

CONFERENCE

REAL WORLD PENETRATION TESTING



.... ..

HACK > DAY

.... ..

WHOAMI

Mehdi Nacer KERKAR

Information security student



You can find me:

- Twitter: @mehdi_kerkar
- LinkedIn: /in/mehdi-nacer-kerkar/

REAL WORLD PENETRATION TESTING

- Penetration Testing
- Penetration Tester
- PTES
- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation (Escalation /Evidence Gathering (Pilfering)/Clean up)
- Reporting (Report Creation/Report Delivery and Review/ Remediation)

PENETRATION TESTING

What is Penetration Testing?

“The process of evaluating systems, applications, and protocols with the intent of identifying vulnerabilities from the perspective of an unprivileged or anonymous user to determine the real-world impact...” “...legally and under contract ”

- Common language for organizations and service providers
- Set the bar for a common standard to be used
- Eliminate hacks

PENETRATION TESTER

Who are a Penetration Tester and what he do ?

Using many tools and techniques, the penetration tester (ethical hacker) attempts to exploit critical systems and gain access to sensitive data.

A penetration test simulates the actions of an external and/or internal cyber attacker that aims to breach the information security of the organization.

- A penetration tester's job is to demonstrate and document a flaw in security.
- In a normal situation, a pen tester will perform reconnaissance to find some vulnerabilities, exploit those vulnerabilities to gain access, then possibly extract some small piece of data of value to prove that the system is not secure.

PTES (PENETRATION TESTING EXECUTION STANDARD)

What is mean PTES ?

It is a new standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing.

It started early in 2009 following a discussion that sparked between some of the founding members over the value and lack of penetration testing in the industry.

TYPES OF TESTS (White, Black And Gray)

- “White box” uses vulnerability assessment and other pre-disclosed information.
- “Black box” is performed with no knowledge of the target system and tester must perform their own reconnaissance.
- Gray means partial knowledge.

TYPES OF PENETRATION TESTS

- Network Pentesting (Perimeter Infrastructure / Wireless, WEP/WPA cracking / Telephony systems / VoIP)
- Application Pentesting (Web & Mobile applications / Databases)
- Website Pentesting (web server / OWASP)
- Physical Pentesting (Warehouses and storage facilities / Data centers / CCTV systems / Door entry systems)
- Cloud Pentesting
- Social Pentesting (phishing, media drops, tailgating, pretexting)

Pre-engagement Interactions

- Introduction to Scope (black or white box, type of the test)
- Metrics for Time Estimation
- Scoping Meeting
- Additional Support Based on Hourly Rate
- Questionnaires
- Scope Creep
- Specify Start and End Dates
- Specify IP Ranges and Domains (Validate Ranges)
- Dealing with Third Parties (Cloud Services / Countries Where Servers are Hosted)

Pre-engagement Interactions

- Define Acceptable Social Engineering Pretexts
- DoS Testing
- Payment Terms (Net 30 / Half Upfront / Recurring)
- Goals (Primary / Secondary compliance / Business Analysis VA)
- Establish Lines of Communication
- Emergency Contact Information (Incident Reporting Process / Incident Definition / Status Report Frequency)
- Rules of Engagement
 - (Timeline / Locations / Evidence Handling / Regular Status Meetings / Time of the Day to Test / Dealing with Shunning / Permission to Test / Legal Considerations)

Pre-engagement Interactions

Questionnaires

- Network Penetration Test (active, passive scan / IP addresses are being tested)
- Web Application Penetration Test (How many web applications / login systems / static, dynamic pages)
- Wireless Network Penetration Test (How many wireless / type of encryption .)
- Physical Penetration Test (How many floors / 3rd party / armed / video cameras . Alarms)
- Social Engineering (How many people / list of email / list of phone)
- Questions For Business Unit Managers (What is the main datum that would create the greatest risk to the organization if exposed, corrupted, or deleted?)
- Questions For Systems Administrators (systems with tendencies to crash / older operating systems / unpatched systems)

Intelligence Gathering

- Intelligence Gathering is performing reconnaissance against a target to gather as much information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases. The more information you are able to gather during this phase, the more vectors of attack you may be able to use in the future.
- Reconnaissance determines...**"What can a potential attacker learn about your company?"**
- Utilizes publicly available information.





















Intelligence Gathering

- Identification and Naming of Target
- Consider any Rules of Engagement limitations
- Consider time length for test & end goal of the test
- Open Source Intelligence (OSINT) (Passive/semi-passive/active Information Gathering)
- Locations/Relationships (Clients/partners)
- Individual Employee (Social Network Profile/ Internet Presence / Mobile Footprint / Physical Location)

Intelligence Gathering

Some sources of information:

- Search Engines
- Websites
- Registrars (Ex: [Netcraft.com](#))
- SEC
- Recruiting sites

	Site	Site Report	First seen	Netblock	OS
1.	www.mytelus.com		December 1999	Alberta Government Telephones	unknown
2.	webmail.telus.net		September 2008	AGT Limited.	F5 Big-IP
3.	www3.telus.net		November 1999	Edmonton Telephones Corporation	unknown
4.	www.telusmobility.com		January 1999	TELUS MOBILITY	Solaris 9/10
5.	www.telus.com		October 1995	TELUS Communications Inc.	F5 Big-IP
6.	www.telusplanet.net		November 1996	Edmonton Telephones Corporation	unknown
7.	money.mytelus.com		April 2003	WORLD WIDE QUOTE	Windows 2000
8.	about.telus.com		November 2001	TELUS Communications Inc.	Solaris 8
9.	www.telusmobilite.com		December 1999	TELUS MOBILITY	Solaris 8
10.	www.telusquebec.com		October 2000	Results for “telus”	Windows Server 2003
11.	www.telus.ca		December 1999		F5 Big-IP
12.	webmail.telusplanet.net		August 1999	ED TEL	F5 Big-IP
13.	mytelus.com		December 2004	Alberta Government Telephones	Solaris 9/10
14.	automotive.mytelus.com		August 2005	Autoling inc.	Linux
15.	www.webmail.telus.net		August 2005	AGT Limited.	F5 Big-IP
16.	businesscontent.telus.com		June 2004	TELUS Communications Inc.	unknown
17.	hosting.telushosting.com		March 2002	InternetNamesForBusiness.com	Linux
18.	store.telusmobility.com		May 2001	Rackspace.com, Ltd.	Linux
19.	www.mytelusmobility.com		April 2001	TELUS MOBILITY	Solaris 9/10
20.	www.telus.net		November 1996	Alberta Government Telephones	Solaris 9/10

Footprinting

- External information gathering, also known as footprinting, is a phase of information gathering that consists of interaction with the target in order to gain information from a perspective external to the organization.
- Passive Reconnaissance (**WHOIS Lookups**)
- Active Footprinting (**Port Scanning / Banner Grabbing / DNS & Web Application Discovery**)

THREAT MODELING

- Business Asset Analysis
- Business Process Analysis
- Threat Agents/Community Analysis
- Threat Capability Analysis
- Motivation Modeling
- Finding relevant news of comparable Organizations being compromised

THREAT MODELING

Business Asset Analysis

- Organizational Data (Policies, Future Plans, and Procedures/ Product and Marketing Information / Infrastructure Design, System Configuration Information / User Account Credentials)
- Employee Data (National Identification Numbers / Protected Health Information / Financial Information)
- Customer Data
- Human Assets (Grade)

THREAT MODELING

Business Process Analysis

- Technical infrastructure supporting process (IT infrastructure such as computer networks, processing power, information and managing the business process)
- Information assets supporting process (reference, support material, decision making, legal, marketing)
- Human assets supporting process
- 3rd party integration and/or usage of/by process

THREAT MODELING

Threat Agents/Community Analysis

Internal	External
Employees	Business Partners
Management (executive, middle)	Competitors
Administrators (network, system, server)	Contractors
Developers	Suppliers
Engineers	Nation States
Technicians	Organized Crime
Contractors (with their external users)	Hacktivists
General user community	Script Kiddies (recreational/random hacking)
Remote Support	

THREAT MODELING

Threat Capability Analysis

- Analysis of tools in use
- Availability to relevant exploits/payloads
- Communication mechanisms
- Accessibility

THREAT MODELING

Motivation Modeling

- Profit (direct or indirect)
- Hacktivism
- Direct grudge
- Fun / Reputation
- Further access to partner/connected systems

Finding relevant news of comparable Organizations being compromised

VULNERABILITY ANALYSIS

Testing

Vulnerability testing is the process of discovering flaws in systems and applications which can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration, or insecure application design. Although the process used to look for flaws varies and is highly dependent on the particular component being tested, some key principals apply to the process.

- Active testing (involves direct interaction)
- Passive testing
- Validation
- Research

VULNERABILITY ANALYSIS

Active Testing

- Automated
- Network / General Vulnerability Scanners
- Service Based (specific service protocols)
- General application flaw scanners
- Directory Listing / Brute Forcing
- Web Server Version / Vulnerability Identification (POST / GET / PUT / DELETE)
- Network Vulnerability Scanners / Specific Protocols (VPN / Voice Network Scanners / Manual Direct Connections / Obfuscated)

VULNERABILITY ANALYSIS

Passive Testing

- Metadata Analysis (Ex: document, list author, company, paths to servers, internal IP addresses)
- Traffic Monitoring (capturing data for offline analysis)

VULNERABILITY ANALYSIS

Validation

- Correlation between Tools (specific and categorical correlation of items / metrics and statistics)
- Manual Testing/Protocol Specific (VPN / Enumeration / DNS / Web / Mail)
- Creation of attack trees (developed and regularly updated)
- Isolated Lab Testing
- Visual Confirmation

VULNERABILITY ANALYSIS

Research

- Public Research (research the potential exploitability of the vulnerability)
- Exploit Databases and Framework Modules (actively maintained and publicly accessible on the Internet)
- Common / default Passwords
- Hardening Guides / Common Misconfigurations
- Private Research (Testing Configurations / Fuzzing)
- Identifying potential avenues / vectors
- Disassembly and code analysis

EXPLOITATION

The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. If the prior phase, vulnerability analysis was performed properly, this phase should be well planned and a precision strike..

- Shows how far an attacker can get (within scope of test).
- Security tester should be able to explain exploitation technique and:
- Why it worked.
- What exploit did.

EXPLOITATION

- Countermeasures

(Anti-Virus / Encoding / Packing/ Encrypting / Whitelist / Process Injection / Human)

- Evasion (escape detection during a pentest)

- Customized Exploitation Avenue

- Tailored Exploits (Exploit Customization)

- Zero-Day Angle (Source Code Analysis)

- EXPLOITS

- Buffer Overflows (is to overwrite a given register and jump to the shellcode)
- Traffic Analysis (protocol works & manipulate that traffic)
- Physical Access / Human Angle / PC Access
- Proximity Access / WiFi Attacks

POST EXPLOITATION

- Rules of Engagement
- Infrastructure Analysis
- Pillaging
- High Value/Profile Targets
- Persistence
- Further Penetration Into Infrastructure
- Cleanup

POST EXPLOITATION

Rules of Engagement

Protect the Client

- All modifications, including configuration changes, executed against a system must be documented.
- All settings should be returned to their original positions if possible.
- A detailed list of actions taken against compromised systems must be kept.
- Sensitive data (screenshots, tables, figures, passwords) must be sanitized or masked using techniques that render the data permanently unrecoverable.

Protecting Yourself

- Ensure that the contract and/or statement of work signed by both the client and provider.
- Obtain a copy of the security policies that govern user use of company systems and infrastructure.
- Use full drive encryption for those systems and removable media that will receive and store client data.

POST EXPLOITATION

Infrastructure Analysis

Network Configuration

- Interfaces
- Routing
- DNS Servers
- Cached DNS Entries
- Proxy Servers
- ARP Entries

Network Services

- Listening Services
- VPN Connections
- Directory Services
- Neighbors

POST EXPLOITATION

Pillaging

- Installed Programs (Startup Items)
- Installed Services (Security Services / File/Printer Shares / Database Servers / Directory Servers / Name Servers / Deployment Services / Certificate Authority / Source Code Management Server / Dynamic Host Configuration Server / Virtualization / Messaging / Monitoring and Management / Backup Systems / Networking Services)
- Sensitive Data (Key-logging / Screen capture / Network traffic capture / Previous Audit reports)
- User Information (On System / Web Browsers / IM Clients)
- System Configuration (Password Policy / Security Policies / Configured Wireless Networks and Keys)

POST EXPLOITATION

High Value/Profile Targets

Data Exfiltration

- Mapping of all possible exfiltration paths (through different accessible subnet)
- Testing exfiltration paths
- Measuring control strengths

POST EXPLOITATION

Persistence

- Installation of backdoor that requires authentication.
- Installation and/or modification of services to connect back to system.
- Creation of alternate accounts with complex passwords.
- When possible backdoor must survive reboots.

POST EXPLOITATION

Further Penetration Into Infrastructure

From Compromised System

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

Thru Compromised System

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

POST EXPLOITATION

Cleanup

- 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 were modified during the assessment.
- Remove all backdoors and/or rootkits installed.
- Remove any user accounts created for connecting back to compromise systems.

REPORTING

The report is broken down into two major sections in order to communicate the objectives, methods, and results of the testing conducted to various audiences.

- The Executive Summary (audience any members of the organization)
- Technical Report (technical details of the test)

REPORTING (The Executive Summary)

- Background (explain details within the Pre Engagement / objectives changes)
- Overall Posture
- Risk Ranking/Profile (score risk of security implies the potential for compromised and financial losses)
- General Findings (Graphic representations, testing results, processes, attack scenarios, success rates, and other trendable metrics)
- Recommendation Summary (tasks needed to resolve the risks / implementation level of resolution path)
- Strategic Roadmap (plan for remediation / business objectives / level of potential impact)

REPORTING (Technical Report)

- Introduction (Personnel involved / Objectives and scope of Test / Threat/Grading Structure)
- Information Gathering
- Passive Intelligence (indirectly, DNS /Google dorking for IP/ infrastructure)
- Active Intelligence (infrastructure mapping / port scanning / architecture assessment)
- Corporate Intelligence
- Personnel Intelligence
- Vulnerability Assessment
- Exploitation/ Vulnerability Confirmation
- Post Exploitation
- Risk/Exposure (Evaluate incident frequency / Estimate loss magnitude per incident / Derive Risk)
- Conclusion

REFERENCES

- www.ptes.org
- www.owasp.com

THANK YOU FOR YOU PRESENCE

Any Questions ?

REAL WORLD PENETRATION TESTING

KERKAR MEHDI NACER