YAYASAN PERGURUAN CIKINI
INSTITUT SAINS DAN TEKNOLOGI NASIONAL

Jl. Moh. Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640
Telp. 021-7270090 (hunting), Fax. 021-7866955, hp: 081291030024
Email : humas@istn.ac.id Website : www.istn.ac.id

SURAT PENUGASAN TENAGA PENDIDIK

Nomor : 86/03.1-I/IV/2023

SEMESTER GENAP TAHUN AKADEMIK 2022/2023

Nama	: **Aryo Nur Utomo, S.T., M.Kom.**	**Status Pegawai**	: **Edukatif Tetap**
NIP/NIK/NIDN	: **01.121225/35091009/0319046803**	**Program Studi**	: **Sistem Informasi**
Jabatan Akademik	: **Asisten Ahli**		

Bidang	Perincian Kegiatan	Ruang/ Tempat	Jam/ Minggu	Kredit (sks)	Keterangan
I PENDIDIKAN DAN PENGAJARAN	**MENGAJAR DI KELAS (KULIAH/RESPONSI DAN LABORATORIUM)**				
	1. Big Data dan Bussines Intellegent	A-6	3 Jam/Minggu	0	Kamis, 17:00-19:30 WIB
	2. ERP (Enterprise Resource Planning)	A-5	3 Jam/Minggu	1,5	Kamis, 17:00-18:30 WIB
	3. IS Strategy	A-3	2 Jam/Minggu	1	Senin, 14:30-16:30 WIB
	4. Jaringan Komputer	A-6	2 Jam/Minggu	1	Rabu, 08:00-09:40 WIB
	5. Kecerdasan Buatan	A-1	2 Jam/Minggu	1	Rabu, 13:40-15:00 WIB
	6. Kriptografi	A-2	3 Jam/Minggu	1,5	Kamis, 09:40-11:40 WIB
	7. Penetrasi Test (PIS)	A-1	2 Jam/Minggu	1	Kamis, 16:00-17:40 WIB
	8. Pemrog Perangkat Bergerak	A-3	2 Jam/Minggu	1	Rabu, 08:00-09:40 WIB
	9. Proyek	A-1	2 Jam/Minggu	2	Jumat, 10:00-11:40
	10. Rootkis (PIS)	A-2	2 Jam/Minggu	1	Rabu, 13:00-14:40 WIB
	11. Prak. Pemrog Perangkat Bergerak	LabKom	2 Jam/Minggu	1	Kamis, 15:00-16:40 WIB
	12. Menduduki Jabatan Struktural Ka.Prodi Tekni Informatika		36 Jam/Minggu	3	
	13. Membimbing Skripsi / KP				Insidential
II PENELITIAN	Penulisan Karya Ilmiah			1	
II PENGABDIAN DAN MASYARAKAT	Pelatihan dan Penyuluhan			0	
IV UNSUR-UNSUR PENUNJANG	Berperan Serta Aktif dalam Pertemuan Ilmiah/Seminar			0	
	Jumlah Total			16	

Kepada yang bersangkutan akan diberikan gaji/honorarium sesuai dengan peraturan penggajian yang berlaku di Institut Sains dan Teknologi Nasional, penugasan ini berlaku tanggal 21 Maret 2022 sampai dengan 28 Agustus 2022.

Tembusan :
1. Direktur Akademik - ISTN
2. Direktur Non Akademik - ISTN
3. Ka. Biro Sumber Daya Manusia - ISTN
4. Kepala Program Studi Sistem Informasi
5. Arsip

Jakarta, 21 Maret 2022
Dekan,

FAKULTAS SAINS DAN TEKNOLOGI INFORMASI ISTN

(Marhaeni, S.Kom., M.Kom.)

DAFTAR HADIR PESERTA KULIAH MAHASISWA

GENAP REGULER TAHUN 2022/2023

FAK / JURUSAN : Teknik Informatika S1 HARI/TANGGAL : Rabu

MATA KULIAH : Rootkit

KELAS /PESERTA : A / 8 JAM KULIAH : 13.00 – 14.40

KURIKULUM : 2018

DOSEN : Aryo Nur Utomo, S.T.,M.Kom. RUANG **:**

NO	NIM	NAMA MAHASISWA	TANGGAL PERTEMUAN								JUMLAH
			22/ 03	29/ 03	5/ 04	12/ 04	26/ 04	3/ 05	10/ 05	17/ 05	
1	20360002	Muhammad Satria Wibowo	√	√	√	√	√	√	√		7
2	20360008	Iqbal Muhammad Hasbi	√	√	√	√	√	√	√		7
3	21360501	Muhamad Firdaus	√	√	√	√	√	√	√		7
4	22360701	Riefaldiva Muhammad	√	√	√	√	√	√	√		7

Jakarta , ... Mei 2023

Dosen Pengajar

(Aryo Nur Utomo, S.T.,M.Kom.)

BERITA ACARA PERKULIAHAN
(PRESENTASI KEHADIRAN DOSEN)
SEMESETER GENAP TAHUN AKADEMIK 2022/2023
PROGRAM STUDI TEKNIK INFORMATIKA S1 FSTI-ISTN

Mata Kuliah	:	Rootkit	Semester	:	366153
Dosen	:	Aryo Nur Utomo, ST, M.Kom	SKS	:	2
Hari	:	Rabu	Kelas	:	A
Jam	:	13:00-14:40	Ruang	:	B-2

No.	TANGGAL	MATERI KULIAH	JML MHS HADIR	TANDA TANGAN DOSEN
1.	22-Maret 2023	Review Rootkits	4	
2.	29-Maret 2023	Tools Detektor untuk Rootkit. Tindakan jika di Sistem terdeteksi Rootkit.	4	
3.	5-April 2023	Trojan, Backdoors, and Rootkit.	4	
4.	12-April 2023	Perbedaan antara Rootkit dan Virus.	4	
5.	26-April 2023	Menangkap Program Berkeliaran di Komputer.	4	
6.	3-Mei 2021	Persenjataan Memerangi Rootkit. Hooking.	4	
7.	10-Mei 2023	Checksum File App project.	4	
8.	17-Mei 2023	**Ujian Tengah Semester (UTS)**	4	

DOSEN PENGAJAR

(Aryo Nur Utomo, ST. M.Kom)

DAFTAR NILAI

SEMESTER GENAP REGULER TAHUN 2022/2023

Program Studi : Teknik Informatika S1
Matakuliah : Rootkits (PIS)
Kelas / Peserta : A
Perkuliahan : Kampus ISTN Bumi Srengseng Indah
Dosen : Andi Suprianto, Ir.M.Kom

No	NIM	N A M A	ABSEN	TUGAS	UTS	UAS	MODEL	PRESENTASI	NA	HURUF
			10%	10%	40%	40%	0%	0%		
1	20360002	**Muhammad Satria Wibowo**	100	65	75	68	0	0	73.7	**B+**
2	20360008	**Iqbal Muhammad Hasbi**	100	70	78	68	0	0	75.4	**A-**
3	21360501	**Muhamad Firdaus**	100	70	76	65	0	0	73.4	**B+**
4	22360701	**Riefaldiva Muhammad**	81	65	77	62	0	0	70.2	**B**

Rekapitulasi Nilai							
A	0	B+	2	C+	0	D+	0
A-	1	B	1	C	0	D	0
		B-	0	C-	0	E	0

Jakarta,16 August 2023

Dosen Pengajar

Andi Suprianto, Ir.M.Kom

Andi Suprianto, ir.M.Kom

Security ID 25b9b2333328ad95531dedfdebecb4e1

Apa itu Rootkits ?

Aryo Nur Utomo, ST, M.Kom

Under Graduate Electrical Engineering – Computer Engineering, University of Indonesia

Post Graduate Program, Faculty of Computer Science, University of Indonesia

aryonurutomo.blogspot.com

Perbedaan antara ROOTKIT dan VIRUS

No	ROOTKIT	VIRUS
1.	Rootkit adalah sekumpulan program jahat yang memungkinkan akses tingkat administrator ke jaringan komputer.	Virus adalah kode berbahaya yang dapat dijalankan yang dilampirkan ke file lain yang dapat dijalankan yang tidak berbahaya atau dapat mengubah atau menghapus data.
2.	Tujuan utama rootkit adalah mencuri informasi identitas, seringkali untuk mendapatkan kendali atas sistem.	Tujuan utama virus adalah untuk mengubah informasi.
3.	Mendeteksi dan menghapus rootkit adalah proses yang kompleks dan biasanya membutuhkan penggunaan alat khusus.	Perangkat lunak antivirus digunakan untuk perlindungan terhadap virus.
4.	Rootkit adalah salah satu jenis malware.	Virus merupakan salah satu jenis malware.
5.	Ini memberikan akses dan kontrol sistem yang tidak sah kepada penyerang.	Itu dapat mengontrol data dan sumber daya, menyebabkan kesalahan, menghancurkan sistem dan memperlambat kinerja.
6.	Itu lebih berbahaya.	Ini kurang berbahaya dibandingkan.
7.	TDSS, ZeroAccess, Alureon dan Necurs adalah beberapa rootkit yang umum.	Virus *resident* dan *non-resident* adalah dua jenis Virus.

Bagaimana Rootkit Diinstal ?

- Rootkit perlu dipasang oleh pengguna tingkat administratif (*user root*).
- Ini dapat dilakukan dengan akses fisik ke sistem, atau dengan tanpa disadari penginstalan aplikasi atau driver perangkat yang berisi trojan, oleh admin sistem.

Memeriksa Rootkit

- Memeriksa penginstal rootkit dapat dilakukan sebelum sistem disusupi melalui pemindaian tanda tangan (*checksum*) pada file oleh program anti-virus.
- Namun, setelah rootkit dijalankan, sistem tidak dapat dipercaya, karena rootkit masuk ke mode *stealth* dan mengubah hasil pemindaian untuk menyembunyikan dirinya sendiri.

Memeriksa Rootkit

- Misalnya, rootkit sebagian besar akan mengubah keluaran dari daftar proses sehingga tidak muncul dengan sendirinya.
- Demikian pula, daftar file tidak akan menampilkan file rootkit.

Detektor - chkrootkit

- Chkrootkit → http://www.chkrootkit.org/
- chkrootkit adalah alat yang memeriksa tanda-tanda rootkit.
- Ia memeriksa perubahan dalam binari, mode promiscuous NIC, penghapusan log terakhir, gangguan log, perubahan log, file konfigurasi rootkit, dan proses tersembunyi.
- chkrootkit telah diuji pada:
  Linux 2.0.x, 2.2.x, 2.4.x and 2.6.x; FreeBSD 2.2.x, 3.x, 4.x and 5.x; OpenBSD 2.x, 3.x and 4.x.; NetBSD 1.6.x; Solaris 2.5.1, 2.6, 8.0 and 9.0; HP-UX 11; Tru64; BSDI and Mac OS X

Daftar deteksi Chkrootkit

Rootkit, worm, dan LKM berikut saat ini terdeteksi:

01. lrk3, lrk4, lrk5, lrk6 (and variants);
02. Solaris rootkit;
03. FreeBSD rootkit;
04. t0rn (and variants);
05. Ambient's Rootkit (ARK);
06. Ramen Worm;
07. rh[67]-shaper;
08. RSHA;
09. Romanian rootkit;
10. RK17;
11. Lion Worm;
12. Adore Worm;
13. LPD Worm;
14. kenny-rk;
15. Adore LKM;
16. ShitC Worm;
17. Omega Worm;
18. Wormkit Worm;
19. Maniac-RK;
20. dsc-rootkit;
21. Ducoci rootkit;
22. x.c Worm;
23. RST.b trojan;
24. duarawkz;
25. knark LKM;
26. Monkit;
27. Hidrootkit;
28. Bobkit;
29. Pizdakit;
30. t0rn v8.0;
31. Showtee;
32. Optickit;
33. T.R.K;
34. MithRa's Rootkit;
35. George;
36. SucKIT;
37. Scalper;
38. Slapper A, B, C and D;
39. OpenBSD rk v1;
40. Illogic rootkit;
41. SK rootkit.
42. sebek LKM;
43. Romanian rootkit;
44. LOC rootkit;
45. shv4 rootkit;
46. Aquatica rootkit;
47. ZK rootkit;
48. 55808.A Worm;
49. TC2 Worm;
50. Volc rootkit;
51. Gold2 rootkit;
52. Anonoying rootkit;
53. Shkit rootkit;
54. AjaKit rootkit;
55. zaRwT rootkit;
56. Madalin rootkit;
57. Fu rootkit;
58. Kenga3 rootkit;
59. ESRK rootkit;
60. rootedoor rootkit;
61. Enye LKM;
62. Lupper.Worm;
63. shv5;

Detektor - rkhunter

- Rootkit Hunter → http://www.rootkit.nl/projects/rootkit_hunter.html
- Rootkit Hunter (rkhunter) adalah alat pemindaian rootkit.
- Ia memeriksa perubahan dalam binari, file rootkit, file tersembunyi, dan izin biner yang salah, itu antara lainnya.
- *Tools* ini didukung pada sebagian besar distribusi Linux dan BSD, dan Solaris SunOS. *Tools* itu tidak didukung (kompatibel) di NetBSD.