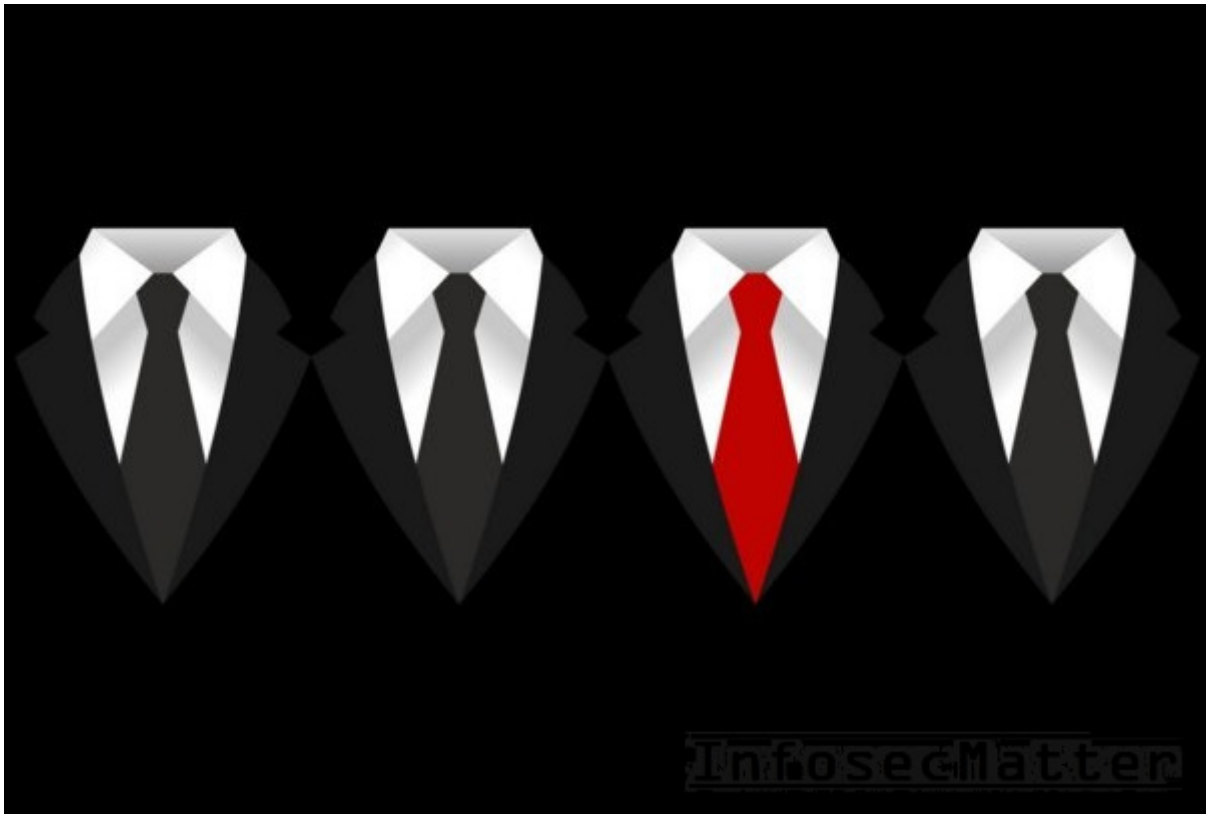
Top 25 Penetration Testing Skills and Competencies (Detailed)

infosecmatter.com/top-25-penetration-testing-skills-and-competencies-detailed

April 2, 2020



What soft skills and technical competencies does it take to became a professional penetration tester or ethical hacker? In this article we will discuss in detail what are the top 25 areas every pentester should be familiar with and what skills you should focus on if you want to become a professional penetration tester.

Let's dive right into it.

Hardware and Networks

Naturally, we all in the infosec industry know about hardware and networks. But let's discuss what is particularly important for pentesters.

1. Computer networks

Every pentester should understand computer networks and the OSI model. It is important to know at least the most common network protocols such as:

Link layer (L2) protocols

- 802.3 (Ethernet/ARP)
- 802.1Q (VLANs)
- 802.11 (Wi-Fi)

Network layer (L3) protocols

- IP (IPv4, IPv6)
- ICMP

Transport layer (L4) protocols

- TCP
- UDP

Application layer (L7) protocols

DNS, HTTP, HTTPS, DHCP, LDAP, FTP, SMTP, IMAP, POP, SSH, Telnet etc.

We should understand how these protocols work, what is their function and purpose.

For instance, we should be able to describe in detail what happens when we visit a website and answer questions such as:

- How does the communication occurs between our browser and the remote web server?
- How and which network protocols are being utilized on each OSI layer?

Furthermore, we should be comfortable using packet capturing tools such as Wireshark. We should understand which network protocols are safe and which are not safe, allowing anyone to sniff sensitive information from the network.

We should also understand, for instance, how to perform man-in-the-middle attack using ARP poisoning.

Lastly, we should be able to read network diagrams and schemas, because many times these things are discussed with the client. This brings us to the next point..

2. Network components

We should understand what kind of network equipment it takes for a network to function, how a typical organization builds their network, what security controls are typically implemented and so on.

At minimum, we should be familiar with:

- Network switches
- Routers / gateways
- Firewalls, NAT
- Zoning, VLANs

From the pentester perspective, we should be able to perform assessment of the network access controls (NAC) implementation and know tactics how to bypass it (e.g. MAC cloning, MITM).

We should also know how to check for VLAN hoping.

Furthermore, we should be somewhat familiar with common network device manufacturers such as:

- Brocade
- Checkpoint
- Cisco
- F5 Networks
- Fortinet
- Juniper
- PaloAlto
- etc.1

As pentesters, we should have at least basic experience in using them so that we can leverage situations when we get access to them (e.g. via weak or default credentials)

Once we get access to them, we should know how to go through the configuration and identify sensitive information such as SNMP community strings, for example.

With regards to Cisco devices, we should know how we can decrypt various Cisco password types that we find stored in them.

3. Wireless networks

Wireless networks are everywhere and we simply have to understand them. We must be knowledgeable about the following topics:

- Wi-Fi security and encryption modes, e.g.:
  - WEP
  - WPA/2/3 Personal
  - WPA/2/3 Enterprise
  - EAP authentication
- Pros and cons of SSID broadcast hiding
- Captive portal security
- Client isolation

We should have understanding of known attack vectors against wireless networks.

For instance, we should know when does it makes sense to run a de-authentication attack or when to deploy a rogue access point.

We should know how to obtain password hashes and how to crack them (e.g. using aircrack-ng).

We should also know which equipment to use for testing and know how to analyze wireless networks (e.g. using Kismet).

4. Server room hardware

Having experience with physical hardware and knowing our way throughout the server racks in a data center is not really essential for our job, but it can definitely help.

Here's some of the equipment we can find in a typical server room:

- Patch panels
- Core routers
- Network switches
- KVM switches
- Physical servers
- Storage and backup systems
- Firewalls, IDS, IPS and other network appliances
- UPS systems

From our perspective, we should understand that many of these things have administrative interfaces. And if we happen to get into them, we should know what we can do with them. Let's have a look on some examples.

Physical servers

One thing we should know about physical servers is that they typically have management web consoles which are online even if the server is powered down.

Here are some examples:

- Dell iDRAC (integrated Dell Remote Access Controller)
- HP iLO (integrated Lights-Out)
- Huawei iMana (Intelligent Management System)
- IBM HMC (Hardware Management Console)
- Sun Oracle ILOM (Integrated Lights Out Manager)

As pentesters, we should understand the ramifications of having access to these things. Typically it means that we can take complete control over the server including the operating system installed on it, thanks to the KVM functions and the remote console (display).

We should also understand that we should not be able reach these interfaces from the user VLAN, for example.

Network devices and appliances

Another thing to keep in mind is that some systems may be integrated with other systems together. For instance, an intrusion detection system (IDS) may be communicating with firewalls or honeypot systems deployed in the network.

In case we happen to gain access to such device, we should know how to navigate through its administrative interface. For instance, we should know techniques how to reveal credentials that are stored within the interface.

Go back to top.

Software and Services

5. System administration

Having professional experience in system administration can be a really great advantage for a pentester.

At minimum, we should be able to administer the following operating systems:

- Linux or other UNIX like system
- Microsoft Windows

We should know how to configure them, where the important configuration file are, where the log files are and also we should know how to perform network and system diagnostics.

We should also understand permissions and access controls in each system and have knowledge about various vulnerabilities and attack techniques on each system.

Here's one of the best resources covering broad spectrum of attack techniques: https://attack.mitre.org/

6. Network services

As pentesters, we should have extensive experience with administering various network services and servers.

This topic is obviously huge, but we should know how various network services work, what are some of the common misconfigurations or deficiencies in their protocols. For instance:

- SMTP open relay
- DNS zone transfer
- SMB NULL session
- LDAP NULL bind
- FTP anonymous login
- Webserver directory listing

As pentesters, we have to have extensive knowledge about these things.

Furthermore, we should also know how to setup things when we need them.

For instance, knowing how to quickly setup up a HTTP server, DHCP server or a SMB/CIFS shared folder can be truly essential during pentests.

7. Active Directory

Windows Active Directory (AD) deployments are practically everywhere and so we have to know them.

We should be able to assess security posture of the AD from multiple angles and know about various attack techniques against it. For instance:

- GPP cpasswords
- Password spraying
- Lateral movement
- Privilege escalation
- Mimikatz
- Kerberoasting

We should have extensive knowledge about these things. We should also know what are some of the countermeasures such as LAPS or PAM.

Here's one of the best resources on AD security and in fact the whole Microsoft ecosystem: Active Directory Kill Chain Attack & Defense.

Checkout also the Top 16 Active Directory Vulnerabilities typically found during internal infrastructure penetration tests and vulnerability assessments.

And one more thing. As pentesters, we should never call it a day after we get Domain Admin privileges. We should understand that we have to keep digging for more vulnerabilities.

8. Command-line tools

We have to be comfortable with command-line. This is simply a must. It is absolutely essential that we can navigate through the file system, work with files easily and do other things from the command-line.

Whether we have a UNIX background or a Windows background, we simply have to know the command-line by hearth on both.

On UNIX (Linux), we should be comfortable using the following text-processing tools:

- grep
- head
- tail
- sort
- uniq
- tr
- cut
- wc
- sed
- awk

These tools give us tremendous power for processing textual data – log files, outputs from other programs and so on. They give us ability to extract any piece of information we need.

On Windows the PowerShell interpreter has equivalent functionalities. In fact, it can be even more powerful thanks to its objectification.

Check out the PowerShell infosec reference with examples of equivalent commands on both Linux and Windows systems.

That brings us to the next topic..

9. Regular expressions

Regular expressions (regex or regexp) are the most powerful way of pattern matching. Knowing regular expressions can be extremely beneficial for a pentester because it allows us to do:

> **Pattern searching**. With regexps we can for instance filter out all IP addresses from a text file. We can find email addresses, domain names, host names, MAC addresses or pretty much anything really.
>
> **Text replacement**. Regexps have powerful search & replace functionalities which allows us to do various textual transformations.
>
> **Data grouping and splitting**. Using regexp we can group certain data together, or split them apart. This is essential for further automation / machine processing.

As pentesters, we must know regular expressions by hearth as well.

10. Shell scripting

Regardless of which Linux hacking distribution is your favorite, one thing is common to all of them – the **shell**.

As pentesters, we spend significant portion of our time working in shell. Therefore, every pentester should absolutely master it.

Knowing the shell gives us tremendous power and ability to automate things. For instance, we can:

- Automate repetitive tasks quickly and easily
- Write powerful one-liners from top of our head
- Interconnect pretty much all thinkable utilities together
- Write custom scripts and tools quickly
- Grow our efficiency exponentially

Every senior pentester should be able to throw intricate one-liners left and right.

11. Programming language

Let's be honest. As hackers, we are trying to find vulnerabilities in computer systems and programs which were most likely written in some programming language. How are we supposed to find bugs in these things if we don't have experience with programming?

Throughout our reports we are giving advice to programmers and developers and we should understand what it takes to implement something.

For instance, we should understand how a registration / login procedure works, how to store data in a database or how to safely read input from a user.

We should understand these things at least to the extent that we can comprehend the SANS TOP 25 most common software errors.

12. Python scripting language

Knowing Python scripting language can be a tremendous advantage for every pentester. Here's why.

First of all, Python is:

- Extremely powerful
- Easy to learn
- Easy to code in
- Multi-platform

Moreover, Python has been widely adopted by the infosec community and many great projects were written in Python. Here are some examples:

- mitmproxy
- Impacket
- sqlmap
- Scappy
- httpi

Furthermore, many security researchers and exploit writers write their code in Python. And sometimes we need to modify something here and there.

Therefore, we should definitely know this language at least so that we can modify what we need.

This brings us to the next skill..

13. Ability to find PoCs and exploits

Every pentester needs to know where to find a Proof of Concept (PoC) code or an exploit to verify a vulnerability.

Once our scanners tell us that the target is vulnerable to CVE-XXX-YYYY, we cannot simply take this as it is and blindly report it to the customer.

We should always verify everything. That's our job. We have to provide evidences and proofs. The more evidences we provide in our report, the happier and more impressed our customer is going to be.

Therefore, we need to know where to look for PoCs and we also need to know how to use them. The following list provides some resources on where to find PoCs and exploit codes:

- https://www.exploit-db.com/
- https://github.com/offensive-security/exploit-database
- https://github.com/offensive-security/exploit-database-bin-sploits
- https://github.com/qazbnm456/awesome-cve-poc
- https://github.com/Mr-xn/Penetration_Testing_POC
- https://github.com/Medicean/VulApps
- https://github.com/nixawk/labs
- https://github.com/Coalfire-Research/java-deserialization-exploits
- https://github.com/toolswatch/vFeed
- https://github.com/Metnew/uxss-db (Browser vulns)
- https://github.com/tunz/js-vuln-db (JavaScript vulns)

Go back to top.

Technology and Methodology

14. Internet services

As pentersters, we should have extensive knowledge about the Internet. We should know not only how it works, but also how to setup a server on the Internet, for instance.

We should have experience and know how to:

- Register a new domain
- Setup a virtual private server
- Associate the domain with the server
- Setup a secure network service using a certificate

Sometimes we need to prepare infrastracture for other activities (e.g. a phishing site) and as pentesters we should definitely know how to do it.

15. OSINT gathering

Every pentester should be able to navigate through the public sources to find technical and other information about a particular organization and their employees.

At minimum, we should be able to use sources such as:

- DNS records
- WHOIS records
- Search engines
- Social networks

For instance, we may need to perform an OSINT exercise on a target organization and collect a list of the following information:

- Registered domain names
- Host names and subdomains
- IP addresses and network ranges
- Email addresses
- Phone numbers

We should know how to do that e.g. by using various automated tools.

Here's one of the best resources available on OSINT: https://github.com/jivoi/awesome-osint

16. Databases

Every pentester should be somewhat knowledgeable about databases. I'm not suggesting to become a database administrator or a PL/SQL developer, but we should at least have experience using the most popular databases such as:

- MySQL
- MongoDB
- PostgreSQL
- Microsoft SQL
- Elasticsearch
- Oracle
- Redis

We should know how to connect to them, how to list logical databases in them, how to list tables and how to read data from them.

We should also understand what can we do with them after they are compromised.

Can we write onto the file system? Can we read arbitrary files? Are we able to achieve remote code execution (RCE) and get a shell? These things are essential for a pentester.

See for instance our guide on Firebird database exploitation.

17. Web technologies

As pentesters, we should have extensive range of skills about web technologies in order to perform web application penetration tests.

This topic is obviously huge, but for instance we should be knowledgeable about topics such as:

- HTML, JavaScript, CSS, PHP and ASP
- JSON, URL encoding, HTML entities
- HTTP family protocols
- SOAP and REST web services
- Web servers and application servers
- Web frameworks (SharePoint, Silverlight etc.)
- CMS (WordPress, Drupal etc.)
- Web application firewalls and filters

We should have extensive experience using testing tools such as:

- Burp Suite
- Fiddler Proxy
- Nikto
- Dirbuster
- Curl/Wget
- Sqlmap

We should know techniques and methods on how to assess security posture of web servers and deployed web applications.

For instance, we should know how to port scan a website.

We should also know about insecure coding practices, misconfigurations and other things that are included in the OWASP TOP 10 most common vulnerabilities.

18. Mobile technologies

When it comes to performing mobile application penetration tests, every pentester should know the core concepts and testing methodologies at least for the following two platforms:

- Android
- Apple iOS

We should know how to perform static and dynamic analysis of the mobile application. For instance, we should know how to:

- Use mobile phone emulators
- De-compile and re-compile an application
- Reverse engineer an application
- Inspect the network communication

We should know about code obfuscation, certificate pinning or how the application should be storing data on the phone. We should know about jailbreaks, rooting and other things.

Another thing that we should know is, for instance, that typically there is a server-side component involved – a system on the Internet which the mobile application communicates with.

This means that a typical mobile app pentest is partially also a web app pentest. Therefore, we should also have extensive knowledge of web technologies.

Here's one great resource on mobile security: https://mobisec.reyammer.io/.

19. Cryptography

As pentesters, we should have somewhat extensive knowledge about cryptography and related topics.

For starters we should know:

- Concepts of symmetric and asymmetric cryptography
- Difference between HTTP and HTTPS, or Telnet and SSH
- SSL and TLS encryption and concept of certification authorities
- How SSH public key authentication works

We should also understand differences between:

- Encoding (e.g. Base64)
- Checksum (e.g. CRC32)
- Obfuscation (e.g. XOR)
- Hashing (e.g. MD5, SHA1, SHA256, SHA512)
- Encryption (e.g. RC4, DES, BlowFish, AES)

We should know when to use them and how. We should know which ones we can decode, decrypt or which ones we can only attempt to crack. For instance, see our blog post about decrypting and cracking Cisco passwords.

As pentesters we should also know, for instance, how to employ obfuscation or encryption to bypass various defenses and other things.

20. Password and hash cracking

Another thing every pentester should know is how to crack things.

We should have extensive experience with cracking tools such as John the ripper or Hashcat.

We should be knowledgeable about cracking not only password hashes, but also other things. For instance:

- Documents (MS Office, PDF..)
- Compressed archives
- Password managers
- Encrypted volumes

We should understand methods and limitations when it comes to cracking speed, cracking on CPU vs. GPU or what is realistic to crack and what is not.

We should also know where to find dictionaries and which cracking tactics to use, e.g.:

- Wordlist
- Wordlist with rules
- Brute-force

Here's one of the best publicly available repository of wordlists: https://github.com/danielmiessler/SecLists

21. Physical security

Although penetration testing is mostly focused on information technology, sometimes there is also a physical penetration to be done and we should know how to execute such test.

We should have an understanding of physical security controls and at minimum be able to recognize deficiencies such as:

- Weak locks being in use
- Insecure door mechanisms
- Insufficient restrictions to enter restricted areas
- Insecure cabling (e.g. for an access control system)
- Insufficient video surveillance
- Unsafe disposal practices

We should also know something about RFID access card cloning and related topics.

22. Auditing and Compliance

We should also understand topics of compliance audits and security benchmarks. This includes CIS, PCI DSS, DISA STIG and so on.

Not everybody knows them, but knowing them can make a big difference not just in front of the client. For instance we should know:

- What are the organizations who made them?
- What are they actually testing / bench-marking?
- When and why does it makes sense to comply with them?

Here's a quick way to get up to speed:

CIS

- Center for Internet Security (homepage)
- CIS Benchmarks (link)
- FAQ (link)

PCI DSS

- Payment Card Industry (homepage)
- Data Security Standard (link)
- FAQ (link)

DISA STIG

- Defense Information Systems Agency (homepage)
- Security Technical Implementation Guides (link)
- FAQ (link)

MSCT

> Microsoft Security Compliance Toolkit (link)

Go back to top.

Other skills

23. Soft skills

Although penetration testing is mostly technical, we also need certain soft skills to do our job. Here's a list of 5 most important soft skills every pentester should have.

Ethics

Penetration testing is extremely sensitive area which often times includes dealing with confidential information and other people's data.

Therefore, we have to be extremely cautious and always keep the work private. Protecting our client is the number one mission and we must never forget this.

Articulation

Although our work is mostly technical comprising of working with computers, we also have to interact with people and clients a lot.

Therefore, we have to be able to explain our work and various technical information to others in a way that they can understand us.

Empathy

Empathy can help us understand who our audience is and how best to serve them.

Whether we are presenting our work in front of a group of company executives, or a technical crowd, we should always tailor our delivery to provide the most value to our audience.

Writing skills

Reports are the output of our work. They represent all that we have been doing during the engagement. Therefore, it is extremely important to know how to write high quality reports.

Our reports should look professional, clean and be without grammar mistakes and typos. We should always use spell checker even before passing it on to our teammates for a QA.

Audacity

The work of a pentester sometimes also require certain level of **boldness**. For instance during social engineering attacks, vhishing calls or physical intrusions.

As professional pentesters, we must appear confident and keep our cool during these times.

24. Note-keeping

Effective note-keeping is absolutely essential skill for every pentester, because of the sheer amount of information we have to remember on daily basis.

We should cultivate this skill as our personal gardens. The items that we can put into our notebooks are:

- Methods and techniques
- Command examples
- Code snippets
- Tools and links

There are many different note-taking and wiki projects out there. My personal choice is TiddlyWiki which I've been using already for many years.

Start building your own personal knowledge base now, if you don't have one yet. Your efficiency and abilities will sky rocket as I have witnesses so many times among my coworkers.

25. Staying informed

Staying informed in the cybersecurity industry is the last essential skill every pentester should have. We should all maintain a collection of resources that keeps us up-to-date. For instance:

Conclusion

To be a professional penetration tester or a cyber security expert does not mean that you have to be a rockstar in all of these areas. If you possess a solid understanding in some of these areas and you are enthusiastic about this industry, you can easily find a suitable job for you, for example on jooble.org.

Feel free to follow me on Twitter, Facebook or subscribe to my mailing list to stay informed. I also encourage you to bookmark some of the blogs and websites mentioned here.

You can also buy me a coffee to support this website.