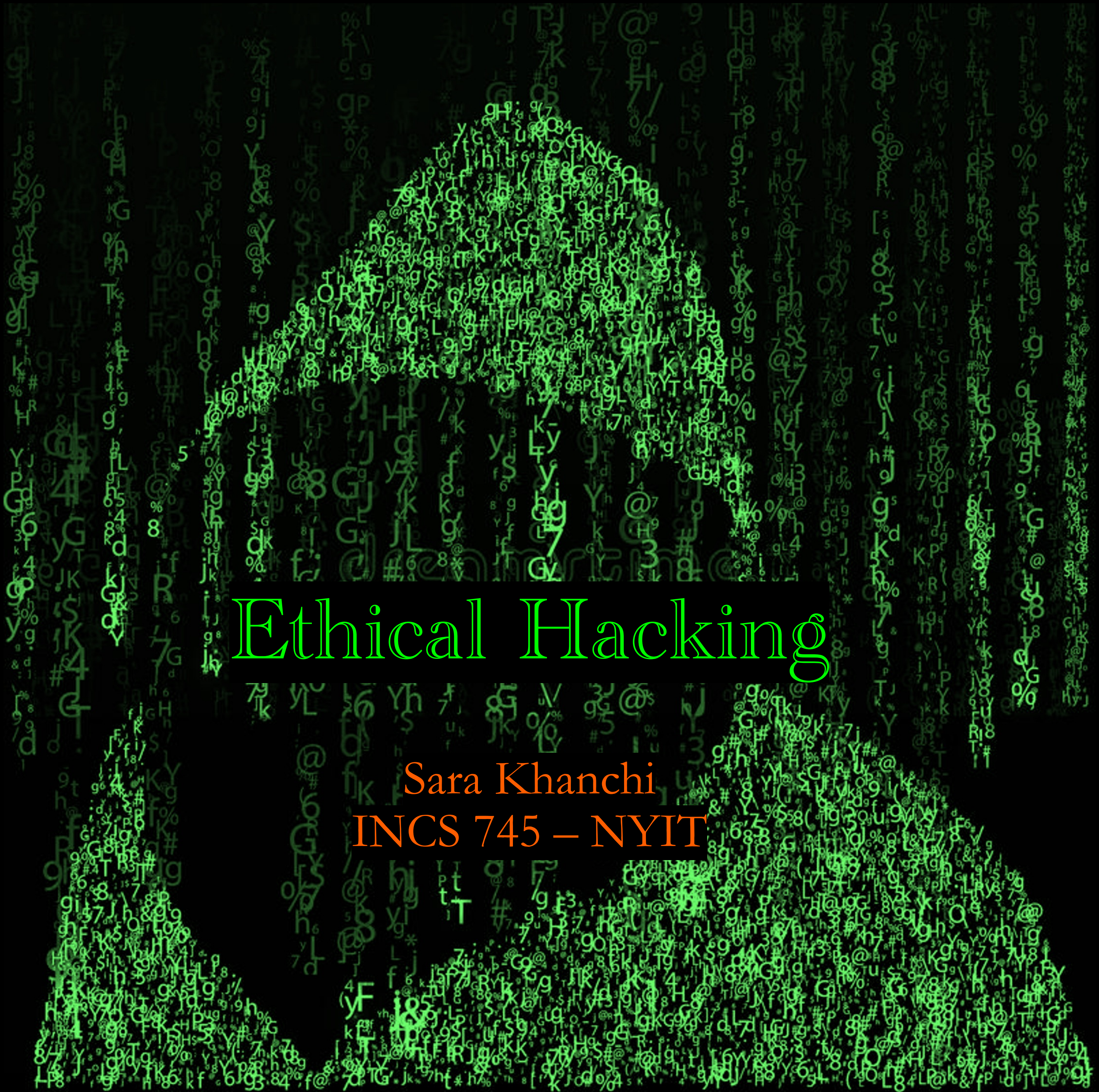


Ethical Hacking

Sara Khanchi

INCS 745 – NYIT

Outline

- Ethical Hacking
- Penetration Testing Phases
- First Phase – Reconnaissance
- Second Phase – Scanning
- Tools

Ethical Hacking

- Cracking is the term for illegally hacking into a computer system without the permission of the system's owner.
- Hacking is a term that is often used interchangeably with "cracking," but some hackers find it offensive.
- Whatever a computer cracker's motivations - a love of difficult challenges, curiosity, patriotism, a desire for recognition or financial gain or revenge - cracking a system is a crime.

Hacker Communities

- A **black hat hacker** is a malicious hacker.
- A **white hat hacker** does what a black hat hacker does, breaking into companies and systems, with their permission, of course, in hopes of finding and exploiting vulnerabilities.
- A **grey hat hacker** is somewhere in the middle.
  - One type of grey hat hacker might break into a system and prove it to the administrator, then the grey hat will request payment to fix it, and if denied, will move on without any malicious actions.

Hackers

White Hat

People who specialized hacking check the faults of the system

Grey Hat

Exploit a security to the attention of the owners

Black Hat

People who break into networks and harm to the network and property

White Hat is known as Ethical Hacker

Purpose and Intention

The FBI defines the motivation of individuals who commit espionage against the country, with the acronym, **MICE**:

- **M**oney
- **I**deology
- **C**ompromise or **C**oercion
- **E**go or **E**xtortion.

Researcher, Max Kilger, proposed that the motivations for the hacker community can be thought of as **MEECES:**

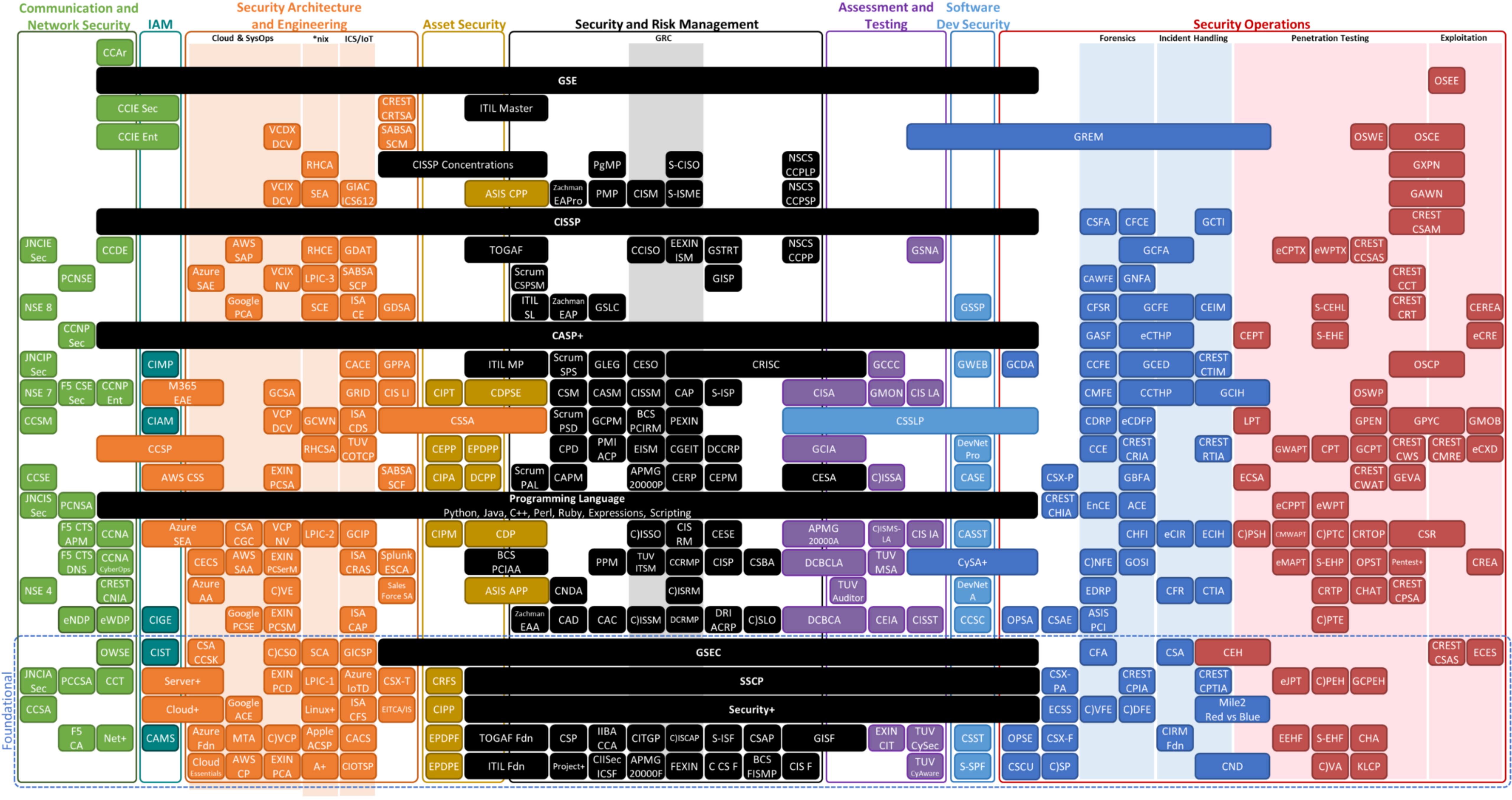
- **M**oney
- **E**go
- **E**ntertainment
- **C**ause
- **E**ntrance
- **S**tatus.

Ethical Hacking

- Ethical hackers and unethical hackers use the same reading materials and techniques
- What distinguishes between the two groups is
  - The permission of the network owner
  - The choice of whether to defend or attack

Security Certification Progression Chart 7.0 | (ISC)² CBK Security Domain Alignment

More info @ www.pauljeremy.com/security-certification-roadmap | 356 certs listed | October 2020



Spanning: GSE · CISSP · CASP+ · Programming Language
Python, Java, C++, Perl, Ruby, Expressions, Scripting · GSEC · SSCP · Security+

Foundational

Communication and Network Security

CCAr, CCIE Sec, CCIE Ent, JNCIE Sec, CCDE, PCNSE, NSE 8, CCNP Sec, JNCIP Sec, NSE 7, F5 CSE Sec, CCNP Ent, CCSM, CCSE, JNCIS Sec, PCNSA, F5 CTS APM, CCNA, F5 CTS DNS, CCNA CyberOps, NSE 4, CREST CNIA, eNDP, eWDP, OWSE, JNCIA Sec, PCCSA, CCT, CCSA, F5 CA, Net+

IAM

CIMP, M365 EAE, CIAM, CCSP, AWS CSS, CIGE, CIST, Server+, Cloud+, CAMS

Security Architecture and Engineering

Cloud & SysOps · *nix · ICS/IoT

CREST CRTSA, VCDX DCV, SABSA SCM, RHCA, VCIX DCV, SEA, GIAC ICS612, AWS SAP, RHCE, GDAT, Azure SAE, VCIX NV, LPIC-3, SABSA SCP, Google PCA, SCE, ISA CE, GDSA, CACE, GPPA, GCSA, GRID, CIS LI, VCP DCV, GCWN, ISA CDS, CSSA, RHCSA, TUV COTCP, EXIN PCSA, SABSA SCF, Azure SEA, CSA CGC, VCP NV, LPIC-2, GCIP, CECS, AWS SAA, EXIN PCSerM, ISA CRAS, Splunk ESCA, Azure AA, C)VE, Sales Force SA, Google PCSE, EXIN PCSM, ISA CAP, CSA CCSK, C)CSO, SCA, GICSP, EXIN PCD, LPIC-1, Azure IoTD, CSX-T, Google ACE, Linux+, ISA CFS, EITCA/IS, Azure Fdn, MTA, C)VCP, Apple ACSP, CACS, Cloud Essentials, AWS CP, EXIN PCA, A+, CIOTSP

Asset Security

ASIS CPP, CIPT, CDPSE, CEPP, EPDPP, CIPA, DCPP, CIPM, CDP, ASIS APP, CRFS, CIPP, EPDPF, EPDPE

Security and Risk Management

GRC

ITIL Master, CISSP Concentrations, PgMP, S-CISO, NSCS CCPLP, Zachman EAPro, PMP, CISM, S-ISME, NSCS CCPSP, TOGAF, CCISO, EEXIN ISM, GSTRT, NSCS CCPP, Scrum CSPSM, GISP, ITIL SL, Zachman EAP, GSLC, ITIL MP, Scrum SPS, GLEG, CESO, CRISC, CSM, CASM, CISSM, CAP, S-ISP, Scrum PSD, GCPM, BCS PCIRM, PEXIN, CPD, PMI ACP, EISM, CGEIT, DCCRP, Scrum PAL, CAPM, APMG 20000P, CERP, CEPM, CESA, C)ISSO, CIS RM, CESE, BCS PCIAA, PPM, TUV ITSM, CCRMP, CISP, CSBA, CNDA, C)ISRM, Zachman EAA, CAD, CAC, C)ISSM, DCRMP, DRI ACRP, C)SLO, TOGAF Fdn, CSP, IIBA CCA, CITGP, C)ISCAP, S-ISF, CSAP, GISF, ITIL Fdn, Project+, CIISec ICSF, APMG 20000F, FEXIN, C CS F, BCS FISMP, CIS F

Assessment and Testing

GSNA, GCCC, CISA, GMON, CIS LA, CSSLP, GCIA, C)ISSA, APMG 20000A, C)ISMS-LA, CIS IA, DCBCLA, TUV MSA, CySA+, TUV Auditor, DCBCA, CEIA, CISST, EXIN CIT, TUV CySec, TUV CyAware

Software Dev Security

GSSP, GWEB, DevNet Pro, CASE, CASST, DevNet A, CCSC, CSST, S-SPF

Security Operations

Forensics · Incident Handling · Penetration Testing · Exploitation

OSEE, GREM, OSWE, OSCE, GXPN, GAWN, CSFA, CFCE, GCTI, CREST CSAM, GCFA, eCPTX, eWPTX, CREST CCSAS, CAWFE, GNFA, CREST CCT, CFSR, GCFE, CEIM, S-CEHL, CREST CRT, CEREA, GASF, eCTHP, CEPT, S-EHE, eCRE, GCDA, CCFE, GCED, CREST CTIM, OSCP, CMFE, CCTHP, GCIH, OSWP, CDRP, eCDFP, LPT, GPEN, GPYC, GMOB, CCE, CREST CRIA, CREST RTIA, GWAPT, CPT, GCPT, CREST CWS, CREST CMRE, eCXD, CSX-P, GBFA, ECSA, CREST CWAT, GEVA, CREST CHIA, EnCE, ACE, eCPPT, eWPT, CHFI, eCIR, ECIH, C)PSH, CMWAPT, C)PTC, CRTOP, CSR, C)NFE, GOSI, eMAPT, S-EHP, OPST, Pentest+, CREA, EDRP, CFR, CTIA, CRTP, CHAT, CREST CPSA, OPSA, CSAE, ASIS PCI, C)PTE, CFA, CSA, CEH, CREST CSAS, ECES, CSX-PA, CREST CPIA, CREST CPTIA, eJPT, C)PEH, GCPEH, ECSS, C)VFE, C)DFE, Mile2 Red vs Blue, OPSE, CSX-F, CIRM Fdn, EEHF, S-EHF, CHA, CSCU, C)SP, CND, C)VA, KLCP

Certificates Information

- Information Systems Audit and Control Association (ISACA): www.isaca.org
- EC-Council: www.eccouncil.org/certification.aspx
- ISC2: www.isc2.org/cgi-bin/index.cgi
- CompTIA: http://certification.comptia.org/getCertified/certifications/security.aspx
- Global Information Assurance Certification (GIAC): www.giac.org/certifications/security

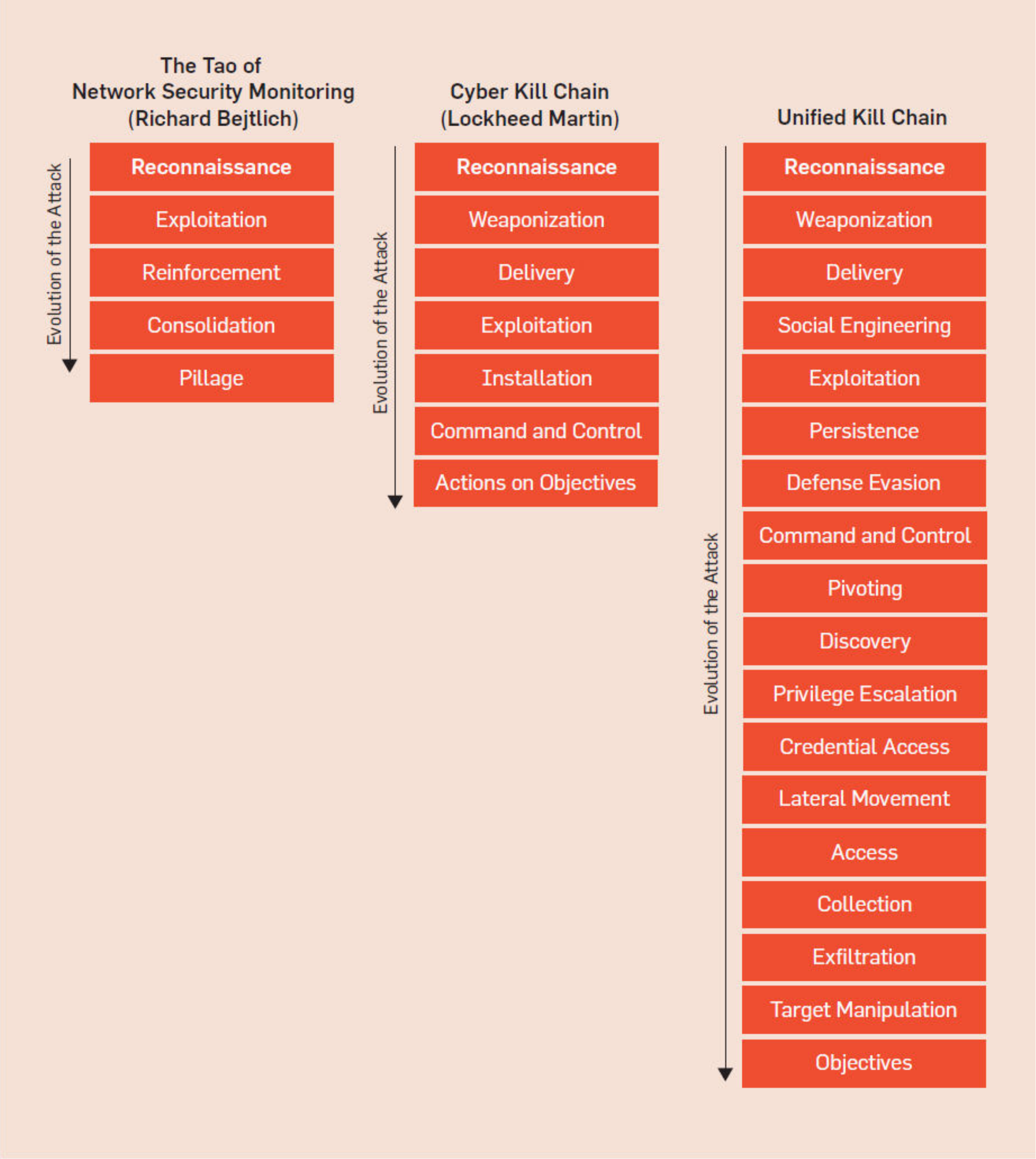
Vendor-specific Certificate

- Cisco’s CCNA
- Microsoft’s MCITP

Why Hire an Ethical Hacker?

- Companies would rather pay an ethical hacker to discover their systems' vulnerabilities than wait for an unethical hacker to do it for them.

Reference mode



The Tao of
Network Security Monitoring
(Richard Bejtlich)

- Reconnaissance
- Exploitation
- Reinforcement
- Consolidation
- Pillage

Cyber Kill Chain
(Lockheed Martin)

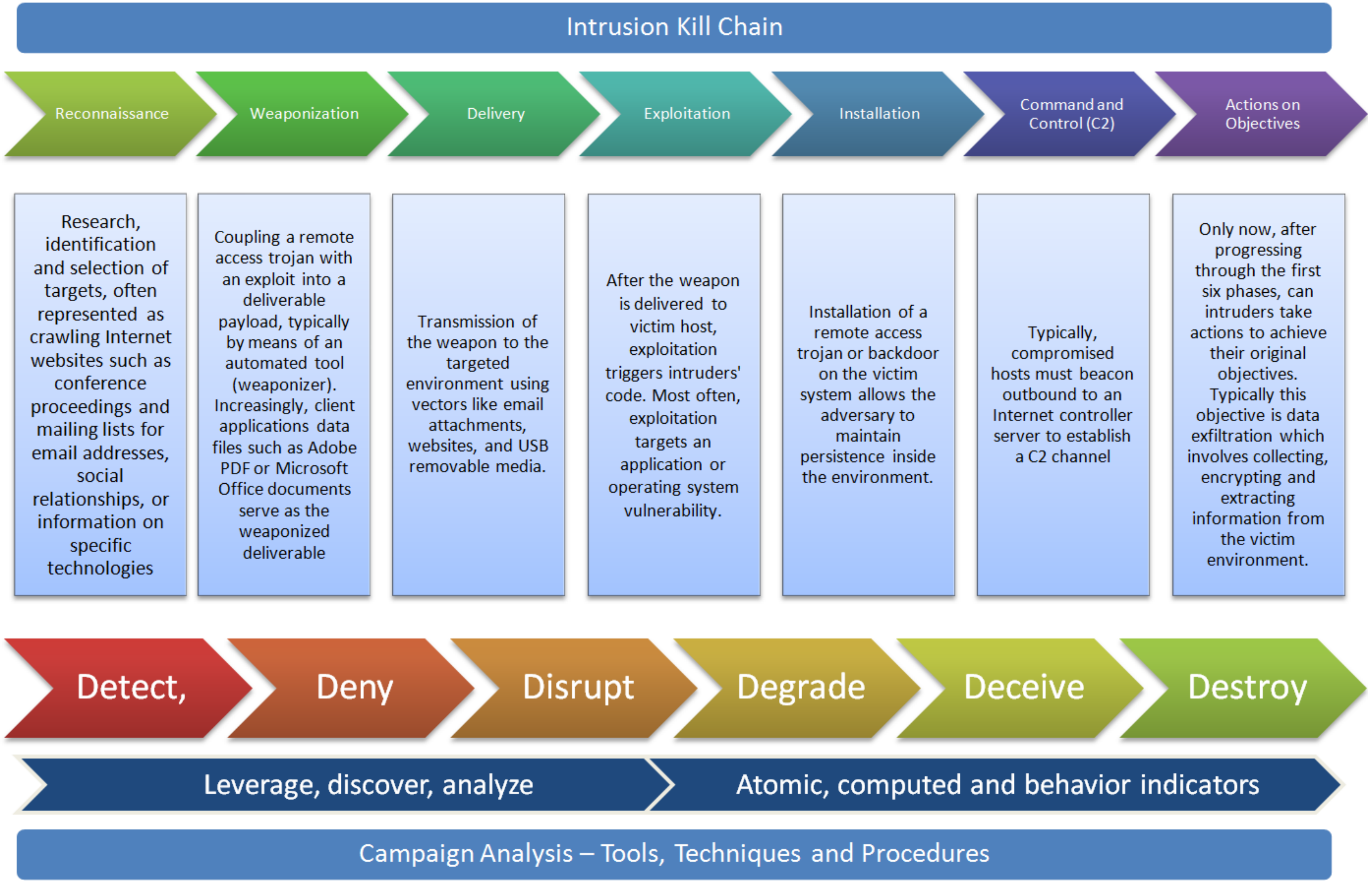
- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

Unified Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Social Engineering
- Exploitation
- Persistence
- Defense Evasion
- Command and Control
- Pivoting
- Discovery
- Privilege Escalation
- Credential Access
- Lateral Movement
- Access
- Collection
- Exfiltration
- Target Manipulation
- Objectives

Source: https://cacm.acm.org/research/cyber-reconnaissance-techniques/

Cyber Kill Chain



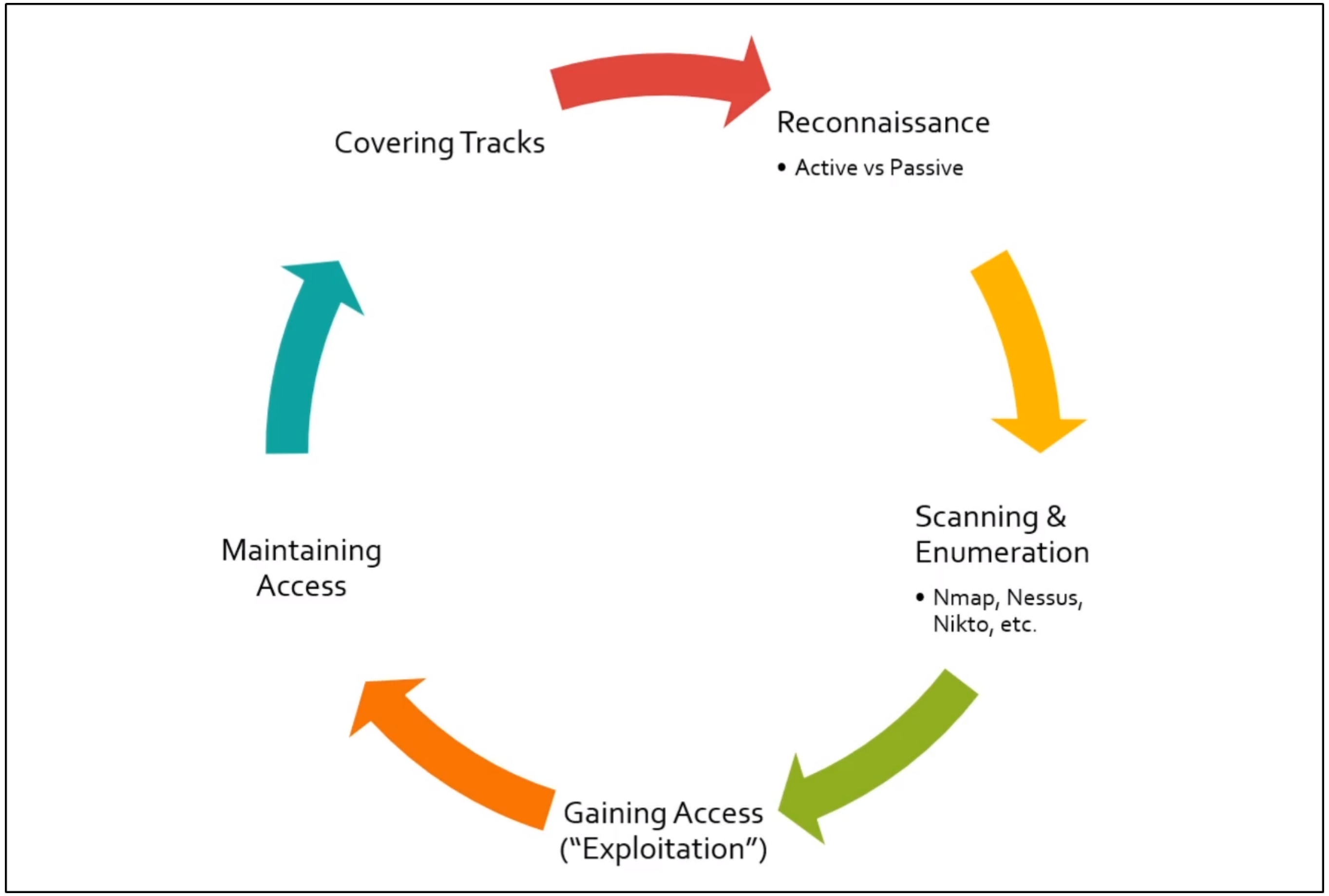
Intrusion Kill Chain

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control (C2)	Actions on Objectives
Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies	Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client applications data files such as Adobe PDF or Microsoft Office documents serve as the weaponized deliverable	Transmission of the weapon to the targeted environment using vectors like email attachments, websites, and USB removable media.	After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability.	Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.	Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel	Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment.

Detect,
Deny
Disrupt
Degrade
Deceive
Destroy
Leverage, discover, analyze
Atomic, computed and behavior indicators
Campaign Analysis – Tools, Techniques and Procedures

Source: https://countuponsecurity.com/wp-content/uploads/2014/08/killchain.png

Penetration Testing Steps



Reconnaissance

- Active vs Passive

Scanning & Enumeration

- Nmap, Nessus, Nikto, etc.

Gaining Access ("Exploitation")

Maintaining Access

Covering Tracks

First Phase - Reconnaissance

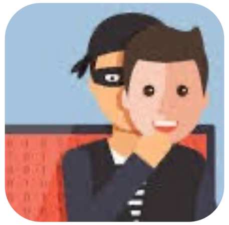
- Reconnaissance is the act of locating targets and developing the methods necessary to attack those targets successfully
- Important sources of information include:
  - Physical location of the target
  - Data about the users at the facility
  - Administrative shortcuts (such as assigning the same password to all new accounts and expecting the user to change the password later)
  - Operating systems
  - Network structure
  - Hardware configuration
  - Available services
  - Business strategies
  - Employee phone lists
  - Staffing structure of the organization
  - Internal newsletters
  - All available published , information about the company, either on its Web site or by other writers

Reconnaissance Types

- Legal Reconnaissance
  - It is completely legal to look up all the information that’s available about a company on the Internet
- Questionable Reconnaissance
  - Local laws vary, but in much of the world, performing a passive port scan is legal
  - Example: War driving - checking for unsecured wireless networks - is legal in some places and not in others
- Illegal Reconnaissance
  - Surreptitiously installing a keylogger - a tool that records users’ keystrokes - on a vulnerable machine is illegal

Reconnaissance Methods

Reconnaissance methods fall into three categories



Social engineering

Dumpster diving

Internet footprinting

Social Engineering

- Social engineering involves an act of deception on the part of an attacker, which is meant to trick well-meaning individuals into providing access to unauthorized information or systems
- Social engineering is typically considered unethical behavior but is sometimes used by ethical hackers as part of a penetration test
- People are trusting and want to be helpful

Social Engineering Techniques

- Impersonation
  - The hacker poses as a legitimate user or an employee who has the authority to collect information, i.e. IT support executive
- Bribery
  - The hacker pits an employee's greed against his or her loyalty to the organization.
  - Blackmail
- Deception
  - Actually joining the organization as an employee or consultant
- Conformity
  - People's tendency to believe that they are "typical" and that an apparent similarity between themselves and other (unknown) persons is an actual similarity.
  - Who are the target of attention are likely to feel victimized regardless of the fact that the ethical hacker had no malicious intent
- Reverse social engineering
  - A sting operation in which the hacker pretends he's an authority figure invested with the power to solve peoples' problems
  - They create the problem themselves

Physical Intrusion

- Physical intrusion refers to social engineers actually entering an organization’s premises with the sole purpose of collecting information
  - Learning the organization’s schedules
  - Knowing the floor plan of the building or buildings
  - Engaging in surveillance or research to understand the existing security procedures

Communication Media

- Social engineers use postal mail, e-mail, instant messaging, social networking, and telephone communication to get useful information from target individuals within an organization
  - Postal Mail
    - The victim receives a letter announcing that he or she has won a prize
  - E-Mail
    - A social engineer can send an e-mail purported to be from a legitimate IT e-mail account
    - Phishing
  - Instant Messaging
    - Befriending the victim
    - Ask to click on a link
  - Telephone Communication
    - They may manipulate background sounds and their own voices to produce the required effect
    - Also have tools to generate false entries in caller-ID technology, making it appear that a call is coming from a legitimate source

Countering Social Engineering

- Educate users
  - Included in your security policy
- Some precautions:
  - Do not provide any information to unknown people
  - Do not disclose any confidential information to anyone over the telephone without confirming the legitimacy of the person on the other end of the line
  - Do not type passwords or other confidential information in front of unknown people.
  - Do not submit information to any insecure Web site
  - Do not use the same username and password for all accounts
  - Verify the credentials of persons asking for passwords, and recognize that authentic administrators often do not need your password to access your files
  - Keep confidential documents locked
  - Lock or shut down computers when away from the workstation
  - Establish protocols that require help desk employees to provide information only after they have gained proper authentication

Internet Footprinting

- Internet foot-printing is a technical reconnaissance method that interests budding hackers and network security specialists alike
- Five Internet foot-printing methods:
  - Social networking
  - Web searching
  - Network enumeration
  - Domain Name System-based reconnaissance
  - Network-based reconnaissance

Social Networking

- Social networking services such as Facebook and Twitter
    - An example would be a network administrator who posts on his Facebook page that he is about to embark on a vacation
    - HR employee posts for specific job position, which reveals the technical specifics of the organization's infrastructure

Web Searching

- The majority of organizations have Web sites that contain crucial information
- Hackers use a variety of Web-based resources to find information about potential targets:
  - E-mail
  - Search engines
  - Hypertext Markup Language (HTML) source code
  - Newsgroups
  - Security-related Web sites
  - Newsletters

Network Enumeration

- Network enumeration is the process of identifying domain names as well as other resources on the target network
  - IP addresses of the computers
  - The contact persons of the target network
- WHOIS
  - An Internet tool that aids in retrieving domain name-specific information from the Network Solutions (NSI) Registrar database
  - CLI command: `whois options target`

Network Enumeration

- DNS Lookup
  - Help Internet users discover the DNS names of target computers
  - Websites:
    - www.dnsstuff.com
    - www.network-tools.com
    - www.networksolutions.com
- DNS Zone Transfer
  - Hackers use the following commands to perform DNS zone transfers:
    - nslookup
    - host
    - dig

Network-Based Reconnaissance

- Network-based reconnaissance is the process of identifying active computers and services on a target network
- Ping utility
  - Helps to verify whether a host is active
  - ping target_host
- Traceroute utility
  - Track all the intermediate servers
  - Unix: traceroute target_host
  - Win: tracert domain_name

Network-Based Reconnaissance

- Netstat utility
  - View all on a computer
    - Transmission Control Protocol (TCP)
    - User Datagram Protocol (UDP)
    - IP connections

Second Phase - Scanning

- Scanners
  - A scanner is a software tool that examines and reports about vulnerabilities on local and remote hosts
    - Legitimate use
    - Illegitimate use
- Network administrators
  - To find and fix vulnerabilities in remote machines on their networks
- Crackers
  - To find and exploit vulnerabilities that are discovered, not fix them

Port Scanner

- Examines and reports on the condition (open or closed) of a port as well as the application that is listening on that port, if possible
  - dig, ping, and trace are limited-use port scanners

How Scanners Work

- Scanners automate the process of examining network weaknesses
- Check for known vulnerabilities and open ports

- Scanner functions:
  - Connects to target host(s)
  - Examines the target host for the services running on it
  - Examines each service for any known vulnerability

- Can be set to target a single IP address or a range of IP addresses

Types of Scanning

- Transmission Control Protocol (TCP) connect scanning
- Half-open scanning
- User Datagram Protocol (UDP) scanning
- IP protocol scanning
- Ping scanning
- Stealth scanning

TCP Connect Scanning

- A TCP connect scan attempts to make TCP connections with all the ports on a remote system
  - Connection-succeeded message for active ports
  - Host-unreachable message for inactive ports
- IDS can easily detect the attempts

Half-Open Scanning

- Half-open scanning is TCP connection scanning, but it does not complete the connections
  - Only the SYN is sent from the scanner
- IDS cannot detect it
- Needs root or system administrator privileges

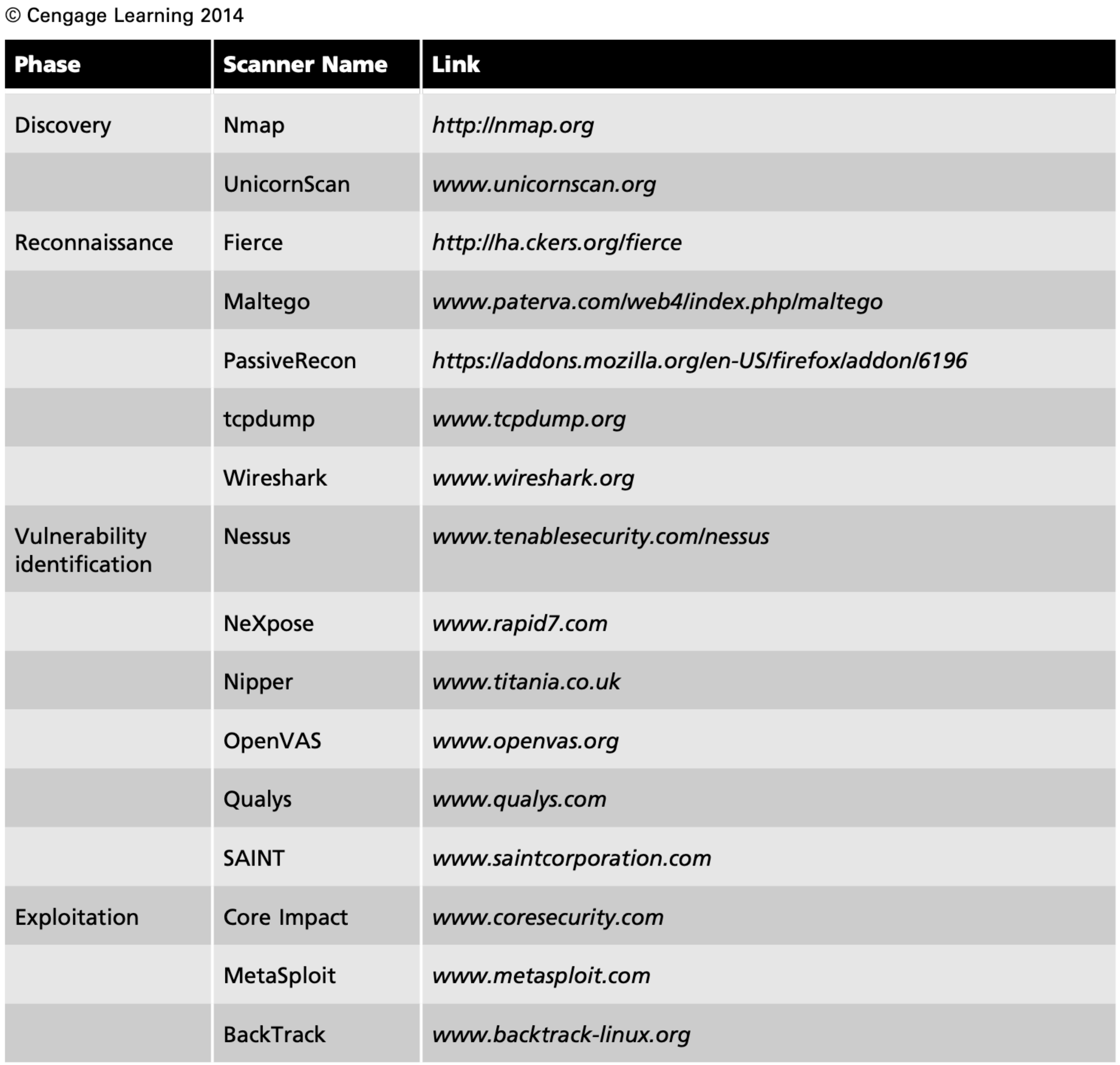
UDP Scanning

- Examines the status of UDP ports on a target system
- 0-byte UDP packet is sent to all the ports on a target host
- If port is closed
  - ICMP unreachable message

Other Types of Scanners

- IP Protocol Scanning
  - Examines a target host for supported IP protocols
- Ping Scanning
  - Demonstrates whether a remote host is active by sending ICMP echo request packets to that host
- Stealth Scanning
  - Examine hosts behind firewalls and packet filters
  - Similar to half-open scanning

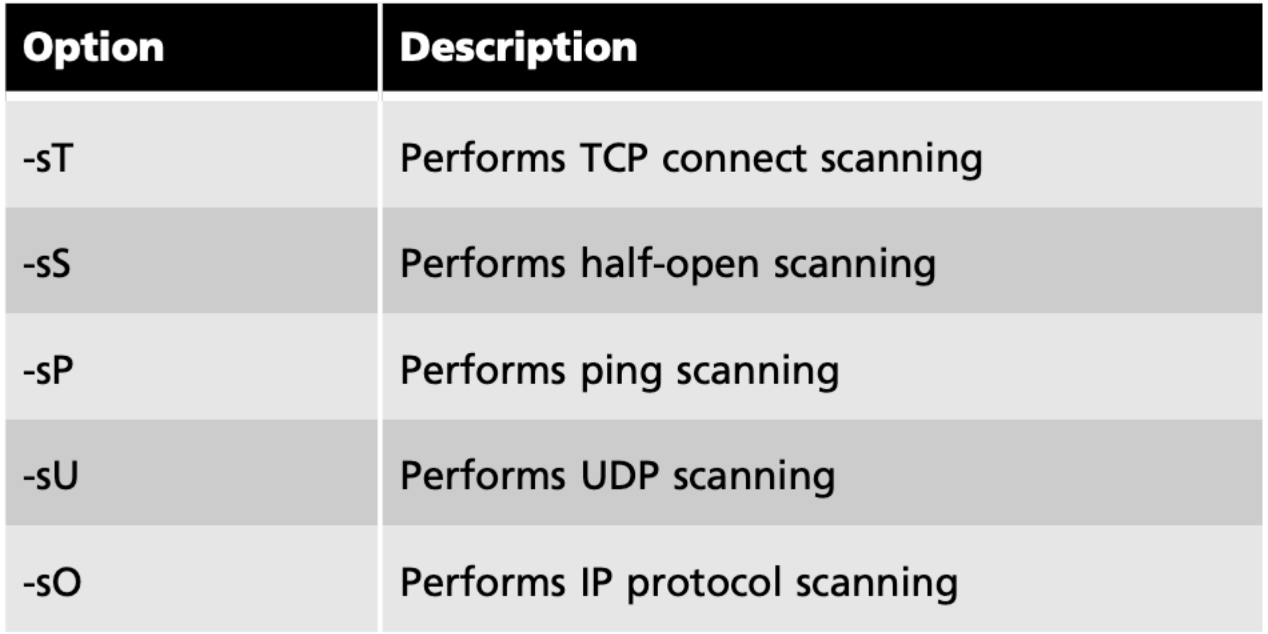
Tools



Phase	Scanner Name	Link
Discovery	Nmap	*http://nmap.org*
	UnicornScan	*www.unicornscan.org*
Reconnaissance	Fierce	*http://ha.ckers.org/fierce*
	Maltego	*www.paterva.com/web4/index.php/maltego*
	PassiveRecon	*https://addons.mozilla.org/en-US/firefox/addon/6196*
	tcpdump	*www.tcpdump.org*
	Wireshark	*www.wireshark.org*
Vulnerability identification	Nessus	*www.tenablesecurity.com/nessus*
	NeXpose	*www.rapid7.com*
	Nipper	*www.titania.co.uk*
	OpenVAS	*www.openvas.org*
	Qualys	*www.qualys.com*
	SAINT	*www.saintcorporation.com*
Exploitation	Core Impact	*www.coresecurity.com*
	MetaSploit	*www.metasploit.com*
	BackTrack	*www.backtrack-linux.org*

Discovery

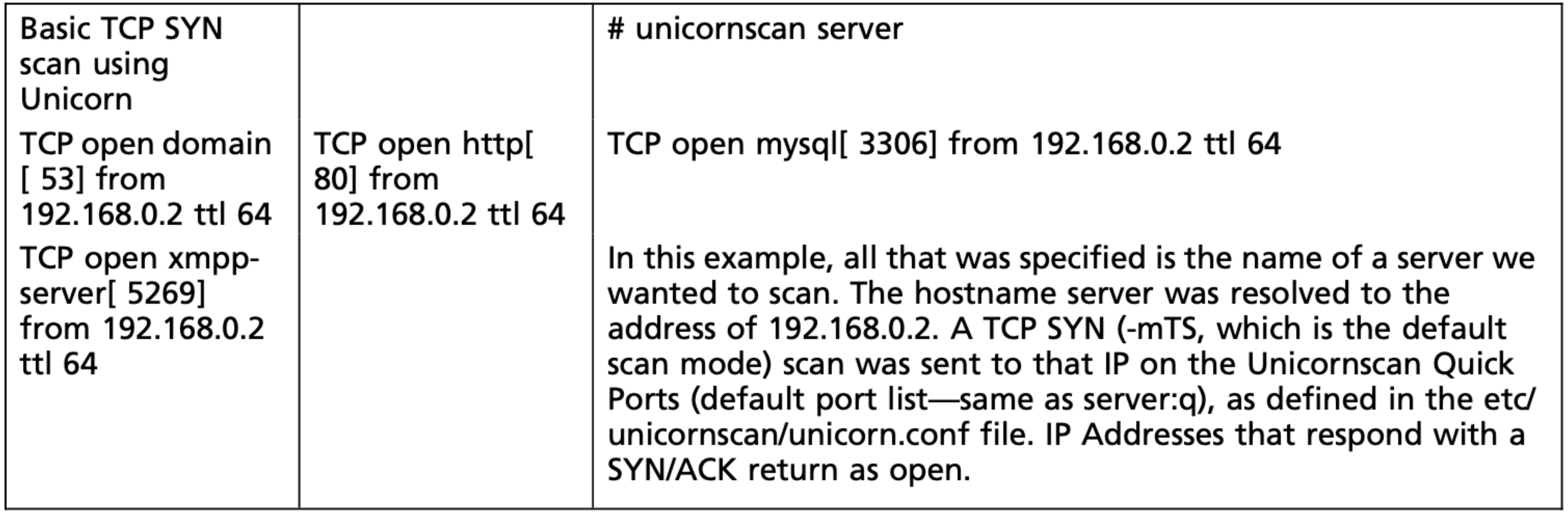
- Nmap
- Zenmap: Nmap with GUI



Option	Description
-sT	Performs TCP connect scanning
-sS	Performs half-open scanning
-sP	Performs ping scanning
-sU	Performs UDP scanning
-sO	Performs IP protocol scanning

Discovery

- Unicornscan
  - Open-source tool designed to identify information related to TCP flags and banners

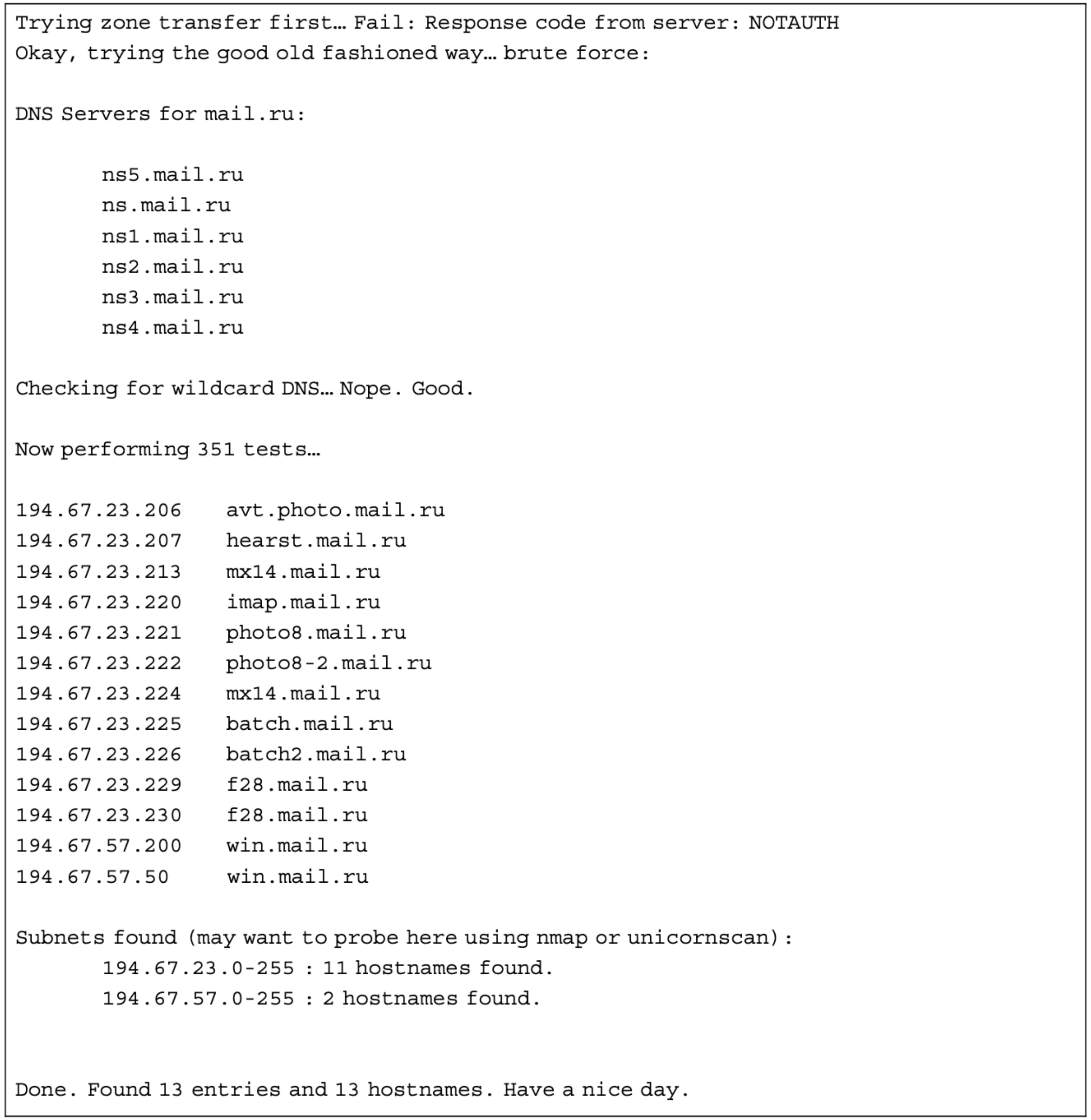


Basic TCP SYN scan using Unicorn		# unicornscan server
TCP open domain [53] from 192.168.0.2 ttl 64	TCP open http[80] from 192.168.0.2 ttl 64	TCP open mysql[3306] from 192.168.0.2 ttl 64
TCP open xmpp-server[5269] from 192.168.0.2 ttl 64		In this example, all that was specified is the name of a server we wanted to scan. The hostname server was resolved to the address of 192.168.0.2. A TCP SYN (-mTS, which is the default scan mode) scan was sent to that IP on the Unicornscan Quick Ports (default port list—same as server:q), as defined in the etc/unicornscan/unicorn.conf file. IP Addresses that respond with a SYN/ACK return as open.

Figure 3-2 Unicorn TCP scan example

Reconnaissance Tools

- Fierce
  - Open-source, Perl-based tool that focuses on particular targets using pattern matching



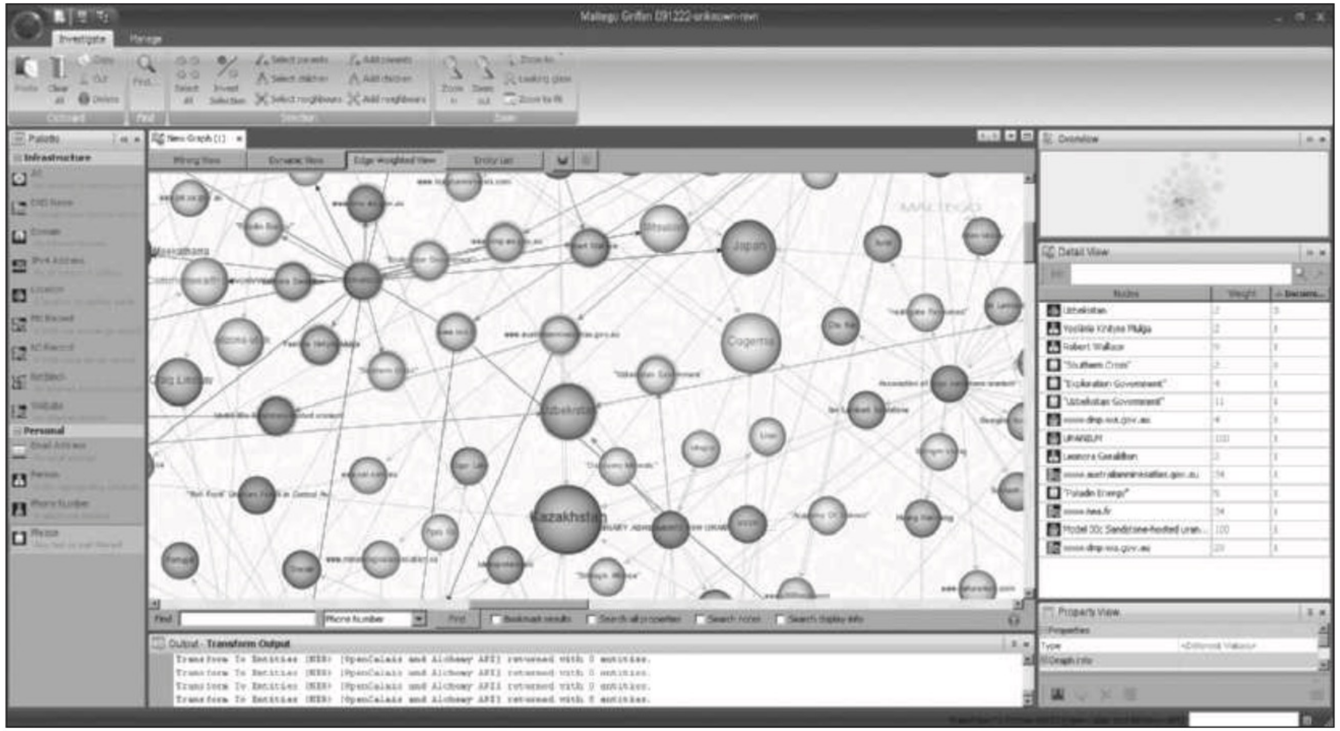
```
Trying zone transfer first… Fail: Response code from server: NOTAUTH
Okay, trying the good old fashioned way… brute force:

DNS Servers for mail.ru:

       ns5.mail.ru
       ns.mail.ru
       ns1.mail.ru
       ns2.mail.ru
       ns3.mail.ru
       ns4.mail.ru

Checking for wildcard DNS… Nope. Good.

Now performing 351 tests…

194.67.23.206    avt.photo.mail.ru
194.67.23.207    hearst.mail.ru
194.67.23.213    mx14.mail.ru
194.67.23.220    imap.mail.ru
194.67.23.221    photo8.mail.ru
194.67.23.222    photo8-2.mail.ru
194.67.23.224    mx14.mail.ru
194.67.23.225    batch.mail.ru
194.67.23.226    batch2.mail.ru
194.67.23.229    f28.mail.ru
194.67.23.230    f28.mail.ru
194.67.57.200    win.mail.ru
194.67.57.50     win.mail.ru

Subnets found (may want to probe here using nmap or unicornscan):
       194.67.23.0-255 : 11 hostnames found.
       194.67.57.0-255 : 2 hostnames found.



Done. Found 13 entries and 13 hostnames. Have a nice day.
```

Figure 3-3 Fierce scan example

Source: Fierce

Reconnaissance Tools

- Maltego
  - A Java-based tool that is offered in both community and commercial versions and is marketed as a forensic tool



Output - Transform Output

```
Transform To Entities (NER) [OpenCalais and Alchemy API] returned with 0 entities.
Transform To Entities (NER) [OpenCalais and Alchemy API] returned with 0 entities.
Transform To Entities (NER) [OpenCalais and Alchemy API] returned with 0 entities.
Transform To Entities (NER) [OpenCalais and Alchemy API] returned with 0 entities.
```

Nodes	Weight	Betweenness...
Uzbekistan	2	[illegible]
Yoslinda Kristyna Mulga	2	[illegible]
Robert Wallace	9	[illegible]
"Southern Cross"	2	[illegible]
"Exploration Government"	4	[illegible]
"Uzbekistan Government"	11	[illegible]
www.dmp.wa.gov.au	4	[illegible]
URANIUM	100	[illegible]
Leonora Geraldton	2	[illegible]
www.australianminesatlas.gov.au	34	[illegible]
"Paladin Energy"	5	[illegible]
www.nea.fr	34	[illegible]
Model 30c Sandstone-hosted uran...	100	[illegible]
www.dmp.wa.gov.au	20	[illegible]

Figure 3-4 Maltego interface example

Source: Maltego

Reconnaissance Tools

- PassiveRecon
  - a Firefox add-on that allows users to visit a target Web site and gather a variety of publicly available information useful in the enumeration or reconnaissance phase of a penetration test
- Tcpdump
  - An open-source command-line packet analyzer
- Wireshark
  - Similar to tcpdump but with GUI

Summary

- Ethical Hacking
  - Hacker Communities
  - Certificates
- Penetration Testing Phases
- First Phase – Reconnaissance
  - Types
  - Social Engineering
  - Physical Intrusion
  - Communication Media
  - Internet Footprinting
- Second Phase – Scanning
  - Port Scanner
  - Types of Scanning
- Tools
  - Reconnaissance
  - Scanning