Seminário Nacional de Segurança da Informação e Criptografia

O Ensino da Análise Forense Computacional em Defesa Cibernética

Prof. M.Sc. Marcelo Caiado, CISSP, GCFA, GCIH, EnCE
Chefe da Divisão de Segurança da Informação
Procuradoria Geral da República

Intelligence

The U.S. Government Wants 6,000 New 'Cyberwarriors' by 2016

By Dune Lawrence | April 15, 2014

SEND TO kindle

Illustration by Hisashi Okawa

The Pentagon plans to triple its cybersecurity staff by 2016, U.S. Secretary of Defense Chuck Hagel announced recently.

A few days later, FBI Supervisory Special Agent Charles Gilgen said at a conference on cybercrime that his agency's cyber division plans to hire 1,000 agents and 1,000 analysts in the coming year.

Just those two agencies are looking for 6,000 people with cybersecurity skills in the next two years. That's a very tall order. A look at one way the government has tried to build and recruit such talent—offering university scholarships—shows why.

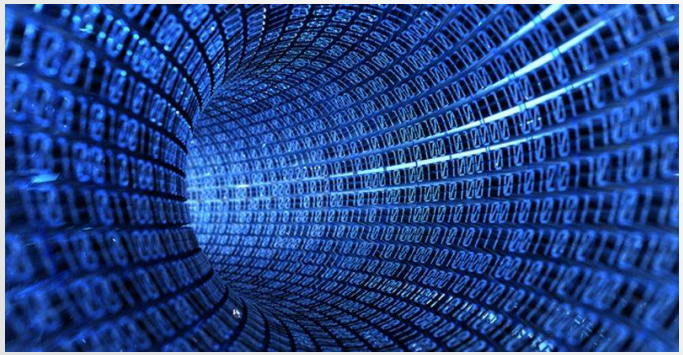
STORY: Why Heartbleed, the Latest Cybersecurity Scare, Matters

http://www.businessweek.com/articles/2014-04-15/uncle-sam-wants-cyber-warriors-but-can-he-compete

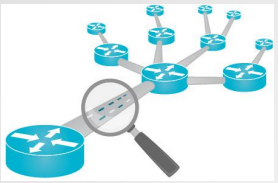
Análise Forense Computacional

DEFINIÇÃO

É a **preservação, aquisição, análise, descoberta, documentação e apresentação** de evidência presente em meio digital



Análise Forense Computacional



ALGUMAS ÁREAS:

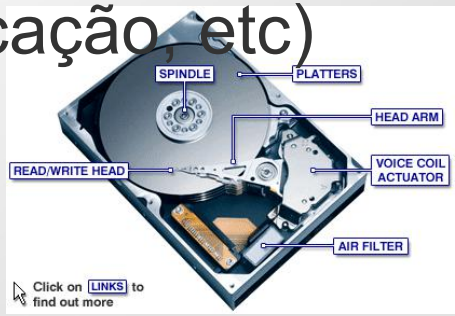
- Forense de dispostivos (computadores, discos rígidos, dispositivos móveis, mídias removíveis, etc)

- Forense de redes (invasão de redes, abuso de redes, etc)

- Forense de software (análise de malware, análise e auditoria de de códigos, etc)

- Forense live (equipamentos comprometidos, abuso de sistemas, antiforensics, criptografia, etc)

- Resposta a Incidentes (preparação, identificação, etc)



Government and military leaders have for years warned of increasingly pervasive and nefarious cyber-attacks. The network intrusions, perpetrated by nation states, hacktivists and thieves, are growing rapidly, experts have said.

To quell attacks, a premium has been put on so-called "cyberwarriors" — professionals trained to root out and stop network intrusions at some of the nation's largest institutions and military and government agencies.

At U.S. Cyber Command, based at Ft. Meade, Md., officials said the importance of having a properly trained workforce is essential to stopping attacks.

"There is nothing more vital to our mission of defending our nation's networks than a trained and ready cyberworkforce. Cyber has become an integral part of our interconnected world and our warfighting capabilities," Air Force Maj. Gen. Jim Keffer, chief of staff for USCYBERCOM, told National Defense in an email.

Programs that allow trainees to tinker with computers to fix vulnerabilities or stave off attacks from simulated hackers are immensely useful, he said.

"One of the best tools we use at USCYBERCOM for training is our exercise network, not

"From industry conferences to on-the-job, learn-by-doing training exercises to researching, analyzing and reverse engineering the cyber-attacks that have garnered worldwide attention, our workforce has their fingers on the pulse of the latest cyber-attack techniques and the innovative approaches for defending against them," she said.

The company uses knowledge gained by its experts who have been "on the front lines of the military and government network defense and exploitation," she said.

Trainees study advanced persistent threats, malware analysis and network defense, to name a few, Short said.

"We think it is important that our folks have a plethora of course work, training and exercises readily available to continuously update and fine tune their skillset. The better educated our people are, the better chance we have of mitigating advanced cyberthreats," said Short.

Industry is also working to keep their network security experts sharp.

At Lockheed Martin, employees practice their skills using simulated attack software, said Lee Holcomb, deputy to the technical operations vice president at Lockheed Martin's Information Systems and Global Solutions branch.

The program, called Experiential Cyber Immersion Training and Exercises, or EXCITE, uses a centrally-managed environment to simulate a real attack scenario. Until a year ago, the program was exclusively used to train employees internally. Now the company is looking

http://www.nationaldefensemagazine.org/archive/2013/December/Pages/Industry,MilitaryEmphasizeNeedfor%E2%80%98Cyberwarrior%E2%80%99TrainingasAttacksIncrease.aspx

Ciberataque atinge New York Times e Twitter

AFP - Agence France-Presse

Publicação: 28/08/2013 08:17 Atualização: 28/08/2013 08:39

O site do jornal New York Times e o Twitter foram alvo nesta terça-feira de ciberataques, atribuídos imediatamente a um grupo que apoia o presidente sírio, Bashar al-Assad.

"Nosso fornecedor de DNS experimentou um problema no qual os dados de DNS de várias organizações foram modificados, incluindo um dos domínios do Twitter utilizados como servidor de imagens, twimg.com", revelou a rede social. "Nenhuma informação dos usuários foi afetada pelo incidente" e o problema durou menos de duas horas, informou o Twitter.

Entretanto, o problema continua até a manhã desta quarta-feira com a página principal da rede social totalmente desconfigurada, impossibilitando a leitura e a publicação das postagens, embora seja possível entrar e postar através de outras mídias. A rede também funciona normalmente através do aplicativos de celular.

O jornal The New York Times informou que seu site foi tirado do ar por um ciberataque. A porta-voz do jornal, Eileen Murphy, escreveu no Twitter que "a estimativa preliminar é que o problema está provavelmente ligado a um ataque externo malicioso". "Estamos trabalhando para resolver isto". A conta oficial do diário nova-iorquino no Twitter indicou que o site do jornal "enfrentava dificuldades técnicas", mas que as notícias eram publicadas através do Twitter e de outras mídias.

A ação foi reivindicada no Twitter pelo Exército Sírio Eletrônico (SEA): "Os veículos caíram". O SEA foi responsabilizado no passado por ataques a grandes meios de comunicação, como o que ocorreu contra o jornal The Washington Post, no mês passado.

O ciberataque foi dirigido ao sistema de nomes de domínios (DNS), que age como diretório para o tráfego on-line aos endereços das páginas.

Os hackers conseguem sequestrar o tráfego da Web alterando a informação na direção dos DNS para enviar os usuários a outros sites.

O Washington Post revelou em janeiro que um grupo de hackers havia roubado suas senhas corporativas e acessado os computadores pessoais de 53 funcionários depois de o diário ter publicado uma notícia sobre a fortuna familiar do primeiro-ministro chinês, Wen Jiabao.

Israeli Defense Forces official Blog Hacked by Syrian Electronic Army

Posted on June 30, 2014 by Waqas

Syrian Electronic Army has made a major comeback by hacking and defacing the official blog of Israel Defense Forces (IDF) yesterday. The high profile hack was conducted on 28th June, 2013 in which Syrian hackers, loyal to President Bashar Al Assad took control of the official IDF blog by uploading a deface page along with a message. According to the message:

> **The Israeli govt commits war crimes on a daily basis, towards the Palestinians and is the biggest violator of Human Rights. in addition to the Palestinian case the message was also to warn Israel of the attacks which they carried over Syrian Military sites.**

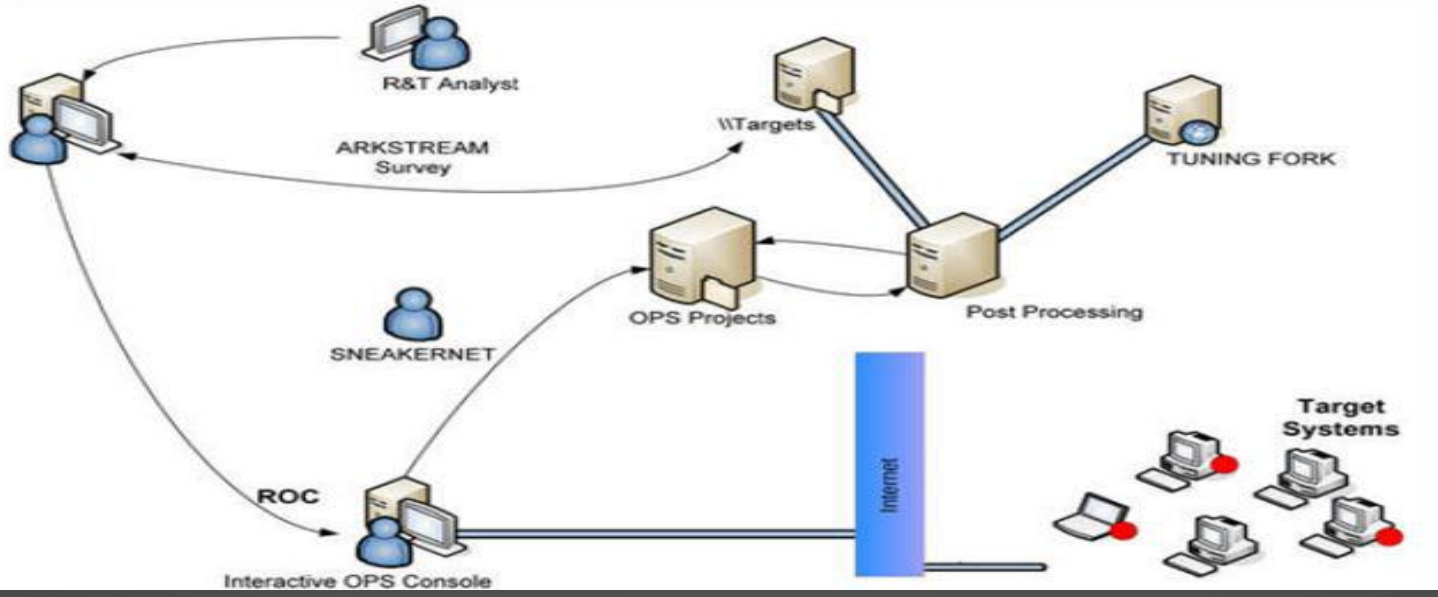
NSA BIOS Backdoor a.k.a. God Mode Malware
Part 1: DEITYBOUNCE

This article is the first part of a series on NSA BIOS backdoor internals. Before we begin, I'd like to point out why these malwares are classified as "god mode." First, most of the malware uses an internal (NSA) codename in the realms of "gods," such as DEITYBOUNCE, GODSURGE, etc. Second, these malwares have capabilities similar to "god mode" cheats in video games, which make the player using it close to being invincible. This is the case with this type of malware because it is very hard to detect and remove, even with the most sophisticated anti-malware tools, during its possible deployment timeframe.

This part of the series focuses on the DEITYBOUNCE malware described in the NSA ANT Server document, leaked by Edward Snowden. The analysis presented in this article is based on technical implications of the information provided by the document. The document lacks many technical specifics, but based on the BIOS technology at the day DEITYBOUNCE started to become operational, we can infer some technically sound hypotheses—or conclusions, if you prefer :-).

Introduction to DEITYBOUNCE Malware

DEITYBOUNCE operates as part of the system shown in Figure 1. Figure 1 shows several peculiar terms, such as ROC, SNEAKERNET, etc. Some of these terms are internally used by NSA. ROC is an abbreviation for remote operation center. ROC acts as NSA's point of control of the target system; it's located outside NSA's headquarter. SNEAKERNET is a fabulous term for physical delivery of data, i.e., using humans to move data between computers by moving removable media such as magnetic tape, floppy disks, compact discs, USB flash drives (thumb drives, USB stick), or external hard drives from one computer to another.



SEC504: Hacker Techniques, Exploits & Incident Handling

- Contents | Additional Info
- **Delivery Methods:** Live | Online
- GCIH Certification
- Affiliate Pricing
- 37 CPEs
- Laptop Required
- Masters Program
- DoDD 8570 (IAT Level III)
- Cyber Guardian

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

This challenging course is particularly well-suited to individuals who lead or are a part of an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

More

Notice: It is imperative that you get written permission from the proper authority in your organization before using these tools and techniques on your company's system and also that you advise your network and computer operations teams of your testing.

DF

SANS

Find Training | Live Training | Online Training | Programs

FOR508: Advanced Computer Forensic Analysis and Incident Response

- Contents | Additional Info
- **Delivery Methods:** Live | Online
- GCFA Certification
- Affiliate Pricing
- 36 CPEs
- Laptop Required
- Masters Program
- Cyber Guardian

NEW FOR508! -This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics. Don't miss the NEW FOR508!

Overview

DAY 0: A 3-letter government agency contacts you to say that critical information was stolen by a targeted attack on your organization. Don't ask how they know, but they tell you that there are several breached systems within your enterprise. You are compromised by an Advanced Persistent Threat, aka an APT - the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 90% of all breach victims learn of a compromise from third party notification, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Gather your team - it's time to go hunting.

FOR508: Advanced Computer Forensic Analysis and Incident Response will help you determine:

1. How did the breach occur?
2. What systems were compromised?
3. What did they take? What did they change?
4. How do we remediate the incident?

The field of digital forensics is not for the faint-hearted, especially involves intelligence-gathering for the military. Michael Kassner ta to Melia Kelley about the path that took her to Iraq.

Recently, I ran across the following job post.

Wanted:

"Computer Forensic Examiner/MEDEX -- Afghanistan"

Requirements:

- *% Travel : 100*
- *Clearance: Must currently possess a minimum Final Secret in JPAS, DIA Access preferred.*
- *Must be able to pass a SI and POLY.*

The posting goes on to list 17 skills -- specific to digital forensics -- in which potential candidates must be proficient.

Been there. Done that.

Did you know jobs like that existed? I didn't. I had to find out more. My search took me to the blog: Girl, Unallocated.

That's where I found the real deal, Melia Kelley -- aka *Girl, Unallocated*. She met all qualifications. In fact, she's already been there and done that. The only difference; *there* was Iraq, not Afghanistan.

Made a promise

I better step back for a second. I had mentioned in a previous article that I know just enc about digital forensics to be dangerous. Some students called me out on it, particularly young lady -- something about me being a guy and knowing very little.

I'm about to fix that.

PREMIUM

Search for people, jobs, companies, and more...

Job description

Computer Forensic Examiner/ MEDEX - Afghanistan Full Time Regular posted 9/23/2011

Job Category: MIS - Info Tech / Telecommunications
Req ID: 210074
Able to obtain security clearance? None
Currently possess security clearance? Secret
Location: McLean, VA
% Travel: 100
Relocation: No

Requirements: The MIBU currently has an opening for a Computer Forensic Examiner/ MEDEX.

CLEARANCE: Must currently possess a minimum Final Secret in JPAS, DIA Access preferred. Must be able to pass a SI and POLY.

RESPONSIBILITIES:

1. Receiving, categorizing, documenting, and tracking digital and analog storage mediums to include maintaining and ensuring a chain of custody for all items received.

2. Ensure media capture data is accounted for and provided to the examiner and linguists assigned to the case; prioritize work with MEDEX Linguists to rapidly exploit media.

3. Produce forensically sound duplicates of original media for examination/exploitation.

4. Acquire and exploit digital images using forensic tools to examine file structure, conduct text searches, examine deleted files and extract information; develop, copy and/or digitize audio and video mediums, such as cassette and video tapes and 35mm film for examination/exploitation.

5. Create thorough and complete MEDEX reports that follow given standards; review reports and manage quality control on outgoing products; write scripts to refine workflow and exploitation automation; update databases to be used in cross-case comparisons and link analysis; upload reports and files to the HARMONY database; transfer images, reports and files to various hardware or applications for shipment; provide technical support to various team members.

MANDATORY REQUIREMNTS:
EDUCATION: A HS diploma or any combination of education and experience is required.
EXPERIENCE: A minimum of 2 years of general work experience is required.

SUBSTITUTION/EQUIVALENCY:

1. AA/AS = Two (2) years general experience.
2. BA/BS = Six (6) years general experience.
3. MS/MA = Ten (10) years general experience.
4. Ph.D. = Thirteen (13) years general experience.

LANGUAGE TEST:
Must provide proof of achieving a minimum ILR writing test score of 4 in English.
Must pass English language test that are dated no earlier than six months prior to submission for consideration, regardless of previous work experience.

http://www.techrepublic.com/blog/it-security/breaking-into-the-digital-forensics-field-melia-kelleys-path/

Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

Strategies to Mitigate Targeted Cyber Intrusions

Originally published 18 February 2010, updated for February 2014

Mitigation Strategy Effectiveness Ranking for 2014 (and 2012)		Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Helps Detect Intrusions	Helps Prevent Intrusion Stage 1: Code Execution	Helps Contain Intrusion Stage 2: Network Propagation	Helps Contain Intrusion Stage 3: Data Exfiltration
1	(1)	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.	Essential	Medium	High	Medium	Yes	Yes	Yes	Yes
2	(2)	**Patch applications** e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.	Essential	Low	High	High	No	Yes	Possible	No
3	(3)	**Patch operating system vulnerabilities.** Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.	Essential	Low	Medium	Medium	No	Yes	Possible	No
4	(4)	**Restrict administrative privileges** to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	Low	No	Possible	Yes	No

Once organisations have effectively implemented the Top 4 mitigation strategies, firstly on workstations of users who are most likely to be targeted by cyber intrusions and then on all workstations and servers, additional mitigation strategies can then be selected to address security gaps until an acceptable level of residual risk is reached.

5	(18)	**User application configuration hardening**, disabling: running Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.	Excellent	Medium	Medium	Medium	No	Yes	No	No
6	(N/A)	**Automated dynamic analysis** of email and web content run in a sandbox to detect suspicious behaviour including network traffic, new or modified files, or other configuration changes.	Excellent	Low	Medium	Low	Yes	Yes	No	Possible
7	(21)	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Excellent	Low	Medium	Low	Possible	Yes	Possible	No
8	(11)	**Host-based Intrusion Detection/Prevention System** to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Excellent	Low	Medium	Medium	Yes	Yes	No	Possible
9	(5)	**Disable local administrator accounts** to prevent network propagation using compromised local administrator credentials that are shared by several workstations.	Excellent	Low	Medium	Low	No	No	Yes	No
10	(7)	**Network segmentation and segregation** into security zones to protect sensitive information and critical services such as user authentication by the Microsoft Active Directory service.	Excellent	Low	High	Medium	Yes	No	Yes	Possible
11	(6)	**Multi-factor authentication** especially implemented for remote access, or when the user is about to perform a privileged action or access a sensitive information repository.	Excellent	Medium	High	Medium	No	No	Possible	No
12	(8)	**Software-based application firewall, blocking incoming network traffic** that is malicious or otherwise unauthorised, and denying network traffic by default.	Excellent	Low	Medium	Medium	Yes	Yes	Yes	No
13	(9)	**Software-based application firewall, blocking outgoing network traffic** that is not generated by a whitelisted application, and denying network traffic by default.	Excellent	Medium	Medium	Medium	Yes	No	Yes	Yes
14	(10)	**Non-persistent virtualised sandboxed trusted operating environment**, hosted outside of the organisation's internal network, for risky activities such as web browsing.	Excellent	High	High	Medium	Possible	No	Yes	Possible
15	(12)	**Centralised and time-synchronised logging of successful and failed computer events**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
16	(13)	**Centralised and time-synchronised logging of allowed and blocked network activity**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
17	(14)	**Email content filtering**, allowing only whitelisted business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.	Excellent	High	High	Medium	Yes	Yes	No	Possible
18	(15)	**Web content filtering** of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.	Excellent	Medium	Medium	Medium	Yes	Yes	No	Possible
19	(16)	**Web domain whitelisting for all domains**, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Excellent	High	High	Medium	Yes	Yes	No	Yes
20	(19)	**Block spoofed emails** using Sender ID or Sender Policy Framework (SPF) to check incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organisation's domain.	Excellent	Low	Low	Low	Possible	Yes	No	No
21	(22)	**Workstation and server configuration management** based on a hardened Standard Operating Environment, disabling unneeded/undesired functionality e.g. IPv6, autorun and LanMan.	Good	Medium	Medium	Low	Possible	Yes	Yes	Possible
22	(25)	**Antivirus software using heuristics and automated Internet-based reputation ratings** to check a program's prevalence and its digital signature's trustworthiness prior to execution.	Good	Low	Low	Low	Yes	Yes	No	No
23	(24)	**Deny direct Internet access from workstations** by using an IPv6-capable firewall to force traffic through a split DNS server, an email server, or an authenticated web proxy server.	Good	Low	Low	Low	Yes	Possible	No	Yes
24	(23)	**Server application configuration hardening** e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.	Good	Low	High	Medium	Possible	Yes	No	Possible
25	(27)	**Enforce a strong passphrase policy** covering complexity, length, expiry, and avoiding both passphrase reuse and the use of a single dictionary word.	Good	Medium	Medium	Low	Possible	No	Yes	No
26	(29)	**Removable and portable media control** as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.	Good	High	Medium	Medium	No	Yes	Possible	Yes
27	(28)	**Restrict access to Server Message Block (SMB) and NetBIOS** services running on workstations and on servers where possible.	Good	Low	Medium	Low	No	Yes	Yes	No
28	(20)	**User education** e.g. Internet threats and spear phishing socially engineered emails. Avoid: weak passphrases, passphrase reuse, exposing email addresses, unapproved USB devices.	Good	Medium	High	Medium	Possible	Possible	No	No
29	(26)	**Workstation inspection of Microsoft Office files** for potentially malicious abnormalities e.g. using the Microsoft Office File Validation or Protected View feature.	Good	Low	Low	Low	Possible	Yes	No	No
30	(25)	**Signature-based antivirus software** that primarily relies on up to date signatures to identify malware. Use gateway and desktop antivirus software from different vendors.	Good	Low	Low	Low	Possible	Possible	No	No
31	(30)	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.	Good	Low	Low	Low	No	No	No	No
32	(32)	**Block attempts to access websites by their IP address** instead of by their domain name, e.g. implemented using a web proxy server, to force cyber adversaries to obtain a domain name.	Average	Low	Low	Low	Yes	Yes	No	Yes
33	(33)	**Network-based Intrusion Detection/Prevention System** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Average	Low	High	High	Possible	Possible	Possible	Possible
34	(34)	**Gateway blacklisting** to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.	Average	Low	Low	High	Possible	Yes	No	Yes
35	(35)	**Capture network traffic** to/from internal critical asset workstations and servers as well as traffic traversing the network perimeter, to perform post-intrusion analysis.	Average	Low	High	Low	No	No	No	No

http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf

DIGITAL EVIDENCE COLLECTION → ADMINISTRATIVE → WORK PLAN → CASE SETUP → IMAGE INTEGRITY → ANALYSIS PREP → ANALYSIS → INTERPRETATION- REVIEW → REPORTING

1. ADMINISTRATIVE STUFF

- Review Policies and Laws
- Chain of Custody form
- Digital Evidence Collection Form
- Consent form (if needed)
- ✓ Evidence Tracked and Stored

2. WORK PLAN (docs)

- Review Policies and Laws (if needed)
- Gain understanding of:
  - -Background
  - -If applicable, previous work
  - - Requirements/Goal of analysis
  - - Deliverable
- Create Analysis Work Plan
- Create Investigative Plan

3. SETUP CASE FOLDER (example)

- EV1 (Evidence Files)
- WC (Working Copy of Files)
  - Case # - Project Name
    - Custodian Name
      - Media Type – EV #
        - Case File
        - Index
        - Reg Files
        - Internet Hist
        - Case Processor Logs
        - (Analysis Folders)
      - Media Type – EV #
      - Media Type – EV #

*Organize output neatly!

4. CONFIRM IMAGE INTEGRITY

- ✓ Compare Acquisition and Verification Hash values (MD5, SHA)
- Save Verification Reports

GENERAL FORENSIC ANALYSIS CHECKLIST V.1.1

THE PURPOSE OF THIS REFERENCE GUIDE IS TO PROVIDE AN OVERVIEW AND OUTLINE OF COMMON PROCESSES, SOFTWARE, AND BEST PRACTICES FOLLOWED BY PROFESSIONALS CONDUCTING COMPUTER FORENSIC ANALYSIS

BY DAVID NIDES (12/16/2011)
TWITTER: @DAVNADS
BLOG: DAVNADS.BLOGSPOT.COM
EMAIL: DNIDES@KPMG.COM
CREDITS TO: ED GOINGS, ROB LEE & SANS
QUESTIONS/FEEDBACK–CONTACT US!

SANS COMPUTER FORENSICS and INCIDENT RESPONSE

5. BEFORE YOU GET STARTED..

- ✓ Check physical size of drive and compare to physical label accounting for all drive space (Check for DCA/ HPA).
- ✓ Identify & compare logical partition size(s) to physical drive size to identify any deleted partitions or unused disk space
- ✓ Retrieve time zone settings for each disk and apply correct time zone, if applicable
- ✓ Rename hard disk volumes as necessary to "Recovery", "C", etc.

GATHER SYSTEM INFORMATION

- ✓ Determine OS, service pack, OS install date, application list, owner, machine name, and other basic information.
- ✓ Retrieve user profile information (names, SIDs, create and last logon dates)

PRE-PROCESSING ANALYTICS

- ✓ Conduct hash analysis, indentify "known" and/or "notable" files.
- ✓ Conduct file signature analysis, review renamed files.
- ✓ Identify encrypted files (entropy)
- ✓ Mount ALL compound files (VHD, VMDK, ZIP,RAR, Email containers, Reg Files, etc
- ✓ Index Case (DT Search, WDS, Encase, AD..)
- ✓ Generate metadata (and extended) listings/ reports

RP / VSC

- ✓ Identify if services turned on/used
- ✓ Extract or make available accordingly for analysis

MOUNTING / VIRTUAL EMULATE

- ✓ Mount - Malware/Virus Scan (Don't forget about MBR)
- ✓ Mount - Stego Scan
- ✓ Virtually Emulate – conduct behavior and live analysis

KEYWORD SEARCHING

- ✓ Create keyword list & QC syntax formatting/code page usage (may be iterative process)
- ✓ Perform targeted or full disk search including unallocated and slack areas.
- ✓ Create hit report/stats

FILTERING

- ✓ Filter data based on meta data and exteneded meta data such as Date and Time values, File Extension, and etc.

EXPORT

Export files from case for independent analysis with specialty tools. For example:

Memory
Memorize
Redline
Volatility (SIFT)
Passwords
AD PRTK
Passware
Ophcrack
Shellbags
Shellbags.py (SIFT)
Internet History
WebHistorian
LNK Files
Tzworks
Lslnk (SIFT)
Event Logs (.evt & .evtx)
Tzworks
GrokEVT
MFT
AnalyzeMFT
Ntfswalk (SIFT)
index/$I30
INDXParse.py (SIFT)
SIFT Workstation is a great resource for tons of tools!

Email
NUIX
Clearwell
Recover My Email
Bulk extractor (SIFT)
Image Mounting
FTK Imager
ImDisk
Live View
OSFMount
Virtual Box
Stego
Outguess
Hashing
Md5deep (SIFT)
Sha256deep (SIFT)
Hashdeep (SIFT)
Registry
Reg Ripper (SIFT)
Registry Decoder
AD Registry Viewer
Reglookup (SIFT)
YARU (SIFT)
Windows Journal Parser
Tzworks

6. EQUATION FOR SUCCESSFUL ANALYSIS: (TIMELINES + MANUAL ANALYSIS) x (PASSION + TIME + RESEARCH + RESOURCES) = "WINNING"

GENERAL AREAS

Analyze general folder locations for artifacts or data of interest. For example:
- >Desktop
- >User folders
- >Documents
- >Desktop
- >Network Shortcuts
- >Recently Opened File folders
- >System Temp folders
- >Browser Temp Folders
- >System Folders (malware)
- >Autorun

TIE IT ALL TOGETHER USING TIMELINE ANALYSIS – FLIP SIDE! 5

REGISTRY ANALYSIS (Win only)

The System registry hives (NTUSER.DAT, SYSTEM, SOFTWARE, SECURITY, SAM..) contain a vast of amount of information that can be imperative to your analysis. For Example:
- -OS Version (SOFTWARE)
- -Last logged on user (SAM)
- -Last Failed Logon (SAM)
- -Username & SID (SAM)
- -Shutdown (SYSTEM)
- -TimeZone (SYSTEM)
- -Drives Mounted by User (NTUSER.DAT)
- -File Ext Associations (NTUSER.DAT)
- -Installed application list (SOFTWARE)
- -Search History (SOFTWARE)
- -Removable Storage Devices (SYSTEM)

Using Registry analysis tools, such as Reg Ripper, can aid your analysis..

SYSTEM ARTIFACTS

There are many system related artifacts that may contain potentially relevant information including:
- -Backups (RP, VSC, others)
- -Event Logs (.evt, evtx)
- -Shell bags (Registry)
- -Jump Lists
- -Misc. Logs (firewall, AV, Apps, etc)
- -Removable Media Connections
- -LNK files
- -Prefetch
- -PageFile

SOFTWARE RESIDUE

Identify software (i.e Wiping tools, P2P, Sticky Notes, hacker tools, etc) and perform analysis on associated files (binary-malware analysis), logs, settings, registry and etc.

MEMORY RESIDUE

If applicable, perform memory analysis to gather volatile information including:
- -Handles; files, directories, processes, registry keys, Semaphores, events and sections
- -Open network ports
- -Hooks: Driver IRP, SSDT and IDT driver tree

E-MAIL/IM/SOCIAL ARTIFACTS

Identify email clients or web access on system and perform analysis on associated data stores or application residue/settings:

Client based (file examples):
Windows - .OST, .PST, .MSG, Temp folder for Outlook attachments, Lotus Notes - .NSF, Mac - .EML, .EMLX, .MBOX

Web based (OWA, Facebook, Twitter, etc.):
-Logs -Internet History reconstruction -Cache

INTERNET

Identify installed browsers and perform analysis on artifact such as:
- -Parse Internet history files (index.dat, sqlite, etc)
- -Check temp folders
- -Parse cookies
- -Cached pages
- -Form History/Auto complete files
- -Favorites/bookmarks
- -Toolbars
- -WebSlices
- -Browser plug ins
- -Registry analysis
- -Carve unallocated for deleted history artifacts

...BUCKETING ANALYSIS "TO DO" ITEMS LIKE THIS CAN HELP.

7. INTERPRETATION/REVIEW OF ARTIFACTS (examples) ..

File Download	Open/Save MRU	Open/Run MRU	Email	Skype History	Index.dat / places.sqlite	downloads.sqlite	P2P Logs
File Opening/ Creation	MACB	MRU by ext	MS Office MRU	LNK Files	Index.dat file://	JumpLists	Shellbags	Prefetch
File Knowledge	XP Search ACMRU	Win7 Search WordWheelQuery	Thumbs.db	Win7 Thumbnails	Recycle Bin	Browser Artifacts	Last visited MRU
USB Usage	Identification	First & Last Insert Times	User Identification	Volume Name	Drive Letter	LNK Files	Event Logs	Mount Point
Program Execution	User Assist	LastVisited MRU	Run MRU (Start->Run)	Prefetch	MUI Cache	Jump Lists	Event Logs
Physical Location	Time Zone	Wireless SSID	Vista/W7 Network History	Cookies	Search Terms	IP	Image exif
Account Usage	Last Password Change	Group Membership	Success/Fail Logons	Logon Types	RDP Usage	Account Logon/ Authentication	SID Attributes
Browser Usage	History	Search Box Terms	Cache	Session Restore	Flash & Super Cookies	Suggested Sites	Memory Fragments of Private Browsing	AJAX Transactions	Typed URLS

Have more? Let me know!

8

8.REPORTNG

- ✓ Document findings comprehensively
- ✓ Fact based Interpretation
- ✓ Remember who the audience is
- ✓ Remember requirements/expectations

DFIR essencial para Cyber Warriors

- Saber o está acontecendo, como atenuar os problemas e, mais importante, quem poderia estar fazendo alguma coisa
- Alcançar atribuição, o que é essencial para a coerção
- Auxiliar na possível cessação das hostilidades
- Possuir uma clara visão do escopo e da escala, auxiliando na definição da resposta
- Eliminar alguns aspectos de FUD do quadro tático e dar contexto para os tomadores de decisão operacional e estratégico

Para concluir

Você somente será um
Cyber Warrior
quando dominar muito bem
Forense Digital e
Resposta a Incidentes (*DFIR*)

http://dfir.com.br
marcelobc@mpf.mp.br