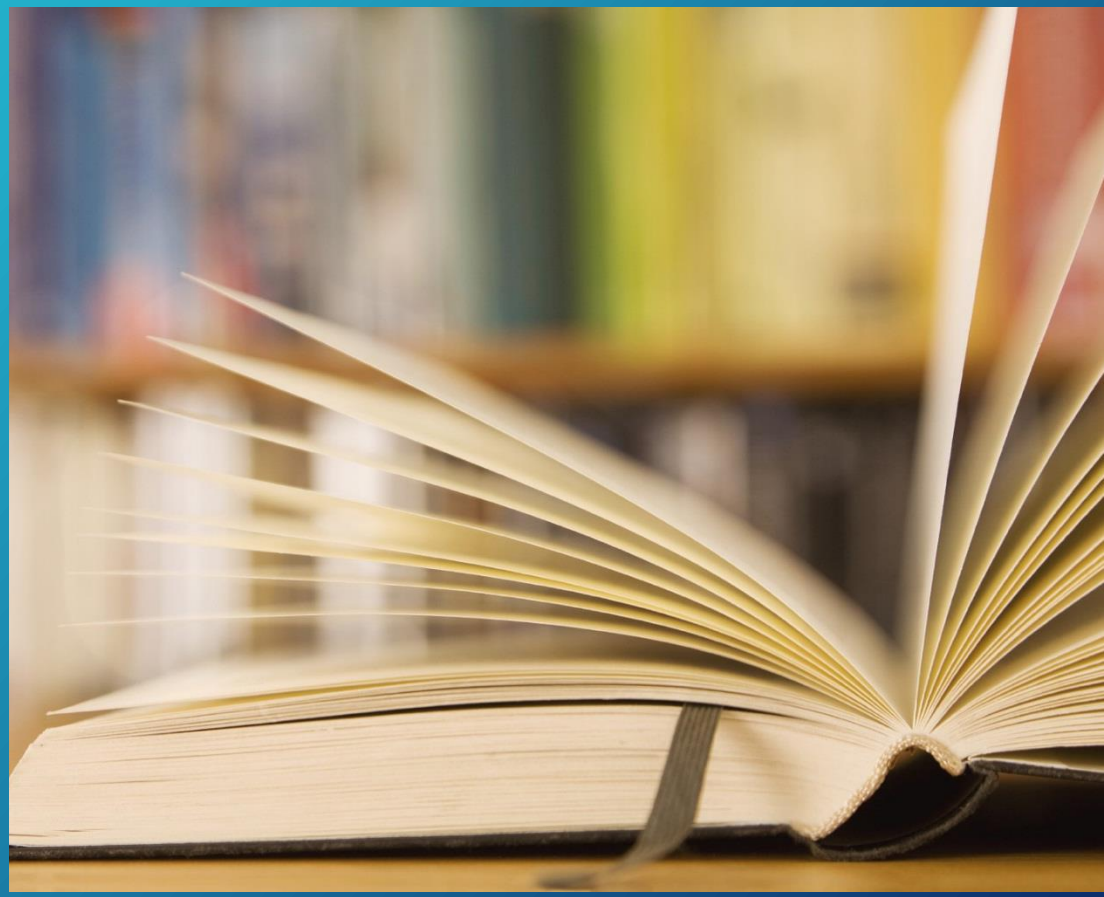
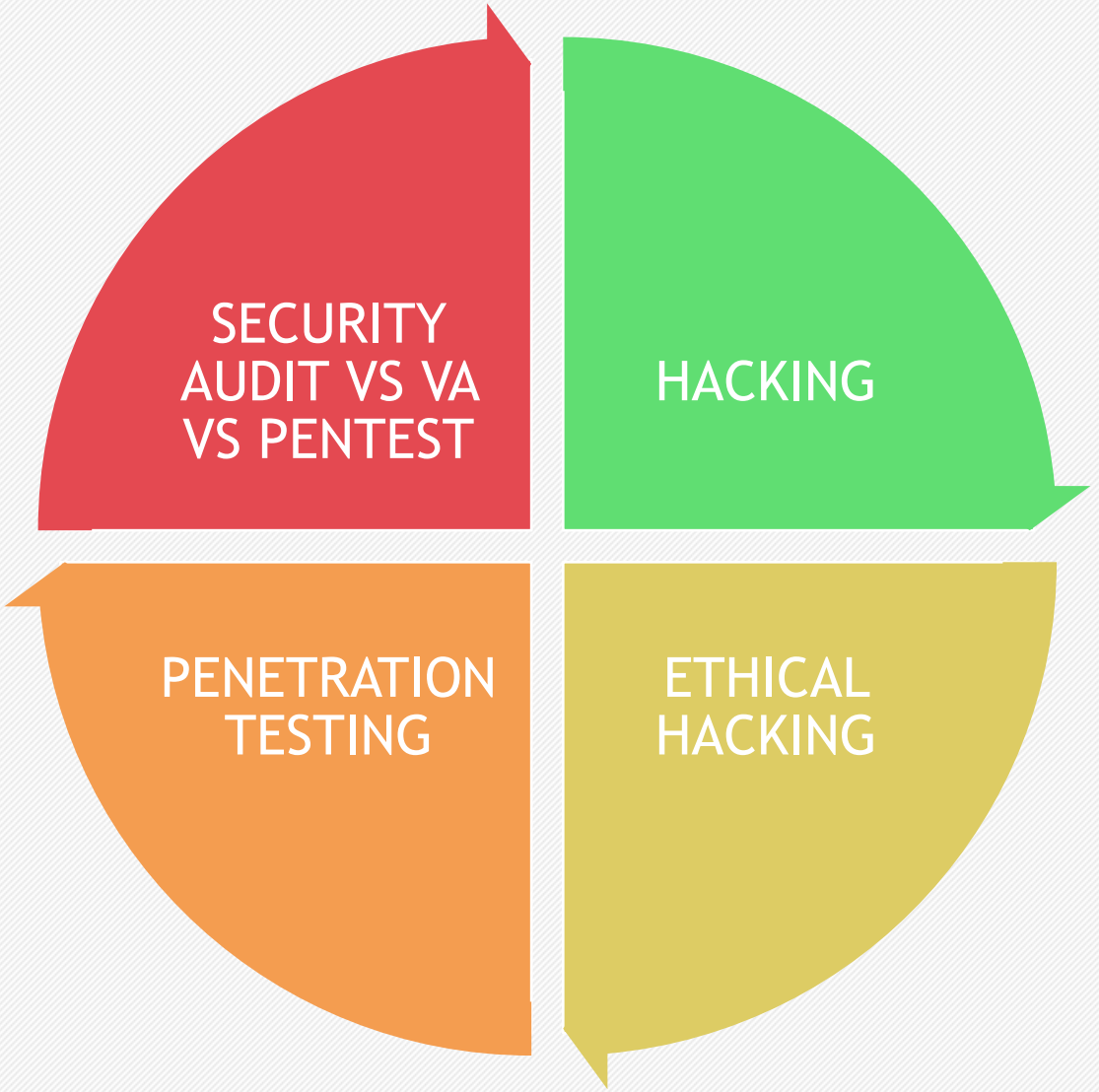
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

ETHICAL HACKING



Keamanan Sistem Informasi – Aditya Putra, ST., MT.

Agenda


SECURITY AUDIT VS VA VS PENTEST
HACKING
PENETRATION TESTING
ETHICAL HACKING

HACKING - Konsep

DEFINISI

- Hacking adalah upaya eksploitasi kelemahan/kerentanan system untuk mengambil akses secara illegal ke resource system
- Hacking sering digunakan untuk mencuri dan mendistribusikan property intellectual yang mengakibatkan kerugian bisnis baik secara finansial maupun bisnis

SIAPA

- Hacker adalah seseorang yang memiliki keahlian computer yang baik yang mampu membuat atau meng-explore software dan hardware
- Motive mereka bisa jadi untuk mendapat pengetahuan, pengalaman, atau iseng semata

HACKING - Klasifikasi Hacker

Black Hats	• Melakukan aktivitas illegal yang merusak (crackers)
White Hats	• Melakukan hacking sebagai assessment dan memiliki izin untuk melakukannya
Gray Hats	• Bisa berperan sebagai black dan white hat pada waktu yang berbeda
Script Kiddies	• Melakukan compromising system menggunakan script, tools dan software yang sudah ada
Cyber Terrorists	• Melakukan Hack dengan motif politis dan mengancam untuk melakukan serangan skala besar
State Sponsored	• Dipekerjakan oleh negara untuk melakukan penetrasi dan mendapatkan informasi rahasia milik negara lain
Hacktivist	• Melakukan Hack dengan motif politik/sosial atas isu2 yang berkembang

ETHICAL HACKING - Konsep

- Ethical Hacking adalah penggunaan tools, trik, dan Teknik hacking untuk mengidentifikasi vulnerability suatu system dengan tujuan assessment atau perbaikan
- Ethical dilakukan dengan cara mensimulasikan proses penyerangan sebagaimana hacker sungguhan untuk memverifikasi adanya vulnerability pada suatu system

Yang menjadi pembeda Ethical Hacking dengan Real Attack terletak pada MOTIF dan IZIN yang dimiliki

ETHICAL HACKING - Mengapa Dibutuhkan

- Untuk mencegah hacker mendapatkan akses ke system informasi organisasi
- Untuk mengungkap adanya vulnerability yang belum disadari potensi resikonya
- Untuk menganalisa dan menguatkan keamanan organisasi termasuk kebijakan, infrastruktur perlindungan jaringan, dan tips-tips teknis praktis yang diperlukan untuk end-user
- Menyediakan pencegahan yang cukup untuk menghindari kebocoran data
- Untuk menjaga data customer yang ada pada transaksi bisnis
- Untuk meningkatkan kewaspadaan keamanan di setiap level organisasi

ETHICAL HACKING - Lingkup dan Batasan

LINGKUP

- Ethical Hacking adalah komponen penting dalam assesmen resiko, audit, menghindari fraud, dan best practice dalam keamanan sistem informasi
- EH bertujuan untuk mengidentifikasi resiko dan menemumkan tindakan remediasi serta mengurangi biaya ICT dengan meminimalisir vulnerability-nya

BATASAN

- Organisasi harus mengetahui tujuan dan apa yang diinginkan ketika meng-hire Ethical Hacker
- Seorang Ethical Hacker memang dapat menemukan kelemahan sistem organisasi, namun keputusan implementasi security kembali lagi kepada kemauan organisasi

PENETRATION TESTING - Konsep

DEFINISI

- Penetration Testing (PenTest) adalah metode evaluasi/assessment dari Ethical Hacking
- Ada beberapa ukuran/parameter keamanan yang menjadi checklist untuk menemukan kesalahan design, kelemahan teknis dan vulnerabilities
- Dalam Pentest, yang didokumentasikan tidak hanya adanya vulnerability namun juga bagaimana "reproduce" bagaimana suatu kelemahan bisa dieksploitasi
- Hasilnya adalah laporan berisi executive summary dan laporan teknis

PENETRATION TESTING - Metode

Blackbox

- Tanpa pengetahuan sama sekali, hanya IP/domain target
- Blind / Double Blind Testing

Whitebox

- Mengetahui infrastruktur yang akan diuji
- Greybox

Greybox

- Pengetahuan terbatas

SECURITY AUDIT/ASSESSMENT vs VA vs PENTEST

Security Audit

- Berupa ceklis keamanan informasi sebagai parameter kesesuaian organisasi terhadap standar keamanan tertentu

Vulnerability Assessment

- Pendekatan dalam melakukan assessmen keamanan berupa pencarian terhadap vulnerability yang ada pada suatu sistem

Penetration Testing

- Pendekatan metodologis untuk melakukan assessmen keamanan mencakup VA dan mencoba melakukan eksploitasi terhadap Vulnerability yang ditemukan

SECURITY AUDIT/ASSESSMENT vs VA vs PENTEST

Parameter Pembanding	Security Audit/Assessment	Vulnerability Assessment	Penetration Testing
TUJUAN	Mengikuti standar keamanan	Mencari adanya vulnerability suatu sistem	Membuktikan apakah suatu sistem yang secure masih bisa dipenetrasi
LINGKUP	Keseluruhan sistem organisasi (Fisik, Sistem, Orang, Policy, dll)	Spesifik ke perangkat/web	Spesifik ke perangkat/web, bahkan ke service tertentu
PENGERJAAN	Manual	Otomatis	Gabungan Otomatis dan Manual
PENGETAHUAN CUCTOMER	Low	Low to Medium	Medium to High