# Post Exploitation

## Contents

# Purpose

The purpose of the Post-Exploitation phase is to determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machines usefulness in further compromising the network. The methods described in this phase are meant to help the tester identify and document sensitive data, identify configuration settings, communication channels, and relationships with other network devices that can be used to gain further access to the network, and setup one or more methods of accessing the machine at a later time. In cases where these methods differ from the agreed upon Rules of Engagement, the Rules of Engagement must be followed.

# Rules of Engagement

The following Rules of Engagement are specific to the Post-Exploitation phase of a penetration test and are intended to ensure that the client’s systems are not subjected to unnecessary risk by the (direct or indirect) actions of the testers and to ensure a mutually agreed procedure to follow during the post-exploitation phase of the project.

### Protect the Client

The following rules are to be used as a guideline of rules to establish with a client to ensure that the day to day operations and data of the client are not exposed to risk:

- Unless previously agreed upon, there will be no modification of services which the client deems “critical” to their infrastructure. The purpose of modifying such services would be to demonstrate to the client how an attacker may:
  - Escalate privileges
  - Gain access to specific data

  - Cause denial of service
- All modifications, including configuration changes, executed against a system must be documented. After finishing the intended purpose of the modification, all settings should be returned to their original positions if possible. The list of changes should be given to the client after the engagement to allow them to ensure all changes were properly undone. Changes that could not be returned to their original positions should be clearly differentiated from changes that were successfully reversed.
- A detailed list of actions taken against compromised systems must be kept. The list should include the action taken and the time period in which it occurred. Upon completion, this list should be included as an appendix to the final report.
- Any and all private and/or personal user data (including passwords and system history) uncovered during the course of the penetration test may be used as leverage to gain further permissions or to execute other actions related to the test only if the following conditions are met:
  - The client's Acceptable Use Policy states all systems are owned by the client and all data stored on those systems are the property of the client.
  - The Acceptable Use Policy states connection to the client's network is considered consent for the connected machine to be searched and analyzed (including all present data and configurations).
  - The client has confirmation that all employees have read and understand the Acceptable Use Policy.
- Passwords (including those in encrypted form) will not be included in the final report, or must be masked enough to ensure recipients of the report cannot recreate or guess the password. This is done to safeguard the confidentiality of the users the passwords belong to, as well as to maintain the integrity of the systems they protect.
- Any method or device used to maintain access to compromised systems and that could affect the proper operation of the system or whose removal may cause downtime may not be implemented without the prior written consent of the client.
- Any method or device which is used to maintain access to compromised systems must employ some form of user authentication such as digital certificates or login prompts. A reverse connection to a known controlled system is also acceptable.
- All data gathered by the testers must be encrypted on the systems used by the testers.
- Any information included in the report that could contain sensitive data (screenshots, tables, figures) must be sanitized or masked using techniques that render the data permanently unrecoverable by recipients of the report.
- All data gathered will be destroyed once the client has accepted the final report. Method used and proof of destruction will be provided to the client.
- If data gathered is regulated by any law, the systems used and their locations will be provided by the client to ensure that the data collected and processed does not violate any applicable laws. If the systems will be those of the penetration testing team the data may not be downloaded and stored on to their systems and only proof of access will be shown (File Permissions, Record Count, file names..etc).
- Third party services for password cracking will not be used, nor will there be sharing of any other type of data with third parties without the clients prior consent.
- If evidence of a prior compromise if found in the assessed environment all logs with actions and times recorded during the assessment by the penetration team will be saved, hashed and provided to the client. The client can then determine how best to respond to and handle the incident response.
- No logs should be removed, cleared or modified unless specifically authorized to do so by the client in the engagement contract/statement of work. If authorized, the logs must be backed up prior to any changes.

### Protecting Yourself

Due to the nature of a penetration test, you must ensure that you cover all your bases when dealing with the client and the tasks you will be performing. Discuss the following with the client to ensure a clear understanding of the roles and responsibilities of both client and provider prior to beginning any work.

- Ensure that the contract and/or statement of work signed by both the client and provider that the actions taken on the systems being tested are on behalf and in representation of the client.
- Obtain a copy of the security policies that govern user use of company systems and infrastructure (often referred to as "Acceptable Use" policies) prior to starting the engagement. Verify that policy covers:
  - Personal use of equipment and storage of personal employee data on the client systems and ownership and rights on that data.
  - Ownership of data stored on company equipment.
- Confirm regulations and laws that govern the data that is managed and used by the client on their systems and the restrictions imposed on such data.
- Use full drive encryption for those systems and removable media that will receive and store client data.
- Discuss and establish with the client the procedures to follow in the case that a compromise from a third party is found.
- Check for laws concerning the capture and/or storage of audio and video since the use of this methods in post-exploitation may be considered a violation of local or country wiretap laws.

# Infrastructure Analysis

## Network Configuration

The network configuration of a compromised machine can be used to identify additional subnets, network routers, critical servers, name servers and relationships between machine. This information can be used to identify additional targets to further penetrate the client’s network.

### Interfaces

Identify all of the network interfaces on the machine along with their IP addresses, subnet masks, and gateways. By identifying the interfaces and settings, networks and services can be prioritized for targeting.

### Routing

Knowledge of other subnets, filtering or addressing schemes could be leveraged to escape a segmented network, leading to additional hosts and/or networks to probe and enumerate. This data could come from a variety of sources on a particluar host or network including:

- Interfaces
- Routing tables, including static and dynamic routes
- ARP Tables, NetBios or other network protocols used for service and host discovery.
- For multi-homed hosts, determine if they are acting as a router.

### DNS Servers

Identify all DNS servers in use, by assessing host settings. DNS servers and information could then be used to develop and execute a plan for discovering additional hosts and services on the target network. In the case that a DNS Server is compromised, the DNS database will provide valueable information about hosts and services that can be used to prioritize targets for the remainder of the assessment. The modification and addition of new records could be used to intercept the data of services depending on DNS.

### Cached DNS Entries

Identify high value DNS entries in the cache, which may include login pages for Intranet sites, management interfaces, or external sites. Cached interfaces provide information of the most recent and most used host used by the compromised host providing a view of the relations and interactions of the hosts providing information that could be used to prioritization of targets for further penetration of the target network and infrastructure. Modification of cached entries if permitted can be used to capture authentication credential, authentication tokens or to gain further information on services used by the compromised hosts leading to further penetration of the target network.

### Proxy Servers

Identify network and application level proxy servers. Proxy servers make good targets when in enterprise-wide use by the client. In the case of application proxies, it may be possible to identify, modify and/or monitor the flow of traffic, or the traffic itself. Proxy attacks are often an effective means to show impact and risk to the customer.

### ARP Entries

Enumerate cached and static ARP table entries, which can reveal other hosts that interact with the compromised machine. Static ARP entries may represent critical machines. If the scope of the assessment allows for intercepting and modifying ARP entries, it is simple to show the possibility of disrupting, monitoring, or compromising a service in a manner that is usually not detected or protected against.

## Network Services

### Listening Services

Identify all the network services offered by the target machine. This may lead to the discovery of services not identified by initial scanning as well as the discovery of other machines and networks. The identification of services not shown in scanning can also provide information on possible filtering and control systems implemented in the network and/or host. In addition, the tester may be able to leverage these services to compromise other machines. Most operating system include a method of identifying TCP and UDP connections made to and from the machine. By checking both connections to and from a compromised machine it is possible to find relationships that were previously unknown. As well as the host the service should also be considered, this may reveal services listening on non-standard ports and indicate trust relationships such as keyless authentication for SSH.

### VPN Connections

All VPN connections into and out of the target machine or network should be identified. Outbound connections can provide paths into new systems which may have not previously been identified. Both inbound and outbound can identify new systems and possible business relationships. VPN connections often bypass firewalls and intrusion detection/prevention systems due to their inability to decrypt or inspect encrypted traffic. This fact makes VPNs ideal to launch attacks through. Any new targets should be verified as in scope before launching attacks against them. The presence of VPN client or server connections on the target host may also provide access to credentials previously not known that could be used to target other hosts and services.

### Directory Services

A targeted host running directory services may provide an opportunity to enumerate user accounts, hosts and/or services that can be used in additional attacks or provide additional targets that may not have been previously discovered in the vulnerability analysis phase. Additionally, the details of users found in directory services could be used for Social Engineering and phishing campaign attacks, thus providing a possible higher success rate.

### Neighbors

In todays network many services and operating systems use a number of protocols for neighbor discovery in an effort make the access of services, troubleshooting and configuration more convenient. Protocols vary depending on the type of target host. Networking equipment may use protocols like CDP (Cisco Discovery Protocol) and LLDP (Link Layer Discovery Protocol) to identify systems, configurations and other details to hosts directly connected to them or present in the same subnet. Similarly, desktop and server operating systems may use protocols like mDNS (Multicast Domain Name Service) and NetBios to find details of hosts and services in the same subnet.

# Pillaging

Pillaging refers to obtaining information (i.e. files containing personal information, credit card information, passwords, etc.) from targeted hosts relevant to the goals defined in the pre-assessment phase. This information could be obtained for the purpose of satisfying goals or as part of the pivoting process to gain further access to the network. The location of this data will vary depending on the type of data, role of the host and other circumstances. Knowledge and basic familiarity with commonly used applications, server software and middleware is very important, as most applications store their data in many different formats and locations. Special tools may be necessary to obtain, extract or read the targeted data from some systems.

## Installed Programs

### Startup Items

Most systems will have applications that can run at system startup or at user logon that can provide information about the purpose of the system, software and services it interacts with. This information may reveal potential countermeasures that could be in place that may hinder further exploitation of a target network and it’s systems (e.g. HIDS/HIPS, Application Whitelisting, FIM). Information that should be gathered includes:

- List of the applications and their associated versions installed on the system.
- List of operating system updates applied to the system.

## Installed Services

Services on a particular host may serve the host itself, or other hosts in the target network. It is necessary to create a profile of each targeted host, noting the configuration of these services, their purpose, and how they may potentially be used to achieve assessment goals or further penetrate the network.

### Security Services

Security services comprise the software designed to keep an attacker out of systems, and keep data safe. These include, but are not limited to network firewalls, host-based firewalls, IDS/IPS, HIDS/HIPS and anti-virus. Identifying any security services on a single targeted host gives an idea of what to expect when targeting other machines in the network. It also gives an idea of what alerts may have been triggered during the test, which can be discussed with the client during the project debrief, and may result in updates to Security Policies, UAC, SELinux, IPSec, windows security templates, or other security rulesets/configurations.

### File/Printer Shares

File and print servers often contain targeted data or provide an opportunity to further penetrate the target network and hosts. The information that should be targeted includes:

- Shares offered by File Servers - Any file shares offered by target systems should be examined. Even just the names and comments of shares can leak important information about the names of internal applications or projects (i.e. if only "Fred" and "Christine" have access to the "Accounting" folder, perhaps they are both accounting employees).
- Access Control Lists and permissions for shares. - From the client side, if it is possible to connect to the share, then it should be checked to see if the connection is read/only or read/write. Remember that if a share contains directories then different permissions may apply to different directories. From the server side both server configuration and file/directory permissions should be examined.
- File share file and content listings
- Identify files of interest from the file share listings. Look for interesting or targeted items such as:
  - Source Code
  - Backups
  - Installation Files
  - Confidential Data (financial data in spreadsheets, bank reports in TXT/PDF, password files, etc.)
- Place trojans or autorun files - Using clever naming, or by mimicking naming conventions already in use, users can be encouraged to execute these payloads, allowing the tester to further penetrate the network. If file server logs can be obtained, specific users may even be targeted.

### Database Servers

Databases contain a wealth of information that may be targeted in an assessment.

- Databases - A list of database names can help the assessor to determine the purpose of the database and the types of data the database may contain. In an environment with many databases, this will help in prioritizing targets.

- Tables - Table names and metadata, such as comments, column names and types can also help the assessor choose targets and find targeted data.
- Table Content, row count for regulated content
- Columns - It is possible in many databases to search all column names of all tables with a single command. This can be leveraged to find targeted data (e.g. If credit card data is targeted on an Oracle database, try executing *select * from all_tab_columns where name = '%CCN%';*.
- Database and Table Permissions
- Database Users, Passwords, Groups and Roles

The information hosted on databases can be also be used to show risk, achieve assessment goals, determine configuration and function of services or to further penetrate a client network and hosts.

### Directory Servers

The main goals of a directory service is to provide information to services and hosts for reference or/and authentication. The compromise of this service can allow the control of all hosts that depend on the service and well as provide information that could be used to further an attack. Information to look for in a directory service are:

- List of objects (Users, passwords, Machines..etc)
- Connections to the system
- Identification of protocols and security level

### Name Servers

Name server provide resolution to host and services depending on the types of records it servers. Enumeration of records and controls can provide a list of targets and services to prioritize and attack to further penetrate a clients network and hosts. The ability to modify and add records can be use to show risk of denial of services as well as aid in the interception of traffic and information on a customer network.

### Deployment Services

Identification of deployment services allows for the access and enumeration of:

- Unattended answer files
- Permission on files
- Updates included
- Applications and versions

This information can be used to further penetrate a client network and hosts. The ability to modify the repositories and configuration of the service allows for

- Backdoor installation
- Modification of services to make them vulnerable to attack

### Certificate Authority

Identification of Certificate Authority services on a compromised client host will allow for the access to

- Root CA
- Code Signing Certificates
- Encryption and Signing Certificates

Control of the service will also allow for the

- Creation of new certificates for several tasks
- Revocation of certificates
- Modification of the Certificate Revocation List
- Insertion of Root CA Certificate

The control of the services shows risk and allows for the compromise of data and services on a client's network and hosts.

#### Source Code Management Server

Identification of source code management systems via by the service running on the compromised host or the client part of the service provides the opportunity for:

- Enumerate projects - The project names can give away sensitive information on company projects.
- Verify access to source code files
- Modify source code files - If it is allowed in scope then modifying source code proves that an attacker could make changes that would affect the system
- Enumerate developers - Developers details can be use for social engineering attacks as well as as inputs for attacking other areas of the system
- Enumerate configuration

#### Dynamic Host Configuration Server

Identification of dynamic host configuration service or use of the service by the compromised host allows for:

- Enumeration leases given
- Enumeration configuration
- Enumeration Options
- Modification of configuration
- Consumption of all leases

The control of the service can be used to show risk of denial of service and for use in man in the middle attacks of hosts and services on the compromised network.

#### Virtualization

Identification virtualization services or client software allow for:

- Enumerate Virtual Machines (name, configurations, OS)
- Enumerate passwords and digital certificates for administration systems.
- Enumerate virtualization software configuration
- Configuration of Hosts
- Show risk of denial of service with control of VM state

- Access to data hosted on VM’s
- Interception of traffic of virtual hosts or services hosted on the compromised host

### Messaging

Identification of services or client software for messaging provides the opportunity to

- Identify Directory Services
- Compromise of credentials
- Access to confidential information
- Identification of hosts on the network
- System and business relationships

All of this information and actions can be used to show risk and to further penetrate a client’s network and hosts.

### Monitoring and Management

Identification of services or client software for the purpose of monitoring and/or management may provide identification of additional servers and services on the target network, in addition the configuration parameters gained may provide access to other targets host and to determine what actions performed by the tester can be detected by the client. Some services to look for:

- SNMP (Simple Network Management Protocol)
- Syslog

Some Management Services and Software to look for to gain credentials, identify host and gain access to other services may be:

- SSH Server/Client
- Telnet Server/Client
- RDP (Remote Desktop Protocol) Client
- Terminal Server
- Virtual Environment Management Software

### Backup Systems

Identification of services or client software for the purpose of backing up data provide a great opportunity to an attacker since these system require access to the data and systems they need to backup providing an attacker:

- Enumeration of hosts and systems
- Enumeration of services
- Credentials to host and/or services
- Access to backup data

The information gained from the service can be used to show risk to the confidentiality, integrity and access tot he system and their information. Access to the backups can also provide opportunity to introduce miss configuration, vulnerable software or backdoors in to the clients systems.

### Networking Services (RADIUS,TACACS..etc)

Identification of services or use of networking services allows for the:

- Enumeration of users
- Enumeration of hosts and systems
- Compromise of credentials
- Show risk of denial of service if alternate methods are not present

## Sensitive Data

### Key-logging

By monitoring key strokes it is possible to detect sensitive information including passwords and PII - Don't know what the legality of this is if the user is say chatting on private IM while also using company software, anyone know? If the company says that all data on the network can be monitored then this should be ok. If the second bullet point in Protect Yourself is present and it states that use of equipment can be monitored and no personal use is permitted yes, if policy does not cover personal user or ownership of data, no. It should be extended to cover Network also.

### Screen capture

Screen capture can be use to show evidence of compromise as well as access to information that can shown on the screen and access thru other means is not possible. Great care should be taken with the data collected thru screen capture so as to nor show private data of employees of customers of the client.

### Network traffic capture

Network traffic capture can be used depending on the controls on the network and medium used for capture can be used to:

- Identify hosts on the network
- Intercept data
- Identify services
- Identify relations between hosts in the network
- Capture of credentials

Care should be taken to only capture traffic covered under the scope of the engagement and that the information captured does not fall under the control of local laws like the capture of Voice Over IP calls. Information retained and shown should be filtered so as to protect client's customer and/or employee personal and confidential data.

### Previous Audit reports

## User Information

In this section the main focus is on the information present on the target system related to user accounts either present on the system or that have connected remotely and have left some trace that the personnel performing the assessment can gather and analyze for further penetration or provide the desired goal of the assessment.

### On System

General information that can be gather on a compromised system are:

- History files - History files store recent commands the user has executed. Reading through these can reveal system configuration information, important applications, data locations and other system *sensitive information.
- Encryption Keys (SSH, PGP/GPG)
- Interesting Documents (.doc/x, .xls/x , password.*) - Users often store passwords and other sensitive information in clear text documents. These can be located in two ways, either searching through file names for interesting words, such as password.txt, or searching through the documents themselves. Indexing services can help with this, for example the Linux locate database.
- User specific application configuration parameters
- Individual Application History (MRU Windows only, history files..etc)
- Enumerate removable media
- Enumerate network shares / domain permission (gpresult)

### Web Browsers

Information that can be gathered from web browsers that can be use to identify other hosts and systems as well as provide information to further penetrate a client's network and hosts are:

- Browser History
- Bookmarks
- Download History
- Credentials
- Proxies
- Plugins/Extensions

Great care should be taken that only data in scope for the engagement is capture since the information from a web browser may contain client's employee confidential and private data. This data should be filtered from the data returned and report.

### IM Clients

Information that can be gathered from IM Clients on a compromised system is:

- Enumerate Account Configuration (User, Password, Server, Proxy)
- Chat Logs

Great care should be taken that only data in scope for the engagement is capture since the information from a web browser may contain client's employee confidential and private data. This data should be filtered from the data returned and report.

## System Configuration

### Password Policy

By enumerating the systems password policy the ability to brute force and crack passwords becomes much more efficient, for example knowing that the minimum password length is 8 characters you can remove any word less than 8 characters from a dictionary.

### Security Policies

### Configured Wireless Networks and Keys

By finding the targets wireless information it becomes possible to launch physical attacks through the companies wifi when on site. It can also allow a fake AP to be set up to lure targets to connect when away from site.

# High Value/Profile Targets

High value/profile targets can be identified and further expanded from the targets identified in the pre-engagement meetings thru the analysis of the data gathered from the compromised systems and the interactions of those systems and the services that run on them This view of the the operation and interactions of these high value/profile targets helps in the identification and measurement of of impact that can be gained to the business do to the data and processes and to the overall integrity of the client’s infrastructure and services.

# Data Exfiltration

## Mapping of all possible exfiltration paths

from each of the areas where access has been achieved, a full exfiltration paths should be created. This includes secondary and tertiary means of getting to the outside world (through different accessible subnetc, etc). Once the mapping is provided, the actual exfiltration testing should be commenced.

## Testing exfiltration paths

Per exfiltration paths mapping, data should be exfiltrated from the organization being tested. This should already be covered in the Pre-engagement scoping and adequate infrastructure should have been setup which adheres to the customer's acceptable engagement policy (i.e. data being exfiltrated is usually exfiltrated to a server in the full control of the tester, and will access and ownership right to the tested organization). The exfiltration itself should simulate real-world exfiltration strategies used by the threat actors that correspond to the Threat Modeling Standard relevant for the organization (i.e. if criminal mostly then "standard" exfiltration using a staging area inside the network where data is archived inside zip/7z encrypted files and then sent to FTP/HTTP servers on the Internet, if a more sophisticated threat actor then using means that simulate such strategies and tactics used for exfiltration).

## Measuring control strengths

When performing exfiltration testing, the main goal of the test is to see whether the current controls for detecting and blocking sensitive information from leaving the organization actually work, as well as exercise the response teams if anything has been detected in terms of how they react to such alerts and how are the events being investigated and mitigated.

# Persistence

- Installation of backdoor that requires authentication.
- Installation and/or modification of services to connect back to system. User and complex password should be used as a minimum; use of certificates or cryptographic keys is preferred where possible. (SSH, ncat, RDP). Reverse connections limited to a single IP may be used.
- Creation of alternate accounts with complex passwords.
- When possible backdoor must survive reboots.

# Further Penetration Into Infrastructure

Pivoting is the action in which the tester will use his presence of on the compromised system to further enumerate and gain access to other systems on the client’s infrastructure. This action can be executed from the compromised host it self using local resourced or tools uploaded to the compromised system.

## From Compromised System

Actions that can be taken from a compromised system:

- Upload tools
- Use local system tools
- ARP Scan
- Ping Sweep
- DNS Enumeration of internal network
- Directory Services Enumeration
- Brute force attacks
- Enumeration and Management thru Management Protocols and compromised credentials (WinRM, WMI, SMB, SNMP..etc)
- Abuse of compromised credentials and keys (Webpages, Databases..etc)
- Execute Remote Exploits

The action that will be executed will depend on the information needed to show specific risk and/or further penetrating the client's network and hosts. Regular planning sessions are recommended to re-evaluate the information gather and decide the best approach to continue the post exploitation until the set goals are meet.

## Thru Compromised System

Actions that can be taken thru a compromised system:

- Port Forwarding
- Proxy to internal network (SSH)
- VPN to internal network
- Execute Remote Exploit

- Abuse of compromised credentials and keys (Webpages, Databases..etc)

The action that will be executed will depend on the information needed to show specific risk and/or further penetrating the client's network and hosts. Regular planning sessions are recommended to re-evaluate the information gather and decide the best approach to continue the post exploitation until the set goals are meet.

## Cleanup

The cleanup process covers the requirements for cleaning up systems once the penetration test has been completed. This will include all user accounts and binaries used during the test.

- Remove all executable, scripts and temporary file from a compromised system. If possible use secure delete method for removing the files and folders.
- Return to original values system settings and application configuration parameters if they where modified during the assessment.
- Remove all backdoors and/or rootkits installed.
- Remove any user accounts created for connecting back to compromise systems.

Retrieved from "http://www.pentest-standard.org/index.php?title=Post_Exploitation&oldid=947"

**This page was last edited on 16 August 2014, at 20:01.**