Carnegie Mellon University
Software Engineering Institute

PENETRATION TESTS ARE THE CHECK ENGINE LIGHT ON YOUR SECURITY OPERATIONS

Allen Householder, Dan Klinedinst

February 2019

Introduction

In 2008, one of this paper's authors was driving to the hospital to visit a close family member when the check engine light came on. At that moment, getting to the hospital took precedence over attending to the vehicle, so he kept driving. Within minutes, however, the light started flashing, and the engine began to sputter as he waited at a traffic light. Luckily, he was close enough to the hospital that he was able to arrive and visit with his family member while he waited for a tow truck. An ignition coil had failed, and the car needed urgent service to remediate the problem. The manufacturer eventually recalled the affected component, and the vehicle was eligible for reimbursement for the repair.

The check engine light on a car serves two purposes: (1) it lights up to alert you that one of the many sensors in your vehicle has detected a non-critical fault that requires your attention, and (2) it begins flashing to alert you of the need for immediate remediation. In both cases, the check engine light is a symptom of a failure in an upstream process. For example, the system might detect a vapor leak if the driver neglects to replace the gas cap. Or, a limited lifetime component could fail under normal operation if the owner neglects to perform a regular maintenance task. Or, as in the example above, the car could have a manufacturing defect whose root cause might only be known to the manufacturer.

You might ask, "What does this example have to do with cybersecurity penetration testing?" The answer is that, just as the check engine light serves as a lagging indicator of a vehicle-production or maintenance-quality problem, a penetration test serves as a lagging indicator of a network security operations problem. Organizations should implement and document several security controls before a penetration test can be useful.

Summary: Verify that Security Controls Are in Place Before Testing Them

Penetration testing is a way of testing your security controls against realistic attacks. However, it assumes that you have a known set of controls to test. Just as you wouldn't build a vehicle maintenance plan based on the check engine light alone, it's suboptimal to start improving network security operations with a penetration test.

The list below includes a set of controls that your organization should ideally have in place before it seeks out a penetration test. The ascending order in which the controls appear roughly reflects organizational maturity.

1. Maintain Documented Security Policies
2. Document and Inventory Your Networks
3. Document and Inventory Applications (Especially Web Applications)
4. Analyze Your Internet Attack Surface
5. Document Third-Party Access to Your Networks and Assets
6. Scan for the Most Common and Known Vulnerabilities
7. Document, Mitigate, or Patch Vulnerabilities
8. Monitor Email for Malicious Attachments
9. Perform Security Testing of Web Applications
10. Manage Wi-Fi and BYOD

In our experience, if your organization lacks these capabilities, a penetration test will prove only that you don't have them. However, the external validation that a penetration test provides can actually be useful for proving to leadership that you need to invest in them.

The remainder of this document briefly covers each of the items above, accompanied by references to relevant documentation drawn from the NIST Risk Management Framework (RMF), the Cybersecurity Framework v1.1 (CSF), and their respective supporting documents. We conclude with a summary of next steps and pointers to more information on penetration testing as well as a list of works cited.

Detailed List of Recommended Security Controls

In this section, we provide an annotated list of information about the security controls listed in the preceding summary.

1. Maintain Documented Security Policies

Organizations should document their security policies and requirements. Doing so provides organizations with a baseline of expectations against which to compare any subsequent evaluation results. Without it, prioritizing the organization's response to findings can be difficult.

Table 1: Security Policy References

Reference	Section	Summary
NIST SP 800-37 revision 2	Task P-15	*Requirements Definition*: Define the security and privacy requirements for the system and the environment of operation.
NIST SP 800-37 revision 2	Task S-4	*Documentation of Planned Control Implementations*: Document the controls for the system and environment of operation in security and privacy plans.
NIST CSF 1.1	ID.GV-1	Organizational cybersecurity policy is established and communicated

2. Document and Inventory Your Networks

To properly scope a penetration test, organizations need to have some sense of their network topology. At minimum, an organization should compile an inventory of IP address space allocations so that evaluators can recognize which networks the organization thinks it's responsible for.[1] Organizations should also maintain an inventory of publicly facing and private-use assets. They should revisit these inventories before conducting a penetration test.

Table 2: Network Inventory References

Reference	Section	Summary
NIST SP 800-37 revision 2	Task P-10	*Asset Identification*: Identify assets that require protection.
NIST SP 800-53 revision 4	CM-8	*Information System Component Inventory*: The organization develops and documents an inventory of information system components that: accurately reflects the current in-

[1] Finding unexpected network blocks in use is not as rare as it should be in penetration tests, but it's preferable that they not *all* be unexpected.

		formation system; includes all components within the authorization boundary of the information system; is at the level of granularity deemed necessary for tracking and reporting; and includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and reviews and updates the information system component inventory [*Assignment: organization-defined frequency*].
NIST CSF 1.1	ID.AM-3	Organizational communication and data flows are mapped

3. Document and Inventory Applications (Especially Web Applications)

Organizations often use penetration tests to target web-based applications out of concern that these applications are often homegrown or exposed to the internet. Therefore, an organization should at least have an inventory of the applications it expects to be in scope for testing. It is also helpful to have some sense of what kind of information processing each system performs.

Table 3: Application Inventory References

Reference	Section	Summary
NIST SP 800-37 revision 2	Task P-10	*Asset Identification*: Identify assets that require protection.
NIST SP 800-37 revision 2	Task P-12	*Information Types*: Identify the types of information to be processed, stored, and transmitted by the system.
NIST SP 800-37 revision 2	Task C-1	*System Description*: Document the characteristics of the system.
NIST SP 800-53 revision 4	CM-8	*Information System Component Inventory*: The organization develops and documents an inventory of information system components that: accurately reflects the current information system; includes all components within the authorization boundary of the information system; is at the level of granularity deemed necessary for tracking and reporting; and includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and reviews and updates the information system component inventory [*Assignment: organization-defined frequency*].
NIST CSF 1.1	ID.AM-2	Software platforms and applications within the organization are inventoried

4. Analyze Your Internet Attack Surface

An organization's internet attack surface is comprised of all its externally accessible services, including web services, teleconferencing, Mobile Device Management (MDM), file exchanges, and any API services. Penetration tests often identify additional attack surfaces that the organization was unaware of, but it's better to have a sense of what to expect them to find up front.

Table 4: External Attack Surface References

Reference	Section	Summary
NIST SP 800-53 revision 4	SA-11(6)	*Developer Security Testing and Evaluation / Attack Surface Reviews*: The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.
NIST SP 800-53 revision 4	SC-7	*Boundary Protection*: The information system: monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
NIST CSF 1.1	PR.PT-4	Communications and control networks are protected
NIST CSF 1.1	DE.CM-1	The network is monitored to detect potential cybersecurity events

5. Document Third-Party Access to Your Networks and Assets

Few organizations have networks that are so isolated that they have no connections to third-party collaborators, partners, or service providers. It is important for an organization to know who these entities are and what access they are expected to have so it can interpret penetration tests in the right context.

Table 5: Third Party Access References

Reference	Section	Summary
NIST SP 800-53 revision 4	CA-3	*System Interconnections*: The organization authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and reviews and updates Interconnection Security Agreements [*Assignment: organization-defined frequency*].
NIST SP 800-53 revision 4	AC-20	*Use of External Information Systems*: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: access the information system from external information systems; and process, store, or transmit organization-controlled information using external information systems.
NIST SP 800-53 revision 4	SI-4(4)	*Information System Monitoring / Inbound and Outbound Communications Traffic*: The information system monitors inbound and outbound communications traffic [*Assignment: organization-defined frequency*] for unusual or unauthorized activities or conditions.
NIST CSF 1.1	ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

6. Scan for the Most Common and Known Vulnerabilities

Penetration testers often scan for known vulnerabilities in systems before moving to more difficult tests. Organizations that can perform vulnerability scanning for themselves can improve the scope of the penetration tests they seek since they don't need the testers to serve as an expensive vulnerability-scanning service.

Table 6: Vulnerability Scanning References

Reference	Section	Summary
NIST SP 800-37 revision 2	Task S-5	*Continuous Monitoring Strategy - System*: A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed.
NIST SP 800-39	Task 2-1	*Threat and Vulnerability Identification*: Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate.
NIST SP 800-54 revision 4	RA-5	*Vulnerability Scanning*: The organization scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported, employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: enumerating platforms, software flaws, and improper configurations, formatting checklists and test procedures, and measuring vulnerability impact; analyzes vulnerability scan reports and results from security control assessments; remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
NIST CSF 1.1	ID.RA-1	Asset vulnerabilities are identified and documented
NIST CSF 1.1	DE.CM-8	Vulnerability scans are performed

7. Document, Mitigate, or Patch Vulnerabilities

If knowing is half the battle, at least some fraction of the remainder is being able to do something about it. Organizations that scan for vulnerabilities can quickly find themselves overwhelmed with issues to fix if they lack good processes for evaluating risk, prioritizing responses, and efficiently deploying remediations. At minimum, organizations should have a way to document and fix known vulnerabilities that they find during scans. They should also document vulnerabilities that they choose not to fix. This is also true of penetration testing. Often, the findings don't get fixed due to resource constraints. Both vulnerability scanning and penetration testing can expose these constraints even if the specific findings can't be fixed immediately.

Table 7: Vulnerability Remediation References

Reference	Section	Summary
NIST SP 800-39	Task 3-1	*Risk Response Identification*: Identify alternative courses of action to respond to risk determined during the risk assessment.
NIST SP 800-39	Task 3-2	*Evaluation of Alternatives*: Evaluate alternative courses of action for responding to risk.
NIST SP 800-39	Task 3-3	*Risk Response Decision*: Decide on the appropriate course of action for responding to risk.
NIST SP 800-39	Task 3-4	*Risk Response Implementation*: Implement the course of action selected to respond to risk.
NIST SP 800-54 revision 4	SI-2	*Flaw Remediation*: The organization identifies, reports, and corrects information system flaws; tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and incorporates flaw remediation into the organizational configuration management process.
NIST SP 800-40 revision 3	Entire Document	*Guide to Enterprise Patch Management Technologies*: Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. There are several challenges that complicate patch management. If organizations do not overcome these challenges, they will be unable to patch systems effectively and efficiently, leading to easily preventable compromises. This publication is designed to assist organizations in

		understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management. This publication also provides an overview of enterprise patch management technologies and briefly discusses metrics for measuring the technologies' effectiveness and for comparing the relative importance of patches.
NIST CSF 1.1	ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
NIST CSF 1.1	ID.RA-6	Risk responses are identified and prioritized
NIST CSF 1.1	PR.IP-12	A vulnerability management plan is developed and implemented

8. Monitor Email for Malicious Attachments

Exploitation of users through the use of malicious email attachments is a common adversary tactic. For that reason, this tool also happens to be a favorite in the penetration tester's toolkit. Organizations lacking adequate ability to defend against these techniques will get more benefit from a penetration test if they work to improve their readiness first.

Table 8: Malicious Email Defense References

Reference	Section	Summary
NIST SP 800-53 revision 4	SI-4(24)	*Information System Monitoring / Indicators of Compromise*: The information system discovers, collects, distributes, and uses indicators of compromise.
NIST SP 800-53 revision 4	SI-3	*Malicious Code Protection*: The organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; configures malicious code protection mechanisms to: perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at [*Selection (one or more); endpoint; network entry/exit points*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
NIST SP 800-53 revision 4	SI-8	*Spam Protection*: The organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
NIST SP 800-53 revision 4	SC-44	*Detonation Chambers*: The organization employs a detonation chamber capability within [*Assignment: organization-defined information system, system component, or location*].
NIST CSF 1.1	DE.CM-4	Malicious code is detected
NIST CSF 1.1	DE.CM-5	Unauthorized mobile code is detected

9. Perform Security Testing of Web Applications

Organizations should require system developers to provide evidence of their security testing prior to deployment. Organizations can also conduct vulnerability scans or other focused testing after systems are deployed.

Table 9: Web Application Security References

Reference	Section	Summary
NIST SP 800-53 revision 4	SA-11	*Developer Security Testing and Evaluation*: The organization requires the developer of the information system, system component, or information system service to: create and implement a security assessment plan; perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*]; produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; implement a verifiable flaw remediation process; and correct flaws identified during security testing/evaluation.

10. Manage Wi-Fi and BYOD

Wireless networks offer adversaries an attack surface that requires protection beyond traditional network traffic filtering and firewalls. Attack paths include compromising employees' BYOD mobile devices or otherwise introducing rogue devices onto a (usually wireless) corporate network. Organizations should take steps to protect their wireless networks before initiating a penetration test.

Table 10: Wi-Fi & BYOD Security References

Reference	Section	Summary
NIST SP 800-53 revision 4	AC-18	*Wireless Access*: The organization establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and authorizes wireless access to the information system prior to allowing such connections.
NIST SP 800-53 revision 4	AC-19	*Access Control for Mobile Devices*: The organization establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and authorizes the connection of mobile devices to organizational information systems.
NIST SP 800-53 revision 4	SI-4(14)	*Information System Monitoring / Wireless Intrusion Detection*: The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.
NIST SP 800-53 revision 4	SI-4(15)	*Information System Monitoring / Wireless to Wireline Communications*: The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.
NIST CSF 1.1	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
NIST CSF 1.1	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed

Next Steps

When You Are Ready to Conduct a Penetration Test

Now that your organization has addressed the items above, a penetration test may be the right next step. The key to getting value out of a penetration test is to map the scope of the test to the controls you want to evaluate. For example, if you don't have any capability to detect malicious attachments or links in incoming email, it might not be useful to have the penetration testers attempt to send phishing payloads. The following documents provide more information on how to maximize the value of a penetration test:

- NIST SP 800-53A revision 4 Appendix E covers penetration testing.
- NIST SP 800-54 revision 4 CA-8 *Penetration Testing* provides guidance on the use of penetration testing as a security control.
- NIST SP 800-115 provides the *Technical Guide to Information Security Testing and Assessment* document and includes a section on penetration testing.

If You're Not Quite Ready to Conduct a Penetration Test

If an organization isn't quite ready for a penetration test, other services may be useful. It's common for third parties to offer "pre-penetration testing" services such as network mapping; configuration checks (e.g., using authenticated Nessus scans or scans for particular systems like databases, app servers or network gear); credential scans and password cracking (depending on privacy laws); vulnerability scans; web security scans; and phishing without active payloads.

Beyond the Basics

Penetration testing activities also tend to scale up as an organization's maturity increases. Additional testing can include the following:

- external testing (from the Internet)
- web testing
- phishing with payloads
- internal testing (either subsequent to the phishing exercise or based on the assumption that phishing will work)
- privilege escalation (locally and then to Domain Admin, for example)
- credential reuse
- lateral movement
- targeting of specific goals (a mission critical web app, financial data, the CEO's email, etc.)
- emulation of insider threats (e.g., start with valid user credentials and a specific goal)
- threat emulation, red teaming, or simulations

Conclusion

Penetration testing can be a valuable component of an organization's security preparedness. However, just like the check engine light in an automobile, it usually serves as a lagging indicator of preventable problems. An organization can address many of those problems more directly without requiring a penetration test to bring them to the organization's attention.

Penetration testing is a way of testing your security controls against realistic attacks, assuming that you have a known set of controls to test. Implementing the controls discussed in this white paper can make penetration testing much more useful to organizations.

Works Cited

[National Institute of Standards and Technology 2008]
National Institute of Standards and Technology. *SP 800-115 Technical Guide to Information Security Testing and Assessment.* September 2008. https://doi.org/10.6028/NIST.SP.800-115

[National Institute of Standards and Technology 2011]
National Institute of Standards and Technology. *SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View.* March 2011. https://doi.org/10.6028/NIST.SP.800-39

[National Institute of Standards and Technology 2014]
National Institute of Standards and Technology. *SP 800-53A Rev. 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.* December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4

[National Institute of Standards and Technology 2015]
National Institute of Standards and Technology. *SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations.* Vers. 4. January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[National Institute of Standards and Technology 2018a]
National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.* April 16, 2018. https://doi.org/10.6028/NIST.CSWP.04162018

[National Institute of Standards and Technology 2018b]
National Institute of Standards and Technology. SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. December 2018. https://doi.org/10.6028/NIST.SP.800-37r2

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0233