Tools, Equipment, Supplies and Materials

Access control (badge readers, sensors)
Application software
Backup power
Cable management system
Cable testers
Cable tools
Cable (copper and fiber)
Cart
Computer (desktop, laptop, tablet)
Diagonal cutters
Equipment racks
Fire suppression system
Firewalls
Fish tape
Hammer
HVAC
IDS/IPS
Keyboard, video, mouse switches
Label maker
Ladder
Lights-out management
Modems
Monitors
Multi-meter
Network access control
Network analyzer
Network appliance
Network storage
Network taps
Offsite storage
Operating system software
Physical access (turnstiles, mantraps)
Power conditioners
Power generator
Removable storage
Routers
Screwdrivers
Server
Software tools
Switches
Tile puller
Tone generator
Torx drivers
Utility cart
Virtual architecture
Wire ties
Wireless access points
Wireless intrusion detection

Future Trends and Concerns

3D printing and 3D/4D technologies
Automation replacing human resources
Automotive technologies
Background checks
Big Data
BYOD
Certification updates
Cloud computing
Cyber law
Data analytics/machine learning
Data centers
Digital currency (bitcoin)
Digital publishing (e-textbooks)
Drones (unmanned)
EAR (Export Administration Regulations)
Electronic surveillance
Embedded operating systems
E-recycling
Green computing
Hacktivism
Heuristics
HIPPA (Health Insurance Portability & Accountability Act)
Home automation
ICS/SCADA security
IoT (Internet of Things)
ITAR (International Traffic in Arms regulations)
Mobile applications
Mobile technologies
Modeling, simulation, visualization
Nano-technologies
New certifications
NFC (apple pay)
Operating systems
Parallel coding (scientific computing)
Penetration testing
PII (Personally Identifiable Information)
Quantum computing
RFID
Robotics
Satellite communications
Satellite technologies
Self-driven vehicles
Social engineering
Social media
Software defined hardware (field programmable gate arrays)
Software defined radios
Supercomputing or HPC
TMSAD
Virtualization
Wearable technologies
White Hat, Black Hat, Gray Hat Hackers
Wireless technologies

Credentials

Certified Information Systems Security Professional (CISSP)
CompTIA A+
CompTIA Network+
CompTIA Security+
ECSA - EC-Council Certified Ethical Hacker (CEH)
CEH – Certified Ethical Hacker
CHFI – Computer Hacking Forensics Investigator
GCIH – GIAC Certified Incident Handler
Linux+
LPIC-1 – Linux Professional Institute Certificate
MCSE – Microsoft Certified Solutions Expert

Professional Organizations

(ISC)^2 – International Information Systems Security Certifications Consortium
CompTIA – Computing Technology Industry Association
EC – Council – International Council of Electronic Commerce Consultants
IEEE – Institute of Electrical and Electronics Engineers
ISSA – Information Security Systems Association
PMI – Project Management Institute
NIST – National Institute of Standards and Technology
SANS – System Administration, Network and Security Institute

Acronyms

ACL – Access Control Lists
BYOD – Bring Your Own Device
CISSP – Certified Information Systems Security Professional
CVE – Common Vulnerabilities and Exposures
GIAC – Global Information Assurance Certificate
HPC – High Performance Computing
HVAC – Heating, Ventilation and Air Conditioning
ICS – Industrial Control Systems
IDS – Intrusion Detection System
INFOSEC – Information Security
IPS – Intrusion Protection System
NFC – Near Field Communication (Apple Pay)
OSI – Open Systems Interconnections
RFID – Radio Frequency Identification
SCADA – Software Control and Data Acquisition
SPAWAR - Space and Naval Warfare Systems Command
SME – Subject Matter Expert
TCP/IP – Transmission Control Protocol/Internet Protocol
TMSAD - Trusted Model for Security Automation Data
3D/4D – Three/four Dimensional

DACUM Research Chart for Cybersecurity Professional

DACUM Panel

Gayle Barrow Burton, CISSP,
Linux+, LPIC-1
Information Systems Security Analyst
Honeywell Technology Solutions Inc.
Suffolk, VA

Jacob M. Freiburger, Net+, SEC+,
CEH, CHFI, ECSA
Cyber Security Analyst
Suffolk, VA

Tregg Delane Hartley, GCIH, MCSE,
Security+, Network+
Computer Network Defense Engineer
Jacobs Technology
Hampton, VA

Timothy L. Kramer, CISSP
Information Assurance Lead
U.S. Navy/SPAWAR
Virginia Beach, VA

Charles Littman, CISSP
Lieutenant
United States Navy
Virginia Beach, VA

David Spicer, CISSP
IT Security Specialist (INFOSEC)
U.S. Fleet Cyber Command
Suffolk, VA

DACUM Facilitators

Kim B. Utley
Bonita J. Volker

Sponsored by

TIDEWATER COMMUNITY COLLEGE
From here, go anywhere.™

Produced by

Tidewater Community College

with campuses in the cities of

Chesapeake, VA
Norfolk, VA
Portsmouth, VA
Virginia Beach, VA

January 27-28, 2015

DACUM Research Chart for Cybersecurity Professional

January 27-28, 2015

	Duties	Tasks											
A	**Maintain System Accreditation**	A-1 Perform system validation	A-2 Maintain system certification	A-3 Assess mitigation impact	A-4 Establish SME relationships								
B	**Conduct Cybersecurity Analysis**	B-1 Conduct business analysis	B-2 Perform systems analysis	B-3 Analyze techniques, tactics, procedures	B-4 Perform link trend analysis	B-5 Analyze network traffic	B-6 Manage system logs	B-7 Analyze system logs	B-8 Conduct forensics analysis	B-9 Perform code review			
C	**Identify Security Threats**	C-1 Investigate security threats	C-2 Identify emerging cyber threat technologies	C-3 Identify physical security threats	C-4 Identify social engineering threats	C-5 Identify insider threats	C-6 Conduct threat code review						
D	**Manage System Configuration**	D-1 Document baseline configuration	D-2 Research organizational policies	D-3 Interpret organizational policies	D-4 Evaluate configuration change requests	D-5 Administer firewall ACL's	D-6 Administer IPS/IDS signatures	D-7 Document configuration changes					
E	**Identify Security Vulnerability**	E-1 Conduct vulnerability assessment	E-2 Identify attack vectors	E-3 Conduct penetration testing	E-4 Protect network architecture	E-5 Monitor CVE notifications	E-6 Detect traffic anomalies	E-7 Perform network scanning	E-8 Assess security vulnerabilities				
F	**Conduct Risk Analysis**	F-1 Assess security risks	F-2 Identify risk counter-measures	F-3 Perform risk mitigation	F-4 Aggregate system risks	F-5 Document lessons learned							
G	**Generate Analysis Reports**	G-1 Select reporting mechanism	G-2 Measure system compliance	G-3 Generate analysis reports	G-4 Distribute analysis reports	G-5 Report system compliance							
H	**Maintain Situational Awareness**	H-1 Review system architecture	H-2 Review system topology	H-3 Detect emerging technologies	H-4 Research wireless technology	H-5 Research cloud technology							
I	**Convey Information to Stakeholders**	I-1 Conduct role-play briefing	I-2 Conduct peer review	I-3 Conduct brainstorm sessions	I-4 Conduct pre-meeting conference	I-5 Schedule required technology	I-6 Write technical papers						
J	**Pursue Professional Development**	J-1 Research emerging cybersecurity technologies	J-2 Interpret industry policies	J-3 Pursue required certifications	J-4 Maintain required certifications	J-5 Identify social media impacts	J-6 Join relevant professional organizations	J-7 Establish SME relationships	J-8 Identify barriers to employment	J-9 Maintain security clearance (DoD only)			
K	**Manage Disaster Response**	K-1 Develop disaster response plan	K-2 Conduct disaster response drill	K-3 Review disaster response plan	K-4 Conduct incident response	K-5 Identify prevailing counter-measures	K-6 Design remediation plan	K-7 Implement remediation plan	K-8 Conduct forensics analysis	K-9 Adhere to legal requirements	K-10 Liaise violations with legal agencies	K-11 Test response plan	K-12 Implement lessons learned
L	**Validate Regulatory Compliance**	L-1 Review policy/laws/regulations	L-2 Ensure policy/law/regulation compliance	L-3 Produce compliance evidence (e.g., federal, state, international, etc.)									

General Knowledge and Skills

- Access control
- Access control lists
- Analytical skills
- Boolean searches
- Budget/financial processes
- Cloud
- Command line knowledge
- Computer forensic investigation
- Conversion (binary, hexadecimal, octal)
- Critical thinking skills
- Cryptography and encryption fundamentals
- Diagnostics
- Hardening systems
- Internet protocol version 4/6
- Interview skills
- Intrusion detection
- Keyboarding
- Listening skills
- Negotiating skills
- Network hardware
- Network log fundamentals
- Network technology
- Networking
- Observation
- Operating systems
- Oral communication
- OSI and TCP/IP network models
- Packet analysis
- Ports protocols services
- Problem-solving techniques
- Programming
- Record keeping
- Routing
- Scripting
- Security fundamentals
- Subnet masking
- Total cost of ownership
- Trouble shooting
- Virtual private networks
- Virtualization
- Writing skills

Worker Behaviors

- Ability to work on a team
- Accepts constructive criticism
- Adaptable
- Analytical
- Assertive
- Creative
- Determined
- Diplomatic
- Ethical
- Fiscally responsible
- Follows instructions
- Forward thinker
- Focus
- Goal-oriented
- Good communicator
- Good listener
- Helpful
- Honest
- Independent thinker
- Initiative
- Inquisitive
- Integrity
- Law-abiding
- Leader
- Loyal
- Mentor
- Motivated
- Non-condescending
- Open-minded
- Organized
- Perseverance
- Planner
- Polite
- Positive attitude
- Professional
- Reliable
- Research-minded
- Respectful
- Safety conscious
- Self-aware
- Self-control
- Self-directed learner
- Self-driven
- Self-reliant
- Strong work ethic
- Tactful
- Thorough
- Trustworthy
- Versatile vocabulary
- Visionary