Pentest+2

Scoping and planning engagements.

* * *Application programming interface (API) documentation describes how software

components communicate. While APIs can be described in many ways, including via the Web Services Description Language (WSDL), tools such as Swagger, Apiary, and RAML are some of the most popular ways of developing and documenting the RESTful APIs that are part of many modern service stacks. So access to a Swagger document provides testers with a good view of how the API works and thus how they can test it.
Software development kits (SDKs) also provide documentation, and organizations may either create their own SDKs or use commercial or open-source SDKs. Understanding which SDKs are in use, and where, can help a penetration tester test applications and services.
Internal documentation may also include examples like sample application requests, API examples, or other useful code that testers can use to validate or improve their own testing. This is particularly useful for penetration tests that are directed at web applications or APIs.

**The W3C and XML-Based Standards
The World Wide Web Consortium (W3C) is an international community organization that defines web standards, including HTML, CSS, XML, web services, and many others. The W3C website at www.w3.org contains information about each of these standards.
As a penetration tester, you won't know every XML-based scheme or markup language you encounter. Fortunately, XML follows a set of standard syntax rules. Classes like w3schools.com's XML tutorial (https://www.w3schools.com/xml/default.asp) can get you started on reading XML documents if you need a quick tutorial.

**Architectural diagrams, dataflow diagrams, and other system and design documentation can provide penetration testers with an understanding of potential targets, how they communicate, and other configuration and design details.
Configuration files can be treasure troves of information and may contain details including accounts, IP addresses, and even passwords or API keys.
***Access and Accounts
White box assessments will provide direct access to the systems that are being tested. Thismay include permitting penetration testers past defenses that are normally in place. A blackbox assessment team won't have that luxury and will have to make their way past those defenses. Common security exceptions for white box tests are as follows:

Whitelisting testers in **Intrusion Prevention Systems** (IPSs), Web Application Firewalls (WAFs), and other security devices will allow them to perform their tests without being blocked. For a white box test, this means that testers won't spend time waiting to be unblocked when security measures detect their efforts. Black box and red-team tests are more likely to result in testers being blacklisted or blocked by security measures.

Security exceptions at the network layer, such as allowing testers to bypass network access controls (NACs) that would normally prevent unauthorized devices from connecting to the network.
Bypassing or disabling certificate pinning.*

***What is Certificate Pinning?
Certificate pinning associates a host with an X.509 certificate (or a public key) and then uses that association to make a trust decision. That means that if the certificate changes, the remote system will no longer be recognized and the client shouldn't be able to visit it.Pinning can cause issues, particularly if an organization uses data loss prevention (DLP) proxies that intercept traffic. Pinning can work with this if the interception proxy is also added to the pinning list, called a pinset.

Access to user accounts and privileged accounts can play a significant role in the success of a penetration test. **White box assessments** should be conducted using appropriate accounts to enable testers to meet the complete scope of the assessment. **Black box tests** will require testers to acquire credentials and access.
That means a strong security model may make some desired testing impossible—a good result in many cases, but it may leave hidden issues open to insider threats or more advanced threat actors.

[Physical access to a facility or system is one of the most powerful tools a penetration tester can have. In white box assessments, testers often have full access to anything they need to test. Black box testers may have to use social engineering techniques or other methods we will discuss later in this book to gain access.
Network access, either on site, via a VPN, or through some other method, is also important, and testers need access to each network segment or protected zone that should be assessed. T

**that means that a good view of the network in the form of a network diagram and a means to cross network boundaries are often crucial to success.Budget
Technical considerations are often the first things that penetration testers think about, but budgeting is also a major part of the business process of penetration testing. Determining a budget and staying within it can make the difference between a viable business and a failed effort.
The budget required to complete a penetration test is determined by the scope and rules of engagement (or, at times, vice versa if the budget is a limiting factor, thus determining what can reasonably be done as part of the assessment!). For internal penetration testers,

a budget may simply involve the allocation of time for the team to conduct the test. ForKey **Legal Concepts for Penetration Tests**

external or commercial testers, a **budget** normally starts from an estimated number of hours based on the complexity of the test, the size of the team, and any costs associated with the test such as materials, insurance, or other expenditures that aren't related to personnel time.

Key Legal Concepts for
Penetration Tests

Penetration testers need to understand the **legal context** and requirements around their work in addition to the technical and process portions of a penetration test. *Contracts, statements of work, NDAs, and the laws and legal requirements each state, country, or local jurisdiction enforces are all important to know and understand before starting a penetration test.*
Contracts
M**any penetration tests start with a contract,** which documents the agreement between the penetration tester and the client or customer who engaged them for the test. Some penetration tests are done with a single contract, while others are done with a s**tatement of work, or SOW, a document that defines the purpose of the work, what work will be done, what deliverables will be created,** the **timeline f**or the work to be completed, the price for the work, and any additional terms and conditions that cover the work. **Alternatives to statements of work include statements of objectives (SOOs)** and performance work statements (PWSs), both of which are used by the **US government.**
Many organizations also create a **master services agreement, or MSA,** which *defines the terms that the organizations will use for future work*. This makes ongoing engagements and SOWs much easier to work through, as the overall MSA is referred to in the SOW, preventing the need to renegotiate terms. *MSAs are common when organizations anticipate working together over a period of time or when a support contract is created.*
In addition, p*enetration testers are often asked to sign nondisclosure agreements (NDAs) or confidentiality agreements (CAs), which are legal documents that help to enforce confidential relationships between two parties*. **NDAs protect one or more parties in the relationship and typically outline the parties, what information should be considered confidential, how long the agreement lasts, when and how disclosure is acceptable, and how confidential information should be handled.**
As a penetration tester, you should also be aware o*f noncompete agreements (sometimes called noncompete clauses or covenants to not compete).* You're unlikely to have a client ask you to sign one, but your employer may! **A noncompete agreement asks you to agree not to take a job with a competitor or to directly compete with your employer in a future job,** and they are **often time-limited,** with **a clause stating that you won't take a job in the same field for a set period of time. Noncompetes are typically used to limit the chances of a competitor gaining a competitive advantage by hiring you away from your employer, but they have also been used to limit employment choices for staff members.**46

Data Ownership and Retention

When a penetration test ends, the penetration tester will typically have a significant amount of data about the target of the test. That data may include sensitive information, internal documentation, usernames, passwords, and of course the report itself with a list of findings. The ownership of this data after the test is an important consideration and should be covered in the contract, MSA, or SOW for each engagement with clear expectations of who owns the data, how it will be stored and secured, and what will be done with it after the engagement is done.

Authorization

Penetration tests also require appropriate authorization. Regardless of whether they are conducted by an internal team or as part of a contract between two parties, penetration tests need signatures from proper signing authorities. If you are conducting an internal penetration test, make sure the person who is approving the test is authorized to do so. As an external penetration tester, you may not be able to verify this as easily and thus will have to rely on the contract. At that point, indemnification language in case something goes wrong is important.

Third-Party Authorization

Additional authorization may be needed for many penetration tests, particularly those that involve complex IT infrastructure. Third parties are often used to host systems, as Software as a Service, Platform as a Service, or Infrastructure as a Service cloud providers, or for other purposes, and a complete test could impact those providers. Thus, it is important to determine what third-party providers or partners may be in scope and to obtain authorization. At the same time, you should make sure you make both your customer and the third party aware of potential impacts from the penetration test.

Environmental Differences

The laws and regulations that apply to penetration testing and penetration testers vary around the world (and even from state to state in the United States!). That means you need to understand what laws apply to the work you're doing.

T**he United Kingdom's Computer Misuse Act (CMA) of 1990 serves as an excellent example of the type of international law that a penetration tester needs to be aware of prior to conducting a test.** The CMA includes criminal penalties for unauthorized individuals who access programs or *data on computers or who impair the operation of systems. It also addresses the creation of tools that can be used as part of these violations. While the CMA primarily targets creators of malware and other malicious tools, exploit tools like the AutoSploit automated exploit tool released in 2018 could potentially be e covered by laws like this that target "dangerous" software

wait, This Tool is illegal?

I*n 2007, a new statute was added to the German Penal code. The statute was intended to implement parts of the Council of Europe Treaty on Cybercrime and focused on the creation or distribution of computer security software, making these criminal offenses. The statute, as written, appeared to make it a crime to create, obtain, or distribute any computer program that violated German's cybercrime laws. Unfortunately, the statute was* *broad enough to potentially impact many of the tools that penetration testers consider critical to their trade: password crackers, vulnerability scanning tools, and exploits.*

Section 202c

A**cts preparatory to data espionage and phishing

(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible

*1. passwords or other security codes enabling access to data (section 202a(2)), or

2. software for the purpose of the commission of such an offence,

shall be liable to imprisonment not exceeding one year or a fine.

Since the statute focused on the purpose of the tool, and not the intent of the author or distributor, possession of these tools was potentially illegal.

You can find a deeper dive into the problems that this created here:

*https://www.securityfocus.com/columnists/502.****

The Export Administration Regulations (EAR) Supplement No 1. Part 740 covers the export of encryption tools, with countries in group B having relaxed encryption export rules; D:1 countries have strict export controls, and E:1 countries are considered terrorist-supporting countries (like Cuba, Iran, and North Korea) and are also under strict export control. You can see the list at

http://www.bis.doc.gov/index.php/forms-documents/

doc_download/944-740-supp-1

Once you have reviewed local and national government restrictions and understand the laws and regulations that cover penetration testing and related activities, you should also make sure you understand the **venue** in which contract issues will be decided. In legal terms, the venue is where any legal action would occur and is often called out in the contract. In general, the venue is likely to be where your client is located, but larger organizations may specify their headquarters or another location. Jurisdiction, or the authority of law over an area, is also important, as the laws that apply to the penetration tester and the target may be different. Since penetration testers often work across state or national borders, the laws that apply in each location need to be understood.

Understanding Compliance-Based Assessments

Laws and regulations like HIPAA, FERPA, SOX, GLBA, and PCI DSS all have compliance requirements that covered organizations have to meet. That means that compliance-based assessments can bring their own set of special requirements beyond what a typical penetration test or security assessment may involve.

The PenTest+ exam specifically targets a few potential limitations and caveats related to compliance assessments, including these:

The rules to complete assessments that are set by the compliance standard. The PCI DSS standard provides examples of this, including its definition of what a cardholder data environment (CDE) penetration test should include: the entire external, public-facing perimeter as well as the LAN-to-LAN attack surfaces. Fortunately, PCI DSS provides specific guidance for penetration testing at https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.

Password policies, which are important for both the scope of the engagement and the rules of engagement. Again, the PCI DSS penetration testing guidance provides a useful example by noting that whether or not the tester must disclose all passwords they discover during their assessment is an important part of the rules of engagement and the scoping of the assessment.

Data isolation may come into play when systems that are covered by a compliance agreement or requirement are maintained separately from other elements of an organization's infrastructure. Scoping the penetration test to only validate the compliance environment can be important, but understanding how the data isolation design fits in the context of the organization's infrastructure is crucial too. Data isolation is also often an important concept to understand when dealing with third-party service providers, as a penetration tester may chase down a link to a data source or related service that resides in a third party's care if the scope of the test is not well defined and clear.

Key management testing may be required to meet a standard like the US federal government's Federal Information Processing Standard (FIPS) 140-2. The organization's practices, policies, and key management system technology may all fall into scope when assessed against requirements like FIPS 140-2. As it does in other compliance assessment areas, using third parties like Amazon's AWS means that their practices and policies may also fall into scope. Fortunately, major cloud providers frequently have pre-certified environments and can provide FIPS 140-2 compliance documentation upon request.

■■

Limited network access and limited storage access are also common in compliance-driven assessments. **PCI DSS–compliant organizations** have often isolated their card processing systems on a separate network with distinct infrastructure, *which means that access to the environment via the network and the ability to access storage or other underlying services may be highly restricted*. Penetration testers need to understand both the environment they will test and any functional or business limitations they must respect when testing in restricted compliance environments.

If your organization needs to be compliant with multiple laws and standards simultaneously, you may want to **investigate design strategies that help you to limit the scope of your assessments**. For example, an organization that had to handle both HIPAA and PCI compliance might choose to isolate their health care and credit card operations from each other, allowing each compliance center to be assessed separately to the specific standard it has to meet rather than requiring both environments to meet the standards for both

HIPAA and PCI.

What Is “Compliant”?

In some cases, compliance-based assessments can be easier to perform because they have specific requirements spelled out in the regulations or standards. Unfortunately, the opposite is often true as well—legal requirements use terms like best practice or due diligence instead of providing a definition, leaving organizations to take their best guess. As new laws are created, industry organizations often work to create common practices, but be aware that there may not be a hard and fast answer to “what is compliant” in every case.

While there are many laws and standards that you may be asked to assess against as part of a compliance-based test, a few major laws and standards drive significant amounts of penetration testing work**. *HIPAA, GLBA, SOX, PCI-DSS, and FIPS 140-2 each have compliance requirements that may drive assessments, making it important for you to be aware of them at a high level.***

HIPAA, the Health Insurance Portability and Accountability Act of 1996, does not directly require penetration testing or vulnerability scanning. It does, however, require a **risk analysis, and this requirement drives testing of security controls and practices. NIST, the National Institute of Standards and Technology, has also released guidance on implementing HIPAA (https://csrc.nist.gov/publications/detail/sp/800-66/rev-1/**final), which includes a recommendation that penetration testing should be part of theevaluation process. Thus, HIPAA-covered entities are likely to perform a penetration test as part of their normal ongoing assessment processes.

GLBA, the Gramm-Leach-Bliley Act, regulates how financial institutions handle personal information of individuals. *It requires companies to have a written information security plan that describes processes and procedures intended to protect that information, and covered entities must also test and monitor their efforts. Penetration testing may be (and frequently is) part of that testing methodology because GLBA requires financial institutions to protect against “reasonably anticipated threats”—something that is easier to do when you are actively conducting penetration tests.*

SOX, the Sarbanes-Oxley Act, is a US federal law that set standards for US public company boards, management, and accounting firms. *SOX sets standards for controls related to policy, standards, access and authentication, network security, and a variety of other requirements. A key element of SOX is a yearly requirement to assess controls and procedures, this potentially driving a desire for penetration testing.*

PCI DSS, the Payment Card Industry Data Security Standard, is an industry standard for security created by the credit card industry*. Documents related to the standard, including the standard and penetration testing guidance, can be found at https://www.pcisecuritystandards.org/document_library*

FIPS 140-2 is a US government computer security standard used to approved cryptographic modules. *These modules are then certified under FIPS 140-2 and can be assessed based on that certification and the practices followed in their* *use. Details of FIPS 140-2 can be found at https://csrc.nist.gov/Projects/**cryptographic-Module-Validation-Program/Standards.*\*

There are many other standards and regulations that may apply to an organization, making compliance-based assessments a common driver for penetration testing efforts. As you prepare to perform a penetration test, be sure to understand the compliance environment in which your client or organization operates and how that environment may influence the scope, requirements, methodology, and output of your testing.

**Penetration testers also need to know about the legal and contractual aspects of a penetration test. A contract or agreement to conduct the test is an important part of most third-party penetration tests, while internal penetration testers will typically make sure they have proper sign-off from the appropriate person in their organization. Master service agreements, SOWs, and nondisclosure agreements are all common parts of a pen-tester's path to starting an engagement.

There are often external legal and compliance requirements as well as the target organization's internal policies. Laws, regulations, and industry standards are all part of the environment that a penetration tester must navigate. In the United States, laws like HIPAA, SOX, and GLBA all drive organizations to seek penetration tests as part of the compliance efforts. Equally important, regulations such as HIPAA strictly forbid protected health information (PHI) from being accessed, even in the process of penetration testing. Industry standards like PCI DSS, and government standards like FIPS-140-2, also have specific requirements that organizations must meet and that penetration testers may be asked either to include in their scope or to specifically address as part of their test.Understand the key legal concepts related to penetration testing. Penetration testers need
to understand legal concepts like master services agreements that define the overall contract between organizations for engagements, statements of work that define the deliverables for those engagements, and nondisclosure agreements that protect the data and information involved in a penetration test. You must also be aware of the legal and regulatory environment in which both you and your target operate so that your testing process and tools are legal. Finally, it's critical to ensure that appropriate legal agreements, with approvals from proper signing authorities, are in place so that you are covered in the event of something going wrong.52

***Explain the issues, objectives, and caveats that you may encounter when conducting compliance-based assessments. Compliance, in the form of laws, regulations, and industry standards, drives many penetration tests. Understanding that laws like GLBA, HIPAA, SOX, and others have specific requirements that you may need to meet as part of your testing process will help you better complete compliance assessments. Standards like PCI DSS that require compliance from credit card merchants provide clearly defined objectives, but also have specific rules that may influence both how you conduct your assessment and the rules of engagement for the overall test.

The Information Gathering and Vulnerability Identification domain of the CompTIA PenTest+ certification exam objec-

tives covers information gathering and vulnerability scanning as well as how to analyze and utilize vulnerability scanning information. I n this chapter, you will explore how to gather information about an organization using passive open source intelligence (OSINT) as well as active enumeration and scanning methods. We will also take a look at other important techniques, including packet crafting, capture, and inspection for information gathering, in addition to the role of code analysis for intelligence gathering and related techniques.

***Scenario, Part 1*::::::
Plan for a Vulnerability Scanning
You have recently been engaged to perform a black box penetration test against MCDS, LLC. You have worked out the scope of work and rules of engagement and know that your engagement includes the organization's website and externally accessible services, as well as all systems on both wired and wireless networks in their main headquarters location. Third-party providers, services, and off-site locations are not included in the scope of the test.
Since this is a black box test, you must first identify the organization's domains, IP ranges, and other information, then build and execute an information-gathering plan.

Footprinting and Enumeration
[The first step in many penetration tests is to gather information about the organization via passive intelligence gathering methods. Passive methods are those that do not actively engage the target organization's systems, technology, defenses, people, or locations. The information gathered through this process is often called OSINT, or open-source intelligence. Among other data that can be gathered, OSINT is often used to determine the organization's footprint: a listing of all of the systems, networks, and other technology that anorganization has. Of course, if you are conducting a white box test, you may already have all of this information in the documentation provided by the target organization.

OSINT
OSINT includes data from publicly available sources, such as DNS registrars, web searches, security-centric search engines like Shodan and Censys, and a myriad of other information sources. It also includes information beyond technology-centric organizational information. Social media, corporate tax filings, public information, and even the information found on an organization's website can be part of open-source intelligence gathering.
The goal of an OSINT gathering process is to obtain the information needed to perform an effective penetration test. Since the tests will vary in scope and resources, a list of desired information is built for each engagement. That doesn't mean you can't work from a standardized list, but it does mean you need to consider the type of engagement, the information you have available, and the information you need to effectively understand your target. OSINT gathering may continue throughout an engagement as you discover additional information that you want to acquire or if you find additional in-scope items that require you to perform more research.

Resources for Testing Standards

Standards for penetration testing typically include footprinting and reconnaissance processes and guidelines. There are a number of publicly available resources, including the Open Source Security Testing Methodology Manual (OSSTM), the Penetration Testing Executing Standard, and National Institute of Standards and Technology (NIST) Special Publication 800-115, the Technical Guide to Information Security Testing and Assessment.

■■OSSTM: http://www.isecom.org/research/

■■***Penetration Testing Execution Standard: http://www.pentest-standard.org/index.php/Main_Page***

■■

SP 800-115: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf****

The Penetration Testing Execution Standard provides a very useful list of OSINT targe that can help you build out a list of potential OSINT targets.

Another type of open-source intelligence is information about vulnerabilities and other security flaws. A number of organizations work to centralize this knowledge.

Computer Emergency Response Teams (CERTs)

The PenTest+ exam objectives mention CERT (Computer Emergency Response Team); however-you should be aware of a number of CERT groups. The Carnegie Mellon

University Software Engineering Institute includes the original CERT as one of its divisions (www.cert.org). CERT tackles a broad range of cybersecurity activities, including its original incident response focus area. **The US-CERT, a**s well as other regional, national, and industry-specific computer emergency readiness teams, also provides alerts about breaking security news, threats, and other ongoing issues. Each of these CERT organizations also provides a variety of publications and serves as an information sharing hub. The U**S-CERT website is https://www.us-cert.gov/, and you can fi nd many others around the world at https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/index.cfm.**

T*he PenTest+ exam objectives specifically call out JPCERT in addition toCERT, but there are many CERT groups around the world. Another similar type of organization that provides centralized information-sharing capabilities is* I**SACs, or Information Sharing and Analysis Centers**. *These are typically industry-centric and can provide more focused information for a specific group. The National Council of ISACs is a good place to start when looking for information about them:*

https://www.nationalisacs.org/member-isacs

NIST

The National Institute of Standards and Technology (NIST) *provides standards, resources, and frameworks for cybersecurity.* **From a penetration tester’s viewpoint, SP 800-115, the Technical Guide to Information Security Testing and Assessment, is a critical guidance**

document, particularly if you do work with the US government or a government contractor. You can read all of SP 800-115 at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

MITRE

The MITRE corporation is a US not-for-profit corporation that performs federally funded research and development. Among the tools it has developed or maintains are a number of classification schemes useful to penetration testers:

■✓

T**he *Common Attack Pattern Enumeration and Classification (CAPEC*) list is a resource intended to help identify and document attacks and attack patterns. It allows users to search attacks by their mechanism or domain and then breaks down each attack by various attributes and prerequisites. It also suggests solutions and mitigations, which means it can be useful for identifying controls when writing a penetration test report. Reading through CAPEC can also help testers identify attack methods theymay have missed, and it can also be useful for developing new attacks. CAPEC can be found at https://capec.mitre.org.

The Common Vulnerabilities and Exposures (CVE) list identifies vulnerabilities by name, number, and description. This makes the job of a penetration tester easier, as vendors, exploit developers, and others can use a common scheme to refer to vulnerabilities. A *CVE listing will be in the format CVE-[YEAR]-[NUMBER]. For example, the 2017 Meltdown bug was assigned CVE-2017-5754, while Spectre is covered by CVE-2017-5754 and CVE-2017-5715. You can read more at* https://www.cve *.mitre.org.*

The Common Weakness Enumeration (CWE) is another community-developed list. *CWE tackles a broad range of software weaknesses and breaks them down by research concepts, development concepts, and architectural concepts. Like CAPEC, it describes each weakness and how it can be introduced to code, what platforms it applies to, and what happens when something goes wrong. Also like CAPEC, it includes mitigation suggestions. You can read more about CWE at* https://cwe.mitre.org*.*

The PenTest+ exam outline specifically mentions Full Disclosure, but practitioners who want to track up-to-the-minute vulnerability and exploit information will want to follow multiple sources. The authors of this book recommend a combination of Twitter feeds and other social media (including active Facebook and LinkedIn groups), mailing list subscriptions, and poscasts and other information. Much like

the CERT sites, the ISC is a clearinghouse for security events and information. SANS also operates a regularly updated penetration testing blog at=

https://pen-testing.sans.org/blog/pen-testing.sibly commercial vulnerability feeds if you need to stay up the minute

on exploits.

Full Disclosure

The Full Disclosure mailing list has been a popular discussion location for security practitioners for years, although it has begun to slow down with the advent of other sources, like Twitter, for disclosure. You may still want to subscribe at http://seclists.org/fulldisclosure/. The list also tweets at https://twitter.com/seclists, and there are many other lists hosted via http://seclists.org that may be of interest to a security practitioner.

Internet Storm Center (ISC) and the **SANS Pen-Testing Blog**

The SANS Internet Storm Center leverages daily handlers who publish diaries about security topics and current issues, as well as pod

Scenario Part 2: Scoping the Penetration Test

To scope the penetration test that you are performing for MCDS, you need to determine the following items:

■■What domain names does MCDS own?

■■What IP ranges does MCDS use for its public services?

■■What email addresses can you gather?

In addition, you should be able to answer the following questions:

■■What does the physical location look like, and what is its address?

■■What does the organization's staff list and org chart look like?

■■What document metadata can you gather?

■■What technologies and platforms does MCDS use?

■■Does MCDS provide remote access for staff?

■■What social media and employee information can you find?

Location and Organizational Data

While penetration testers may be tempted to simply look at the networks and systems that an organization uses as targets, some penetration tests require on-site testing. That may take the form of social engineering engagements or in-person security control testing, wireless or wired network penetration, or even dumpster diving to see what type of paper records and other information the tester can recover. Each of those activities means that a tester may need to know more about the physical locations and defenses that a target has in place.

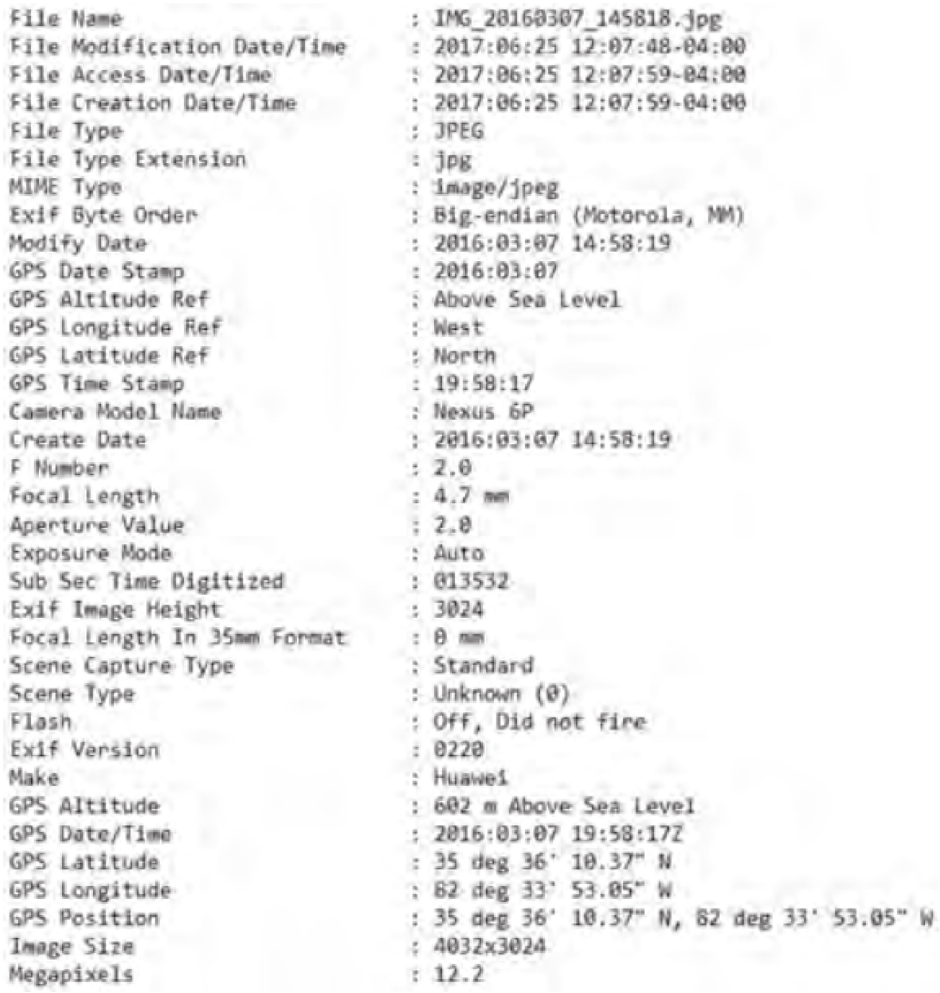
T**esters will typically start by working to understand what buildings and property the target organization use**s. *A black box test can make this harder, but public records can help by providing ownership and tax records.* These records provide contact persons, whose details could help later. Additional physical location information that a tester will look for usually includes the **physical security design**, including locations of *cameras, entrances and exits, guards, fences, and other physical security controls like badges or entry access systems.*

*At this point in the information-gathering process, it isn't uncommon to find out that the organization has other locations, subsidiaries, or remote sites. This will help you to identify Footprinting and Enumeration|some of the organization's structure, but you will usually need to search for more informa-tion to really understand how the target is logically structured.

Electronic Documents

Electronic documents can often help you understand how an organization is structured. They can also provide a wealth of other information, ranging from technologies used to staff names and email addresses, as well as internal practices and procedures. In addition to the information that is contained in the documents, many penetration testers will also carefully review the document metadata to identify additional useful information. Tools like ExifTool are designed to allow you to quickly and easily view document metadata, as shown in Figure 3.1, **which shows the metadata from a photo taken with a Nexus 6P phon**e.

FIGURE 3.1 ExifTool metadata with location



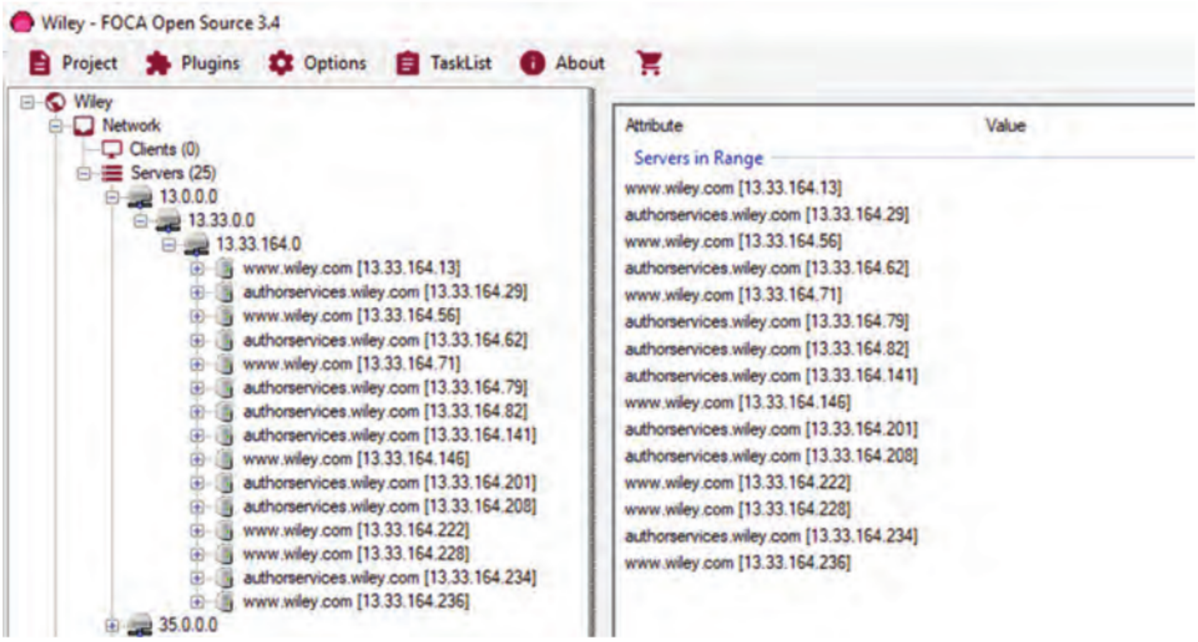
```
File Name                       : IMG_20160307_145818.jpg
File Modification Date/Time     : 2017:06:25 12:07:48-04:00
File Access Date/Time           : 2017:06:25 12:07:59-04:00
File Creation Date/Time         : 2017:06:25 12:07:59-04:00
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Modify Date                     : 2016:03:07 14:58:19
GPS Date Stamp                  : 2016:03:07
GPS Altitude Ref                : Above Sea Level
GPS Longitude Ref               : West
GPS Latitude Ref                : North
GPS Time Stamp                  : 19:58:17
Camera Model Name               : Nexus 6P
Create Date                     : 2016:03:07 14:58:19
F Number                        : 2.0
Focal Length                    : 4.7 mm
Aperture Value                  : 2.0
Exposure Mode                   : Auto
Sub Sec Time Digitized          : 013532
Exif Image Height               : 3024
Focal Length In 35mm Format     : 0 mm
Scene Capture Type              : Standard
Scene Type                      : Unknown (0)
Flash                           : Off, Did not fire
Exif Version                    : 0220
Make                            : Huawei
GPS Altitude                    : 602 m Above Sea Level
GPS Date/Time                   : 2016:03:07 19:58:17Z
GPS Latitude                    : 35 deg 36' 10.37" N
GPS Longitude                   : 82 deg 33' 53.05" W
GPS Position                    : 35 deg 36' 10.37" N, 82 deg 33' 53.05" W
Image Size                      : 4032x3024
Megapixels                      : 12.2
```

I**n addition to tools like ExifTool that excel at exposing metadata for individual files, metadata scanning tools like Fingerprinting Organizations with Collected Archives (FOCA) can be used to find metadata.** *FOCA scans using a search engine—either Google, Bing, or DuckDuckGo—and then compiles metadata information from files like Microsoft Office documents, PDF files, and other file types like SVG and InDesign files.* Figure 3.2 *shows FOCA gathering server information. Once servers are identified, metadata, including detail on users, folders, software, email, operating systems, passwords, and servers, can be automatically gathered.

Figure 3.2

FOCA metadata acquisition

FIGURE 3.2 FOCA metadata acquisition



```
Wiley
  Network
    Clients (0)
    Servers (25)
      13.0.0.0
        13.33.0.0
          13.33.164.0
            www.wiley.com [13.33.164.13]
            authorservices.wiley.com [13.33.164.29]
            www.wiley.com [13.33.164.56]
            authorservices.wiley.com [13.33.164.62]
            www.wiley.com [13.33.164.71]
            authorservices.wiley.com [13.33.164.79]
            authorservices.wiley.com [13.33.164.82]
            authorservices.wiley.com [13.33.164.141]
            www.wiley.com [13.33.164.146]
            authorservices.wiley.com [13.33.164.201]
            authorservices.wiley.com [13.33.164.208]
            www.wiley.com [13.33.164.222]
            www.wiley.com [13.33.164.228]
            authorservices.wiley.com [13.33.164.234]
            www.wiley.com [13.33.164.236]
      35.0.0.0
```

```
Attribute                                   Value
Servers in Range
www.wiley.com [13.33.164.13]
authorservices.wiley.com [13.33.164.29]
www.wiley.com [13.33.164.56]
authorservices.wiley.com [13.33.164.62]
www.wiley.com [13.33.164.71]
authorservices.wiley.com [13.33.164.79]
authorservices.wiley.com [13.33.164.82]
authorservices.wiley.com [13.33.164.141]
www.wiley.com [13.33.164.146]
authorservices.wiley.com [13.33.164.201]
authorservices.wiley.com [13.33.164.208]
www.wiley.com [13.33.164.222]
www.wiley.com [13.33.164.228]
authorservices.wiley.com [13.33.164.234]
www.wiley.com [13.33.164.236]
```

Microsoft Office files, PDFs, and many other types of common business files include metadata that can be useful, ranging from authors and creation dates/times to software versions. In many cases, the metadata of a file can be as useful, or more so, than its actual text or other data!

It is important to remember that the electronic documents that are currently accessible are not the only documents that you can recover for an organization. **Web archives like the Internet Archive (https://archive.org) provide point-in-time snapshots of websites and other data. Even when organizations think that they have removed information from the Web, copies may exist in the Internet Archive or elsewhere, including search engine caches and other locations.**

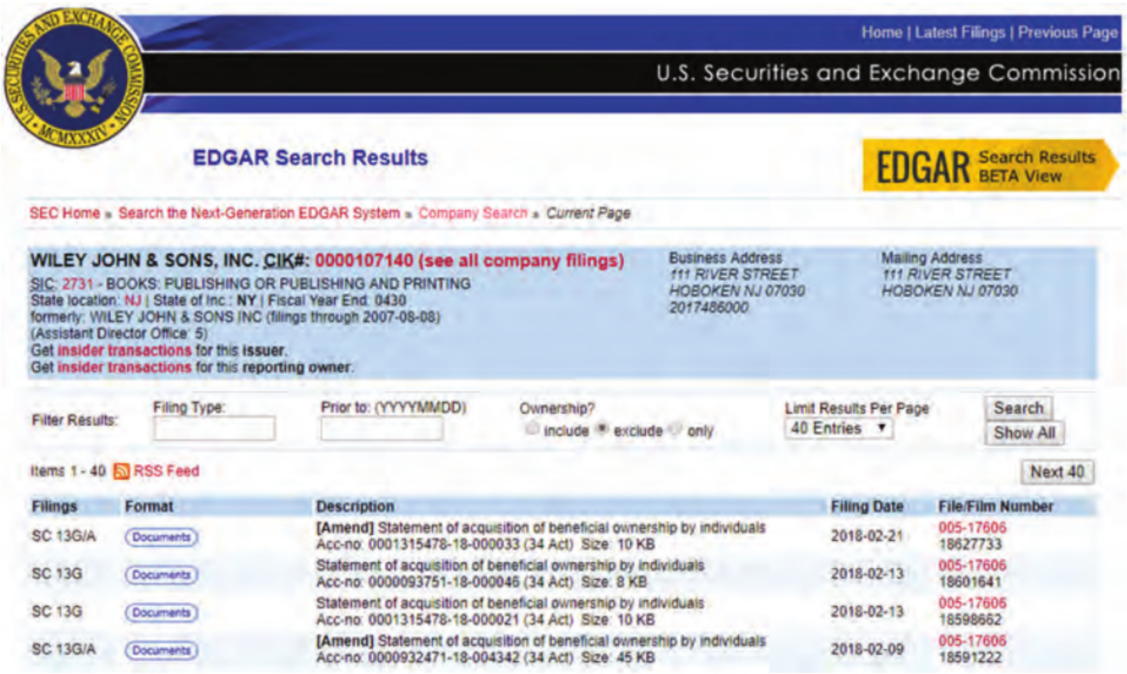
Financial Data

Financial disclosures, tax information, and other financial documents can provide additional information for motivated pen-testers. **The US Securities and Exchange Commission provides the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system, a service that allows you to look up SEC filings. As you can see in Figure 3.3, an EDGAR search can quickly provide information like a corporate address, as well as other details found in individual filings.

Employees

Finding out who is employed by an organization can sometimes be as simple as using an online directory or checking its posted organizational charts. In most cases, identifying employees will take more work. Common techniques include leveraging social media like
LinkedIn and Facebook, as well as reviewing corporate email addresses, publications, and public records. Social engineering techniques can also be useful, particularly when searching for information on a specific individual or group

FIGURE 3.3 SEC reporting via EDGAR


Home | Latest Filings | Previous Page
U.S. Securities and Exchange Commission
EDGAR Search Results BETA View
SEC Home » Search the Next-Generation EDGAR System » Company Search » Current Page
Search
Show All
Next 40
Documents

EDGAR Search Results

WILEY JOHN & SONS, INC. CIK#: 0000107140 (see all company filings)
SIC: 2731 - BOOKS: PUBLISHING OR PUBLISHING AND PRINTING
State location: NJ | State of Inc.: NY | Fiscal Year End: 0430
formerly: WILEY JOHN & SONS INC (filings through 2007-08-08)
(Assistant Director Office: 5)
Get insider transactions for this issuer.
Get insider transactions for this reporting owner.

Business Address
111 RIVER STREET
HOBOKEN NJ 07030
2017486000

Mailing Address
111 RIVER STREET
HOBOKEN NJ 07030

Filter Results: Filing Type: Prior to: (YYYYMMDD) Ownership? ○ include ● exclude ○ only Limit Results Per Page 40 Entries ▾

Items 1 - 40 RSS Feed

Filings	Format	Description	Filing Date	File/Film Number
SC 13G/A	Documents	[Amend] Statement of acquisition of beneficial ownership by individuals Acc-no: 0001315478-18-000033 (34 Act) Size: 10 KB	2018-02-21	005-17606 18627733
SC 13G	Documents	Statement of acquisition of beneficial ownership by individuals Acc-no: 0000093751-18-000046 (34 Act) Size: 8 KB	2018-02-13	005-17606 18601641
SC 13G	Documents	Statement of acquisition of beneficial ownership by individuals Acc-no: 0001315478-18-000021 (34 Act) Size: 10 KB	2018-02-13	005-17606 18598662
SC 13G/A	Documents	[Amend] Statement of acquisition of beneficial ownership by individuals Acc-no: 0000932471-18-004342 (34 Act) Size: 45 KB	2018-02-09	005-17606 18591222

Infrastructure and Networks

Infrastructure and Networks

Information about the infrastructure, technologies, and networks that an organization uses is often one of the first things that a penetration tester will gather in a passive information search. Once you have a strong understanding of the target, you can design the next phase of your penetration test.

External footprinting is *part of most passive reconnaissance and is aimed at gathering information about the target from external sources. That means gathering information about domains, IP ranges, and routes for the organization.*

Domains

Domain names are managed by domain name registrars. Domain registrars are accredited by **generic top-level domain (gTLD**) registries and/or **country code top-level domain (ccTLD) registries****. This means that registrars work with the domain name registries to provide registration services—the ability to acquire and use domain names. Registrars provide the interface between customers and the domain registries and handle purchase, billing, and day-to-day domain maintenance, including renewals for domain registrations.68

The Domain Name System is often one of the first stops when gathering information about an organization. Not only is DNS information publicly available, it is often easily con-Not only is DNS information publicly available, it is often easily connected to the organization by simply checking for WHOIS information about its website. With that information available, you can find other websites and hosts to add to your organizational footprint.

WHOIS

Domain ownership and registration is maintained by registrars, with each registrar covering a specific portion of the world. The central authority is the Internet Assigned Numbers Authority, or IANA. IANA manages the DNS root zone and thus is a good starting place for searches at https://www.iana.org. Once you know which regional authority you should query, you can select the appropriate site to visit:

■**✓AFRINIC (**Africa): http://www.afrinic.net

■✓APNIC (Asia/Pacific): http://www.apnic.net

■✓ARIN (North America, parts of the Caribbean, and North Atlantic islands): http://ws.arin.net

■✓LACNIC (Latin America and the Caribbean): http://www.lacnic.net

■✓RIPE (Europe, Russia, the Middle East, and parts of central Asia): http://www .ripe.net

Each of the regional NICs provides a **WHOIS service. WHOIS** allows you to search databases of registered users of domains and IP address blocks and can provide useful information about an organization or individual based on their registration information.

In the sample WHOIS query for Google shown in Figure 3.4, you can see that information about Google, like the company's headquarters location, contact information, and its primary name servers, is all returned by the WHOIS query.

In addCOMPTIA ---6

ition, external DNS information for an organization is provided as part of its WHOIS information, providing a good starting place for DNS-based information gathering. Additional DNS servers may be identified either as part of active scanning, gathering passive information based on network traffic or logs, or even by reviewing an organization's documentation.

Other information can be gathered by using the host command in Linux, which will *provide information about a system's IPv4 and IPv6 addresses as well as its email (MX) servers, as shown in Figure 3.5. It's important to note that if you ran the same command for www.google.com, you would not see the email servers associated with google.com!

Many domain owners reduce the amount of visible data after their domains have been registered for some time, meaning that historical domain registration information can be a treasure trove of useful details. Services like domainhistory.net and whoismind.com provide a historical view of the domain registration information provided by WHOIS, which means that you can still find that information

DNS and Traceroute Information

The DNS converts domain names like google.com to IP addresses and IP addresses to domain names. The command for this on Windows, Linux, and MacOS systems is Nslookup.

Figure 3.6 shows the results of an Nslookup for netflix.com. Like many major websites, Netflix uses a content delivery network, which means that looking up www.netflix.com resolves to multiple hosts. The Netflix infrastructure is smart enough to point this lookup to a US region based on where the Nslookup was run from. If you run the same command in another part of the world, you’re likely to see a different answer!

Figure 3.6

Nslookup for netflix.com

Zone Transfers

A DNS zone transfer (AXFR) is a transaction that is intended to be used to replicate DNS databases between DNS servers. Of course, this means that the information contained in a zone transfer can provide a wealth of information to a penetration tester and that most DNS servers will have zone transfers disabled or well protected. Knowing how to conduct a zone transfer is still a potentially useful skill for a pen-tester, and you should know the three most common ways to conduct one:

■■

Host:

```
host -t axfr domain.name dns-server
```

■■

Dig:

```
dig axfr @target.nameserver.com domain.name
```

■■

Nmap (using the Nmap scripting engine or NSE):

```
nmap –script dns-zone-transfer.nse –script-args
dns-zone-transfer.domain -p53
```

A zone transfer will show you quite a bit of data, including the name server, primary contact, serial number, time between changes, the minimum time to live for the domain, MX records, name servers, latitude and longitude, and other TXT records, which can show a variety of useful information. Of course, the zone transfer will also contain service records, IP address mappings, and other information too.

**^^^^^^^^

If you’d like to practice zone transfers, Robin Wood provides a domain you can practice with. *You can find details, as well as a great walk-through of what a zone transfer will include, at https://digi.ninja/projects/zonetransferme.php.*

If a zone transfer isn’t possible, DNS information can still be gathered from public DNS by brute force. You can do this by sending a DNS query for each IP address that the organization uses, thus gathering a useful list of systems.

IP Ranges

Once you know the IP address that a system is using, you can look up information about the IP range it resides in. That can provide information about the company or about the hosting services it uses.

The IP address or hostname can also be used to gather information about the network topology around the system or device that has a given IP address. One of the first stops once you have an IP address is to look up who owns the IP range. You can do this at sites like https://www.whois.com/whois/. If you check the final IP address we found in Figure 3.6 (52.41.111.100), you can see that it is owned by Amazon, as shown in Figure 3.7. If we were doing a penetration test of Netfl ix's networks, scanning Amazon might be a violation of our rules of engagement or scope, so this sort of research and review is important!

fIGure3.7

WHOIS of 52.41.111.100

Now that we know who owns it, we can also explore the route to the IP. Using traceroute (or tracert on Windows systems), you can see the path packets take to the host. Since the Internet is designed to allow traffic to take the best path, you may see multiple different paths on the way to the system, but you will typically fi nd that the last few responses stay the same. These are often the local routers and other network devices in an organization's network, and knowing how traffic gets to a system can give you insight into their internal network topology. In Figure 3.8, you can see that in a traceroute for www.netflix.com, some systems don't respond with hostname data, as shown by the asterisks and "request timed out" entries, and that the last two systems return only IP addresses.

tracert of www.netflix.com

Routes

A final type of network information that you may look for is routing information.

The

routing information for an organization can provide insight into how their external network connectivity is set up. Public BGP route information servers known as BGP looking glasses make that information easily accessible. You can find a list of them, including both global and regional servers, at http://www.bgp4.as/looking-glasses.

Help! I'm Drowning in Data!

A variety of tools can help with gathering, aggregating, and analyzing the massive amounts of data that you are likely to acquire during the information-gathering stage of a penetration test.

****Examples include theHarvester, a tool designed to gather emails,**

domain information, hostnames, employee names, and open ports and banners using search engines and Maltego, which builds relationship maps between people and their ties to other resources. Recon-ng is an OSINT gathering tool that allows you to automate information gathering in a Metasploit-like tool with plug-ins to do many types of searches. It's worth noting that while using a tool like theHarvester can help simplifysearches of large datasets, it is not a complete substitute for a human's creativity.

**Security Search Engines

A quick way to search for exposed systems belonging to an organization by domain or IP address is to use a security search engine. These search engines provide a way to review hosts, services, and other details without actively probing networks yourself.Footprinting and Enumeration

Shodan

Shodan is one of the most popular security search engines and provides pre-built searches as well as categories of search for industrial control systems, databases, and other common search queries. Figure 3.9 shows results from a host identified with Shodan. Note that this result tells us that the target has a Cisco device with a default password enabled—a quick hit for a penetration tester!

Shodan tracert of www.netflix.com

Censys

Much like Shodan, Censys is a security-oriented search enShodan is one of the most popular security search engines and provides pre-built searches
as well as categories of search for industrial control systems, databases, and other common search queries. Figure 3.9 shows results from a host identified with Shodan. Note that this result tells us that the target has a Cisco device with a default password enabled—a quick hit for a penetration tester!

Shodan tracert of www.netflix.com

Censys

Much like Shodan, Censys is a security-oriented search engine. When you dig into a host in Censys, you will also discover geoIP information if it is available, a comprehensive summary of the services the host exposes, and drill-down links for highly detailed information. Figure 3.10 shows the same exposed Cisco IOS host we saw in Figure 3.9, this time from a broader view.74

Security search engines may not always have completely up-to-date information, so they're not the final answer for a penetration tester, but they are a very effective early step in passive information gathering and analysis. Prior to the creation of Shodan, Censys, and other search engines, gathering this type of data would have required active scanning by a penetration tester. Now, testers can gather useful information without interaction!

Active Reconnaissance and Enumeration

Building a list of all of the resources or potential targets of a specific type is important in this state of a penetration test. Once sufficient open-source intelligence has been gathered, testers typically move on to an active reconnaissance stage with the goal of first building, then narrowing down the list of hosts, networks, or other targets. Techniques for each of these vary, so you will need to be familiar with each of the following methods.Active Reconnaissance and Enumeration
7

Hosts

Enumerating hosts on a network may be the first task that most penetration testers think of when they prepare to assess a target. Active scans can identify many hosts, and it can be tempting to just rely on port scanners to identify hosts, but there are quite a few other ways to identify hosts on a network, and combining multiple methods can help to ensure that you didn't miss systems. A couple of other ways to identify systems to keep in mind are as follows:

■■

- Leveraging central management systems like SCCM, Jamf Pro, or other tools that maintain an inventory of systems, their IP addresses, and other information.

Network logs and configuration files can provide a wealth of information about systems on a network. Logs from DHCP servers can be particularly valuable, as most modern networks rely heavily on DHCP to issue addresses to network connected systems. Router logs, ARP tables, and other network information can also be very valuable.

In a black box test, you typically won’t be able to get this type of information until later in the test, if you can capture it at all. That doesn’t mean you should ignore it, but it does mean that port scanning remains the first technique that many penetration testers will attempt early in an engagement.

Services

Service identification is one of the most common tasks that a penetration tester will perform while conducting active reconnaissance. Identifying services provides a list of potential targets, including vulnerable services and those you can test using credentials you have available, or even just to gather further information from. Service identification is often done using a port scanner.

Port scanning tools are designed to send traffic to remote systems and then gather responses that provide information about the systems and the services they provide. Therefore, port scans are often one of the first steps in a penetration test of an organization.

While there are many port scanners, they almost all have a number of common features, including these:

- Host discovery
- Port scanning and service identification
- Service version identification
- Operating system identification

An important part of port scanning is an understanding of common ports and services. While ports 0–1023 are known as “well-known ports” or “system ports,” there are quite a few higher ports that are commonly of interest when conducting port scanning. Ports ranging from 1024 to 49151 are registered ports and are assigned by IANA when requested. Many are also used arbitrarily for services. Because ports can be manually assigned, simply76

assuming that a service running on a given port matches the common usage isn’t aassuming that a service running on a given port matches the common usage isn’t always a good idea. In particular, many SSH and HTTP/HTTPS servers are run on alternate ports, either to allow multiple web services to have unique ports or to avoid port scanning that only targets their normal port.

Table 3.1 lists some of the most commonly found interesting ports.

You will want to memorize Table 3.1 as well as the common operating system–specific ports. For example, you should be able to identify a system with TCP ports 139, 445, and 3389 all open as being likely indicators of a Windows system. Don’t worry; we have included practice questions like this at the end of this chapter and in the practice tests to help you practice!

TaBle 3.1

Common ports and services

Port	TCP/UDP	Service
20	TCP, UDP	FTP data
21	TCP, UDP	FTP control
22	TCP, UDP	SSH
23	TCP, UDP	Telnet
25	TCP, UDP	SMTP (email)
53	UDP	DNS
67	TCP, UDP	DHCP server
68	TCP, UDP	DHCP client
69	TCP, UDP	TFTP
80	TCP, UDP	HTTP
88	TCP, UDP	Kerberos
110	TCP, UDP	POP3
123	TCP, UDP	NTP
135	TCP, UDP	Microsoft EPMAP
Port	TCP/UDP	Service
136-139	TCP, UDP	NetBIOS
143	TCP	IMAP
161	UDP	SNMP
162	TCP, UDP	SNMP traps
389	TCP, UDP	LDAP
443	TCP, UDP	HTTPS
445	TCP	Microsoft AD and SMB
500	TCP, UDP	ISAKMP, IKE
515	TCP	LPD print services
1433	TCP	Microsoft SQL Server
1434	TCP, UDP	Microsoft SQL Monitor
1521	TCP	Oracle database listener
1812, 1813	TCP, UDP	RADIUS

*hjghjk

The ability to identify a service can provide useful information about potential vulnerabilities as well as verifying that the service that is responding on a given port matches the service that typically uses that port. Service identification is usually done in one of two ways: either by connecting and grabbing the banner or connection information provided by the service or by comparing its responses to the signatures of known services.

Operating System Fingerprinting

The ability to identify an operating system based on the network traffic that it sends is known as operating system fingerprinting, and it can provide useful information when performing reconnaissance. This is typically done using TCP/IP stack fingerprinting techniques that focus on comparing responses to TCP and UDP packets sent to remote hosts. Differences in how operating systems and even operating system versions respond, what TCP options they support, the order in which they send packets, and a host of other details can often provide a good guess at what OS the remote system is running. Figure 3.11 showsan OS identification test against the scanme.nmap.org sample host. Note that in this case, the operating system identification has struggled to identify the host, so our answer isn't as clear as you might expect.

Figure 3.11

Nmap scan using OS identification

The PenTest+ exam objectives contain an entire subsection (4.1) on the use of Nmap in information-gathering scenarios. Nmap is the most commonly used command-line vulnerability scanner and is a free, open-source tool. It provides a broad range of capabilities, including multiple scan modes intended to bypass firewalls and other network protection devices. In addition, it provides support for operating system fingerprinting, service identification, and many other capabilities.

Using Nmap's basic functionality is quite simple. Port scanning a system merely requires that Nmap is installed and that you provide the target system's hostname or IP address. Figure 3.12 shows an Nmap of a Windows 10 system with its firewall turned off. A series of common Microsoft ports are shown, as Nmap scanned 1,000 of the most commonly used ports as part of its default scan.ff

A more typical Nmap scan is likely to include a number of Nmap's command-line flags:

■■

A scan technique, like TCP SYN, Connect, ACK, or other methods. By default, Nmap uses a TCP SYN scan (-sS), allowing for fast scans that tend to work through most firewalls. In addition, sending only a SYN (and receiving a SYN/ACK) means that the TCP connection is not fully set up. TCP connect (sometimes called "full connect") scans (-sT) complete the TCP three-way handshake and are usually used when the user account using Nmap doesn't have the privileges needed to create raw packets—a common occurrence for penetration testers who may not have gained a privileged account yet during a test.

A final common scan technique flag is the -sU flag, used to conduct a UDP-only scan.

If you just need to scan for UDP ports, this flag allows you to do so.

Active Reconnaissance and Enumeration

Nmap provides a multitude of features, and many flags. You'll need to know quite a few of the common ones, as well as how a typical Nmap command line is constructed, for the exam. Make sure you practice multiple types of scans and understand what their results look like and how they differ. ■✓A port range, either specifying ports or including the full 1–65535 range. ■✓Service version detection using the –sV flag. ■✓OS detection using the –O flag. **■✓Disabling Ping using the -Pn flag. ■✓ ■✓ ■✓ The aggressiveness of the scan via the -T timing flag.** The timing flag can be set either using a numeric value from 0 to 5 or via the flag's text representation name. If you use a number, 0 will run an exceptionally slow scan, while 5 is a very fast scan. The text rep- resentation of these flags, in order, is paranoid|sneaky|polite|normal|aggressive|insane. Some testers will use a paranoid or sneaky setting to attempt to avoid intrusion detec- tion systems or to avoid using bandwidth. As you might suspect, -T3, or normal, is the default speed for Nmap scans. Input from a target file using -IL. Output to a variety of formats. You will want to be familiar with the -oX XML output flag, the -oN “normal” output mode, and even the outdated -oG greppable (searchable) format, which XML has almost entirely replaced. *The -oA file, or “all” output mode, accepts a base filename and outputs normal, XML, and greppable formats all at the same time as basename.nmap, basename.xml, and basename.gmap. If you use multiple tools to interface with your Nmap results, this can be a very useful option! Figure 3.12 shows a sample default scan of a Windows system with its firewall turned off. There are a number of additional services running on the system beyond typical Windows services, but we can quickly identify ports 135, 139, and 445 as typical Windows services. f I G u r e 3 .1 2 Nmap output of a Windows 10 systemChapter 3* ■ *Information Gathering*

Nmap also has an official graphical user interface, known as Zenmap , which provides additional visualization capabilities, including a topology view mode that provides information about how hosts fit into a network. Nmap usage is an important part of almost any penetration test. That means that you should be able to read an Nmap command line and identify what is occurring. For exam- ple, a typical command line might look like this==: nmap -sT -sV -Pn -p 1-65435 -T2 -oA s==canme scanme.nmap.org To understand what this command will do, you will need to understand each of the flags and how the command line is constructed. From left to right, we see that this is a TCP con- nect scan (-sT), that we are attempting to identify the services (-sV), that it will not send a ping (-Pn), that it is scanning a port range from 1–65435 using the -p port selection flag, that the timing is slower than normal with the -T2 flag, and fi nally that this scan will send its output to fi les called scanme.nmap, scanme.xml, and scanme.gmap when it is done. The last part of the command is the target’s hostname: scanme.nmap.org. If you read that command line carefully, you may have noted that the port specification doesn’t actually cover all 65,535 ports—in fact, we specified 65,435! Typos and mistakes happen, and you should be prepared to identify this type of issue in questions about port and vulnerability scans. If you want to practice your Nmap techniques, you can use scanme.nmap.org as a scan target.

The people who provide the service ask that you use it for test scans and that you don’t hit them with abusive or heavy usage. You may also want to set up other scan targets using tools like Rapid 7’s Metasploitable virtual machine (https://information.rapid7 .com/metasploitable-download.html), which provides many interesting services to scan and exploit. scenario, part 2 Now that you have identified the organization’s external IP addresses, you are ready to conduct a scan of its systems. A member of your team suggests running the following nmap scan against your client’s network range from your testing workstations: nmap -sT -T0 10.11.42.0/23Active Reconnaissance and Enumeration 81 Make sure you can answer the following questions: ■✓ ■✓ ■✓ ■✓ ■✓ If the client organization’s IP range is 10.11.42.0/24, what would this command do? What flags would you recommend that you use to identify the services and operating systems found in that scan? Is the TCP connect scan the correct choice, and why? What ports would the command your team member suggested scan, and what might

this mean for your penetration test? What other improvements might you make to this scan?

- *Networks, Topologies, and Network Traffic At the beginning of a black box penetration test, you will know very little about the net- works, their layout and design, and what traffic they may carry. As you learn more about the target's network or networks,* **you can start to lay out a network topology or logical design. Knowing how a network is laid out and what subnets, network devices, and secu- rity zones exist on the network can be crucial to the success of a penetration test. Network Topology Understanding the topology, or layout, of a network helps a penetration tester design their scanning and attack process. A topology map can provide information about what systems and devices are likely to be accessible, thus helping you make decisions about when to pivot to a different target to bypass security controls. Topology diagrams can be generated using tools like the Zenmap GUI for Nmap as well as purpose-built network topology mapping programs. While a Zenmap topology diagram as shown in Figure 3.13 isn't always com- pletely accurate, it can be very helpful when you are trying to picture a network. Using scanning data to create a topological diagram has a number of limitations. Since you are using the time-to-live information and response to scans to determine what the network looks like, firewalls and other net- work devices can mean that your topology will not match reality. Alwaysremember that an Nmap scan will only show you the hosts that respond and that other hosts and networks may exist! Eavesdropping and Packet Capture In addition to actively scanning for hosts and gathering topology information, penetra- tion testers will also gather information using eavesdropping with packet capture or sniffer tools. Tools like Wireshark are often used to passively gather information about a network, including IP addresses, MAC addresses, time to live for packets, and even data about ser- vices and the content of traffic when it is unencrypted.**