Kesiapan personel dan infrastruktur

Personel : Laporan kekuatan ST-5 Jumlah 10 Personil lengkap

Infrastruktur: Material 15 pc dan 4 laptop, Internet 165 Mbps.

Tim Wasdal : Kol Laut (E) Arif Agus Suharto

Tim Penilai : Letkol Laut Mar I Ketut Gk

Tim Duknis Infolahta : Sertu Etk Rizky Agus

Tim cyber Pro : Bapak Iqbal Nasikin

Latihan phase kedua Hari pertama, bralat ….X, jumlah serangan……kali, dengan jenis serangan ………(nama serangan),

Phase kedua Hari kedua, bralat 5 kali, jumlah serangan ….., dengan jenis serangan

ST 5 dapat melaksanakan pengaman web server dan jaringan yang ada selama latihan dengan koordinasi dari tim penangkalan, penanggulangan dan bantuan yang terbentuk di ST 5.

Telah melaksanakan latihan operasi pertahanan siber tni al,

**PHASE 2 HARI PERTAMA,**

TELAH DITERIMA BRALAT SEBANYAK TUJUH KALI (BRALAT 17 S.D. 23) DAN DIDAPAT SERANGAN SEJUMLAH EMPAT BELAS KALI DIMANA DENGAN JENIS SERANGAN SBB:

1. WEB-OTHER GNU BASH ENVIRONMENT VARIABLE HANDLING COMMAND EXECUTION
2. WEB-SERVER APACHE STRUTS DYNAMIC METHOD INVOCATION REMOTE CODE EXECUTION VULNERABILITY
3. WEB-OTHER CISCO PRIME DATA CENTER NETWORK MANAGER
4. WEB-OTHER GENERIC FILE UPLOAD DIRECTORY TRAVERSAL
5. TCP SPLIT HANDSHAKE
6. ATTACK-PROTOCOL EXCEPTION
7. WEB-SERVER APACHE STRUTS 2 REST PLUGIN EKSEKUSI
8. WEB-OTHER GNU BASH ENVIRONMENT VARIABLE HANDLING COMMAND EXECUTION VULNERABILITY
9. WEB-SERVER APACHE STRUTS DYNAMIC METHOD INVOCATION REMOTE CODE EXECUTION VULNERABILITY
10. WEB-SERVER APACHE STRUTS 2 REST
11. WEB OTHER CISCO CISCO PRIME DATA CENTER NETWORK MANAGER PROCESSIMAGESAVE.JSP
12. WEB-SERVER APACHE STRUTS DYNAMIC METHOD INVOCATION REMOTE CODE EXECUTION VULNERABILITY
13. WEB-SERVER APACHE STRUTS DYNAMIC METHOD INVOCATION REMOTE CODE EXECUTION VULNERABILITY
14. ARP-SPOOFING

**PHASE 2 HARI KEDUA,**

TELAH DITERIMA BRALAT SEBANYAK TIGA KALI (BRALAT 24 S.D. 26) DAN DIDAPAT SERANGAN SEJUMLAH DUA BELAS KALI DIMANA DENGAN JENIS SERANGAN SBB:

1. ARP-SPOOFING
2. PORT SCANNING
3. WEB-OTHER GNU BASH ENVIRONMENT VARIABLE HANDLING COMMAND EXECUTION VULNERABILITY
4. WEB-SERVER APACHE STRUTS 2 REST PLUGIN EKSEKUSI
5. HTTP REQUEST METHOD
6. WEB-SERVER APACHE STRUTS 2 REST PLUGIN EKSEKUSI
7. WEB-OTHER GNU BASH ENVIRONMENT VARIABLE HANDLING COMMAND EXECUTION VULNERABILITY
8. WEB-SERVER APACHE STRUTS DYNAMIC METHOD EKSEKUSI
9. HTTP REQUEST METHOD
10. WEB-SERVER APACHE STRUTS 2 REST PLUGIN EKSEKUSI
11. WEB-SERVER APACHE STRUTS 2 CONVERSION ERROR INTERCEPTOR OGNL SCRIPT INJECTION VULNERABILITY
12. WEB-OTHER GNU BASH ENVIRONMENT VARIABLE HANDLING COMMAND EXECUTION VULNERABILITY

Jakarta, 06 Nopember 2018

Komandan ST-5,

ttd

Hari D.Permana, S.T

Mayor Laut (KH) NRP 16262/P