect Permission Assignment for Critical Resource
16	CWE-434	Unrestricted Upload of File with Dangerous Type
17	CWE-611	Improper Restriction of XML External Entity Reference
18	CWE-94	Improper Control of Generation of Code ('Code Injection')
19	CWE-798	Use of Hard-coded Credentials
20	CWE-400	Uncontrolled Resource Consumption
21	CWE-772	Missing Release of Resource after Effective Lifetime
22	CWE-426	Untrusted Search Path
23	CWE-502	Deserialization of Untrusted Data
24	CWE-269	Improper Privilege Management
25	CWE-295	Improper Certificate Validation

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

Legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)

Application Vulnerability Testing Reports

Burp Scanner Sample Report

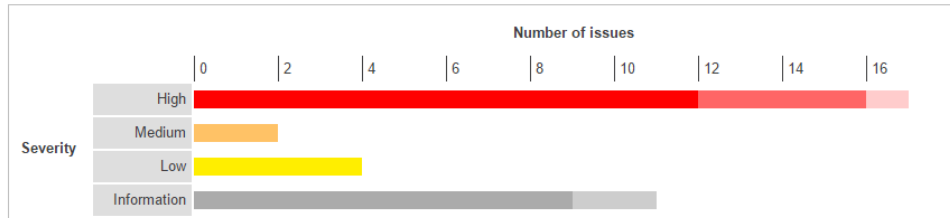


Summary

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

Vulnerability Scanning Lab

Lab: Vulnerability Scanning

By Drs. Dave Eargle and Anthony Vance

This lab uses the following VMs:

- Kali
- Metasploitable2

Important!

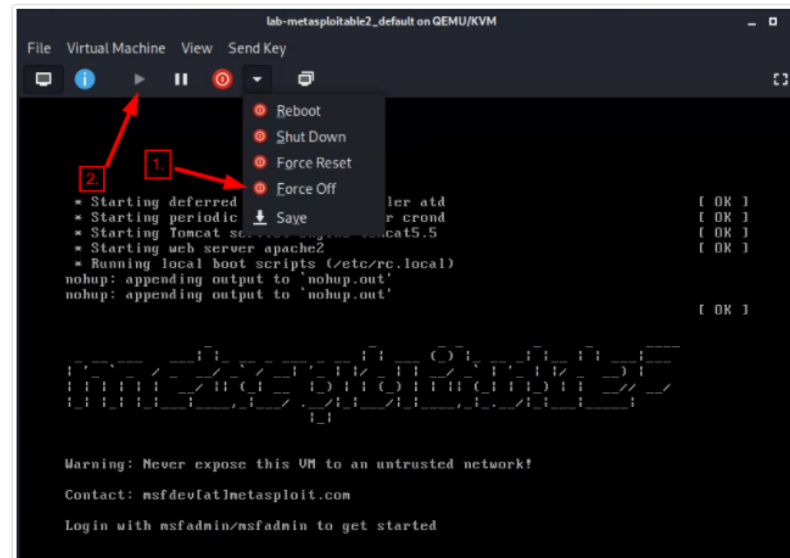
- Read the section **here** on how to launch the Metasploitable2 virtual machine within Kali.
- Ensure that you can **ping** Metasploitable2 from Kali, and Kali from Metasploitable2, before continuing the lab.
- Use the addresses shown in the **infosec-net network map**.

The objective of this lab is to create a report of potential vulnerabilities for a virtual machine. The VM is a Ubuntu-based Linux distribution called MetaSploitable2, which is specifically designed to teach penetration testing skills such as vulnerability scanning.

During the lab, you may envision yourself as a defender, checking an organizational assets for vulnerabilities visible from an external perspective with the ultimate intention of patching them. Alternatively, you may envision yourself as an attacker, checking a target victim asset for vulnerabilities, with the ultimate intention of exploiting them. Both defenders and attackers may perform the same steps of vulnerability scanning.

Troubleshooting

Metasploitable2 is an ancient operating system. It is prone to crashing and otherwise behaving unexpectedly suddenly. If Metasploitable2 stops responding during the lab, then try force-off'ing it and starting it up again:

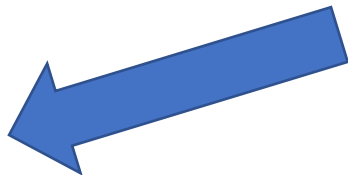


Troubleshooting
Part 1. Host Discovery and Scanning using NMAP
Part 2. Vulnerability scanning using Nessus
Question List



Labs

- Lab1: Threat Modeling with Attack Trees
- Lab2: Web Privacy and Anonymity
- Lab 3: See Tutorials - Introduction to Google Cloud Platform & Introduction to Linux
- Lab4: Symmetric Encryption and Hashing
- Lab5: Asymmetric Encryption
- Lab6: Digital Certificates
- Lab7: Password Cracking
- Lab8: Vulnerability Scanning
- Lab9: Exploitation
- Lab10: Physical Security Scavenger Hunt
- Lab11: Social Engineering
- Lab12: Network Security Monitoring and Security Onion
- Lab13: Malware Analysis



Tutorials

- Tutorial: Introduction to Google Cloud Platform
- Tutorial: Introduction to Linux
- Tutorial: Introduction to Networking

RECENT ANNOUNCEMENTS

[More Announcements...](#)

Lab: Vulnerability Scanning

By Drs. [Dave Eargle](#) and [Anthony Vance](#)

This lab uses the following VMs:

- Kali
- Metasploitable2

Important!

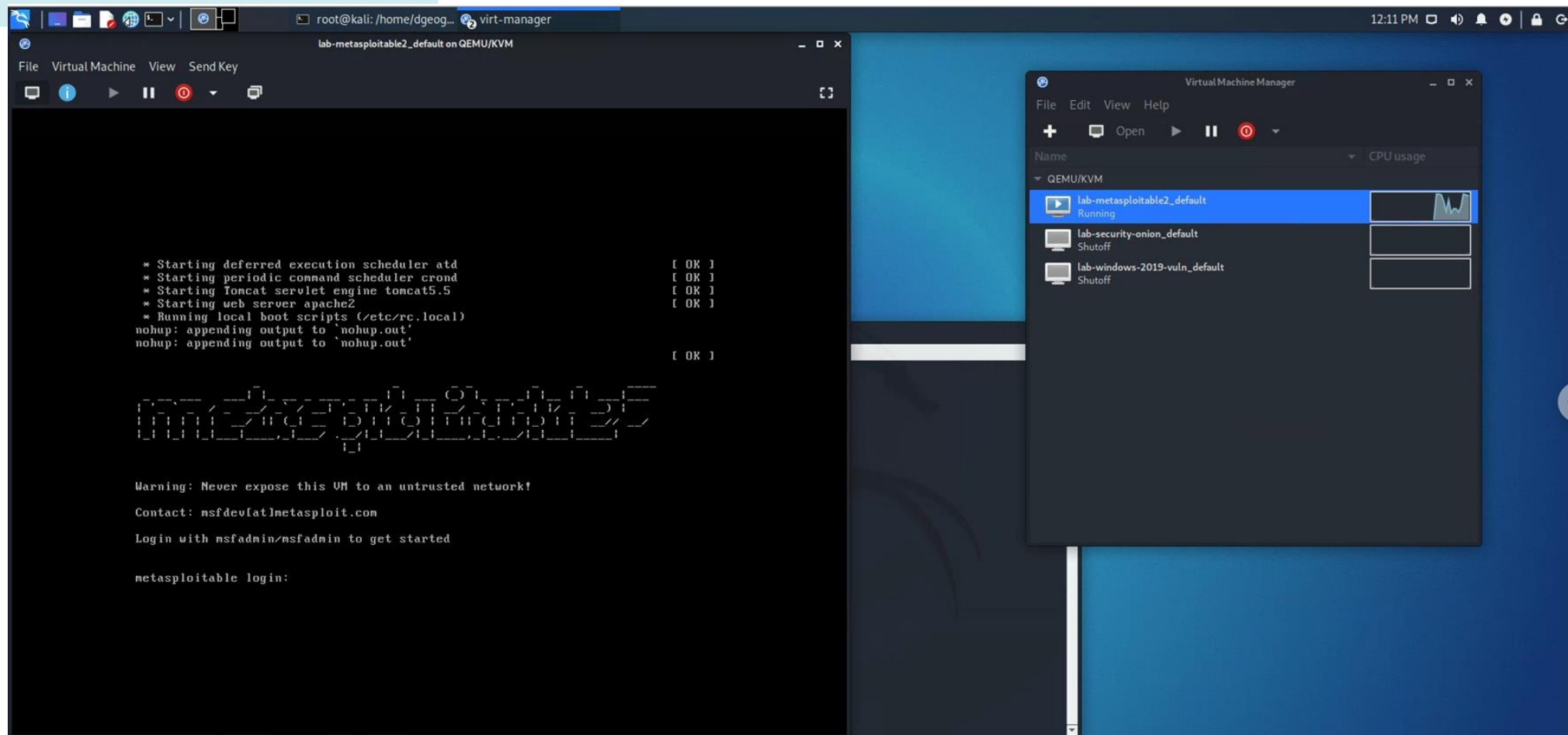
- Read the section [here](#) on how to launch the Metasploitable2 virtual machine within Kali.
- Ensure that you can [ping](#) Metasploitable2 from Kali, and Kali from Metasploitable2, before continuing the lab.
- Use the addresses shown in the [infosec-net network map](#).

Troubleshooting

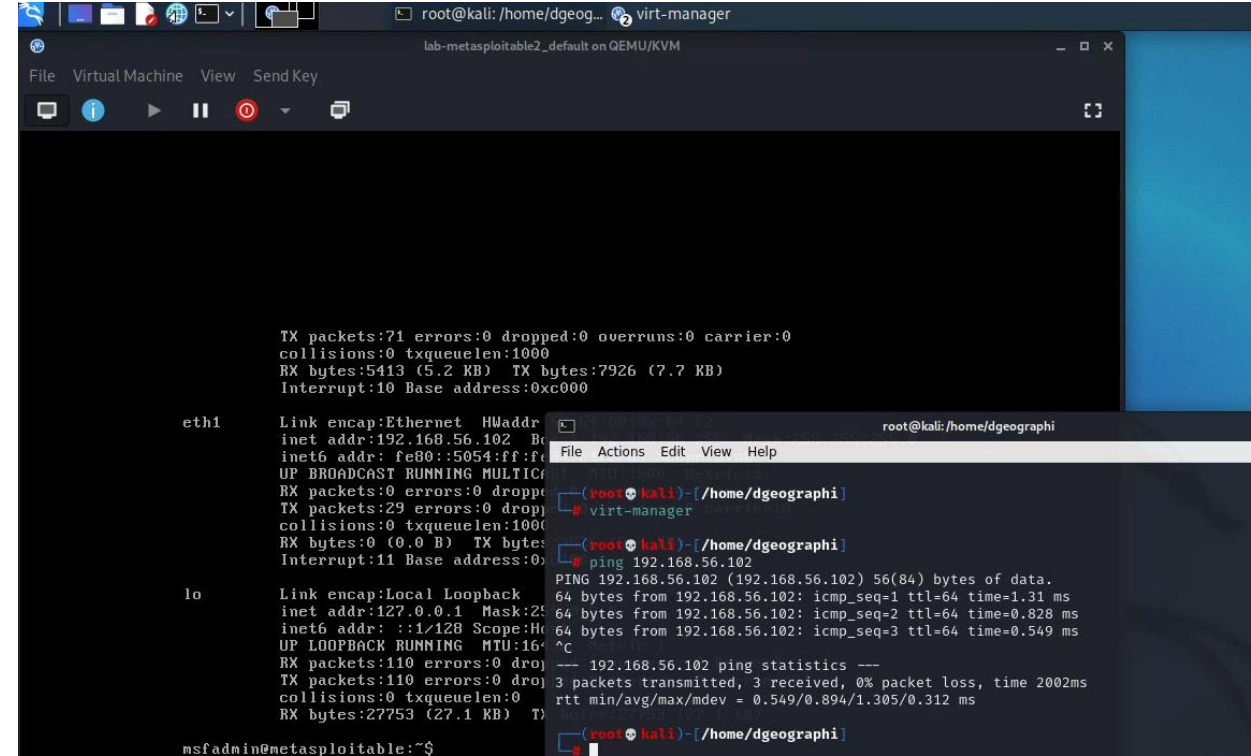
Part 1. Host Discovery and Scanning using NMAP

Part 2. Vulnerability scanning using Nessus

Question List



Use "ifconfig" to find IP address of your metasploitable2 and kali



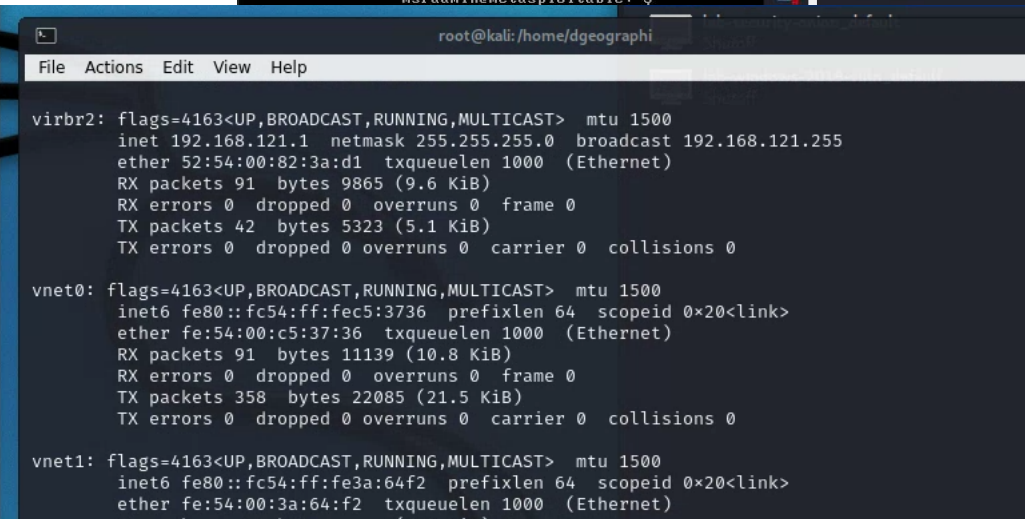
```
TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:5413 (5.2 KB) TX bytes:7926 (7.7 KB)
Interrupt:10 Base address:0xc000

eth1    Link encap:Ethernet HWaddr
inet addr:192.168.56.102 B
inet6 addr: fe80::5054:ff:fe
UP BROADCAST RUNNING MULTIC
RX packets:0 errors:0 droppe
TX packets:29 errors:0 dropp
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:
Interrupt:11 Base address:0x

lo      Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255
inet6 addr: ::1/128 Scope:Ho
UP LOOPBACK RUNNING MTU:16384
RX packets:110 errors:0 drop
TX packets:110 errors:0 dro
collisions:0 txqueuelen:0
RX bytes:27753 (27.1 KB) T
```

```
msfadmin@metasploitable:~$ ping 192.168.121.1
PING 192.168.121.1 (192.168.121.1) 56(84) bytes of data:
64 bytes from 192.168.121.1: icmp_seq=1 ttl=64 time=0.692 ms
64 bytes from 192.168.121.1: icmp_seq=2 ttl=64 time=0.704 ms
64 bytes from 192.168.121.1: icmp_seq=3 ttl=64 time=0.692 ms
64 bytes from 192.168.121.1: icmp_seq=4 ttl=64 time=0.701 ms
64 bytes from 192.168.121.1: icmp_seq=5 ttl=64 time=0.661 ms

[2]+  Stopped                  ping 192.168.121.1
msfadmin@metasploitable:~$
```



```
virbr2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.121.1 netmask 255.255.255.0 broadcast 192.168.121.255
ether 52:54:00:82:3a:d1 txqueuelen 1000 (Ethernet)
RX packets 91 bytes 9865 (9.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 42 bytes 5323 (5.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

vnet0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::fc54:ff:fec5:3736 prefixlen 64 scopeid 0x20<link>
ether fe:54:00:c5:37:36 txqueuelen 1000 (Ethernet)
RX packets 91 bytes 11139 (10.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 358 bytes 22085 (21.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

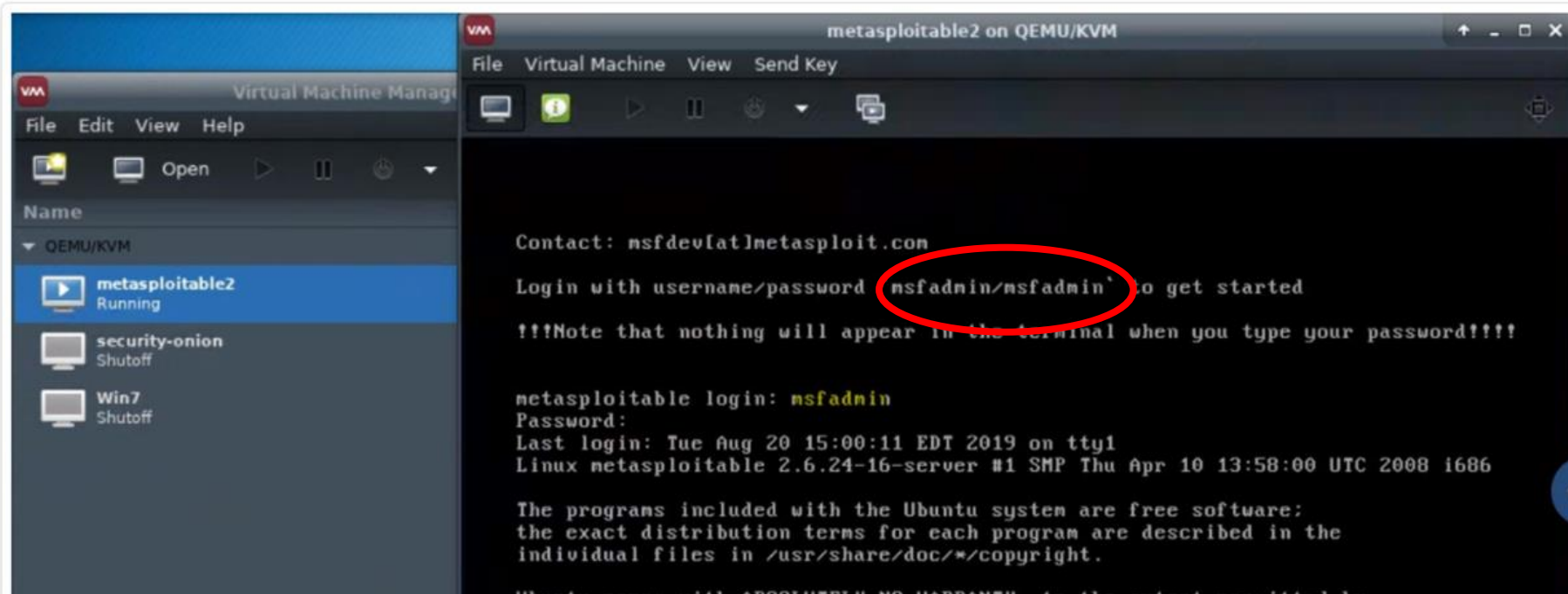
vnet1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::fc54:ff:fe3a:64f2 prefixlen 64 scopeid 0x20<link>
ether fe:54:00:3a:64:f2 txqueuelen 1000 (Ethernet)
RX packets 54 bytes 7152 (6.9 KiB)
```

security-assignments.com/labs/virtual-machines#using-the-virtual-machines-within-kali



metasploitable login:

You can click into this window and interact with it via keyboard, and mouse if it has a GUI.



Setting up your virtual lab

Using the virtual machines within Kali

Starting and accessing virtual machines

Updating the virtual machines

Using snapshots

How I created the virtual machines

Part 1. Host Discovery and Scanning using NMAP

NMAP is the de facto standard of host discovery and port scanning and has a host of features that make the tool very robust. In this section of the lab, you'll try a few of NMAP's features.

Throughout the lab, you should replace `<IP.addr.of.metasploitable2>` with the actual IPv4 address of Metasploitable.

1. Open a "Terminal Emulator" window in Kali.
2. Run all nmap commands as root – you'll get more information as root for some commands.
 - o "Get root" in your shell (i.e., `sudo -s` or `su root`).
3. Run `nmap`. Take a quick look at the available options.
4. Use `nmap` to determine whether the your Metasploitable2 VM is live using a "ping scan":

```
nmap -sn <IP.addr.of.metasploitable2>
```

The ping scan not only sends an ICMP request, but also an ARP ping, TCP pinging, and other techniques to determine if a host is live on the network.

Question 1: What kind of information is shown when you run this ping scan for Metasploitable2?

You could also scan a *range* of IPs using [CIDR block notation](#). See the [network map](#) for the ipv4 block of the infosec-net network. This can be fun to do if you also have your vulnerable Windows 7 vm running at the same time, although this is not required.

```
nmap -sn <ipv4 CIDR block>
```

You can know your network by typing `ifconfig` on either Kali or Metasploitable2, and looking for the `inet` address plus the `mask` value on the same line. For example, a "mask" of `255.255.255.0` applied to an "inet" address of `192.168.56.17` translates to a network of `192.168.56.0/24`. (Where 24 is the number of bits to mask and it takes 8 bits to make 255, $8 \times 3 = 24$, so that would mask three of the "!" blocks.)

5. Once you determine that a host is live, you can use NMAP to scan for open ports. Use a TCP scan to determine which ports are open on Metasploitable2:

```
nmap -sS <IP.addr.of.metasploitable2>
```

Troubleshooting

Part 1. Host Discovery and Scanning using NMAP

```
root@kali: /home/dgeographi
File Actions Edit View Help
(root@kali)-[~/home/dgeographi]
# nmap -sV 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-12 12:24 EDT
Nmap scan report for 192.168.56.102
Host is up (0.028s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql      MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11        (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http       Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 52:54:00:3A:64:F2 (QEMU virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds

(root@kali)-[~/home/dgeographi]
#
```


Looking for vulnerable services...

```
root@kali: /home/dgeographi
File Actions Edit View Help

(root@kali) - [~/home/dgeographi]
# nmap -sV 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-12 12:24 EDT
Nmap scan report for 192.168.56.102
Host is up (0.028s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
```

The screenshot shows the Exploit Database website interface. The search bar contains the text "vsftpd 2.3.4". The search results table is as follows:

Date	D	A	V	Title	Type	Platform	Author
2021-04-12	↓		✓	vsftpd 2.3.4 - Backdoor Command Execution	Remote	Unix	HerculesRD
2011-07-05	↓	📄	✓	vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	Remote	Unix	Metasploit

Additional interface elements include a sidebar with navigation icons, a top navigation bar with the "EXPLOIT DATABASE" logo, and a footer showing "Showing 1 to 2 of 2 entries (filtered from 44,357 total entries)".

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 2. Vulnerability scanning using Nessus

In this part of the lab, you will use Nessus, a product by Tenable, to replicate what you did with `nmap` using a tool used in industry. According to Tenable:

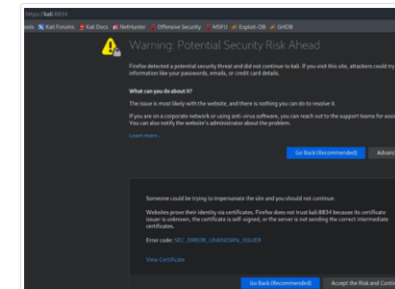
Nessus is trusted by more than 30,000 organizations worldwide as one of the most widely deployed security technologies on the planet - and the gold standard for vulnerability assessment.

Start and register the Nessus Scanner

Nessus should already be installed on your Kali-on-GCP instance. It should also already be running.

1. Open Firefox on Kali and browse to <https://kali:8834>.

To get past the SSL warning, click 'Advanced' > 'Accept the Risk and Continue'.



2. Select "Nessus Essentials"
3. Get a free registration activation code.

The prompt on the <https://kali:8834> webpage seems to never send a registration link when an email is submitted. Instead, get a registration code by visiting the following tenable.com webpage: <https://www.tenable.com/products/nessus/nessus-essentials>

Submit your registration code on the <https://kali:8834> page.

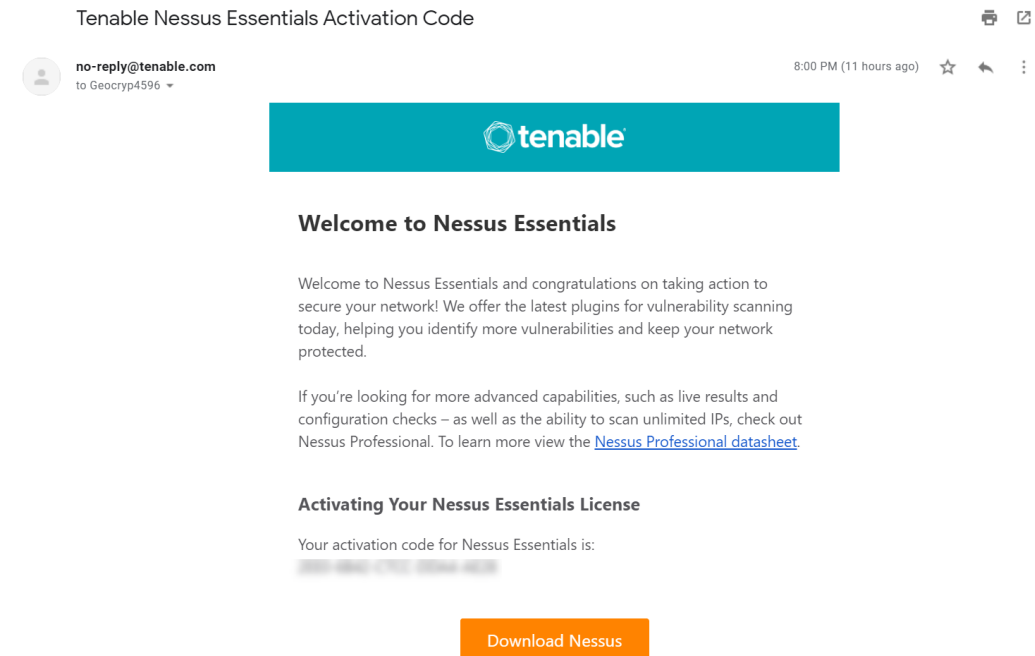
4. Choose any `username:password` you prefer for use with nessus. For instance, you could use user `root` password `toor` when prompted by Nessus. Click "reload" if the page fails to load.

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, including '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 ~20 - 30+ minutes)...

The screenshot shows the Nessus Essentials web interface in a browser window. The browser address bar shows the URL `https://kali:8834/#/scans/folders`. The interface includes a sidebar with navigation options like 'My Scans', 'All Scans', and 'Trash'. The main content area displays a table of scans with columns for Name, Schedule, and Last Modified. A scan named 'Metasploitable2' is selected, showing a schedule of 'On Demand' and a completion time of 'Today at 1:31 PM'. Below the scan list, there are summary statistics: 1 Host, 90 Vulnerabilities, 7 Remediations, 1 VPR Top Threat, and 1 History item. A table lists the host '192.168.56.102' with a bar chart showing the distribution of vulnerabilities by severity: 11 Critical (red), 14 High (orange), 36 Medium (yellow), 7 Low (green), and 167 Info (blue). On the right side, 'Scan Details' are provided, including Policy (Basic Network Scan), Status (Completed), Severity Base (CVSS v3.0), Scanner (Local Scanner), Start (Today at 1:09 PM), End (Today at 1:31 PM), and Elapsed time (22 minutes). At the bottom right, a donut chart visualizes the vulnerability distribution with a legend: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Name	Schedule	Last Modified
<input type="checkbox"/> Metasploitable2	On Demand	Today at 1:31 PM

Metasploitable2

Hosts: 1 | Vulnerabilities: 90 | Remediations: 7 | VPR Top Threats: 1 | History: 1

Host	Vulnerabilities
<input type="checkbox"/> 192.168.56.102	11 Critical, 14 High, 36 Medium, 7 Low, 167 Info

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 1:09 PM
- End: Today at 1:31 PM
- Elapsed: 22 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

[← Back to Hosts](#)

Vulnerabilities 90

Filter ▾

Search Vulnerabilities



90 Vulnerabilities

<input type="checkbox"/>	Sev ▾	Name ▲	Family ▲	Count ▾		
<input type="checkbox"/>	MIXED	7 Web Server (Multiple Issues)	Web Servers	10		
<input type="checkbox"/>	MIXED	5 DNS (Multiple Issues)	DNS	6		
<input type="checkbox"/>	MIXED	4 Phpmyadmin (Multiple Issues)	CGI abuses	4		
<input type="checkbox"/>	CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	3		
<input type="checkbox"/>	CRITICAL	Bind Shell Backdoor Detection	Backdoors	1		
<input type="checkbox"/>	CRITICAL	NFS Exported Share Information Disclosure	RPC	1		
<input type="checkbox"/>	CRITICAL	rexecd Service Detection	Service detection	1		
<input type="checkbox"/>	CRITICAL	Unix Operating System Unsupported Version Detection	General	1		
<input type="checkbox"/>	CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1		
<input type="checkbox"/>	MIXED	14 SSL (Multiple Issues)	General	26		
<input type="checkbox"/>	MIXED	5 ISC Bind (Multiple Issues)	DNS	5		

Host Details

IP: 192.168.56.102
 MAC: 52:54:00:3A:64:F2
 OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
 Start: Today at 1:09 PM
 End: Today at 1:31 PM
 Elapsed: 22 minutes
 KB: [Download](#)

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Vulnerabilities 90

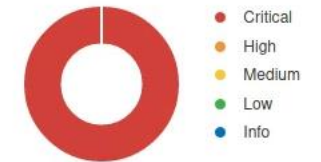
Search Vulnerabilities 🔍 2 Vulnerabilities

<input type="checkbox"/>	Sev ▾	Name ▲	Family ▲	Count ▾	⊙	✎
<input type="checkbox"/>	CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Gain a shell remotely	2	⊙	✎
<input type="checkbox"/>	CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1	⊙	✎

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0 ✎
Scanner: Local Scanner
Start: Today at 1:09 PM
End: Today at 1:31 PM
Elapsed: 22 minutes

Vulnerabilities



Vulnerabilities 90

CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) >**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	192.168.56.102 🔗
25 / tcp / smtp	192.168.56.102 🔗

Plugin Details ✎

Severity: Critical
ID: 32321
Version: 1.27
Type: remote
Family: Gain a shell remotely
Published: May 15, 2008
Modified: November 16, 2020

Risk Information

Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Temporal Score: 8.3
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS v2.0 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

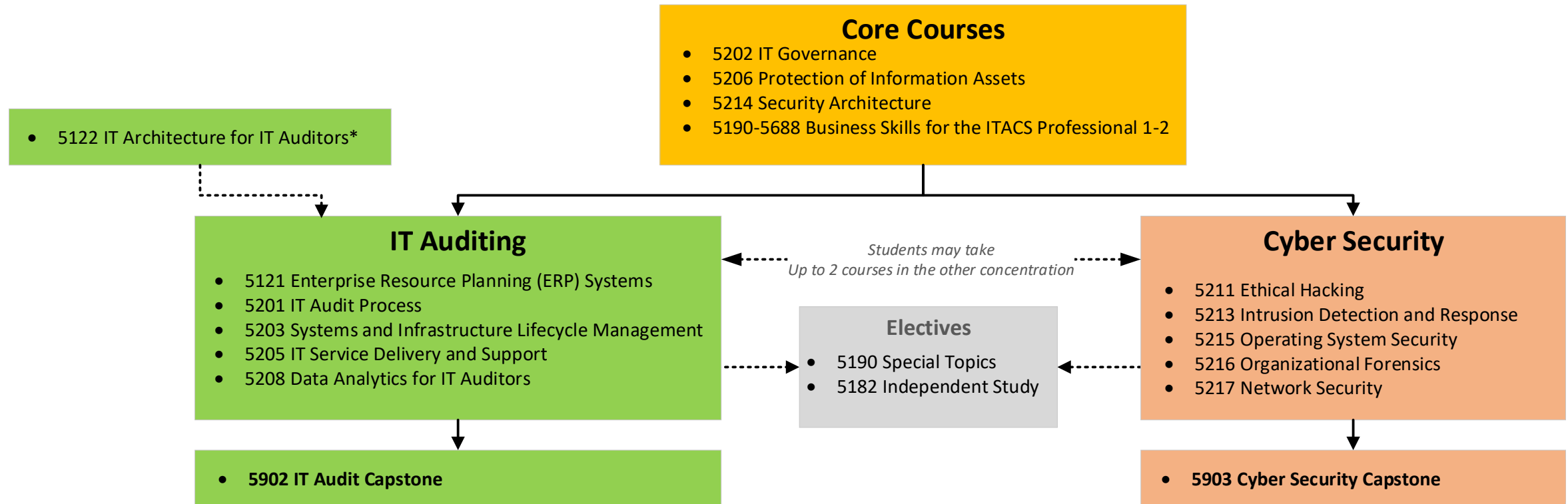
Reference Information

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

See Also... links

- <https://lists.debian.org/debian-security-announce/2008/msg00152.html>
- <https://lists.ubuntu.com/archives/ubuntu-security-announce/2008-May/000705.html>

ITACS MS Program Curriculum

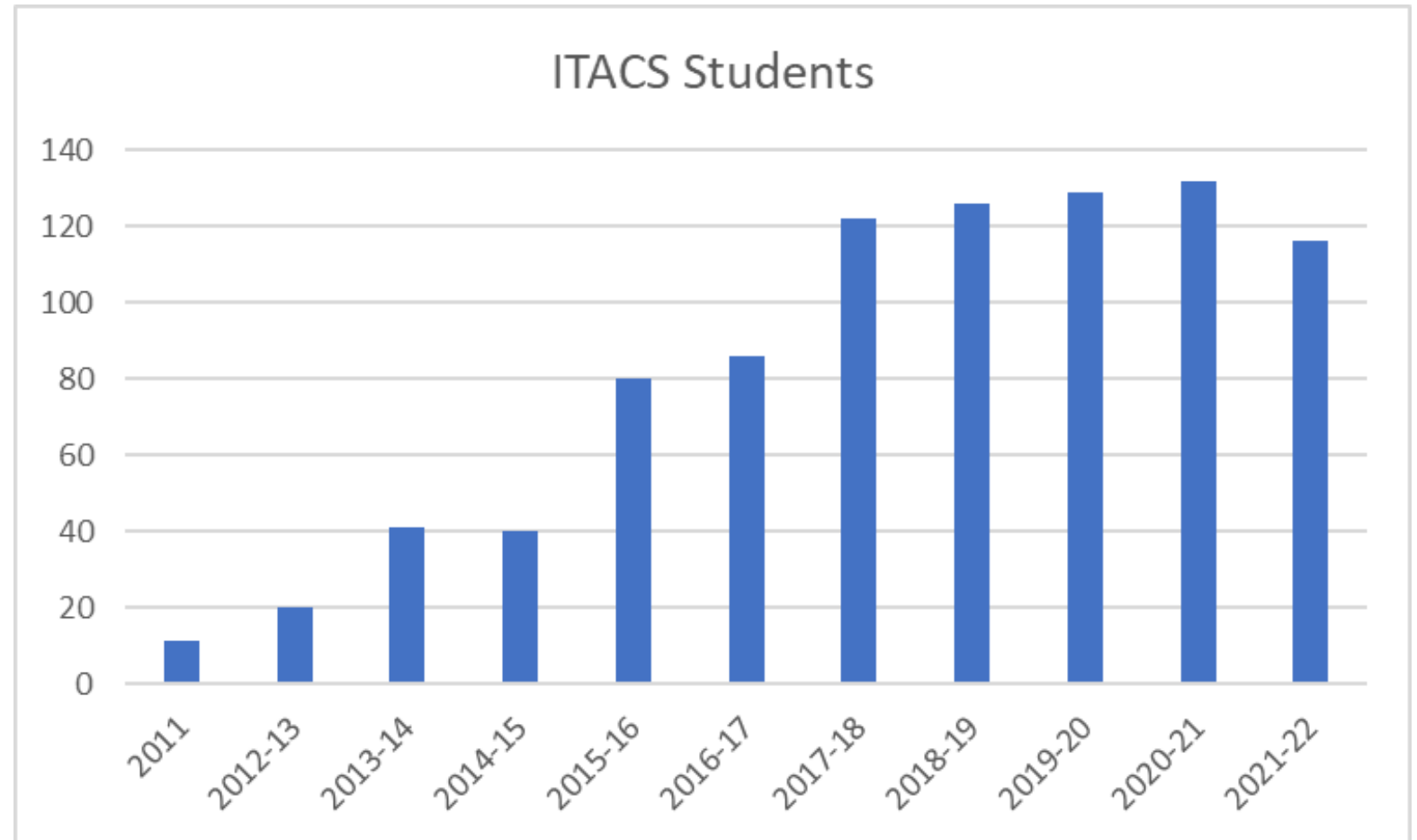


ITACS Faculty

Caswell Anderson	Risk Technical Manager	The Vanguard Group
Bill Bailey	Cyber Security Specialist	Science Applications International Corporation
James Baranello	Information Security & Risk Officer	Citadel Federal Credit Union
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	Managing Partner	436 Research, LLC
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 (retired)	The Vanguard Group
Thu Nguyen	AVP, Integrated and Compliance Audit	Wells Fargo Audit Services
Deval Shah	IT Security	U.S. Department of Homeland Security
Paul Smith	Senior Information Security Architect	CSL Behring
Andrew Sjaljai	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 last Scholarship Competition, and placed 1st & 2nd place in their prior Scholarship Competition*



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

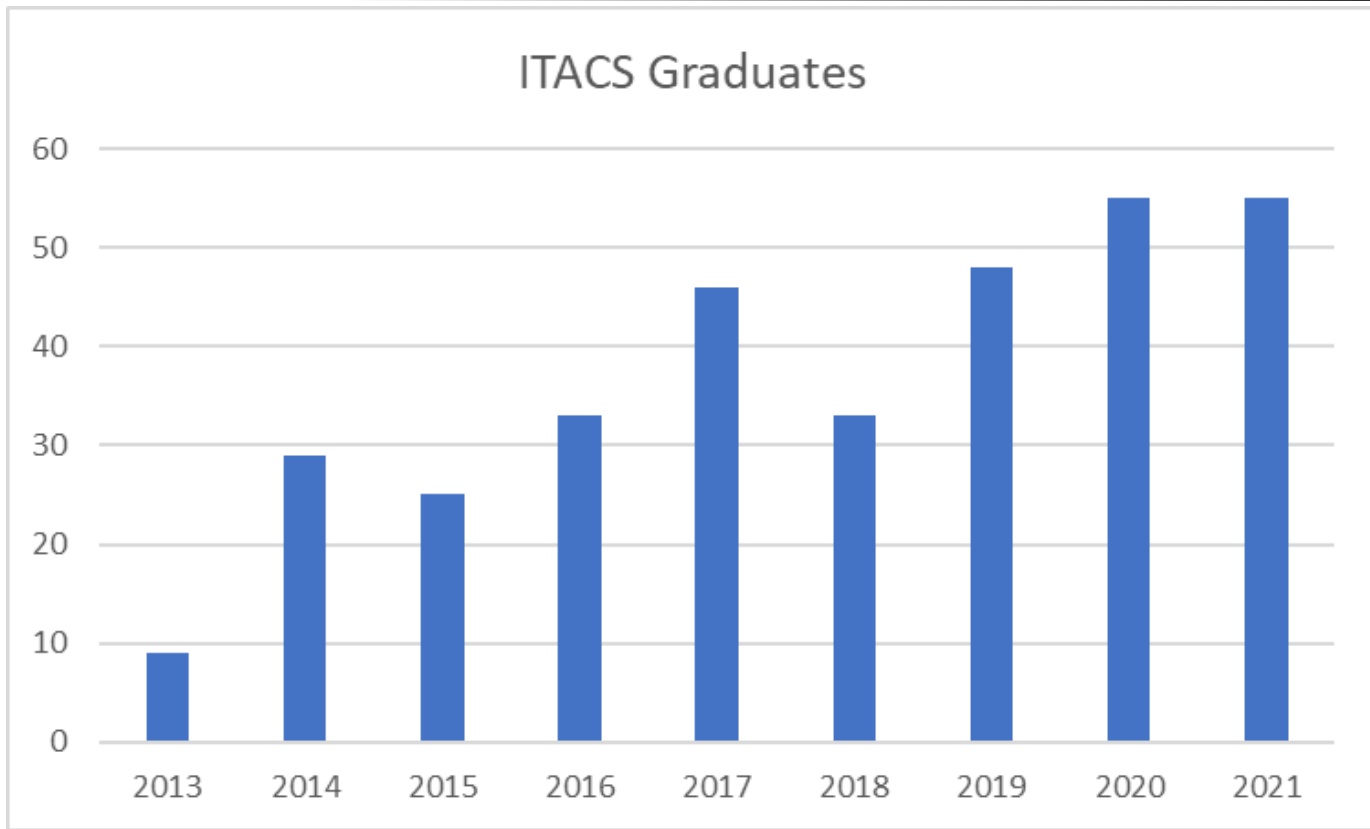


Offered by Internationally Information System Security Certification Consortium, described as "world's largest IT security organization" -Wikipedia.org

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

Salaries courtesy of infosecinstitute.com

ITACS delivers: Job placements and Career Growth!



...

Agenda

- ✓ Change your Kali password!
- ✓ Application vulnerability and security testing
- ✓ Lab 8: Vulnerability Scanning – Part 2: Nessus
- ✓ Scan results
- ✓ Looking at a vulnerability
- ✓ ITACS Program