Cyber Protection Brigade

600 CPT

Discovery and Counter-Infiltration Team

Version: 1.0

Date: 8-12-2015

TABLE OF CONTENTS

1 PRE-DEPLOYMENT

1.1 REQUEST CUSTOMER INFORMATION & DEFINE SCOPE OF THE MISSION

- Send customer questionnaire (**Below**)OR get customer information from MPS/CS

1.1.1 Network Specific Information needed from customer

- Provide overall IP space of network
- Provide the static IPs, Gateway and netmask for 15 IPs to connect to network
- Disable port security for the switch to be used by the CPT
- Need permission(s) for the following software that will be used
    - Blue Scope (**NEEDS** Domain Administrator credentials to perform scans properly)
    - GRR (will need Administrator privileges to install grr agent on windows/linux hosts)
    - Windows Hosts (Needs Administrator privileges)
    - Linux Hosts (Needs user account with root privileges)
- Provide a list of **Key Cyber Terrain** for the mission network
  Key Cyber Terrain is the physical and logical elements of the domain that enable mission essential warfighting functions. A map of the key cyber terrain is a representation of knowledge and/or assumptions that determine or influence cyber decisions.
    - Include system type and descriptions
    - For Industrial Control Systems (ICS) or Distributed Control Systems (DCS), include brands, software versions and any documentation
- Network ranges, hosts, IP, systems etc.
    - Reasoning for exclusion
- Provide latest compliance report
    - Scans to include patch compliance
    - Scans to include DISA STIG compliance
- Prepare Classified Cyber Intel report of recent past, current, and predicted threat activity on the network
- Verify requested Pre-Approved Actions (PAA) list
    - Include any exceptions for sensitive systems
        - Provide point of contact to brief on sensitive systems

- Provide an up-to-date network diagram boundary. Must include hosts, servers and network infrastructure devices.
- Provide normal traffic net-flow baseline – include caveats on host devices that require special access to specific devices/services.
- Provide list of authorized HW/SW in use on network by users and admins
    - Host/Server baseline configuration/settings documentation
    - Network infrastructure configuration settings

1.1.2 Team Support

- Provide Defense Authorization Act (DAA) Letter for all applicable networks for 10x team members
- Embed 1x Server Admin and 1x Network Admin with CPT
    - Each must have authority to approve network changes
    - Each must have technical ability to execute network changes with CPT
    - Each must act as a 24/7-available trusted-agent for duration of mission
- Provide Administrator accounts (non-CAC enabled) for all systems on the network for each of the 10 team members (More accounts could be needed depending on network architecture)
- Provide Standard accounts (non-CAC enabled) for all systems on the network for each of the 10 team members
    - These accounts will need access to the internet
- Provide a secure work area and network connectivity for 10x team members
    - Unused, air-conditioned, locked room to work in and store our equipment
    - Phone
    - Whiteboard w/ markers & erasers
- Provide DSN telephone w/ CONUS-wide DSN & COMM access in CPT work area
- Provide Conference telephone available for use by CPT

1.1.3 Logistics Support

- Provide MPA-Days, Orders, Travel & Per-Diem funding
- Coordinate for base and/or special area access for CPT
- Provide adequate lodging & sustenance for CPT

- Provide crew vehicle(s) adequate for size of CPT

1.1.4 Outline the scope of the mission (Will vary per mission)

1.1.5 Negotiate with customer a list of pre-approved DCI actions on the network

NEED A LIST OF PRE-APPROVED ACTIONS

1.2 Ready Laptops with DCI Image

- The DCI Flyaway laptop image will include Security Onion (SO) as the host with the following installed tools and or VMware images:
  - SANS Investigative Forensic Toolkit (SIFT)
    - REMnux apps installed on SIFT (wget --quiet -O - https://remnux.org/get-remnux.sh | sudo bash)
  - Nmap
  -

1.3 Identify tools to be used

- Make assessment on mission needs
  - Identify necessary tools based on those needs
    - Nessus
    - Nikto/Wikto
    - DumpACL,
    - SuperScan
    - L0pht
    - Cain & Abel
    - Fping
    - L0phtCrack
    - WebInspect
    - IkeScan
    - Metasploit
    - Netcat
    - Dsniff
    - THC Amap/Hydra
    - Firewalk/Hping
    - Nemesis Project

1.4 PREP TOOLS

- Update rules on IDS
- Verify all scripts (Linux & Windows) have been updated
- Confirm all tools are on image and on a backup disk

2 DEPLOYMENT

2.1 ENUMERATE NETWORK DEVICES

- Device Discovery & Live Host List Creation unless already done by MPS

2.1.1 Passive Host Discovery

- Network Maps
- Asset List
- Device Configurations / Logs
  - DHCP logs
  - arp caches
  - netstats
  - DNS logs
  - Proxy logs
  - Firewall logs
  - TACACs /RADIUS
  - Wireless surveys
  - Management logs (WhatsUp, Solarwinds, etc.)
- Network traffic captures

2.1.2 Active Host Discovery

- Ping Sweeps
  - TTLs (Linux ≤ 64, Windows ≤ 128, Solaris/Network Device ≤ 255)
- Windows ICMP Sweep - Command line (Class C)

  Example (Windows): You're on a windows host (159.25.25.26) and need to perform a scan of the network (class C) to identify live host(s).

FOR /L %i in (1,1,254) do @ping –n 1 –w 200 159.25.25.%i | find /I “TTL”

- Windows ICMP Sweep - PowerShell (Class C)

  1..255 | foreach-object { (new-object System.Net.Networkinformation.Ping).Send ("159.25.25.$_") } | where-object {$_.Status -eq "success"} | select Address >> c:\159.25.25.0_24.list

- Linux Ping Sweep - Bash (Class C)

  for i in {1..254}; do ping -c 1 -W 1 159.25.25.$i | grep “WHAT YOUR LOOKING FOR”; done

- Nmap Host Discovery (Class C) (SEE APPENDIX)

  nmap -sn -n 159.25.25.0/24 -iL c:\>159.25.25.0_24.list | find /I "Nmap scan report" | awk "{print $5}" > c:\159.25.25.0_24.list

  nmap for service detection

  nmap –sS –n

- Generate OS Discovery and OS Host List
  - Window OS List
  - *Nix OS List
  - Network Device List
  - Other List
- Initial System Information Collection
  - OS Version Info
  - Device Purpose (Workstation, Server, DC, etc…)
- Compare scans to network map
- Scan baseline image with survey scans
  - Windows Discovery script (SEE APPENDIX)
  - Linux Discovery script (SEE APPENDIX)

2.2 Analyze Network Traffic

- Place IDS sensor w/ full packet capture on the network as soon as possible **OR** Get pcap data from MPS
- Identify all network protocols/services running
- Identify any anomalous traffic
    - encrypted traffic over unencrypted ports / unencrypted traffic over normal encrypted ports
    - High port to High port traffic
    - Services running on nonstandard ports
- Compare traffic to network map
- Characterize hosts by determining daily bandwidth usage, protocol usage, frequent domains visited, processes running & daily connections

2.3 Identify Vulnerabilities

- Identify unnecessary services running
- Analyze router & firewall configurations
- Identify "key assets" & "footholds"
    i. **Key Assets**
        1. Customer defined systems that's that store critical / sensitive data.
    ii. **FootHolds**
        1. Systems that DCI has identified as vulnerable to being exploited and allowing access to those key assets.
- Use MPS data or past vulnerability data to compare against current vulnerabilities

2.4 Host Analysis

- Run survey scans on hosts identified as vulnerable
- Compare survey scans to baseline image scan
- Identify firewall states/rules
- Enumerate users/permissions/accounts
- Identify patch level
- Validate any Connections
- Analyze logs on host

- Document exact commands when touching a host
- If suspected malicious file is found, take steps to further analyze that file (submit hash to bad file database, sandbox, etc)

2.5 Report Findings

- Use template to report findings
- Document all values (hostnames, IP, hashes of files, etc.)
- Include the 5 W's and how the behavior was detected
- Give recommendations to customer

3 Post-Deployment

3.1 Decide what should be brought back for analysis

- Make a decision if further analysis is needed
- Remove all hard drives that contain data to be kept
- Obtain courier orders if needed for transport

3.2 Wipe all data not being brought back for analysis

- Remove all scan data & pcap data from laptops
- Clear all alert databases and traffic capture logs that will not be kept from IDS
- Wipe the Super High-Speed Incident Tracking System (SHITS)

4 Wiping Windows / Linux

4.1.1 Windows

When you delete something on windows and empty the trash can the file(s) are not totally deleted. Windows (2000, 2003, XP, Vista & 7) by default have a utility called cipher that will allow you to erase all unused space on the partition. When running cipher it'll create a directory (EFSTMPWP) on the volume then it will create one or more files in that directory and write data to those files.

Cipher will make three passes:

- one pass with zeros
- one pass with ones
- one pass with random numbers

Note: After completion cipher will not remove the EFSTMPWP folder created

Open the command prompt (Start > Run > CMD) and type cipher /w:driveletter:\

Example #1: You want to wipe the C drive.

- cipher /w:c:\

Example #2: You want to wipe a folder titled "SECRET" on the C drive.

- cipher /w:c:\SECRET

Note: Cipher will not remove the folder (SECRET) when the wiping is complete.

/w - Removes data from available unused disk space on the entire volume. If this option is chosen, all other options are ignored. The directory specified can be anywhere in a local volume. If it is a mount point or points to a directory in another volume, the data on that volume will be removed.

You can use a for loop to run cipher wiping a drive volume multiple times.

Example #1: You want to overwrite unallocated space on your C: drive 9 times.

- FOR /L %i in (1,1,3) do @cipher /w:c:\

4.1.2 Linux

Credit: The Linux portion was taken from:

(http://blog.commandlinekungfu.com/2009/05/episode-32-wiping-securely.html)

Wiping in Linux is a little different than Windows. There is a utility called "shred" that can be used to overwrite files and delete them. By default shred will make 25 overwriting passes, you can increase and decrease the number (-n) of overwriting passes.

Example #1: You want to wipe and remove file (SECRET) that have sensitive information on it.

· shred -n 3 -z -u SECRET

-n: specifies the number of times to overwrite the file.

-z: specifies to do a final overwrite with zeros.

-u: specifies to remove the file once the wiping is complete.

Now if you want to wipe all the unallocated space in Linux similar to what was done with cipher for Windows, I was told by a Linux guru (Hal Pomeranz) that "dd" was the best and simplest way to do this.

Example #2: You want to wipe all of the unallocated space on your Linux partition.

· # dd if=/dev/urandom of=junk bs=4096; rm junk

This will consume all remaining disk space in the partition with a file called junk. The "dd" command will stop when the partition fills and then remove it immediately. Be sure to run this command as root, because the last 5% of the space in the file system is normally reserved for root-owned processes and not accessible to normal users.

5 INCIDENT RESPONSE

5.1 PRIMARY PHASES

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons learned

5.1.1 Preparation

5.1.1.1 Necessary resources should be prepared before deployment

- Jump bags
  - Blank media to hold file system images
  - Binary image creation software
    - To move data across the network
    - Netcat, ncat, winscp
  - Forensic software
  - Investigative tools
    - SIFT
    - Wireshark
    - Volatility
    - Ssdeep and md5deep
  - Additional software
    - All forensic tools that may be needed should be saved on a USB flash drive or CD-ROM with a Windows or Linux-based environment (use statically linked binary files)
      - Message digest should be computed and saved to verify integrity (MD5sum –p // MD5sum –u)
      - Licensing and version of each tool noted
  - Hardware
    - External hard drive
    - Ethernet tap
    - Patch cables
      - 2 straight-through and 1 cross-over

- USB cable

- Serial cable with multiple adaptors
- Forensic workstations
  - Laptop with multiple operating systems
- Bootable Linux environment *avoid bootable windows*
- Backup devices
- Evidence handling supplies
- Chain of custody forms
- Evidence storage bags and tags
- Digital cameras
- Notebooks

5.1.1.2 Members of incident response team

- Incident response officer
  - Has definitive accountability for the actions of the IR team and IR purpose
- Incident response manager
  - Leads the efforts of the IR team and coordinates activities between all of its respective groups
  - Reports to the IR officer
  - Normally receives the initial IR alerts, is responsible for activating the IR team and managing all parts of the IR process
    - From discovery, assessment, remediation and resolution
- Incident response assessment team
  - Composed of different areas serviced by the IR team
    - IT: Responsible for the care of the company's data. In the event of an incident, needs to know where the data can be accessed and the off limit areas
    - IT Auditor: Used to observe, learn the cause of the incident, make sure all procedures are being followed, and work with IT/security to avoid future issues.
    - Security: When the incident involves direct contact with the system, (s)he is responsible for assessment of physical damage, investigating physical evidence, and

guarding evidence during a forensics investigation to maintain a chain of evidence.
- Attorney: Ensures the usability of any evidence collected during an investigation in the event that the company chooses to take legal action.
- Human resource: Provides advice on the best way to handle situations involving employees. *Usually not called until after investigation has begun, and only if an employee is discovered to be involved*
- Public Relations: If unable to keep the incident out of the media, this individual can give the best advice on the message that should stem from the company, and the best way to broadcast that message
- Financial Auditor: Responsible for placing a monetary figure on the damage caused by an incident.

        - Discuss the details of the incident and assign an initial severity of the incident
    - Remote incident response coordinator
        - Qualified and capable individuals that are located in other geographic areas
        - Manage the efforts of local custodians during an incident
        - Report to the IR manager
    - Incident response custodians
        - Technical experts and application support representatives
            - Information Security: Trained in area of handling electronic incidents; responsible for assessing the extent of the damage, containment, basic forensics, and recovery.
        - Assist in the remediation and resolution of a given incident
        - Report to the Incident Response Manager or to the Remote IR Coordinator(s) depending on their location(s).
    - Entire team should retain logs on the status of the incident and relevant information (Redmine)
    - Develop an Emergency Communications Plan
        - Create credit-card sized list of incident response team contact info

5.1.1.3 Considerations

- An "event" is any apparent happening in a system and/or network
  - System crash
  - Provide the bulk of the organization's case if the offender of an incident is caught and prosecuted.
- How and when the incident should be contained
  - Isolating the systems from external influences may be necessary to prevent further damage
    - Disconnecting network cables to prevent remote users
    - Disabling internal network adapter if wireless network connection is used
- Impact of containment strategies on ability to operate effectively
- Make a list of all users who have access to the computer
  - May be able to provide passwords or where data is located
- Law Enforcement should be notified for specific reasons:
  - Significant impact to third party
  - Threat to public health or safety
  - Legal requirement based on the industry
- Law Enforcement should not be notified for specific reasons:
  - Control
  - Publicity
  - Risk of continued hacking
  - Risk of equipment seizure and/or interruption to business
  - You will become an agent acting on behalf of law enforcement if they ask you to do something

5.1.1.4 Chain of custody should be determined before collecting data

- To avoid allegations of evidence tampering or mishandling
- One person should be assigned as Evidence custodian
  - Keep log of every person who had physical custody of evidence
  - Document actions performed on the evidence, where performed, who performed them, and the time
    - Keep detailed log of every step taken to collect data
      - Include information on each tool used
    - Evidence should be photographed and labeled

        - Visual reminders of computer setup and attached devices
    - Actions on monitor should be photographed before touching the system
        - Document if screen-saver is active
- Store the evidence in secure location when not being used
- Make copy of evidence and perform examination and analysis using only copied evidence

5.1.1.5 Data collection

- Identify possible sources of data
    - Desktop computers
    - Servers
    - Thumb drives
    - Memory cards
    - Portable digital devices
        - Cellphones
        - digital cameras
    - alternate data sources when organizations' policies will not allow collection from primary data source
- Organizations may be proactive and collect data that may be useful
    - Audit records
    - Centralized logging (prevents unauthorized users from tampering with logs)
    - Regular backups of systems
    - Logs generated by ids, antivirus software, etc.
- Develop plan to acquire data (prioritization)
    - Likely value of data
        - Based on analyst's understanding of the situation and previous experience in similar situations, if any.
    - Volatility
        - Chances that data will be lost due to powered down, passage of time, or other actions performed on the system
            - Volatile data
                - Ram

        - CPU cache
    - Non-volatile
        - Flash memory
        - Rom
        - Prom
        - Eprom
  - Effort required
    - Time spent by analysts and others within organization
    - Cost of equipment and services
- Acquire the data
  - Forensic tools to collect volatile data
  - Duplicate non-volatile data sources to collect their data
  - Secure original non-volatile data sources
- Verify integrity of data
  - Use tools to compute the message digest of the original and copied data, then compare them (md5sum and ssdeep)

- Examination
  - Assessing and extracting significant pieces of information from collected data
    - Text and pattern searches
    - Using tools that can determine type of contents of each data file (TrID or Tridnet)
    - Databases containing information about known files (google)
  - May involve bypassing or modifying OS or application features that obscure data and code
    - Data compression
    - Encryption
    - Access control mechanisms
- Analysis
  - Inclusion of identifying people, places, items, and events
    - Determine how these elements are related
    - May involve correlating data between different sources
      - Comparing system characteristics to known baselines
    - Perform research

- Reporting
    - Alternative explanations when a definitive explanation could not be determined
    - Know the audience that information will be presented to
    - Identify actionable information that may allow an analyst to collect new sources of information
        - List of contacts
        - Information that could prevent future attacks
            - Backdoors
            - Vulnerabilities
    - Report problems that may need to be fixed
        - Policy or procedural

5.1.2 Identification

5.1.2.1 Assign incident handlers

- Assign individual as primary incident handler
    - Assign that individual a specific set of events on specific set of systems to analyze
- Assign a helper to assist with each incident

5.1.2.2 Collection of volatile data

- Login sessions (psloggedon // w)
- Contents of memory
    - Windows: ramcapture.exe
    - Linux: LIME
- Running processes
    - Windows: tasklist
    - Linux: ps -ef
- Open files
    - Windows: openfiles.exe
    - Linux: lsof
- Network configuration
    - Windows: ipconfig
    - Linux: ifconfig
- Operating system time
    - Windows: date &time
    - Linux: date

- View services and their settings
  - Windows: Net start & sc query | more
- Check file space usage
  - C:\> dir c: \
    - Find files larger than 10 MB
      - C:\> FOR /R C:\ %i in (*) do @if %~zi gtr 10000000 echo %i %~zi
- File shares
  - Net view \\127.0.0.1
- Network Usage
  - Net session (with machine)
  - Net use (with other systems)
  - Nbtstat –S
  - Netstat –ano 5 (owning pid & updated output)
    - -b (requires elevation & shows exe and associated DLL's)
- Check the registry
  - Regedit – gui
  - Reg query HKLM or HKCU\software\microsoft\windows\currentversion\run
    - Runonce &runonceEx

5.1.2.3 Collection of non-volatile data

- Perform graceful OS shutdown
  - Causes OS to perform cleanup
  - Can trigger removal of malicious material
- Or remove power from system
  - Can preserve files and other information that might be altered or deleted during graceful shutdown.
  - Can cause OS to corrupt data (ex. open files)
- Inventory and label all components of computer if needed for evidence
  - Include model #, serial #, and description of item
  - Document and photograph how each item is connected to computer
  - Use antistatic bracelets to guard against electrostatic discharges that can damage item

- Accounts
  - Windows: net user
  - Windows: net localgroup [groupname]
  - cat /etc/passwd & cat /etc/groups; groups & users)
- Passwords
  - FGdump.exe
  - cat /etc/shadow & cat /etc/passwd)
- Network shares
  - net share
  - smbstatus --shares)
- Network firewalls
  - Netsh firewall show config (XP/2003)
  - Netsh advfirewall show currentprofile (Vista-Win2008)
- Scheduled tasks
  - Schtasks
    - Look for unusual scheduled tasks, esp running as user in admin group, SYSTEM, or blank user name
  - User's Auto start folder
    - dir /s /b "c:\Documents and Settings\[user name]\Start Menu\"
    - dir /s /b "c:\Users\[user name]\Start Menu\"
    - wmic startup list full
- Log entries
  - Eventquery.vbs /L security
  - Wevtutil qe security /f:text (Windows Vista, 7, & 8)
  - Secpol.msc → local policies → audit policy → double click "audit logon events" → select "failure"
- Performance monitor
  - Task manager → performance tab
- Application logs
  - Web applications, Application servers, and Cloud-based services
  - Useful data
    - Dates
    - Timestamps
    - Users
    - Actions/transactions

5.1.2.4 Data from network traffic

- IDSs
- Security event management software
    - Imports security event info from various network traffic-related security event data sources and correlating events among the sources
- Network Forensic Analysis tools software
- Firewalls, proxy servers, remote access servers and routers logs
    - Data analysis over time could indicate trends, but usually provides little understanding into the nature of events.
- Packet sniffers and protocol analyzers
    - Can collect the most information on network traffic, but a lot of the information can be benign
    - Can provide more data on events that other devices or software have identified as possibly malicious
    - Packet sniffers are best reviewed with protocol analyzer
- Network monitoring
    - Helpful in identifying significant deviations from normal traffic flows
- Identify a host of interest by mapping an IP address to a Mac address of a particular nic
    - ISP records information is of value in tracing an attack back to its source; ex. For spoofed ip addresses.

5.1.2.5 Initial identification assessment

- Check for simple mistakes by users or admins
- Assess the evidence in detail
- What are the other likelihoods
- Maintain situational awareness
- Be able to explain:
    - What data was accessed, if any?
    - Who is responsible for the incident?
    - What do the logs reveal?

5.1.2.5.1 Assessment questions

- How widely deployed is the affected platform or application?
    - More widely deployed, higher the risk
- What is the effect of vulnerability exploitation, if there is a vulnerability?

        - Denial of service
        - Reconnaissance
        - Privileged user compromise
    - The value of the impacted systems, and the value of data on those systems?
    - Can the vulnerability be exploited remotely?
    - Is a public exploit available, or has one recently been released?
        - Check cve.mitre.org, Bugtraq, Isc.sans.edu

5.1.3 Containment

5.1.3.1 Prevent the attacker from spreading or getting deeper

- Characterize incident
    - General category
        - Denial of Service
        - Compromised information
        - Compromised Asset
        - Unlawful Activity
        - Internal Hacking
        - External Hacking
        - Malware
        - Email
        - Policy Violations
    - Criticality ratings
        - 1. Incident impacts critical systems: 60 min
        - 2. Incident impacts non-critical systems: 4 hrs
        - 3. Possible incident, non-critical: 24 hrs
    - Sensitivity metric – determines who should be informed
        - 1. Extremely sensitive (ex. CSIRT, management)
        - 2. Sensitive (ex. CSIRT, management, system owner, operations)
        - 3. Less sensitive (ex. Employees informed of isolated virus)

5.1.3.2 Initial analysis

- Avoid looking for the intruder with noticeable methods from the compromised machine

        - Traceroute, ping, nslookup
    - Local handlers continue making reports to command center as evidence is gathered and analyzed.

5.1.3.3 Short Term Containment

- Possible actions:
    - Disconnect network cable
    - Pull power cable – loses volatile memory, may damage drive
    - Isolate switch port so system cannot receive or send data, using network management tools
    - Apply filters to routers and firewalls
    - Change the name in DNS to point to a different IP address
- Make sure someone responsible for the system is advised, in writing, and acknowledges if short-term containment will disable the system.
- Determine the risk of continuing operations
    - Review logs of neighboring systems

5.1.3.4 Long Term Containment

- Get back-up for forensic analysis
- System can be kept off line
    - Move to eradication phase
- System must be kept on line
    - Perform long-term containment
        - Allows you to build a clean system while staying in production

5.1.3.4.1 Long-term actions

- Patch the system/ neighboring systems
- Insert IPS or in-line Snort(IDS)
- Null routing (routing table entry)
- Change passwords
- Alter trust relationships
- Apply firewall and router filter rules
- Remove the accounts used by the attacker
- Shutdown any backdoor processes used by the attacker

5.1.3.5 Keep system owners and administrators briefed on the progress

- DO NOT PLAY THE BLAME GAME
- If necessary, wait until Lessons Learned Phase to assign fault

5.1.4 Eradication

- Mission: Get rid of the attacker's items on the machine
  - Accounts
  - Pirated software
  - Malicious code
- Mission: Determine cause and symptoms of incident
  - Use information gathered during identification and containment
  - Attempt to quarantine the attack and determine how it was executed
- Mission: Reformatting and reinstalling the operating system from scratch
  - Valuable shortcut in the handling process
  - Opportunity for re-infection thru the same channel after the operating system is reloaded is still there.

5.1.4.1 Improving defenses

- Mission: Apply suitable protection practices
  - Applying firewall and/or routing filters
  - Move the system to a new name/IP address
  - Null routing particular IP addresses
  - Changing DNS names
  - Applying patches and hardening the system
- Vulnerability analysis
  - Perform system and network vulnerability analysis
    - OpenVAS or NESSUS
    - Run security scanner on neighboring systems in a compromise (NMAP)
  - Search for related vulnerabilities
  - Scan entire network for interesting ports (NMAP)

5.1.5 Recovery

- Mission: Get the impacted systems back into production in a safe way

        - Validate the system
            - Always ask for test plans and baseline documentation
            - Make sure the operation was successful and the system is back to normal condition
                - Have the machine owner sign that it is in full operation
            - Have the business unit test the machine before going back into production
        - Restore operations
            - Decide when to restore operations
                - Try for an off-hours timeslot
                    - Easier to monitor carefully
                    - Will often be over-ruled because business will want service restored immediately
                - Final decision should be put on the system owner
                    - Document your advice in a signed memo
    - Mission: Monitor
        - Continuous monitoring for backdoors that may not have been detected
            - Use network and host-based IDS's and IPS's
                - Create custom signature to alert on original attack course if plausible
            - Check operating system and application logs meticulously
        - Look for artifacts to return
            - Check often for re-compromise
                - Remember to look into normal ways of logging in, not just malware
                - A script that checks to see if artifacts left by the attacker return is recommended
                    - Ran daily, or even more often, for several months
                    - Look for changes to registry keys
                        - reg query

- Look for unusual processes
  - Tasklist (can be run remotely with psexec) or ps
- Look for accounts used by the attacker
  - Net user or cat /etc/passwd
- Look for simultaneous logins
- Look for previous artifacts mentioned
  - Scheduled tasks
  - Open files

5.1.6 Lessons Learned

- Mission: Document what occurred and improve our proficiencies
  - Develop a follow-up report
    - Begin immediately after recovery
    - Assign the task to the on-site team
    - Include incident forms
      - www.sans.org/score/incident-forms
    - Encourage affected parties to review the draft
    - Attempt to reach an agreement and get sign off
    - If someone does not agree, have them sign off on their own version of events
  - Conduct a Lessons Learned Meeting
    - Within two weeks of recommencing production
    - Review the report
    - Finalize the Executive Summary
      - Most important thing is how much the organization saved because of the team and incident handling procedure
    - Keep it short and professional
  - Apply the fixes
    - Get appropriate approval and funding to fix
      - Processes
      - Technology
      - Incident handling capabilities

6 HEADING

6.1 HEADING

6.1.1 Heading

7 HEADING

7.1 HEADING

7.1.1 Heading

8 HEADING

8.1 HEADING

8.1.1 Heading

9 APPENDIX A – TCPDUMP COMMANDS

Commands	Comments
tcpdump -D	List of interfaces on which tcpdump can listen.
tcpdump -i eth0	Listen on interface eth0.
tcpdump -v	Be verbose while capturing packets.
tcpdump -vv	Be more verbose while capturing packets.
tcpdump -vvv	Be very verbose while capturing packets.
tcpdump -c 100	Limit the capture to 100 packets.
tcpdump -w capture.cap	Record the packet capture to a file called capture.cap.
tcpdump -r capture.cap	Display the packets of a file called capture.cap.
tcpdump dst host 10.0.0.1	Capture any packets where the destination host is 10.0.0.1.
tcpdump src host 10.0.0.1	Capture any packets where the source host is 10.0.0.1.
tcpdump host 10.0.0.1	Capture any packets where the source or destination host is 10.0.0.1.
tcpdump dst net 10.0.0.0/24	Capture any packets where the destination network is 10.0.0.0/24.

tcpdump src net 10.0.0.0/24	Capture any packets where the destination network is 10.0.0.0/24.
tcpdump -n net 10.0.0.0/24	Capture any packets where the source or destination network is 10.0.0.0/24.
tcpdump dst port 3389	Capture any packets where the destination port is 3389.
tcpdump dst portrange 1-1023	Capture any packets where the destination port is between 1 and 1023 inclusive.
tcpdump "dst host 10.1.1.1 and dst port 23"	Capture any packets with destination IP 10.1.1.1 and destination port 23.
tcpdump "dst host 10.1.1.1 and (dst port 80 or dst port 443)"	Capture any packets with destination IP 10.1.1.1 and destination port 80 or 443.
tcpdump not port 22	“not port 22″ is a filter specification that tells tcpdump to filter out packets with IP source or destination port 22. As you know port 22 is SSH port. Basically, when you tell tcpdump something like this, it will make tcpdump ignore all SSH packets.

10 APPENDIX B – WINDOWS NET COMMANDS

Commands	Comments
C:\>net use	List SMB sessions.
C:\>net user	List local users.
C:\>net share	List currently configured shares.
C:\>net share [share name]=c:\ [shared folder's path] /Remark:"My Secret Stuff"	Create a share with a remark. Note: If there are spaces in the share name and or remark, wrap them with quotation marks.
C:\>net share [share name] /del	Remove a share. Note: If there are spaces in the share name, wrap it with quotation marks.
C:\>net share [share name] \\targetIP /del	Remove a share from a remote server.
C:\>net share [share name]	List detailed information about share.
C:\>net session	List outbound SMB connections.
C:\>net localgroup	List local groups.
C:\>net localgroup Administrators	List members of local Administrator Group.

C:\>net user [user name] [password] /add	Add a user.
C:\>net user [user name] [password] /add active:no	Add a user but deactivate the account.
C:\>net localgroup Administrators [user name] /add	Add user to local Administrators group.
C:\>net localgroup Administrators [user name] /del	Remove user from local Administrators group.
C:\>net user [user name] [password] /del	Remove a user.
C:\>net accounts	List local account settings on a machine.
C:\>net accounts /domain	List account settings on a machine that is in a domain.
C:\>net start [service_name]	Starts a service.
C:\>net stop [service_name]	Stops a service.

11 APPENDIX C – ADDITIONAL COMMANDS

Commands	Comments
C:\>type [file] | find /c /v ""	Count the number of lines in a file.
C:\>type [file]	Lists the contents of a file on standard output.
C:\>type *.txt C:\>type [file1] [file2] [file3]	Lists the contents of multiple files.
C:\>type [file] | find “[string]”	Searching for a string within a file.
C:\>type [file] | findstr [regex] /R	Searching for regular expressions.
C:\>set	Lists all environment variables within a shell.
C:\>set username	Lists the current user logon name similar to the Linux/Unix command *whoami*.
C:\>set u	Lists the userdomain, username, and user profile path.
C:\>set systemroot	Display where the operating system is installed.
C:\>cd %systemroot%	Will change to the system root directory.
C:\>cd	Lists the current working directory (like Linux/Unix *pwd* command).
C:\>netsh /?	Lists an overview of the firewall capabilities.
C:\>netsh firewall show config	Lists the complete settings of the firewall.

C:\>netsh firewall set opmode disable	To disable the firewall entirely. *If group policy is enforced this command will not work.*
C:\>netsh firewall set opmode enable	To enable the firewall. *If group policy is enforced this command will not work.*
C:\>sc query	Lists running services on the local machine.
C:\>sc \\[targetIP] query	Lists running services of a remote machine.
C:\>sc query state= all	Lists all services on the local machine, regardless of whether they are currently started or not.
C:\>sc qc [service_name]	Lists details about a particular service's status.
C:\>sc start [service_name]	Starts a service.
C:\>sc stop [service_name]	Stops a service.
C:\>sc config [service_name] start= demand	If the service_type is disabled, you first have to enable it before starting it.
C:\>reg query [key name]	Reads a key from the registry.
C:\>reg add [keyname] /v [valuename] /t [type] /d [Data]	Add a key to the registry.
C:\>reg export [KeyName] [filename.reg]	To export registry key settings to a reg file.
C:\>reg import [filename.reg]	To import registry key settings from a reg file.

12 APPENDIX D – GOOGLE ADVANCE OPERATORS

Operators	Meaning	Example
site:	Searches only the site selected.	admission site:www.stanford.edu
" "	Finds only what is written between the double quotes.	“stanford”
link	Find pages that link to the Stanford University website.	link:www.stanford.edu
related	Lists web pages that are similar to the web page you specify.	related:www.stanford.edu
inurl	Lists the search result not just in the URL, but also in other place like for this example in the content.	inurl:star wars
intitle	Lists the pages that has the search word “flu shot” in the title, and the word "help" anywhere in the page.	flu shot intitle:help OR intitle:flu shot help
info	Lists information about the corresponding web page.	info:gothotel.com
filetype:	Finds matches for the file type selected.	Han Solo filetype:ppt Han Solo filetype:doc
define:	Finds definitions of the words from the internet.	define:cocondrum
-	Excludes words from a search.	“Han Solo” -stormtrooper

~	Searches not only for a particular keyword, but also for its synonyms. Indicate a search for both by placing the tilde sign ("~") immediately in front of the keyword.	~food~facts
+	Google will not correct words, find plurals or synonyms.	+Hen Solo (not a search for Han Solo)
*	Fills in the missing information.	George Lucas was born on *
[#]…[#]	Search within a range of numbers. Search for DVD players between $100 and $150	DVD player $100..150

13 APPENDIX E – WINDOWS BASELINE SCRIPT

```
@ECHO OFF
cmd.exe /c echo.
cmd.exe /c echo ########################################
cmd.exe /c echo # YOUR WINDOWS SURVEY IS ABOUT TO BEGIN #
cmd.exe /c echo ########################################
cmd.exe /c echo.

cmd.exe /c echo.
cmd.exe /c echo #####################################
cmd.exe /c echo # PROCESS LISt WITH MEMORY USAGE STATS #
cmd.exe /c echo #####################################
cmd.exe /c echo.

powershell -command "Get-Process | sort ws | select name,ws"

cmd.exe /c echo.
cmd.exe /c echo #################################
cmd.exe /c echo # PROCESS LIST WITH CPU TIME STATS #
cmd.exe /c echo #################################
cmd.exe /c echo.

powershell -command "get-process |sort cpu | select name,cpu"
```

```
cmd.exe /c echo.
cmd.exe /c echo #################
cmd.exe /c echo # CHECKING USER #
cmd.exe /c echo #################
cmd.exe /c echo.

powershell -command "get-wmiobject win32_loggedonuser | select antecedent -unique"

 cmd.exe /c echo.
cmd.exe /c echo ############
cmd.exe /c echo # OS CHECK #
cmd.exe /c echo ############
cmd.exe /c echo.

powershell -command "Get-WmiObject win32_operatingsystem | select-object caption, installdate, servicepackmajorversion,osarchitecture, bootdevice, buildnumber, csname | FL"
```

```
cmd.exe /c echo.
cmd.exe /c echo ###################
cmd.exe /c echo # 32 OR 64-BIT CHECK #
 cmd.exe /c echo ###################
cmd.exe /c echo.
powershell -command "get-wmiobject win32_operatingsystem | select-object
osarchitecture | FL"

cmd.exe /c echo.
cmd.exe /c echo ###############################
cmd.exe /c echo #  CURRENT WORKING DIRECTORY #
cmd.exe /c echo ###############################
cmd.exe /c echo.

powershell -command pwd

cmd.exe /c echo.
cmd.exe /c echo ###################
cmd.exe /c echo # TARGET DATE\TIME #
cmd.exe /c echo ###################
cmd.exe /c echo.

net time || date /t & time /t

cmd.exe /c echo.
cmd.exe /c echo ################################################
cmd.exe /c echo # NOW CHECKING NETWORK INTERFACE
INFORMATION #
cmd.exe /c echo ################################################
cmd.exe /c echo.

ipconfig /all

cmd.exe /c echo.
cmd.exe /c echo ########################################
cmd.exe /c echo # CHECKING COMPUTER'S PUBLIC IP ADDRESS #
cmd.exe /c echo ########################################
cmd.exe /c echo.
```

```
nslookup myip.opendns.com resolver1.opendns.com

cmd.exe /c echo.
cmd.exe /c echo ##########################################
cmd.exe /c echo # NOW CHECKING NETWORK CONNECTION INFO #
cmd.exe /c echo ##########################################
cmd.exe /c echo.

netstat -ano
```

```
cmd.exe /c echo.
cmd.exe /c echo ######################################
cmd.exe /c echo # NOW CHECKING NETWORK ROUTING INFO #
cmd.exe /c echo ######################################
cmd.exe /c echo.

route print

cmd.exe /c echo.
cmd.exe /c echo ########################
cmd.exe /c echo # NOW CHECKING ARP INFO #
cmd.exe /c echo ########################
cmd.exe /c echo.

arp -a

cmd.exe /c echo.
cmd.exe /c echo ##############################
cmd.exe /c echo # NOW DISPLAY NETWORK SHARES #
cmd.exe /c echo ##############################
cmd.exe /c echo.

net share

net use

cmd.exe /c echo.
cmd.exe /c echo ###################################
cmd.exe /c echo # NOW DISPLAY LOCAL USER ACCOUNTS #
cmd.exe /c echo ###################################
cmd.exe /c echo.

net users

cmd.exe /c echo.
cmd.exe /c echo ############################
cmd.exe /c echo # NOW DISPLAY LOCAL GROUPS #
cmd.exe /c echo ############################
```

cmd.exe /c echo.

net localgroup

```
cmd.exe /c echo.
cmd.exe /c echo ##############################################
cmd.exe /c echo # NOW DISPLAY USERS BELONGING TO ADMIN GROUP #
cmd.exe /c echo ##############################################
cmd.exe /c echo.

net localgroup administrators

cmd.exe /c echo.
cmd.exe /c echo ##########################################
cmd.exe /c echo # NOW DISPLAY COMPUTERS IN MY WORKGROUP #
cmd.exe /c echo ##########################################
cmd.exe /c echo.

net view

cmd.exe /c echo.
cmd.exe /c echo ############################
cmd.exe /c echo # NOW DISPLAY DOMAIN INFO #
cmd.exe /c echo ############################
cmd.exe /c echo.

systeminfo | findstr /B /C:"Domain"

cmd.exe /c echo.
cmd.exe /c echo ####################
cmd.exe /c echo # DRIVE INFORMATION #
cmd.exe /c echo ####################
cmd.exe /c echo.

powershell -command "get-psdrive -psprovider filesystem"

echo Free Disk Space on C:

fsutil volume diskfree C:

cmd.exe /c echo.
cmd.exe /c echo ##########################
```

```
cmd.exe /c echo # WHAT TYPE OF DRIVE IS C: ? #
cmd.exe /c echo ############################
cmd.exe /c echo.

fsutil fsinfo drivetype C:
```

```
cmd.exe /c echo.
cmd.exe /c echo ##############################################
cmd.exe /c echo # IF THERE ARE ANY MORE DRIVES RUN FSUTIL AGAIN
#
cmd.exe /c echo ##############################################
cmd.exe /c echo.

cmd.exe /c echo.
cmd.exe /c echo ######################
cmd.exe /c echo # SYSTEM INFORMATION #
cmd.exe /c echo ######################
cmd.exe /c echo.

echo Procsser(s)

cmd.exe /c echo.
cmd.exe /c echo ##########################
cmd.exe /c echo # CHECKING SOFTWARE KEY #
cmd.exe /c echo ##########################
cmd.exe /c echo.

reg query "HKLM\software\microsoft\windows\currentversion"

cmd.exe /c echo.
cmd.exe /c echo ################################
cmd.exe /c echo # VALUE IN LOCAL MACHINE RUN KEY #
cmd.exe /c echo ################################
cmd.exe /c echo.

reg query "HKLM\software\microsoft\windows\currentversion\run"

cmd.exe /c echo.
cmd.exe /c echo #####################################
cmd.exe /c echo # VALUE IN LOCAL MACHINE RUNONCE KEY #
cmd.exe /c echo #####################################
cmd.exe /c echo.

reg query "HKLM\software\microsoft\windows\currentversion\runonce"
```

```
cmd.exe /c echo.
cmd.exe /c echo ###################################
cmd.exe /c echo # VALUE IN CURRENT USER RUN KEY #
cmd.exe /c echo ###################################
cmd.exe /c echo.

reg query "HKCU\software\microsoft\windows\currentversion\run"
```

```
cmd.exe /c echo.
cmd.exe /c echo ####################################
cmd.exe /c echo # VALUE IN CURRENT USER RUNONCE KEY #
cmd.exe /c echo ####################################
cmd.exe /c echo.

reg query "HKCU\software\microsoft\windows\currentversion\runonce"

cmd.exe /c echo.
cmd.exe /c echo ###################################
cmd.exe /c echo # NETWORKS IN NETWORK LIST PROFILES #
cmd.exe /c echo ###################################
cmd.exe /c echo.

reg query "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\NetworkList\profiles"

cmd.exe /c echo.
cmd.exe /c echo ################################################
cmd.exe /c echo # LISTING THE DEFAULT GATEWAY MAC FOR NET
PROFILES #
cmd.exe /c echo ################################################
cmd.exe /c echo.

reg query "HKLM\SYSTEM\CurrentControlSet\Services\Tcpip"

cmd.exe /c echo
cmd.exe /c echo ############################################
cmd.exe /c echo # VIEW AVAILABLE WIRELESS NETWORKS IN THE
AREA #
cmd.exe /c echo ############################################
cmd.exe /c echo.

netsh wlan show network mode=bssid

cmd.exe /c echo.
cmd.exe /c echo ##############################
cmd.exe /c echo # CHECKING FOR COMPUTER NAME #
```

cmd.exe /c echo ################################
cmd.exe /c echo.

hostname

```
cmd.exe /c echo.
cmd.exe /c echo ############################
cmd.exe /c echo # CHECKING IE INFORMATION #
cmd.exe /c echo ############################
cmd.exe /c echo.

rem //COMMAND NEEDED

cmd.exe /c echo.
cmd.exe /c echo ##############################
cmd.exe /c echo # CHECKING USER'S IE START PAGE #
cmd.exe /c echo ##############################
cmd.exe /c echo.

rem //COMMAND NEEDED

cmd.exe /c echo.
cmd.exe /c echo ##############################
cmd.exe /c echo # CHECKING USER'S IE TYPED URL's #
cmd.exe /c echo ##############################
cmd.exe /c echo.

rem //COMMAND NEEDED

cmd.exe /c echo.
cmd.exe /c echo ##############################
cmd.exe /c echo # CHECKING FW CONFIGRUATIONS #
cmd.exe /c echo ##############################
cmd.exe /c echo.

echo Firewall ON or OFF?
netsh advfirewall show allprofiles state

echo Firewall Policy (Authorized Applications)
netsh advfirewall firewall show rule name=all verbose

cmd.exe /c echo.
cmd.exe /c echo ############################
```

```
cmd.exe /c echo # CHECKING SCHEDULED TASKS #
cmd.exe /c echo ############################
cmd.exe /c echo.

schtasks /query
```

```
cmd.exe /c echo.
cmd.exe /c echo ##############################
cmd.exe /c echo # CHECKING PREFETCH DIRECTORY #
cmd.exe /c echo ##############################
cmd.exe /c echo.

dir c:\windows\prefetch

cmd.exe /c echo.
cmd.exe /c echo ####################
cmd.exe /c echo # CHECKING "AT" JObs #
cmd.exe /c echo ####################
cmd.exe /c echo.

at

cmd.exe /c echo.
cmd.exe /c echo ######################
cmd.exe /c echo # Your script is complete #
cmd.exe /c echo ######################
cmd.exe /c echo.
```

14 APPENDIX F – LINUX BASELINE SCRIPT

```
#!/bin/bash

###########
# Got r00t? #
###########
if [[ $(/usr/bin/id -u) -ne 0 ]]; then
    echo "This script needs to be run as root. Please try again using sudo."
    exit
fi

echo "######################"
echo "# Linux Discovery Script #"
echo "######################"

#list date and time
date
echo -e "\n"

#list hostname
echo "hostname:  `hostname`"
echo -e "\n"

echo "####################"
echo "# network interfaces #"
echo "####################"
ifconfig -a
echo -e "\n"

echo "########################################"
echo "# connections & programs with associating pids #"
echo "########################################"
netstat -ntlp
echo -e "\n"

echo "################################"
echo "# show all TCP connectiosn with pids #"
```

```
echo "################################"
netstat -antp
echo -e "\n"

echo "################################"
echo "# show all UDP connectiosn with pids #"
echo "################################"
netstat -anup
echo -e "\n"
echo "#################"
echo "# linux distribution #"
echo "#################"
cat /etc/*elease
echo -e "\n"

echo "##################"
echo "# kernal information #"
echo "##################"
uname -a
echo -e "\n"

echo "########################"
echo "# who's currently logged in #"
echo "########################"
who | cut -d' ' -f1 | sort -u
echo -e "\n"

echo "####################################"
echo "# who's logged in and what they're doing #"
echo "####################################"
w
echo -e "\n"

echo "############################"
echo "# listing of last logged in users #"
echo "############################"
last
echo -e "\n"

echo "###################"
```

```
echo "# list of user accounts #"
echo "#####################"
awk -F':' '{ print $1}' /etc/passwd
echo -e "\n"

echo "#########################"
echo "# list users in the sudo group #"
echo "#########################"
cat /etc/group | grep sudo
echo -e "\n"

echo "######################"
echo "# display the sudoers file #"
echo "######################"
cat /etc/sudoers
echo -e "\n"

echo "#############"
echo "# bash history #"
echo "#############"
cat ~/.bash_history
echo -e "\n"
#unset HISTFILE HISTFILESIZE HISTSIZE

echo "####################"
echo "# Apache service status #"
echo "####################"
service apache2 status
echo -e "\n"

echo "##################"
echo "# SSH service status #"
echo "##################"
service ssh status
echo -e "\n"

echo "####################"
echo "# MYSQL service status #"
echo "####################"
service mysql status
```

```
echo -e "\n"

echo "########################"
echo "# list cronjobs for each user #"
echo "########################"
for user in `cat /etc/passwd | awk -F":" '{print $1}'`; do crontab -l -u $user; done
2>&1
echo -e "\n"

echo "##############################"
echo "# list files in each users home folder #"
echo "##############################"
for user in `cat /etc/passwd | awk -F":" '{print $1}'`; do ls -l /home/$user; done
2>&1
echo -e "\n"

echo "####################################"
echo "# looking for programs in the rc.local folder #"
echo "####################################"
cat /etc/rc.local
echo -e "\n"

echo "##############################"
echo "# list the mounted partitions #"
echo "##############################"
mount
echo -e "\n"
echo "########################"
echo "# md5sum the cronjob files #"
echo "########################"
for file in `find /etc/cron* -type f`; do md5sum $file; done
echo -e "\n"

echo "######################"
echo "# md5sum the etc folder #"
echo "######################"
for file in `find /etc/* -type f`; do md5sum $file; done
echo -e "\n"

echo "#########################"
```

```
echo "# list files with the sticky bit on #"
echo "############################"
find / -type f -perm /4000 2>/dev/null
echo -e "\n"

echo "############################"
echo "# display the hosts.allowed file #"
echo "############################"
cat /etc/hosts.allowed
echo -e "\n"

echo "###################################"
echo "# list uncomplicated firewall (ufw) rules #"
echo "###################################"
service ufw status
echo -e "\n"

echo "########################"
echo "# list IPtables firewall rules #"
echo "########################"
iptables -L
echo -e "\n"

#echo "######################"
#echo "# listing kernal modules #"
#echo "######################"
#lsmod
#echo -e "\n"

#echo "########################################"
#echo "# information about the hardware and memory #"
#echo "########################################"
#dmidecode
#echo -e "\n"
```

15 APPENDIX G – NMAP COMMANDS

By default nmap performs a SYN scan (-sS) unless you do not have privileged access, then TCP connect scan (-sT) is the default.

Most scans need privileged access (root or administrator)

Nmap -sT: TCP connect scan (3-way handshake completed) *Most likely to be logged

Nmap -sU: UDP scan (combine with tcp scan (sS or sT)) *use --host-timeout to skip slow hosts

Nmap -sS: SYN scan (half-open tcp scan)

Nmap –arp-type <type>: Used when targets block icmp. *Targets must be in the same subnet

By default, the most common 1000 ports are scanned.

-p: allows one to specify ports to scan *use hyphen to specify port range (i.e. 4-35)

Nmap -sA: ACK scan is used to determine firewall rulesets (whether firewalls are stateful or not, and which ports are filtered). *DOES NOT determine if ports are open or closed

-Sv: Used to identify the version of the services used on specified ports. *use --allports to prevent scan from excluding ports on the exclusion list by default, like port 9100 (printers).

-O: Used for OS detection, -A can be used as an alternative for both –Sv and -O. *--osscan-limit used to limit scans to hosts that have at least one open and one closed tcp port (for faster scanning).

Examples:

1. Scan a network, only ports 4-15, detect the OS. You have root access

    Sudo Nmap –sS –p 4-15 –O 10.10.10.0/24

2. Scan a network that blocks icmp traffic. You have root access

Sudo Nmap --arp-type request 10.10.10.0/24

3. Scan a network, identify the versions of the services, and identify udp ports. You have root access

Sudo Nmap –sS –Sv –sU --allports --host-timeout 10.10.10.0/24

4. Scan a network, determine OS. You do not have root access

Nmap –sT –O –host-limit 10.10.10.0/24

** If the target is a windows host, you can specify port 445, 135, and/or 139 (smb), usually not blocked by the firewall.

** If the target is a *nix host, you can specify port 22 or 631 (printer)

** Most ports that are commonly open that one should try to specify for connection are: 443, 80, 22, 110, 25, 445.

16 APPENDIX H – UNNECESSARY SERVICES

- Http (on port 80) showing encrypted traffic
- Servers starting off the three-way handshake (possible beaconing, with reverse connection)
- Unsolicited emails being sent out to various email addresses on the network, could contain malicious links/downloads (possible spamming)
- Multiple logon failures (possible brute force attack)
- Multiple packets hitting the same port on different hosts or different ports on one host (scanning)
- Numerous amounts of ping requests with no replies
- User-Agents with incorrect web-browser identification
- Downloading of executables using http traffic (look for that executable and put the md5 in www.virustotal.com if you can find it on the system)

17 APPENDIX I – RAMCAPTURE.EXE, LIME, AND VOLATILITY

- Using ramcapture.exe to acquire memory dump from windows
  - Winscp ramcapture.exe to investigated host
  - Run cmd as administrator and save file to desired directory, defaults to desktop
  - Winscp raw dump back to forensic workstation
  - Remove ramcapture.exe, ramcapture.sys and raw dump file
- Using volatility to analyze memory dump
  - Set a profile to tell volatility what OS the dump came from
    - Default profile is WinXPSP2x86
    - ./vol.py - - profile=<OS of memory dump>
    - If unaware of the OS, use ./vol.py imageinfo –f <destination of the memory dump>
  - Use command line options to analyze memory
    - ./vol.py --help
    - ./vol.py --profile=WinXPSP2x86 pstree –D <destination directory> -f memory image location>
    - Pslist (basic active processes)
    - *look in share \\FS01\CPB$\cpt600\dci* for other options
- Using lime to acquire memory dump from linux
  - Insmod ./lime.ko “path=<outfile | tcp:<port>> format=<raw|padded|lime> {dio=<0|1>]”
  -
    - Path:
      - Outfile: name of file to write to on local system
      - Port: network port to communicate over
    - Format:
      - Raw: concatenates all system RAM ranges
      - Padded: pads all non-system RAM ranges with 0s
      - Lime: each range prepended with fixed-size header containing address space info
    - Dio (optional):
      - 1: attempt to enable direct IO
      - 0: default, do not attempt direct IO
    - Localhostonly (optional):
      - 1: restricts tcp to only listen on localhost
      - 0: binds on all interfaces (default)
  - Example: # insmod /tmp/lime.ko “path=tcp:4121 format=lime”

- *on host machine*: establish connection and acquire memory using netcat:

  $ nc localhost 4121 > ram.lime