

## ABSTRACT

*In every type of organizations, one of the few rules created by network and system administrator is improve security from infrastructure computer. However with increasing complexity from information system, sometimes although system and network that have gone through the proses of overall patch still possible have vulnerability. This can cause irreversible damage (data theft, harm the system, interference, damage to reputation, etc).Some examples like FH UGM andUGM online library website which had been hacked as ever reported by the online news [mediatribunnews.com](http://mediatribunnews.com) and [viva.co.id](http://viva.co.id).*

*There are some steps different security that can be done by administrator for secure network and systems, however, the best way to prove security of network and systems is by doing penetration test. Penetration test can provide network and system administrator a realistic assessment of the security fort by identifying vulnerability and exploits which exist in computer network infrastructure. Penetration test use the same principle as the hacker for penetration computer network infrastucture and check for any deficiencies and vulnerability and help to establish security measures.*

*The result of the research after methodological penetration testing and assessment using ISSAF to the existing service on the server using hostname [server.te.ugm.ac.id](http://server.te.ugm.ac.id) which is a server that accommodates the domain services in the DTETI engineering faculty. There are three security holes in the three services that exist in DTETI engineering faculty based on calculations using OWASP Risk Rating has a potential risk of overall value is 6.375 for local file inclusion vulnerability, 6.375 for SQL Injection vulnerability, and 6.25 for XSS vulnerability.*

*Keyword : sever security, assessment, penetration test, security awareness*

## INTISARI

Dalam organisasi, besar atau kecil, salah satu dari beberapa aturan yang dibuat oleh administrator jaringan dan sistem adalah meningkatkan keamanan dari infrastruktur komputer. Namun, dengan meningkatnya kompleksitas dari sistem informasi, terkadang walau sistem dan jaringan yang sudah melalui proses *patch* secara keseluruhan masih memungkinkan memiliki celah keamanan, hal ini dapat menyebabkan Kerusakan ireversibel (pencurian data, membahayakan sistem, gangguan, kerusakan reputasi, dan sebagainya) beberapa contoh seperti situs notariat FH UGM dan perpustakaan *online* UGM yang pernah dibobol *hacker* seperti yang pernah dikabarkan oleh media berita *online* [tribunnews.com](http://tribunnews.com) dan [viva.co.id](http://viva.co.id).

Ada beberapa langkah pengamanan yang berbeda yang dapat dilakukan administrator untuk mengamankan jaringan atau sistem, namun, cara terbaik untuk membuktikan keamanan suatu jaringan atau sistem adalah dengan melakukan uji penetrasi. Uji penetrasi dapat memberikan administrator sistem dan jaringan penilaian yang realistis terhadap benteng keamanan dengan mengidentifikasi celah keamanan dan *exploits* yang ada di infrastruktur jaringan komputer. Uji penetrasi menggunakan prinsip yang sama dengan peretas untuk penetrasi infrastruktur jaringan komputer dan memeriksa adanya kekurangan dan celah keamanan dan membantu untuk menetapkan tindakan keamanan.

Hasil dari penelitian setelah dilakukan uji penetrasi dan asesmen secara metodologis menggunakan ISSAF terhadap layanan yang ada pada *server* yang menggunakan *hostname* [server.te.ugm.ac.id](http://server.te.ugm.ac.id) yang merupakan *server* yang menampung layanan-layanan *domain* yang ada di Fakultas Teknik DTETI UGM. terdapat tiga celah keamanan pada tiga layanan yang ada pada Fakultas Teknik DTETI UGM yang berdasarkan perhitungan menggunakan *OWASP Risk Rating* memiliki nilai kemungkinan resiko secara keseluruhan 6.375 pada celah *local file inclusion*, 6.375 pada celah *SQL Injection* dan 6.25 pada celah *XSS*.

Kata kunci : keamanan *server*, Asesmen, Uji penetrasi, Kesadaran keamanan