

NIST SPECIAL PUBLICATION 800-115

Technical Guide to Information Security Testing and Assessment

NIST (National Institute of Standards and Technology)

Lembaga federal di bawah Departemen Perdagangan AS.

Bertanggung jawab untuk **mengembangkan standar, panduan, dan praktik** terbaik untuk meningkatkan keamanan dan keandalan sistem informasi.

menyediakan kerangka kerja bagi badan-badan federal dan organisasi lain untuk mengelola dan melindungi informasi sensitif, khususnya dalam konteks keamanan informasi

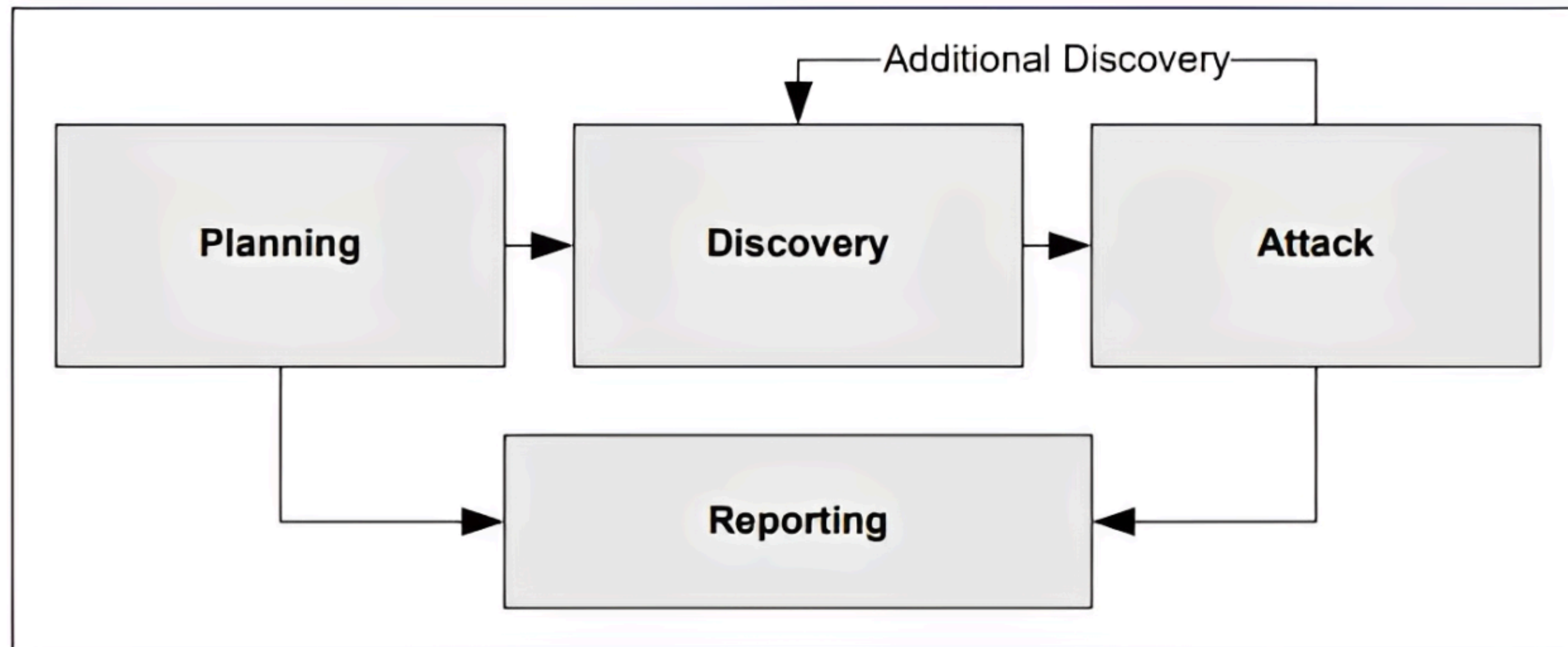
NIST Special Publication 800–115, titled "Technical Guide to Information Security Testing and Assessment," memberikan **rekomendasi komprehensif** untuk melakukan **pengujian dan penilaian keamanan informasi**. Dokumen ini menguraikan **metodologi dan praktik terbaik** untuk mengevaluasi postur keamanan sistem informasi, membantu organisasi **mengidentifikasi kerentanan dan meningkatkan langkah-langkah keamanan mereka**.

Penetration Testing

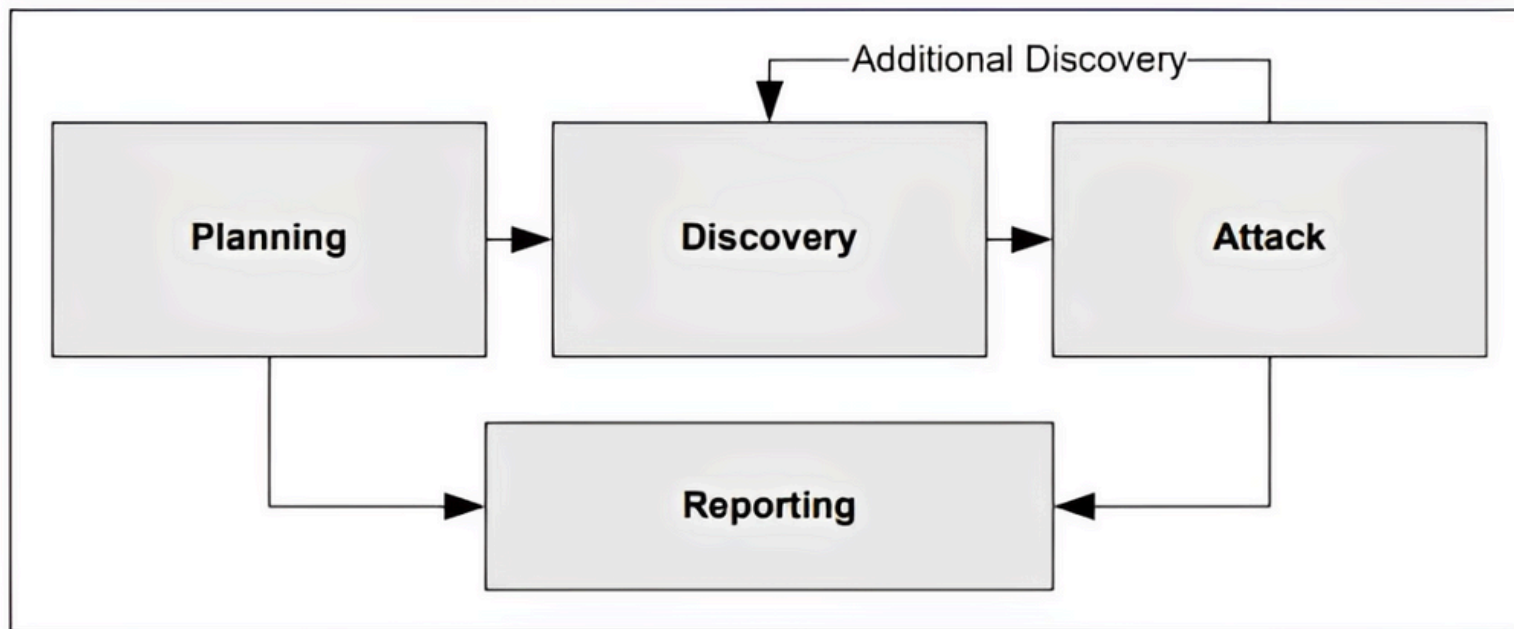
suatu **metode pengujian keamanan** di mana **penetration tester** (pentester) mensimulasikan serangan dunia nyata untuk mengidentifikasi cara menghindari fitur keamanan aplikasi, sistem, atau jaringan. Ini melibatkan serangan nyata menggunakan **alat dan teknik** yang biasa dipakai oleh penyerang, dengan fokus pada pencarian berbagai **kerentanan** yang dapat memberikan akses lebih besar daripada satu kerentanan saja

- Menilai seberapa mampu sistem dalam **menangani serangan**
- Apakah Kemampuan pertahanan untuk **mendeteksi serangan** dan **merespons** dengan tepat.

Penetration Testing Phases



Sumber : <https://csrc.nist.gov/external/nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>



PEMILIK SISTEM (ORGANISASI)

1. mengembangkan kebijakan penilaian (rules)
2. Menentukan sistem mana yang harus dinilai & frekuensi penilaiannya.
3. Menentukan sasaran & tujuan penilaian

PLANNING

TIM PENTESTER

- Mengikuti dan memenuhi poin 1 & poin 2
- Menetapkan peran dan tanggung jawab TIM
- Menyiapkan segala peralatan hardware & Software
- memilih lingkungan dan lokasi untuk melakukan penilaian dengan pertimbangan poin 1
- Melakukan penetration testing

1. Mengumpulkan Informasi

Contoh:

- Aset yang Dinilai: Website perusahaan e-commerce (***www.contoh-ecommerce.com***).
- Resiko: Serangan DDoS, Password Attack, injeksi SQL, dan serangan XSS.

2. Menetapkan Sasaran dan Tujuan

Contoh:

- Sasaran: Mengidentifikasi ***kerentanan di website*** untuk ***melindungi data pelanggan***.
- Tujuan: Mendeteksi dan melaporkan semua ***kerentanan kritis*** dan ***tinggi*** maupun ***sedang*** sebelum peluncuran fitur baru dalam ***waktu 4 minggu***.

3. Menentukan Ruang Lingkup

Contoh:

- Ruang Lingkup:
 - Sistem: Website utama & database backend.
 - Batasan: Tidak melakukan pengujian pada ***sistem internal dan server pengembangan***.

4. Mengidentifikasi Peran dan Tanggung Jawab Tim

Contoh:

- Tim Penetrasi:
 - Pemimpin Proyek: Ahmad – bertanggung jawab atas ***pengawasan dan pelaksanaan*** keseluruhan.
 - Analis Keamanan: Roy – melakukan ***pengujian dan analisis kerentanan***.
 - Spesialis Laporan: Putri – menyusun ***laporan dan presentasi hasil***.

5. Rencana Manajemen Proyek

Contoh:

- Persyaratan Penilaian: Melaksanakan pengujian dalam empat minggu.
- Faktor Keberhasilan: Komunikasi yang efektif dengan tim IT perusahaan.
- Sumber Daya: Alat pengujian seperti ***Burp Suite dan Nmap***.
- Jadwal:
 - Minggu 1 : ***Planning***.
 - Minggu 2 : ***Discovery*** (information gathering and scanning & vulnerability analysis).
 - Minggu 3 : ***Attack***
 - Minggu 4 : ***Reporting***

6. Pertimbangan Logistik

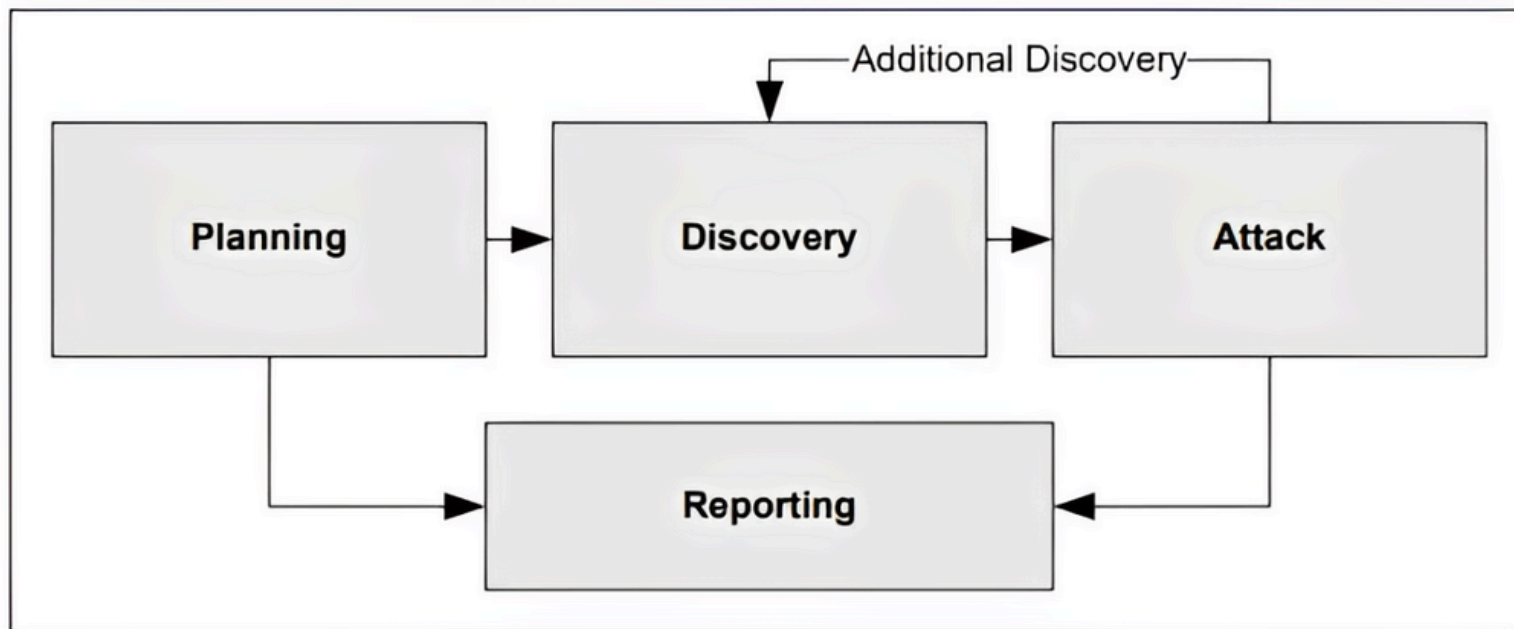
Contoh:

- Penjadwalan: Penjadwalan pengujian pada ***malam hari*** untuk menghindari gangguan pada pengguna.
- Alokasi Sumber Daya: Menggunakan satu server khusus untuk pengujian.
- Pertimbangan Hukum: Mendapatkan ***izin*** tertulis dari manajemen(pemilik sistem/organisasi) untuk melaksanakan pengujian.

7. Pendekatan Penilaian

Contoh:

- Metodologi: Menggunakan ***NIST SP 800-115 atau OWASP Testing Guide*** sebagai panduan.
- Pendekatan: Kombinasi pengujian ***manual dan otomatisasi*** untuk memaksimalkan efisiensi.



DISCOVERY

- Information Gathering

Mengumpulkan Informasi terkait sistem yang dinilai berupa **Host aktif, Sistem Operasi & Versinya, Port terbuka & Layanan terbuka serta versi Layanan** dengan cara menggunakan pemindai otomatis.

- Vulnerability Analysis

Menemukan keterentanan (vulnerability)/Membandingkan dengan basis data kerentanan dapat berupa **sistem operasi lawas/rentan, layanan rentan, sql injection** dll. dengan cara **manual** atau/kombinasi **vulnerability scanner**.

Basis data kerentanan : National Vulnerability Database (NVD) atau Common Weakness Enumeration (CWE)

- Information Gathering















```
1 http://testphp.vulnweb.com [200 OK] ActiveX[D27CDB6E-AE6D-11cf-96B8-444553540000],
2 Adobe-Flash, Country[UNITED STATES][US], Email[wvs@acunetix.com],
3 HTTPServer[nginx/1.19.0], IP[44.228.249.3],
4 Object[http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0]
5 [clsid:D27CDB6E-AE6D-11cf-96B8-444553540000], PHP[5.6.40-38+ubuntu20.04.1+deb.sury.org+1],
6 Script[text/JavaScript], Title[Home of Acunetix Art],
7 X-Powered-By[PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1], nginx[1.19.0]
```

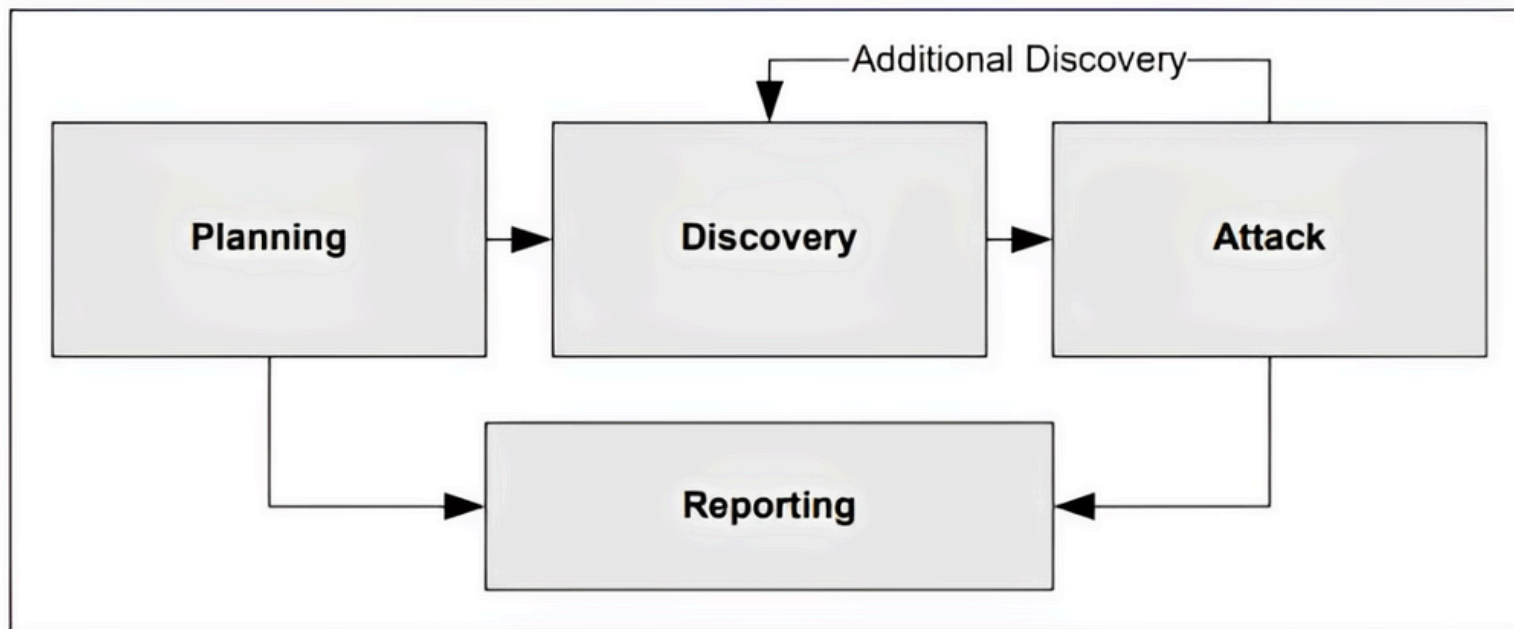
```
PORT      STATE SERVICE
20/tcp    open  ftp-data
22/tcp    open  ssh
80/tcp    open  http
```

```
PORT      STATE SERVICE VERSION
80/tcp    open  http  nginx 1.19.0
```

- Vulnerability Analysis

ID	Target	PluginName / VulnType
	1 http://testphp.vulnweb.com/listproducts.php	sqldet/error-based/default
	2 http://testphp.vulnweb.com/listproducts.php	sqldet/error-based/default
	3 http://testphp.vulnweb.com/artists.php	sqldet/blind-based/default
	4 http://testphp.vulnweb.com/listproducts.php	sqldet/blind-based/default
	5 http://testphp.vulnweb.com/product.php	sqldet/blind-based/default
	6 http://testphp.vulnweb.com/listproducts.php	sqldet/blind-based/default
	7 http://testphp.vulnweb.com/userinfo.php	sqldet/blind-based/default
	8 http://testphp.vulnweb.com/secured/newuser.php	sqldet/error-based/default
	9 http://testphp.vulnweb.com/userinfo.php	sqldet/blind-based/default
	10 http://testphp.vulnweb.com/search.php	sqldet/blind-based/default
	11 http://testphp.vulnweb.com/search.php	sqldet/blind-based/default
	12 http://testphp.vulnweb.com/secured/newuser.php	sqldet/blind-based/default

***error-based injection,
boolean-based injection,
and time-based blind
injection***



ATTACK

Aktivitas ***inti*** dalam pentest, dimana melakukan Simulasi (praktek) serangan selayaknya seorang hacker terhadap daftar kerentanan yang ditemukan pada Phase ***Discovery***.

- Jika serangan/exploitasi berhasil maka kerentanann valid/terverifikasi dan langkah mitigasi juga ter-identifikasi
- Jika serangan/exploitasi tidak berhasil maka pentester lanjut ke kerentanan lain.

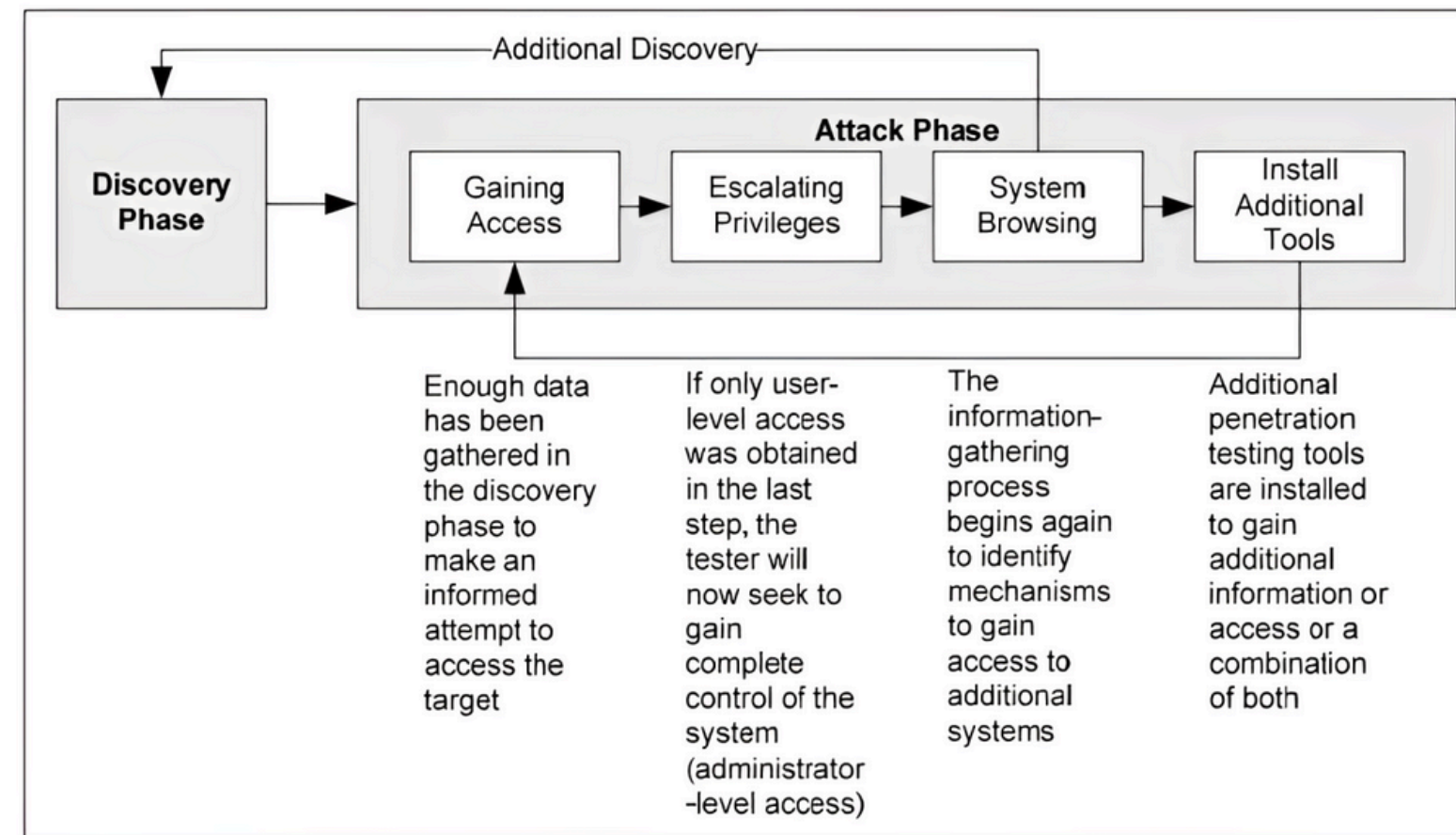


Figure 5-2. Attack Phase Steps with Loopback to Discovery Phase

- **Gaining Access** : Berupaya mengakses target (ex, login) berdasarkan tahap Discovery atau bisa dengan ***Password Cracking***.
- **Privilege Escalation** : Jika akses berhasil dan hanya login akses user biasa (pelanggan), pentester akan berusaha untuk meningkatkannya (user to admin)
- **System Browsing** : Menelusuri file konfigurasi yang mungkin terdapat informasi penting berupa data keuangan, kontak, kredensial, dll sehingga bisa di ekspor data atau menemukan kerentanan atau terdapat sistem tambahan lain sehingga bisa kembali ke tahap Discovery untuk diidentifikasi dan analisis kerentanan.

← → ↻ 🏠 testphp.vulnweb.com/listproducts.php?cat=extractvalue(1,concat(char(126),md5(1420595670))) 📄 ☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

acunetix **acuart**

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

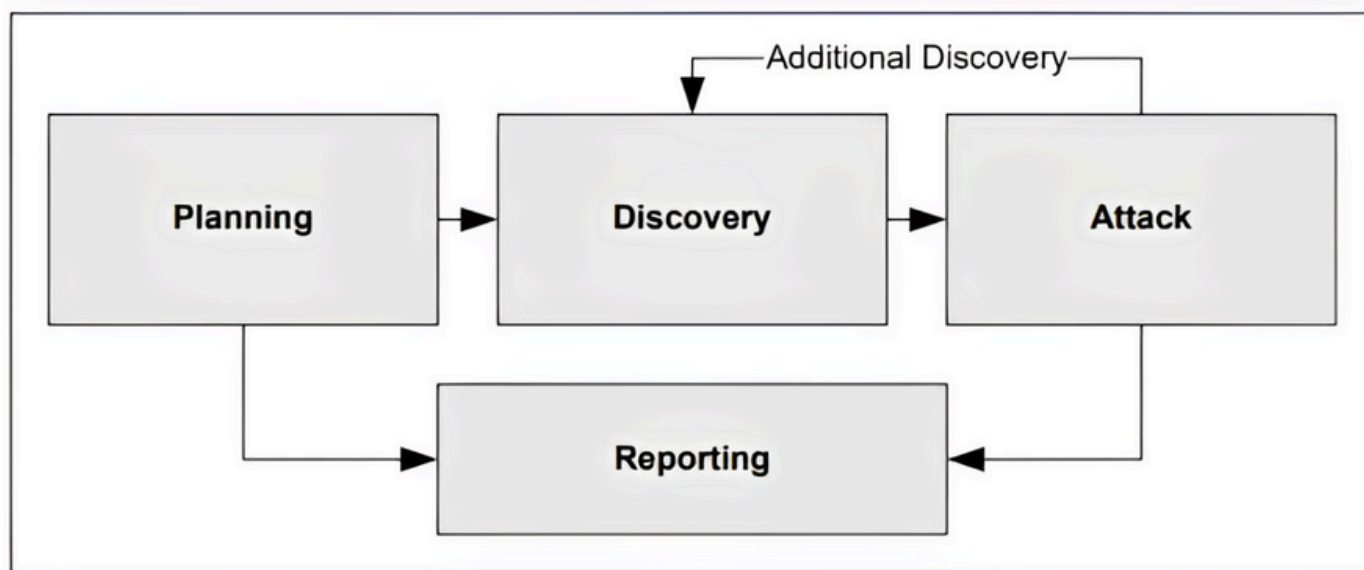
search art

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)

Links
[Security art](#)
[PHP scanner](#)
[PHP vuln help](#)
[Fractal Explorer](#)

Error: XPATH syntax error: '~cc63bc40a12e15e328f029493637dc6'
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd



REPORTING

Dilakukan secara bersamaan dengan phase Planning, Discovery dan Attack sehingga apapun aktivitas yang telah dilakukan pada tahap tersebut di dokumentasinya.

Pada akhir pengujian, sebuah laporan biasanya dikembangkan untuk menggambarkan ***Daftar Kerentanan, Deskripsi Kerentanan, Tingkat Resiko (ex. Critical, High, Medium, Low & Informational) & Panduan Mitigasi.***

Hasil pengujian keamanan dapat digunakan dengan cara berikut: (1) sebagai referensi untuk tindakan korektif, (2) sebagai referensi untuk kegiatan mitigasi untuk mengatasi kerentanan, dan (3) sebagai tolok ukur untuk memantau kemajuan organisasi dalam memenuhi persyaratan keamanan.

SEKIAN & TERIMA KASIH
CREATED BY HABBAS DUPUTURA HUTABARAT
<https://www.linkedin.com/in/userhabbas/>