

PENETRATION TESTING

BLUEPRINT: BUILDING A BETTER PEN TESTER

High-value penetration testing involves modeling the techniques used by real-world computer attackers to find vulnerabilities, and, under controlled circumstances, to exploit those flaws in a professional, safe manner according to a carefully designed scope and rules of engagement. This process helps to determine business risk and potential impact of attacks, all with the goal of helping the organization improve its security stance.

Here are recommendations for each phase of penetration testing to help you provide higher business value in your work.

PRE-ENGAGEMENT

Discuss **black-box** versus **crystal/white-box** testing while building your **rules of engagement**, noting that crystal box testing often provides more detailed results, is safer, and delivers better business value.

Discuss with target system personnel the **particularly sensitive information they have in their environment** (such as PII) and how you can measure access to it without actually downloading it. Consider going after generic sample records planted to demonstrate your access instead of the actual sensitive data.

Make sure you get **written permission** to test any third parties that own or operate target systems (MSSPs, cloud providers, ISPs, shared hosting environments, border routers, DNS servers, etc.)

Keep your skills fresh by setting aside an hour or two per week to participate in **Capture the Flag** competitions, including the **free** SANS Holiday Hack Challenge at www.holidayhackchallenge.com or the numerous free CTFs at <http://www.amanhardikar.com/mindmaps/Practice.html>

Use a template to guide a voice conversation to **identify the scope** and **rules of engagement**.

Conduct a **daily debriefing call with target system personnel** to exchange ideas and lessons learned. If daily is too frequent, consider calls two or three times per week.

Identify targets by **IP address** (IPv4 and IPv6 if you have it), domain name, and (if you have it) MAC address (especially for compromised client machines using DHCP).

Include **screenshots in your report** to illustrate findings clearly. **Annotate screenshots** with arrows and circles pointing out the important aspects of the illustration.

To add extra value to your recommendations, **consider including steps an operations person can take to verify that a recommended fix is in place**, such as a command to check for the presence of a patch. For some findings, this can be hard to do, so in those cases recommend that the given issue be retested.

Write for the proper audience in each section:

- The Executive Summary should be for the decision-makers who are allocating resources.
- Findings should be written from a technical perspective, informed by business issues.
- Recommendations should take into account the operations team and their processes.

RECONNAISSANCE

Carefully **consider all interactions with third-party servers and searches** to ensure you do not divulge sensitive information about the target or violate a non-disclosure arrangement by using them. You may want to **consider using the TOR network** to obscure your relationship with the target organization.

Look for common office documents posted on target websites by using Google searches for:

site:<TargetDomain> ext:doc | ext:docx | ext:xls | ext:xlsx | ext:pdf

Remember to **check social networking sites** (especially LinkedIn, Facebook, and Twitter) to learn about target personnel and the technologies they use.

Use the **Shodan search engine's "net:" directive** to look for unusual or interesting devices in the target network address ranges. Also, use **unique footer information** (such as a common copyright notice on target web pages) to find additional pages via Shodan using the "html:" directive.

Double-check that all IP addresses included in the scope belong to the target organization and aren't a mistake. Use **whois** lookups and **tracert** to check that the addresses make sense and actually belong to the target organization.

In LinkedIn, **look for long-term IT and InfoSec employees to see which technologies they are familiar with**, including firewalls, development environments, and more.

VULNERABILITY ANALYSIS

Run a **sniffer such as tcpdump** while you are scanning a target so you can **continually verify** that your scanner is still running appropriately.

While open ports such as **TCP 445** often indicate a Windows machine, this is not always the case. The target could be a **Samba daemon** or another **SMB-based target**.

Verify discovered vulnerability findings by **researching how to check the issue manually** or through a bash, PowerShell, Nmap Scripting Engine (NSE) script, or other script.

Try to **identify false positives** by running a different tool to corroborate a finding.

Put vulnerabilities that you have identified in the context of how critical the asset is, as this helps you assign priority and assess risk.

If you are using a **virtual machine** for your attacks, **configure it for bridged networking** to avoid filling up NAT tables and to ensure reverse shell connections can come back to you.

PASSWORD ATTACKS

Create a **word list fine-tuned to the target organization** based on words from its website.

Create a **word list fine-tuned for users** based on their social networking profiles.

When you successfully crack a password using word-mangling rules, **add that password to your dictionary for further password attacks on that penetration test**. That way, if you encounter the same password in a different hash format, you won't have to wait for word-mangling to re-discover that password.

Remember, passwords can be gathered using a variety of techniques, including **automated guessing, cracking, sniffing, and keystroke logging**.

For password guessing, always **consider the account lockout policy** and try to avoid it by using **password spraying techniques** (a large number of accounts and targets with a small number of passwords).

As **soon as you get hashes** from targets, **start a password cracker** to try to determine the passwords. Don't let any time go by until you start cracking the hashes you've gotten.

Sometimes you **don't need a password** for authentication because simply using the hash can get the job done, as with **pass-the-hash attacks against Windows and SMB targets**, and with **hashes of passwords stored in cookies** for some websites.

If you have a compatible GPU on your system, **consider using a GPU-based password cracking tool**, such as **Hashcat**, as you'll get 20 to 100 times the performance.

EXPLOITATION

When creating payloads that evade anti-malware tools, **do NOT submit your sample to online scanning sites** like virustotal.com to check for evasion, as that may defeat your payload as new signature updates are distributed.

Set up a **command or script that checks the availability of the target service** every few seconds while you are attacking it. That way, if you do crash it, you'll notice quickly and can work with target system personnel to get it restarted.

Build your payloads so that they make a reverse connection back to you, increasing the chance you'll get through a firewall that allows outbound connections.

For your payloads, **use a protocol that is likely allowed outbound from the target environment**, such as HTTPS (with a proxy-aware payload like those available in PowerShell Empire, Metasploit, and the Veil Framework) or DNS (such as the DNScat tool).

To **lower the chance of crashing Windows target systems and services**, once you gain admin-level credentials and SMB access to them, **use psexec or similar Windows features (WMIC, sc, etc.) to cause them to run code**, instead of a buffer overflow or related exploit.

If your exploit fails, **read the output of your exploitation tool carefully to see where it errors out**. Also, run a sniffer such as tcpdump to see how far along it gets in making a connection, sending the exploit, and loading the stager and stage. If your stager worked but your stage couldn't be loaded, your anti-virus evasion tactics may be failing.

When you gain access to a target, if a **sniffer is installed on the machine** (like tcpdump or Wireshark's tshark tool), **run it to look for network traffic** to identify other possible target machines, as well as cleartext protocols containing sensitive or useful information.

Even without root, system, or admin privileges on a target machine, you can **still usually perform very useful post-exploitation activities**, including getting a list of users, determining installed (and possibly vulnerable) software, and pivoting through the system.

When you get on a Windows box, look for **ESTABLISHED TCP connections** to ports 445 (SMB) and 3389 (RDP), as these other systems may be excellent systems to pivot to, provided they are in scope:

```
c:\> netstat -na | find "EST" | find ":445"
c:\> netstat -na | find "EST" | find ":3389"
```

While they can be very useful for management demonstrations, **be careful turning on video cameras and capturing audio from compromised target machines**. Conduct that level of invasive access only with written permission, and have it reviewed by your legal team to ensure compliance with local laws.

BLUEPRINT: BUILDING A BETTER PEN TESTER

SANS PEN TEST CURRICULUM

PEN TEST BLOGS, CHEAT SHEETS, DOWNLOADS, RESOURCES:
<https://pen-testing.sans.org>